Yuval Ne'eman Workshop
for Science, Technology and Security
Tel Aviv University

ICRC
Blavatnik Interdisciplinary
Cyber Research Center

Prime Minister's Office
National Cyber Bureau

The Blavatnik Interdisciplinary Cyber Research Center
Yuval Ne'eman Workshop for Science, Technology and Security
Tel Aviv University

The Annual Cyber Security International Conference Proceedings 2014-2015

TEL AVIV UNIVERSITY
אוניברסיטת תל אביב

THE ANNUAL CYBER SECURITY INTERNATIONAL CONFERENCE PROCEEDINGS 2014-2015

THE YUVAL NE'EMAN WORKSHOP
FOR SCIENCE, TECHNOLOGY AND SECURITY

THE BLAVATNIK INTERDISCIPLINARY
CYBER RESEARCH CENTER

MAY 2016

THE ANNUAL CYBER SECURITY INTERNATIONAL CONFERENCE PROCEEDINGS 2014-2015

The Annual International Cybersecurity Conference is held by the Blavatnik Interdisciplinary Cyber Research Center (ICRC), Yuval Ne'eman Workshop for Science, Technology and Security, Tel Aviv University and the Israeli National Cyber Bureau, Prime Minister Office.

With each passing year the conference grows as the awareness of the increasing threats becoming a matter of international concern and common knowledge. Israel, known as the start-up nation, is now becoming a cyber-nation, one which combines high-end technology, innovation and the talented innovators. The conference will include speakers and delegations from both Israel and abroad who will share their insights on the most recent developments in cybersecurity and discuss key dilemmas and opportunities arising from the evolving technologies.

The conference receives extensive global media coverage. The last conference enjoyed the presence of more than 5,000 attendees from 48 countries. Attendees included: decision makers, diplomats, academics, respected members of the defense industry and intelligence units, Israeli and international students, hi-tech entrepreneurs, leading experts from the cyber industry, cyber professionals, corporate C-suite executives and senior decision makers representing policy circles, the private sector and defense in Israel and abroad.

YUVAL NE'EMAN WORKSHOP FOR SCIENCE, TECHNOLOGY AND SECURITY OFFICIALS:

Major Gen. (Ret.) Prof. Isaac Ben Israel, Head of the Workshop
Mrs. Gili Drob – Heistein, Executive Director of the Workshop
Ms. Revital Yaron
Mrs. Roni Sharir
Ms. Dafna Kovler

Editor: Yael Luxman-Bahat
Technical editor and professional advisor: Yul Bahat
Graphic Editing: Michal Semo
Printed by: Tel Aviv University Press, Israel, 2016

The Blavatnik Interdisciplinary Cyber Research Center (ICRC) was established at the Tel Aviv University on April 2014, as a joint initiative with the National Cyber Bureau, Prime Minister's Office. The Center is based on researchers from Tel-Aviv university and emphasizes the importance of interdisciplinary research. Currently, there are 50 faculty members and over 200 cyber researchers from different faculties such as Exact Sciences, Computer Sciences, Law, Engineering, Social Sciences, Management and Humanities.

The Center aims to become a leading international body in its field and to increase the academic efforts and awareness in the field of cyber security. Research topics at the Center include key issues such as security software, attacks on hardware and software, cryptography, network protocols, security of operating systems, and networks as well as interdisciplinary research such as the impact on national security, the impact on society, regulation, and the effects on the business sector.

The Center operates a research fund which is supported by the Israeli National Cyber Bureau, Prime Minister's Office.

The Yuval Ne'eman Workshop for Science, Technology and Security was launched in 2002 by Major-General (Res.) Prof. Isaac Ben-Israel in conjunction with the Harold Hartog School of Policy and Government and the Security Studies Program at Tel Aviv University. The Workshop was founded with the clear directive of exploring the links between science, technology and security. The Workshop conducts a broad range of research activities that include the publication of research papers and policy reports in the field of national security strategy & policy. Alongside its research activities, the Workshop also holds a senior executive forum that promotes public-private partnerships and initiatives and a popular series of monthly conferences at Tel Aviv University with the participation of senior IDF staff and security organization members, politicians, academia, and executives from leading Israeli and International companies. The goal of the Workshops' activities is to create an open and fruitful dialogue with the general public in the fields of interest of the Workshop: Cyber Security, Space and Emerging Issues of National Security.

CONTENTS

THE 4TH ANNUAL INTERNATIONAL CYBERSECURITY CONFERENCE – 2014

OPENING REMARKS

MAJOR GEN. (RET.) PROFESSOR ISAAC BEN ISRAEL, HEAD OF ICRC & YUVAL NE'EMAN WORKSHOP, TEL AVIV UNIVERSITY

I would like to welcome everyone coming to our 4th international cyber-security conference. Unfortunately, Israel is a target to many hostile entities. Starting with anarchists, going through everyone who hates America or the West and ending with the real enemies of Israel. We are a target in many senses, and in cyber security as well. Therefore we have gathered a lot of experience in dealing with this threat and this conference is going to reflect this. We will have a mix of people coming from academy, industry, and defense, not only in Israel, but from other countries as well.

PROFESSOR JOSEPH KLAFTER, PRESIDENT OF TEL AVIV UNIVERSITY

While only in its 4th year, the conference has already become a household name in cyber circles. It attracts top experts from Israel and abroad. Abroad academic community, dignitaries, professionals, representatives from industry as well as the next generation of cyber innovators and entrepreneurs. They come firstly because of the wide ranging reputation and impact of the Ne'eman workshop led by Professor Ben Israel. They come because of the broad inter-disciplinary scope of the speakers and research topics that will be presented over the next two days. And especially come because of

the back and forth that only a leading global institution like Tel Aviv University, which is so comprehensive, can provide. And this goes back and forth between Israel and the world, between scientists and policy makers and between people with problems, and people who can help solve problems. I would like to thank the organizers and sponsors of the conference for making this such a high quality and high profile event. Cyber security is an issue of vital importance for Israel and for the world and I'm certain that this gathering will make an enormous contribution.

PROFESSOR JACOB A. FRENKEL, CHAIRMAN OF THE BOARD OF GOVERNORS, TEL AVIV UNIVERSITY, CHAIRMAN OF JP MORGAN CHASE INTERNATIONAL, FORMER GOVERNOR OF THE BANK OF ISRAEL

There is no need to emphasize the importance of cyber and the entire subject that is being discussed here today. It is enough to say that the awareness for issues in this subject had been growing tremendously all over the world. It has economic dimension, it has security dimension, it has scientific dimension, it has national dimension, and it has broad dimensions all over the spheres of life.

Five years ago, when you went around the world and spoke about cyber, you needed to explain what the issue is and what the scope is. Today, everyone knows that. A few weeks ago, on August 28th, in the morning, I flipped through the pages of the *Wall Street Journal* and the *Financial Times*. The main headlines described how American authorities were probing cyber-security attacks on banks and how the FBI was working with the American secret service to examine different aspects of these attacks. At the same time it was reported that the US treasury was hosting a meeting between US officials and the representatives of the biggest banks to discuss this issue. Last week, the American secretary for homeland security called for more legislation on this front. The Blumberg network reported about an investigation into attacks linked to the Russian government.

There is practically no single area that has not been under an active attack. We are all familiar with the banking area; in this field, both the frequency of the cyber-attacks and the resources that have been spent on protecting the banking system have been tremendous. In the

past few months we were informed of attacks on gaming companies, on Sony's PlayStation network, of an attack on E-bay which reportedly resulted in more than 200 million stolen records. These are not only commercial matters but also national matters; these are the issues that will be discussed in this conference.

It's not a coincidence that the conference is being held here, in Tel-Aviv University, Israel. Being the start-up nation, we have also witnessed more than 200 start-ups being established just in this particular area, and Tel-Aviv University has been spearheading this national scientific effort. The dimensions are global. Israel is a small country but the approach, the market and the awareness – are all global. Israel is indeed covering the entire breadth of this area. When you ask people in the world 'what are you most concerned about?' they will tell you 'water, health, airline traffic, trains, financials' etc. Well, ladies and gentlemen, those are all the areas that have been potential targets for cyber. There is nothing more important today than providing a serious response to this. It requires resources. Both human capital and financial capital. Human capital is produced indeed in institutions of the type that we are now present in and it is great pleasure and pride to identify specifically Tel Aviv University in this regard. In terms of financial resources, you will meet today quite a few of the ministers in our cabinet, as well as the Prime Minister, a fact which emphasizes time and again that cyber has become a national priority. When one speaks about national priority the only operation and meaning of it is the financial allocation of resources. So it is in this regard that we are here in the beginning of a fantastic event.

DR. GIORA YARON, CHAIRMAN OF THE UNIVERSITY'S EXECUTIVE COUNCIL AND CHAIRMAN OF 'RAMOT' THE TECHNOLOGY TRANSFER ARM OF TEL AVIV UNIVERSITY

There are two initial questions that should be considered in the context of Cyber. The first question is based on the assumption that the person who is going to 'get you' is the one you have not thought about. So the real question is what type of products do you need in order to develop the cyber frontier, and what are the types of products that you need to develop to be able to address future threats. The second question has to do with resources. Unlike conventional combat, where you need to over-resource the attack side, in the cyber world, the relations

are reversed. The bigger investment goes into defense capabilities. How do you know whether you have invested enough? Or whether you need another layer of defence? Or what should you do to have enough layers of defence?

GENERAL (RET.) KEITH ALEXANDER, CEO AND PRESIDENT OF IRONNET CYBER SECURITY

Over the past several years I have been looking at what's going on in Cyber Space and Cyber Security. One of the greatest honours and privileges I've had as I took off the uniform was to think about what I'm going to do next in life. Several people came up to me and said 'you need to help in cyber-security, because the mission is not over, we need better cyber security'. Indeed, Cyber-security is a team sport: between industry players, between industry and government and between nations. We have to work together in cyber-security. It cannot be done by any one single organization, as good as anyone of us may think we are. It had got to be done with the cooperation of many of us. What the US Congress and the current administration is pushing for currently in cyber-legislation is vitally needed. Cyber Space is the new frontier. The IPhone, the IPad and other electronic gadgets are wonderful. We are more wired today, through these devices, than ever before. Data is a natural resource. Look at how connected we are. There is a video clip titled 'did you know 2014' which I recommend watching, it helps to lay the foundation for what's going on in Cyber Space.

First, this year, the amount of unique data that will be created is 3.5 zeta bytes. That's 3.5 with 21 zeros after it. That's more than all the information that was created in the last 5,000 years. The amount of technical information is doubling every two years. The top 10 most 'in demand' jobs in 2013 did not exist in 2004. What does that mean? It means that if you're a college student, 50% of the information you learn in your freshmen year will be outdated by your junior year. Or, for universities like this, it means that we are preparing students for jobs that don't exist, using technology that hasn't been created to solve problems we don't even know are problems. That's what's going on.

Even one year olds and two year olds can grab an IPad and be connected. It brings together four generations into the work space:

the traditionalists, the baby-boomers, the gen-x, and the millennials. That is 'write me, call me, e-mail me, text me' all working in the same space. And you think about how we coordinate those things. You now have 2.4 billion people using the internet and 170 billion google searches done a month. 14 billion text messages a day. Think about the way this technology is going. Many of you saw IBM Watson. This was a machine that beat the best human players in Jeopardy. IBM is now using Watson to work with a genome centre in New York City to address cancers, specifically brain cancer. In the past if you were diagnosed with brain cancer, the doctors would have told you that you have 14 months to live. How do you diagnose and get the right therapy inside the brain? It takes too long. Five doctors take 30 days to come up with the correct regiment of chemotherapy and radiation. With IBM's Watson they've got that down to 9 minutes.

With current and future technology we'll solve cancer over the next decade. It's that important. If Facebook were a country, when I started talking about it in this way, they were third largest. Now they're between the first and second largest with 1.3 billion users. One out of six couples married in the US met online. Now, here's the thing that should concern all of you: one out of five divorces are blamed on Facebook. So I immediately went home and asked my wife 'do we have a Facebook account? We need to get rid of that'.

Any person with access to Google has access to more information than the President did in the United States in 1990. In 2019 the electronics industry will make more money than the airline industry does today. Regarding Human knowledge: in 1900 they said that human knowledge would double every 100 years. In 1945 it was down to 25 years. This year it's down to 13 months. In 2020 it's going to be measured in days. The new issue with data is how do we capture it, how do we harness it, how do we protect it. Look at what's going on in cyber space. Cyber-attack, cyber espionage, cybercrime. Theft of intellectual property. Jim Lewis from SIS says that 'global cybercrime is worth about 445 billion dollars a year. That excludes the impact in theft of intellectual property.

Let's look at what's going on in cyber-attacks, starting with what hit Estonia in May 2007. This event was the biggest 'Distributed Denial of Service Attack' (DDoS) that we had seen to date, it came from hackers inside Russia and they knocked down the network in Estonia. If you talk

to Estonian president Toomas Hendrik Ilves, he would tell you that it was a significant event for a small country that lives on the internet. They vote, they bank, and they do everything on the internet. In 2008 Georgia was attacked at the same time that the Russia military invaded.

In 2008 there was also, interestingly, an exploit into the US defense networks in an operation that we called 'Buck shot Yankee'. William J. Lynn, U.S. Deputy Secretary of Defense, mentioned this at the time.[1] It presented a set of exploits into the network; some malicious software got into our classified network, it was one of the reasons that we set up the US cyber command.

In 2012 we started to see a shift in what was going on. We were hit with a set of DDoS attacks and a destructive attack. In 2013 South Korea suffered two sets of attacks, one in March and one in June. Meanwhile, our financial networks were hit with 3,500 DDoS attacks. If you were to put those on a chart and look at those, you would see those pick up; there's a lot more that we need to do in cyber security.

There are several things that we need to do. There are five principles we use in the defense department in talking about the cyber command. First, from a cyber-command's perspective, a defensible cloud-based architecture. In my mind, we didn't have a cloud-based architecture and it wasn't defensible. We had 15,000 enclaves. Each one of those was manned and operated as an individual entity. And the ability to ensure all of them were properly defended was almost impossible. From my perspective, that's not a defensible architecture.

Training: here's where universities can really help. We need to train people on this problem, the operators, the CIO's, the SISO's the CEO's, governments, parliamentarians, congress members. We need to train people on what's going on here. If you can't talk and explain what's going on, how can you defend it? That's a big gap that we have to address.

From the US perspective, we need cyber legislation. The initiative that Secretary Johnson's promoting – we need to get that through.

Command and Control: how do you command the control? Setting up cyber command was a big step. What we will learn, what we can learn together in cyber space, is going to be the key for setting up cyber

1 See article by William J. Lynn, U.S. Deputy Secretary of Defense: http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain

security. We need a comprehensive solution. It's not a single solution. It's not fixing a firewall. It's not fixing our routers. It's not fixing the end point. It's the strategy of how we come up with a comprehensive solution. No single company, no single country, can solve this problem by itself. This is an area where we have to work together. This is an area, where if we work together we can come up with solutions that take a lot of cyber risk off the table. And that's what I think makes us a special area. Because it is one where partnerships are really the value in what we're going to do. What's going on in the network? We don't want to slow it down. The ability to solve cancer, to improve our quality of life, to educate our kids, it's so compelling. We've got to solve the cyber security problem.

NADAV ZAFRIR, (CO-FOUNDER OF TEAM8, A CYBER SECURITY VENTURE CREATION, FORMER HEAD OF IDF UNIT 8200)

I will start my talk by speaking about the latest cyber scandal. The latest scandal has to do with nude photos of celebrities and the iCloud. If you take a moment to think about all the regular people that had to deal with the moral dilemma of thinking about whether clicking on Jennifer Lawrence's nude photos on Google was morally okay? Of course, we cyber experts, we had to do it. You know, for professional reasons. I actually have to say that my wife overheard me rehearsing for the keynote and said that wasn't a very good excuse.

I want to speak about something else: Advanced persistent threat (APT). The reason that I want to speak about APT is the following: first of all, think about APT, the resources that are directed over time at a specific entity very persistently, In order to get a very specific target. I think it's the only threat in cyber that has the potential of being devastating for an organization. And it's the only threat that can actually bring a company to its knees.

We don't really have an effective solution for it. In team8 we've being exploring several cyber domains over the past year, and the one that I personally find most intriguing is APT. Unlike other areas in cyber, in APT it's not about the malware. So the approach that we have right now of trying to pinpoint the tools, the malware, are missing the big picture. Because it's not about the malware. It's about the ghost in the machine if you like. It's about the people and the process behind

the malware. Any malware at the end of the day, is actually as good as the people behind it. It's as good as the decision making process that the people behind the malware are capable of.

It's about the tenacity, it's about the capacity, and it's about the resources that the people behind have, it's about game theory. To give a more specific example I wanted to speak to you about 'Target Corporation' (and the cyber-attack against it). It's the end of 2013, it's the holiday season, and it's not the best of time for Gregg Steinhafel, the CEO of Target, and Beth Jacob, the CIO. Through the attack 7 million people were targeted, their personal records were disclosed, information about 40 million credit cards was stolen. The company sustained a 46% drop in the value of its share in the last quarter, compared with 2012. And this is the third largest retailer in the United States.

But, that's not the whole story. Let's look at it from a technical point of view. The attackers started by stealing the credentials issued to Fazio Mechanical, a heating, air conditioning and refrigeration firm that did maintenance work for Target. They stole the credentials by using a malware called 'Citadel', an offspring of the Zeus malware. Eventually they got to a stores, or the point of sales, using another malware.

If you were to buy an old version of 'citadel' off the market, you'd probably get some change from 5,000$. It is not a bad return on investment if you think about selling the details of 40 million credit cards for approximately 30-40 each in the black market. So I urge you to look at something else – it's the people behind it. It's the decision making behind it. What you don't see is the timetable of how long it took, you don't see the road not taken. What you don't see are the dead ends that these people had to deal with along the way. What you don't see are the U-turns along the way. And if you would have seen all of these, it wouldn't be such a neat program because you don't see the decision making process behind it, so you don't see the mistakes behind it.

If we are to deal effectively with APT, we must take into consideration all those loops and nets. We should understand that APT are, at the end of the day, not about the malware. We have to change our mind sets. We have to engage the puppet master. Because it's not about the puppet, it's about the master. It's about the people that you don't

see, in the back rooms. They are the masters. Currently we are after the puppets, the malware, and that's not going to work for us. Why? Because we are missing out an opportunity.

The opportunity is to leverage the human factor. Because at the end of the day there are people behind it. And people get tired, they get sloppy, they get greedy and they make mistakes. And their mistakes are an opportunity. If we can take advantage of their mistake we can seize the opportunity, we can come up with a new approach.

The new approach is to pro-actively disrupt the attack while it's happening. We have to use tools and techniques from within the network where we have the upper hand. The defender has the upper hand in their own network. We know it best, so we can use tools and techniques from within the network that will take advantage of the human factor and create a situation where the offense makes more mistakes than we do in the defense. And if we can do that, we can eventually flip the a-symmetry.

We are in an a-symmetric situation right now. The defense has to be perfect on every instance. Every single instance. We have to be perfect all the way, otherwise the offence will have the upper hand. And this status-quo is something that we cannot live with anymore if we want to solve the APT situation. It must be solved if we want to prosper and use all those technologies and that we've been using in the last decade or decades.

If we can flip the a-symmetry, then all of a sudden it won't be the offence that looks at the defense and aggregates mistake after mistake after mistake after mistake after mistake, but vice versa. And if we manage to do it, we can take the initiative back to our hands. If we take the initiative back to our hands we can flip the whole story. The same thing that happened in Target, perhaps even the same people, happened to 'home depot'. And we cannot afford it in the future. We must change the way in which we look at cyber defense and specifically APTs.

לגבי פרשת מכתב הסרבנות. סרבנות היא סרבנות, גם אם היא מנוסחת היטב. אין מקום לסרבנות. אנחנו לא נוכל להתקיים כאן במדינה דמוקרטית עם שיח, וראוי לקיים שיח במדינה דמוקרטית וטוב שיש שיח במדינה דמוקרטית. אבל יש מקום לקיים אותו ואני אומר לכם, בתור אזרח, בתור מפקד, בתור חייל, אין מקום לסרבנות מכל סוג שהוא ובטח לא מהמקום שאנחנו באים ממנו.

DR. ROEY TZEZANA, FELLOW & RESEARCHER YUVAL NE'EMAN WORKSHOP FOR SCIENCE, TECHNOLOGY & SECURITY, TEL AVIV UNIVERSITY

The Yuval Ne'eman workshop for science, technology and security was launched in 2002 by Professor Issac Ben Israel in conjunction with the Security Studies Program and the Harold Hartog school of policy and government at Tel Aviv University. The workshop was founded with the clear directive of exploring the links between science, technology and security. The workshop conducts a broad range of research activities that includes the publication of research papers and policy reports in the field of national security strategy and policy.

The workshop also holds a senior executive forum that promotes partnerships and initiatives between public and private bodies. For a long time now, the workshop has been holding a popular series of monthly conferences at Tel Aviv University with the participation of senior IDF staff, members of security organizations, researches from the academia and executives from leading Israeli and international companies. The goal of these meetings is to foster the creation of an open and fruitful dialogue with the general public in the main fields of interest: cyber security, space and issues of national security.

So far, the workshop has held more than 90 conferences. Each attended by hundreds of participants. On cyber security, the Yuval Ne'eman workshop has been leading research and initiatives in this field for more than a decade, and it aims to assist in finding security solutions to help protect cyber space from growing threats. We keep on making progress as a society, with most of the progress relying on information and communication technologies. These are inherently related and interwoven with the cyber space. The many possibilities the cyber world offers, are unfortunately perceived by our enemies as vulnerabilities. With every passing day we witness evolving cyber threats and targeted attacks on critical infrastructure, with new forms of 'hack-tivism'.

The growing danger of cybercrime creates a complicated threat landscape to nations worldwide. The Yuval Ne'eman workshop has set as a goal for itself to advance awareness of cyber-security issues and the unique challenges they present. The cyber domain, including the internet and the social networks, has brought forward many opportunities and challenges along with new legal, ethical and social

dilemmas. These challenges are particularly relevant to politics, public policy and the international relations.

In 2010 as part of a decision to streamline and coordinate the allocation of national resources towards cyber security, the Prime Minister of Israel has set up the National Cyber Initiative task force with professor Ben-Israel as its head. Ram Levi, from the workshop, coordinated the work of the task force and the resulting recommendations were accepted by the Prime Minister and were approved by a government decision.

The government voted to establish a national cyber directorate to coordinate national cyber security activities and to formulate cyber security policy. Of all the conferences, the crown jewel of the workshop conferences is the annual international cyber security conference. This conference is held every summer since 2011 and enjoys the participation of senior politicians, foreign diplomats, members of the academy, and senior representatives of the IDF and cyber security experts from Israel and around the world. Each year we're are getting bigger and better. Last year we've had 2,000 participants from 20 countries. This year, we've had nearly 4,000 applications from 40 countries. In addition to the conference we also hold a competition and an exhibition of emerging technologies that could disrupt current security strategies.

AMNON BAR-LEV, PRESIDENT CHECK POINT SOFTWARE TECHNOLOGIES

In my presentation I will give a very short brief about what happened in IT security in recent years, then we will jump into architecture questions and pragmatic actions, pragmatic architecture, not specific for Check Point. When you're looking to build your own security, what would you do in your environment? Technology is everywhere. But there's two interesting things about technology that's everywhere. The first is that it became much more open and commonly used, and I'll take different system that some of you familiar with. For example: ATM machine. You go to the bank to take money out. Five years ago it used to be an IBM closed system. Today it's Windows. And actually even Windows XP which is terrible.

When you go to the Cinema and you buy tickets, you use your credit card. Do you know how easy it is to break into those machines and steal your credentials? You go to an airport, the gate is empty, and you plug your computer into a port.

Technology is really everywhere, not to talk about water, electricity, power plants. They all run on an IP protocol called SCADA, which means that a lot of things can happen to it.

The second thing about technology is that it has become vulnerable. Would you buy a car that needed to be fixed at the shop every month? We do it every day when we buy software. Software has to be patched roughly on a monthly basis. Cyber threats continue to grow; hacking has become much more popular now than it was 5 or 10 years ago. Hacking has become a commodity.

Many years ago if a person wanted to hunt down an animal, that person had to build their own weapon, tack down the animal and hunt it. Today, if you want to hunt an animal, you buy a gun at the shop and you use it for hunting. The same idea applies with regard to hacking. You can rent bot-nets, which are now dramatically cheaper than before, and you can send a 'few day exploit'. Instead of delivering the information to the vendors, hackers sell it to third parties.

Ransomware for example, is a soft which gets downloaded into your computer, it encrypts your files and demands ransom. If you do not pay, the files are lost, you will never get access to your information. There is also a prices difference; if you are from the US the ransom is 300 USD, if you are from Europe that ransom is 300 Euros, which makes the American price cheaper. The same exact software now runs on Android devices.

Technology is very important in our lives. Technology is vulnerable, and it's everywhere. Hacking activities continue to grow dramatically, mostly because hacking has become a commodity, and also because the motivations are greater than before. There are financial motivations and we see more and more political motivation as well. Right? Most of the militaries in the West and many militaries around the world will have in the future cyber warriors, not just cyber defenders.

In recent years networks have become broader. Seven years ago a network included a few servers, some desktops, and an internet

connection. Today, the networks have become much more complicated. We have clouds, mobile users, and branch offices, data centres, and private clouds.

People understood that networks became a mess and they sought to protect these networks by adding more and more technologies to them. Customers use firewalls, anti-virus software, filtering applications. Most clients talk about two issues; they do not know how to manage the environment of the network, and they are not sure whether or not they are doing 'the right thing'. Only a small number of people have a deep understanding of any given network. Security comes from the administrative part. Most executives will say: 'I want to be secure. I want to feel that I'm doing the right things.'"

There are three major elements for enhancing the security of a network.

The first point is that all the architecture must be modular, mostly since this is a very complicated problem. The only way to tackle this problem is to break it into small modules, and deal with each module separately. The second point is that the network must be agile. The advances and the changes in technology in general, and in in hacking technologies specifically, required an agile security. Security is the only realm of IT where you are not fighting as an individual and you are not fighting physically. It is about outsider threats. And you need to react much faster compared with any other realm of technology. The third point is that the infrastructure of the technology must be very secure. You must temporarily ignore considerations of speed and feeds and consider the security aspect of it. It must be very secure.

We came up with an architecture, which we call 'Software Define Protection'. There are three layers of architecture, enforcement points that know how to block the black traffic, and controls for generating the protection. Enforcement points can be everywhere; we know how to block traffic when it is on the network with big appliances. It could be on the cloud, it could be on mobile devices, on n-points, it could be a virtual gate. Where do I put the product? Years ago, the answer would be straightforward. A gateway to the internet, it's called power-meter. The question is: where do I protect it? Where's the parameter? So this is more of a philosophical approach to how to look at networks. The idea here is 'stop thinking about the parameter, and start thinking about segmentation'.

Ships have compartments. If a ship gets hit, it doesn't sink because the risk is contained. The same idea should be applied here as well. The idea is to look at the network and map it, and figure out how to create an island inside the organization. The goal is to make sure that each and every compartment is secure. Let's consider the targeted attacks that we know about, such as the attack against 'home depot', and STUXNET and others. You will notice that if we follow this basic guideline, than the damage sustained in the attack will be contained.

Segmentation is the next parameter. There's a full methodology on how to do segmentation. Starting with the creation of an atomic segment, a very basic segment at the same level of classification, and the same level of authorization. If you implement the segmentation properly than there will be a policy for each segment of the network. It's clear, clean and easy to use.

The issue of controls is interesting and unique. The idea is to use controls to generate protection to push 'bad elements' back to the enforcement, which way the enforcement will know about it and block traffic. There are two kinds of control. The fit one is access control which basically defines who can access which parts. There's no 'server to server' and of course you cannot get to google drive inside the organization. This is a very simple and straightforward solution. Most people call this a 'firewall' or a 'next generation firewall'. Most organizations around the world have firewalls.

The big questions is – Is that enough? The answer is a definitive No. The threats fall into three distinct categories:

1. The threat that we know, and we know how to protect from. The very basic threat is the virus, for which we have the signature. We know how to identify the virus and we know how to block it.
2. The second type of threat is the threat is that we know about, but which we do not know how to identify specifically. We know that there are vulnerabilities inside files like Word documents and excel sheets, power point slides. But we don't know where they are exactly. That's called 'zero day', and we use some kind of exploitation of a zero day inside different software. There are technologies that block these threats as well, it emulates the documents and looks at abnormal behaviour, and knows how to block it.

3. The third threat is the 'unknown-unknown', threats that we don't know and we don't even know that we don't know about them, so we don't know how that we need to protect ourselves against them. These threats will evolve in the following years and we need to build an architecture that will allow us to take those technologies and run them at the same environment that was familiar before.

There are different technologies that do all of those controls multi-layer protections. In addition to access control we need to also adopt 'threat prevention technology' and place it in the same environment. This way we would have one architecture, one enforcement point, you would be able to push 'access control' and then 'threat prevention'.

The challenge with threat prevention is that how to ensure its quality. The best threat prevention will be based on very sophisticated intelligence. We need to understand the people behind the threat. We need to understand what's going on with the actors, what they do. We need to get ongoing, real time updates of events.

Our company collects information from internal and external resources, from gateways around the world. Through Checkpoint we have about a million gateways around the world from which we can collect information. Research organizations around the world collect information. For threat prevention, collaboration is the most important part, and this is similar to physical security, like what militaries, intelligence units and police forces do around the world.

You need to collect a lot of information from different places, and at the end of the day you need to analyse it and translate it into protection, and apply it in 'real time' to your network. So, what we did for example at check point, we said 'let's take this huge database of software protections and let's collaborate with intelligence units.' There are intelligence units around the world, commercial intelligence companies, which collect information mostly for governments or for the finance industry.

They purchase malware, examine it, and attempt to understand who are the actors and where do they come from. In most cases these intelligence units produce reports. The report is important for understanding the threat, but it does not offer protection.

We believe in prevention. Most commercial companies only care about not being attacked. They care less about the identity and the motivation of the attacker. They wish to be safe from attacks and they want to run their business. The security of their network enables that.

We take the information offered by the intelligence companies and we offer customers the opportunity to pick and choose feeds like in a market place. And we take the chosen feeds, analyse them, translate them into protection, and implement them.

At the end of the day, companies want to be protected. They don't care much about where the threat originates from and how. Generally speaking, in IT in general and in security specifically, the only things that work are the simple things.

The last point is about how to manage the environment. In conclusion, there are three relevant points regarding the management. The first is modularity, the ability to manage all the modules, and implement some automation, in addition to the ability to understand what's going on in your network. This is a very critical part. The idea in management is to create layers of policy. A layer can protect a whole segment, which can, and its turn, protect another segment.

It's crucial to adopt a very sophisticated, smart, policy. Automation, the idea is to make security simple, connected and automated. The last point is about visibility, the ability to actually go out there and take information from N-point, from gateways, from mobile devices, from the cloud, and understand the big picture. The tasks are not as simple as they look. You need to understand what's happening in different places in order to understand that something is wrong.

Once you understand that something is wrong, you can generate a new protection and apply it on the network in order to protect it. In conclusion, the main points we discussed here today are the three layers architecture, robust enforcement points, control the protection and the way to manage it all together. We need the ability to create an environment that is very dynamic, that can take real time intelligence and translate it into protection that will defend us today, and also as we move forward.

KEREN ELAZARI, SENIOR RESEARCHER AT YUVAL NE'EMAN WORKSHOP FOR SCIENCE, TECHNOLOGY AND SECURITY

We started this conference four years ago, in 2010. Since then more than 100 new Israeli cyber security start-ups were established in Israel. And according to IVC research, they raised more than 400 million dollars in funding. More than 20 international companies now base their R&D centres, or centres of excellence for cyber-security research, here in Israel. The reason for that is innovation. The key to this phenomenon can be summed up in three words: pressure makes diamonds. This is a singular description for the Israeli tendency for incredible innovation under unmatched pressure.

Today we are going to have a fascinating discussion about how the unique Israeli industry and the defense and military side contributes to cyber security innovation. We're going to hear about how huge companies, 500 pounds gorillas, are struggling to innovate. We'll see if we can learn any lesson from global perspectives, from analysts, defense professionals and other executives. We talk a lot about new cyber security technologies and what they can offer, but there is another side to the coin of innovation. And that is that the bad guys are not afraid to innovate. We've all heard about the recent attacks and there is no major brand company, technology, retail, financial or defense that has not been implicated with a breach. The reason for that is that the bad guys are not afraid to try new things. They're not afraid to collaborate, they're not afraid to use a new technology in a clever way, or an old technology in a new way. That means we have to work that much harder on using the innovative technologies in a clever ways.

GORDON R. ENGLAND, FORMER U.S. DEPUTY SECRETARY OF DEFENSE, PARTNER AT GLILOT VENTURE CAPITAL

When Glilot capital was started about 4 years ago, it was clear that it was a huge investment on the cyber-attack side, cyber defense need, it's a massive investment and needed some significant innovation. It was necessary to close the gap between the attacker and the defender and to provide organizations with better techniques to defend their networks.

Four years have now passed since we've started and it seems today that many more people understand the situation. More Venture Capitals are investing in this and a new generation of cyber security companies is in now emerging. Digital technology continues to emerge, and as attackers continue to invest heavily on innovative attack techniques. Additional and significant defense innovation is need to protect government, corporate and other networks.

Attackers still have the advantage. The costs of attacking are relatively low, there's a high payoff and the attackers can experiment without precautions. The cyber defense side needs to address a wide spectrum of threats, leaving lots of room for innovation. For countries and large multi-national organizations, the threat is from nation states, although, organized and well-funded terrorists are not far behind.

There are five observations I wish to share. The first observation is that when dealing with high-in threats, cyber and necessity will need to move from discreet development and defense disrupt and destruction functions to more highly integrated and automated response systems. Given the spectrum of damage that the cyber-attacks can impose on an adversary, defenders must be able to not just detect an attack, but to sense an attack.

Ideally we would have a self-healing network. What's critical is to maintain operations while under and after an attack, by temporarily shutting down systems and automatically going to alternates modes of operation. This has to be initiated quickly, which implies fully automated systems.

When I was secretary to the navy, I used to say sort of tongue in cheek, that the navy needed to go back to signal flags. That was only partially in jest. Most developed societies have lost all the skills necessary to back up all the sophisticated systems they have today.

My second observation is that cyber is what I call 'a big systems game', especially when integrated with military operations to generate synchronized effects. Cyber tends to require big systems with large investments by governments and companies. Innovation is still largely occurring from what I call 'big brains in small company environments.' In a constantly expanding and changing digital world, with a creative attack side, defense will require flexibility and agility. And that's generally not associated with large bureaucratic institutions. In the Defence

side innovation happens in small companies which are then bought at premium prices by large integrators. And that's the experience at Glilot. Frankly, many US companies now are flushed with cash. It is quicker and cheaper for them to buy the technology than it is to develop it on their own. What better place to buy it than here in Israel, which is the hot bed of cyber innovation? Some of these large companies are actually establishing their own operations here in Israel.

My third point is stressed systems. A system that's already stressed is more vulnerable to attack because it is less resilient. Let's take for example, a macro example, the financial systems and the governance of developed countries, particularly countries in Europe. Some countries in Europe are at risk because they are facing an economic and financial crisis which will likely continue to deteriorate because of irreversible social and political forces. As the finances of these developed countries become more stressed, they also become more vulnerable to a variety of attacks on their financial systems and infra-structure.

It would be helpful if companies and countries could share cyber techniques. But the problem is that companies do not want to compromise their proprietary and their competitive data. And if a company has been attacked, it does not want to expose its vulnerabilities. Some countries are also reluctant to share information unless they have a special relationship with the other country. Cooperation is necessary, hopefully it will come about, but it's not easy to do.

The fourth observation is that government bureaucracies, regulations and social issues, could very likely override and severely limit the technological advances, innovations and effectiveness of cyber systems. If these constrains prevail, which they seem to be in a lot of countries, then those countries and their institutions will be in a fatal disadvantage in the cyber exchange.

Israel has better internal coordination and communication compared with other countries. Countries like Russia and China have centralized controls and therefore they are also at an advantage. Countries like the US and many of countries in Europe with very liberal media tend to limit cyber effectiveness and the operating spectrum with which you can operate. For example, in the US, the spectrum of operation is limited because privacy concerns. This adds inherent limitations in terms of the defense systems. Furthermore, in a large enterprise,

a large company, even countries, it takes an undue amount of time to respond to an attack. It could take hours, or even days, to respond to an attack, and this certainly is not compatible with my earlier comment about an automated response systems.

The fifth point is that we need to be mindful about the fact that human interactions will continue to operate side by side by cyber systems in order to ex-filtrate data and inject damaging software that can override embedded and sophisticated security measures. Edward Snowden, who was an NSA contractor, joined the saga of Wikileaks, a team known for its exfiltration and publication of classified US military intelligence and diplomatic documents. I would guess that it was Snowden who circumvented approximately ten billions Dollars spent on security safeguards, which were put in place against outside threats. Keith Alexander described continuous cyber exfiltration, the ransacking of American companies, as the greatest transfer of wealth in history. He may be right, but I also wonder how much classified data and proprietary data is ex-filtrated on highly dense storage devices by employees who either wilfully neglect to follow security measures, or intentionally still the data in order to sell to an adversary.

Networks can be damaged or compromised from within, they are relatively simple to compromise. Just take a disc drive from a classified computer to an unclassified computer and you have destroyed the company's security. You can also damage or compromise it from within by opening gateways for other cyber-attacks. Cyber defense is necessary, but it's also not sufficient. If you are managing an enterprise, the human element also needs constant attention.

YOAV TZRUYA: PARTNER AT THE JVP, HEAD OF JVP CYBER LABS, BE'ER-SHEVA

We have been investing in cyber security since 2001. What moved us to double up our efforts and engage with the entrepreneurs that the Israeli market is generating is the fact that we are seeing the landscape changing dramatically. We are seeing that the cyber security sector is moving from being a cost element for costumers to become mega business continuity 'must'.

There are many new opportunities these days; they are created by the changing IT needs and changing Operational Technology needs

on one hand, and on the other hand, by those innovative young people that come to us with ground breaking ideas. In the past year we have invested in five new cyber security start-ups. The statistics for cyber security in terms of the distribution of success rates for companies is not different from any other segment in the market. We do see however, that the quality of start-ups distributed differently compared with other sectors. We see a lot of good companies where the entrepreneurs may need to rethink some of their ideas. We don't see a lot of 'fake belly' as in other sectors.

Those five companies that we invested in, we hope that all of them will become successful, large, companies. At the end of the day, that's a part of the business of doing early decision investments. Not all of them will become like Cyber ark, one of our leading companies, which is now in the process of preparing for an 'Initial Public Offering' (IPO). Not all of the companies will become successful. Taking risks with technology, people, market needs is a part of what we do.

There is no single type of solution that we're actively looking for as the next silver bullet for cyber security. There's no such thing. When we listen to a pitch by a start-up company, we try to understand how the company is going to dramatically change the rules of the game in cyber security. The economic landscape of cyber security is dramatically unbalanced. The hackers have an easy life. They can take as much time as they want, they can test their solutions against the defenders and the infra-structure. They can buy 'off the shelf' products and try evade detection. The cost of launching a new attack for example, on a bank, is very low, it's around hundreds if not thousands of dollars. An attacker can use 'off the shelf' tools, tweak them a bit, and here you go. You have a new attack that is evading the IDS, the IPS, certainly the antivirus and the firewalls and so forth.

The defender does not know when the attack will come, from where, which new tools would be integrated, which evading mechanisms would be integrated into it. The costs of defending against such an attack are very high. The ration is about 1:1000. For each single dollars the 'bad guys' invest, the defence is required to invest a thousand dollars if not much more to protect itself.

The question is – can you change the rules of the game? Can you make it hard enough? You can never stop an attack completely. Attackers will

always find a way, if they have enough resources. But can you make it difficult enough for them, when launching a new attack, when targeting a certain costumer or a certain target, so that they will think of going somewhere else? Or go out of the business of hacking certain types of organizations? So this is what we are looking for.

[How do you build companies that last? How do build large cyber security entities?] Cyberark for example is a company of ours. A few weeks ago we filed for it to go public. We invested in the company in 2001. The company has been on the road for quite a while, it has great entrepreneurs, coming from certain army technology units with the core technology. They started with one product: vaults, for keeping digital documents and such under protection. Then, the market showed them what should be the next generation of products. They shifted their product mix a bit, and started to address different segments, one of the segments being the financial market. They have more than 1,500 customers today and they are ramping up very nicely. It is a profitable company. They identified in time certain dramatic changes that occurred in the market so the APT approach was definitely one of the key drivers for their growth over the last few years. In most cyber-attacks there is typically a stage where the attacker tries to engage in privileged escalation. The attacker essentially attempts to hack into privileged accounts, take advantage of them. This is where Cyberark kicks in. The product protects those privileged accounts.

Another key driver which created some regulation and compliance issues was the Snowden leak. A third party IT manager had a privileged account; he went into the NSA, stole documents and distributed them. These are exactly the things that Cyberark protects against. The founder and the CEO, Udi Mokady splits his time between Boston and Israel. They still have the majority of the company located here at Petach Tikva. The company didn't go and look for an external CEO to take it to the next step. We believe in the entrepreneur, we let him stir the company. I cannot say that we always knew that it will become a huge success, but I think that we always saw the way that Udi managed the company, as the right way to manage the company, building it one step after the other, listening to your costumers, addressing real market needs, coming up with new products at the right time, not ahead of the market, not after everyone else.

Incorporating great technology, but not overdoing it, not focusing only on the technology and leaving aside the products and the marketing side. The company grew year over year significantly. To a certain degree we knew that it will become a large company. We didn't know whether it will be picked up earlier or someone would issue an offer, or that we will take it all the way to an IPO, but certainly, over the last few years, we knew that it was heading in the right direction. In fact together with Goldman Sacks we did a secondary transaction where we bought some of the older, tired investors because we felt the company was going in the right way and that it will eventually be a true market leader.

[About investing in a company that has a minimal chance for an IPO, but a possible successful exit] The short answer is yes, but if you truly build value and you create a market, then an IPO is a natural path to follow. It is by far more interesting in the long term than building a company and selling it off quickly, although purely as an investor, if you can invest 5 million dollars in a company, and in a year or two later sell it for 150 million dollars, it's a great return. You can do this all day long. Eventually, of those companies that are out there now, a lot of them will get sold for 50-100 to 150 million dollars. I think those entrepreneurs and those after them, in the next generation, will be the ones that create companies that would grow and become big public companies or standalone companies, public or not.

[Is Cyber being over-hyped?] If you look at the characteristics of a hyped cycle, there are some basic elements that are common to different sub-cycles. First of all, it's high multiples for public companies in the space. Some would say unjustified multiples. You see a lot of entrepreneurs going into that. You see a lot of money of investors, and being invested in the space. And you see a complete disproportion between all of these to the actual market need, so I think that the first thing that you need to notice about the cyber cycle is that the market need is actually dramatic, it's huge. The market need is something that we didn't have in previous kind of bubble or hype cycles. Here we see a real market need in both IT and OT. For example, just think of the number of connected devices.

We are talking about 2 billion or so people that are connected to the internet today. There are about 50 billion devices that are addressable today. This was not true a few years ago. Think about the enterprise

and its boundaries. Who are the trusted users? Who are the trusted computers? What is the parameter of the enterprise? We need to take into account cloud technology, mobile and so forth. All these things are changing constantly. The first thing to notice about the cyber cycle is that the market need is real. Still, not all of those 250 companies will make it to the end line. Most of them will not. We see a lot of overlap, we see a lot of entrepreneurs that are still not ripe in terms of their maturity, in terms of understanding the market, understanding the customer needs and so forth. The cyber technology market is there to stay, it will grow over the next few years, and we'll see more and more needs that are actually addressed by those start-ups.

An entrepreneur should really try and simplify their pitch. They need to make it understandable. We can go as deep as needed into the technology and into the business practices and so forth, but at the end of the day, what people, customers, partners relate the most to, is a simple piece. So find a way to express very interesting technology, very advanced technology that you have, into a simple pitch that can be understandable by customers and partners.

AMIR ORAD, FORMER CEO OF ACTIMIZE, MEMBER OF THE FOUNDING TEAM OF CYOTA

How can one become a successful cyber entrepreneur? First, you need a real product and not a product with 'niche' features. Many people have great ideas about how to solve a specific problem with a specific solution, which results in a very specific feature that is not a big enough product. Entrepreneurs should make sure that their solution is big enough to justify the time and pain required by the institution which will deploy it. Secondly, if you have an amazing product, make sure it's actually something you can deploy at that institution. I see people that because of their military background come up with solutions that are relevant for governments much more than commercial institutions. It could be a brilliant idea, but one that cannot actually be deployed in the field.

Lastly, people come in and say "we served in the army. We saw this Godzilla attack, and we have the anti-Godzilla solution", but most people have never seen a Godzilla, don't know what a Godzilla is and will never see one. You have to make your product relevant for the

next 24 months. If it's something very futuristic that no one can relate to, it's probably not something that would win investments.

Regarding the typical Israeli cyber entrepreneur, and whether or not they must be a former 8200 unit member. Not having a single DNA is a part of the trick. If everyone came from the same unit, they say the same things, and therefore are much less likely to succeed. If you have a mix of business people and product people, if you have seen clients, if you can talk the business language, and if you can mix it all together, you are much more likely to succeed. If you are coming from the technology side you should partner with a partner that comes from the business side, a partner that can speak to clients and understand the language.

Where would I invest? We need to understand that the CIO or the CISO of a company have endless potential technologies to deploy. There are literally dozens of potential projects they can choose from. And they can invest only in two, three, or five at a given moment. So why would the CIO invest in your product versus another product? One reason is that the product might be the easiest one to deploy; it is as good as the average product but the easiest to deploy. It might also be a product which makes that person dramatically more efficient, effective, or it might solves a real problem that is coming from the top. For example, if the CEO's phone was hacked, the company is probably going to invest in that area, even though it may not be the right one for the company, since it is being pressured internally.

If you look at Israel, and specifically at companies like Cyota, Tra-still, Actimize, all succeeded mainly by focusing on the banks, and the reason is really simple. That's where the money is. If you look at the attacks, besides national level attacks, the attackers are going after assets, things they can steal and monetize. And money is there. After government and military institutions, the banks are the biggest targets in the market. Banks are sophisticated enough, they are willing to take risks and use small start-ups, because they don't have a choice. They are attacked all the time. They have the bandwidth and the assets to try various things and they know they need to rely on innovation, so they will take the risks and try to cooperate with start-ups. Small companies do not have as much to lose and don't have the bandwidth to try new things.

[How do you help big companies?] There are two different types of companies that came out of Israel. There are companies that were established in Israel and the sold, and are still leading in their field out of Israel but with an Israeli leadership, with an IP that was born here. For example 100 of EMC's employees are Israeli. That is a much more helpful, positive exit, than a company that dissolves and disappears, where people are leaving, IP spreading and you lose the company.

If the company disappears and dissolves it's really bad for the Israel. If it's the former, it's much healthier. So I think we should not overly complain about some of those outcomes, because they are healthy for the economy, healthy for the people, and many good people and good companies come out of those companies later on. And that helps the echo-system.

How do you help big companies? Scaling a company is difficult, it's painful, and it requires a different skill set. It's no longer about some guy thinking in the office or the in the shower about how to solve a problem. Some of those are skills that are required to scale a company we don't necessarily have. Most people don't have them and you need to bring them in on time. If you bring the people in charge of scalability early on, it kills the company. If you bring them on too late, you're already dead. So you have to bring then in at the right time.

In security that brand power is extremely powerful. If you're known as a trusted entity to solve APT, to solve breach detection, to solve all sorts of problems, you'll be the winner. Because people will follow that brand. If you are not that brand, you'll be one out of many companies and then you will need massive sales and marketing and it never ends. So Israeli companies have become the name for, being the number one in their field, Cyota was the number one, Cyberark owns a very clear niche. They own it. If you can own a niche, build the brand and scale. You're here for a good run.

[Advice for entrepreneurs] The space is a little bit overhyped. When I look at the 250 companies, most of which are first time entrepreneurs, most of which are very early in the game and many of which have been raising quite a bit of money very early in the game. That's a sign that the market is a little bit overhyped and if there was one piece of advice, I would hand out it is: 80% of the problem is to correctly define the problem. Criticism about Israeli tech is often that we build

the greatest solutions before we go out and search for the problem. The advice is that at the initial phases, just before getting funded, or as you get funded, spend the time to completely understand the problem, because once you do, you will go build the greatest solutions that is very clear.

YUVAL SHACHAR, FOUNDER OF TENTACOM, PQ, FORMER GENERAL MANAGER AT CISCO, MANAGING PARTNER AT MARKER LLC& INNOVATION ENDEAVOURS

Cyber start-ups offer for the first time the opportunity to build truly big companies, as opposed to a technology company which is sold for its technology. As an entrepreneur, I've often been on the defensive side while speaking in public panels, when people ask me 'why do you sell your companies instead of building a big company'. The answer used to be that there wasn't a deep enough bench. There is a very strong technology group in Israel and with the technology group, you can build a product and a vision and you can start selling the product and you may be able to get to 10, 20, 30 million dollars a year. To build it up from there, you need the same kind of talent that would operate market sales. Initially you find a few good people. When you try to build a company, finding the amount of operating talent used to be very hard to do, and I think today, a lot of this talent has come out of acquisitions; people who worked for American or other corporations and got into the discipline of how to run a company, how to run different aspects of it, not just the technology aspect. My passion is to hook up with entrepreneurs that are well rounded, not just from the technology aspect of things. People that identify a big enough problem, that might not be possible to solve, but if it's solvable, then it can create a category leading company.

The specific area of Cyber which is especially interesting is 'advanced targeted attacks'. The outcome of these attacks is so potentially devastating and it's probably one of the more challenging fields intellectually in terms of providing the right kind of defense. The market opportunity is huge and has not even been scraped at this point. I am intrigued by this whole world of 'internet of things' and automotive and the world of industrial defense. For similar reasons. And in some of them, the challenge for an investor is to time the market correctly, because it could be a little bit early to be able to

grow a company at this point in those spaces. At the same time we believe that if you look at these spaces early enough, than you could create 'security by design' and then as the field evolves, it will evolve around some healthy security principals that can be managed.

We are under-hyping cyber. Let's consider some examples. A sabotage of a nuclear plant. Stolen plans for the construction of a future plane. In the last two weeks alone, the largest bank in the US was penetrated, probably by a nation. In the last two weeks alone we had pictures, private pictures, of most celebrities stolen. In the last two weeks alone, 70 million credit cards were stolen from Home Depot and before that, from 'Target'. And in those weeks, we learned that our mobile device will be our wallet, and we'll have data from the watch about our medical status. That's how important and how real that environment is. Be focused, be practical, give value add and make it very easily deployed, because people are surrounded with tools that are too difficult to use.

DR. ORNA BERRY, CORPORATE VICE PRESIDENT GROWTH AND INNOVATION EMC CENTERS OF EXCELLENCE EMEA AND THE US

There is no one single segment or subfield of Cyber Security today which represents a better opportunity compared with other segments. The art of mixing technology and business requires us to face a rapidly changing scene. You want your systems to continue to improve their resilience because it's very much like our life in the Middle East. We're on our toes, waking up because of every noise, because we know something is happening. The same happens with cyber security: you're on your toes, you invent something smart, the bad guys invent something smarter and so you need to continue. It's a continuous process and I wouldn't say one segment is more promising than others. The main challenge is the integration of multiple types of segments and the adoption of constant change in order to improve the protection of the 'good guys' and make the job of the 'bad guys' harder.

It is true that the banks are willing and are able to pay because the attacks are translated into dollars. But not everything is measured by money. The more information you have, the more regulation you are under, and the more obligation you have to retain a certain level of integrity as applied to the information. You can develop certain

technologies, be it for the defense establishment that is willing to pay, but at the end of the day, issues related to privacy, to integrity and to use of massive amount of information, are regulating your ability to protect them.

[Is Cyber being over-hyped?] The 'hype' might be a matter of price, but the topic is not overhyped. This reminds me that less than ten roughly 9-8 years ago, people thought that defending the homeland is not related to defense, that homeland security is not defense. Today everybody recognizes the importance of iron dome for the defense of the homeland. You cannot conduct a war when the home front is being jeopardized. Cyber security is by all means in its infancy. Developing it is going to consume far more energy than before in order to maintain the know-how on the digital infra-structure and to basically face the intrusion, the continuous attempts to use missiles. The attempts to use information for malicious reasons beat defense, beat commercial, beat health and anything else. I don't think that anything is hyped. I think that we are beginning to use the digital infra-structure, the massive amount of information, the machine learning capabilities and everything that we understand about psychology and the human mind in order to define in this context remedies for an evolving situations. We are at the beginning. Find the best investors who understand the space and can guide you very well where to start partnerships so you will succeed.

***

NIR PELEG, DIRECTOR OF THE R&D DIVISION OF THE NATIONAL CYBER BUREAU (CHAIRING A PANEL)

The notion of 'internet of things' (IOT) was born around 2009 when the number of internet connected devices exceeded the number of people in the world. And the expectation according to Cisco is that in 2015 it will stand on 25 billion and in 2020 – 50 billion. The internet of things is also called 'cyber physical systems' because it relates to cyber and connects cyber to physical systems. It creates new markets and new opportunities, but also brings challenges and threatens to change the current landscape.

In technologies such as IP protocol and Sceda system, as well as other legacy protocols, security measures came after these systems were developed and were patched into the architecture. In the case of IOT there is a real opportunity to implement security by design, since it essentially involved a new field and a new architecture.

MOOLY EDEN; SECURING THE INTERNET OF THINGS

While Internet traffic is exploding, billions of people and billions of intelligent, connected systems are all demanding more and more bandwidth. Every minute, there are thirty hours of video posted on YouTube, 100,000 tweets posted on Twitter, six million Facebook page views, twenty million picture views on Flickr, and 47,000 mobile app downloads. None of these sites or services existed before 2004. Also, each minute, 45 new malicious websites are launched. Global internet traffic in any given minute would fill 230,000 DVDs with data, and the amount of content stored would exceed 18,000 HD movies. By 2015, 15 billion devices will be connected to the Internet. Mobile traffic will increase eleven fold. Overall traffic will triple. All of this data points to the need for a more secure, intelligent network.

All of this data, all of these devices, all of these things are exposed to attacks. When it comes to the Internet of things, the scale is going be larger and more frightening. First, it's important to understand the meaning of the "Internet of things," or, the "Internet of everything," because the terms are often used in different ways. The Internet of things encompasses any device that meets three criteria: it computes, it communicates and it's connected to the cloud. 85 percent of the devices today that compute, including refrigerators, dishwashers, automobile systems, etc., are not connected to the Internet, and for that reason, they are not included in the Internet of things. The Internet of things includes devices that compute, communicate and are connected to the cloud, either for data or to perform large data analysis and help improve our lives.

What exactly is the Internet of things? First of all, it's "about me," the individual. It's about my smartphone, it's about my fitness devices. It's about smart glasses. It's about all the things that people carry on them, often all the time, which can record what they hear and see. These devices encompass a small part of the Internet of things. In

the near future, there will be wearable patches that include computer screens, dresses made entirely of computer screens, and so on. Wearable patches will inform us when we are lacking certain vitamins or nutrients. The same device will inform individuals of their heart rate in the gym, and use with wireless connectivity to provide them with other data. Groups of people wearing the technology can meet and share information, videos, or reminders, using their clothing. The same wearable technology can be used to help athletes improve their game, or as a learning aids for children in school.

It is simply a matter of time, as these kinds of wearable devices will exist within two and a half years, and will be commercialized in less than ten years. While this technology is "about" the individual, it is also "around" the individual, as it includes the ability to manipulate the surrounding devices such as air conditioners or laundry machines. Electric companies could theoretically operate the laundry machine based on when it has surplus electricity to provide, and thus could provide special rates for such regulation. Refrigerators would "know" exactly what they contain, and have the ability to order new groceries as needed.

Such technology includes inherent dangers, as an attack on such a refrigerator could result in its owner's bank informing them that they have gone into overdraft because their refrigerator ordered one ton of cheese from China. This kind of technology, in the near future, will encompass the individual's entire world. "Smart cities" will incorporate smart traffic systems and security cameras that will communicate and be connected to the cloud.

Devices are currently defined by their computing power, and their form factor. Servers have the most computing power, and the largest form factor. Currently, efforts to protect data focus primarily on servers, though efforts are also made to protect PCs. Wearable devices and phones, however, are largely left unprotected, often they are not even encrypted. Why should attackers target the well-protected server, when they could easily target a relatively unprotected device, and access the entire network from there?

There are perhaps hundreds of millions of servers in the world. There are likely billions of PCs, and perhaps six or seven billion internet-connected phones. The Internet of things is expected to include 50

billion devices by the year 2020. By then, every facet of modern life will be run by internet-connected devices.

This should be very frightening. One study from HP that examined current Internet of things devices gave their overall security a failing grade. Often such devices are not secured. Common passwords on such devices are 1234. Networks are not encrypted, and can be accessed by anyone. As such devices become more and more involved in people's lives, very personal data about them, such as their current pulse and heartrate, as well as other valuable information, will be available to everyone.

Currently, lost or forgotten Internet passwords are retrieved by citing the user's mother's maiden name. This information is easy to find about anyone, and as soon as it is found, it can be used to change passwords and therefore steal accounts. Firmware, which is actually the lowest level of software on a device, even lower than the operating system, is often updated through automatic patches from the OEM, or original equipment manufacturer. Malicious firmware patches can be sent to install viruses on devices that can be very difficult to remove.

Many different companies offer varying solutions and protocols, but none of them offer actual security. Current security protocols lack contextual, adaptive capabilities. They are too costly, they are not efficient or effective. They are often too complex to manage, and offer fragmented solutions, if any. In several years, these devices will be much more prevalent. Users, for examples, will instruct their smart cars to drive them home and hope that their car won't be hacked on the way.

What will attackers target? The chain is only as strong as its weakest link. The weakest link, in this realm, is the Internet of things device. Rather than trying to attack a network's strongest point, attackers can target simple, unsecured devices, of which there will soon be 50 billion, and then make their way through the network to the real data.

To combat such scenarios, two things must be done. First, security ubiquity must be given more importance. Currently, when designing micro-processors, or software, designers focus on size, power, and performance. That checklist must be expanded to include security as well. There must be sufficient security at every point on the network, from the smallest devices to the servers themselves. Security must

be a priority for every point of access to network communication, including phones and other wearable devices.

Examining security from top to bottom, we start with the phone. At the lowest level of every device is silicon. The silicon can be made difficult to break from a security perspective, because it is a transistor. It cannot be altered from the cloud. Above the silicon is the firmware, which is a low level software that comprises the interface between the hardware and the other layers. Above the firmware is the system, middleware, software, and finally, applications.

The silicon, the lowest level, is the microprocessor. There are numerous mechanisms that can be implemented to protect the microprocessor. There is the manageability engine, which serves as a "small brain" to the microprocessor, which is the "big brain." The manageability engine, which is not affected by the operating system, can be used to determine the status of the microprocessor. For example, if a device's anti-virus software is uninstalled, the manageability engine will notify the user that there is no anti-virus software, and will reinstall it.

Another mechanism is software guard extensions, which will be widely available with Skylake, a next generation microprocessor that will run different pieces of software in different enclaves, to make sure that one is not impacting another. This could prevent a virus affecting a web-run application from attacking another application on the device.

Yet another mechanism is memory protection extension. Many virus attacks are conducted by overflowing a system. This mechanism can stop such an overflow of the system and notify the user that it is under attack. This mechanism will also include a boot guard, which will store information about a device's initial boot up, and compare it with every future boot up, to inform the user if there is something different that could constitute an attack or contamination.

It is no longer a secret that the company Windriver, which was recently acquired, is developing machine to machine operating systems that are meant to take care of security, collectivity and manageability, all of the things that are required for this kind of security. These mechanisms, within Internet of things devices, can communicate over the cloud, but will also communicate with each other.

Even with all of these mechanisms in place, there is still a chance that that a device will be contaminated by some kind of a virus or worm. For that reason, security software will continue to operate on a device's higher levels.

These efforts are not prevention, similar to what is being done with other hardware on the lower levels, but rather merely detection. Comprehensive security such as this must be present at every point on the network from Internet of things devices to the servers. Security on each of these devices must be strengthened from top to bottom, from the silicon, to the firmware and the application level.

Of all the cyber companies in Israel, the one missing is ours. The next generation microprocessor, called Skylake, designed in Haifa, scheduled for release in 2015, will include all of these security mechanisms, including securing enclaves and buffer overflow detection. All of the encryption systems are designed by teams in Petach Tikva. The small manageability engine, which checks the status of the operating system, is designed by teams in Jerusalem. Mechanisms for examining large data in order to identify abnormal behavior that could indicate virus attack are developed in Kiryat Gat. These teams, as well as the presence of three companies in Israel that were purchased from MacAfee, attest to the fact that Israel is ideally positioned to do integration work an all of these mechanisms from the hardware to the software, and will be able to develop something that is very robust.

To summarize, security will be even more important in the future, and it will be necessary to ensure that data will not be exposed to viruses. The Internet of things, therefore, is a great opportunity, but it is a huge new risk. The potential for attack will be much larger, as it will constitute some 50 billion devices. Phones, which sell for $600 or more, can include some security mechanisms in their manufacturing costs. Smaller devices, which would sell for $30, for example, would be much more vulnerable. For example, if every house lamp is connected to a network, it could be a target for hackers. This is the level of dependency on security that we will reach.

Security solutions must be developed to protect every access point on a network from top to bottom. This will probably require cooperation among rival companies in order to define better standards, as standardization will be essential. The necessary work will be impossible

without it. Historically, the world decided to take the necessary steps to combat pirates on the sea, and the threat was extinguished. This is exactly the same thing. It needs to be done together.

A great deal of knowledge in this field exists in Israel, because people here are innovative, because so many people go to the army. The Israeli high tech industry is well positioned to be on the frontline of IT security, because first of all, it is important for everyone. Secondly, it's a great business, and a great opportunity for the Israeli economy.

SUBRAMANIAN RAMADORAI, CHAIRMAN OF THE INDIAN NATIONAL SKILL DEVELOPMENT AGENCY NSDA AND VICE PRESIDENT AND CHAIRMAN OF TATA CONSULTANCY SERVICES

Welcome to the age of the internet of things. Having been in the industry for over four decades, I've had the good fortune of being a part of the three ways of disruption that computing and the internet have brought about, each of which have brought about their own amazing transformations. The first is the internet of computers that flattened the world, breaking down knowledge barriers between nations. Making one world a reality. Next came the revolutionized socialization amongst humans, making the concept of one people a reality. The devices in our physical world turned into a seamless extension of ourselves. The internet of things or IOT, is turning the concept of one entity into a reality, and the core of IOT is to bring together people, data, process and objects or things, and connect them to communicate smartly, taking the user experience in a different level altogether.

What is most exciting about this phase is that today we can only make an intelligent estimate about its future impact. It will exponentially enhance personalized experiences, our efficiencies and convenience and at the same time it raises fundamental questions like geographical boundaries that determine our legal systems and its use personal privacy.

There are already more connected devices than people on the planet. And there will be about 26 billion connected devices on this planet by 2020. The IOT vision enhances a notion of connectivity from anytime, anyplace for anyone to anytime to anyplace for anything. The consequence of network things is smarter processes and services.

It can support our economies and of course this means businesses have the opportunity of working smartly.

Here is an example: we all heard of automobile companies recalling cars when a defect was identified. In a recent occurrence in the US, the national highway traffic and safety administration issued recall for two vehicle models: a pickup truck from a major auto manufacturer and a TESLA model with 29,000 units on roll. A software update was required to be installed to reduce the risk of fire during an accident. The truck manufacturer had no option but to recall the 370,000 trucks, update software and bare costs and damage to the brand value. On the contrary, all the TESLA models were constantly connected to the wireless, so Tesla just pushed the software updates to each of its cars over the network and the cars were turned off. Thus, instead of suffering the blowback to the Tesla brand, it showed that Tesla is one of the most forward thinking car makers.

GE Aviation which produces aircraft engines is another example. They are providing new capabilities relevant for in flight diagnosis, prognosis and monitoring. This is also applicable for other sectors; gas, water, energy. It is possible to use IOT in analysis and prediction results in smart network. IOT helps resource saving in many Indian cities, since the urban poor are prone to steal electricity from the power grid.

By using IOT the authorities will be able to get more information on the systems and hence will be able to fix the problems and address these leaks which are one of the reasons for the high cost of delivering utilities to these areas. IOT has the potential to bring more effectiveness in the system as well as bring about societal changes by enabling consumers to pay less. For example, a power plant with a 'real time' sensing of vital parameters can be managed more efficiently from a centralized centre providing for efficient operations and proactive actions for the utility.

Clearly, internet of things fundamentally changes the industry in terms of sensing, information collection, analytics and of course, service optimization. Enabling companies to adapt to this evolution would make them more successful globally. The future will see the shift of the manufacturing companies from the ICT automation and production to a connected manufacturing by deploying industrial internet using

IOT, cyber systems enabling a connected and to conduct productive prognosis, diagnosis and of course, the optimize supply chain.

Having established the business advantage, we must look at the agenda, especially from the perspective of emerging economies. For countries like India IOT can be hugely significant in terms of data through networks. These technologies need to be low cost and affordable for a scalable solution.

Another critical areas is of course health care. Internet of Things will enable a connected cost effective health care system that will focus on preventive measures rather than on curing an existing problem. It will enable remotely monitoring elderly people, patients with chronic diseases, and cut down the number of visits to the hospital due to remote monitoring techniques.

In the famous James Bond movie 'Casino Royal', Mr. Bond faces a cardiac arrest while playing poker. He rushes to his car, connects himself to a health monitoring device, this device sends his vital parameters to central M16 medical team and the medical team remotely gives him instructions as well as treatment to resist the cardiac arrest. While this was a movie, the same can actually be replicated in real life with the power of internet of things.

Most of the developing countries lack the software background and they cannot integrate the physical world into the digital world.

With this total revolution of internet, each country will eventually embrace internet of things. Many countries are pushing the envelope on leveraging, IT including Internet of Things. As for the global information technology report 2014, the countries who are leading the network readiness index are the Netherland, Switzerland, US and the UK. These countries recognized the need and are investing in liberating the future of growth. In a recent event the British Prime Minister publicly urged the UK and Germany to work together on three specific areas: finding faster internet, quick enough to download a full feature film in less than a second, Internet of Things and the use of a digital single market. The UK prime minister has set up a 45 million dollar funding for research in areas linked to the Internet of Things, taking the total available funds to 73 million pounds for the European Internet of Things grant fund to support companies who want to exploit some new opportunities. London's Heathrow is also to become the first

airport in the world to use IOT technology to rewire the experience of catching a flight. And while the US and Europe are moving ahead, China is establishing its leadership as well.

'M to M' and IOT are closely linked, and China's success has been attributed to the collaboration between their mobile operators and their enterprises. A dedicated unit called 'China internet of things' has been established. IOT and three verticals in particular are being focused upon: energy, transport and smart cities. The future of IOT raises two important questions: security and governance, but even before that, it's important to be sensitized to some related issues. There is a sensitive aspect to Internet of things: more and more personal data is flowing through the network devices, which makes them susceptible to hackers.

We need to establish what is private and what the relevant privacy rights are. Can smart meters leak information on whether the user is at home? What rules shall govern companies to respect the confidentially and seek permission prior to sharing this information? It is important to understand as to who owns your private data and who has the right to monetize it.

Apart from the ethical aspect, there are also existing challenges which are technical and social. The first basic challenge to IOT involves different technologies and systems. It is important to have one standard up road, so as not to reinvent the wheel every time.

Open IOT platforms will encourage competition and innovation in device management, as devices are going to be spread across numerous locations. It'll be a difficult task to ensure the operation and remote management of these devices. It also lends itself to problems of updating the devices, which cause security issues.

As IOT expands to its full potential, the enormity of the data cannot be ignored. We need to store and manage huge data volumes, and this need will lead us to build more data centres across the world. Data processing, networking and storage will consume enormous amounts of energy. This is challenge is partly being addressed by producing low power devices, but that is just a small part of the solution. The world's energy demands are predicted to rise exponentially. There are a lot of rare elements and heavy metals going to the manufacturing of these small devices, and their disposal produces pollutants which are not

very easy to recycle. There are a lot of environmental considerations to think about.

The most visible challenge to security comes from the small size and power of these devices. Modern culture analysis advances that a certain minimum key size and complexity are a requirement needed to secure devices from any malicious attacks. Usual IOT devices are so small that most of these techniques are not suitable to use, making them susceptible to data leaks.

IOT can have multiple or multitude of devices across technologies including arcane mainframe devices connected to new sensors. This creates a problem during updates. Given the security that is used on such a devices, it is likely that the thousands of already deployed devices will remain un-patched due to a variety of reasons like connectivity, size et cetera. In fact, it's not even a certain that a patch will be available from the manufacturer.

The idea of advance persistence threats (APT) is by now well known in the security industry. Due to 'upgradability' using IOT, such devices will probably play a big part in the persistent aspect of APT. If attacks on IOT devices succeed, leading to hacking a connected car or hacking a traffic light, threats to physical and personal safety issues will become more acute.

Since IOT devices can also be used for surveillance, it's very important that such devices are secure, especially after what we know from the recent Snowden affair. Unfortunately, government regulations and ethical codes of behaviour with regards to privacy and data have lagged behind the technology development and IOT is only exasperating the problem. Let's learn a lesson from the past. When it comes to protecting our environment we fail to set in place governance for all nations, and we could see a real threat to the planet before us. Now cyber security is on the rise. We need to step back and formulate global governance norms on how we prepare, we as a people from around the world, and what can we do to make the world more secure. There does not exist any governance on the usage of IOT.

Basic questions are left unanswered, these include questions like 'who owns data?' 'Who has the stewardship of the data?' 'Who determines what data standards are to be set?' 'Where is the data to be kept?' 'Who has the access to the data' and 'who has the right to monetize it?'

Questions also arise about where and on which device does the data reside? All these questions are valid and important. Unfortunately, there is no black and white answers to these questions. I believe we need to set in motion an institutional mechanism for IOT governance, with are representations from business and civil society. This will also help in sharing to develop and deploy our best practices for cyber security and IOT. We need to define limits of privacy and its protection. Does it requires a general agreed upon framework on guarantees that an individual has in terms of cyber liberties? Recent revelations of global surveillance by governments have created a strong indication that we need to re-establish legal frameworks to deal with issues regarding territorial jurisdictions, data ownership, data preservation, protection and privacy.

We all need to address the problem of existing cyber laws that do not carry enforcement provisions. Open standards and frameworks for interoperability of devices in IOT need to be created. The free market should be able to decide whether to pursue an open standard or close standard as IOT progresses. Global service providers such as Google, Microsoft, Twitter, Yahoo and Facebook must cooperate with law enforcement agencies in all countries in response to their investigations.

We need to begin by teaching our children about cyber-attacks in school so that we raise responsible citizens. I therefore would like to propose the idea of a national cyber treaty organization that will set up rules for international cooperation on crime together. It will set up the rules of the role and a process to asses when a country has gone over the line in acts of cyber war, coupled with an appropriate sanctions regime. It will set up a privacy 'bill of rights' for citizens worldwide that prevents unwanted intrusion into their private lives.

Finally, I would like to say that technology can be both an accelerator and an enabler for the world of tomorrow. It provides the global community with new opportunities to foster innovation that boost economic and social prosperity in developing and emerging economics.

Thinking back about the birth of the internet, we have clearly come a long way. When we crystal gaze into the future, not just into the next few years, but into the centauries to come, it is clear that technology will present possibilities that seem magical today. Perhaps one day

an ancient Indian scripture will describe a highly advanced civilization guided by highly evolved sages who master metaphysical skills and have unlimited resources of energy to travel to the furthest stars and solar systems in sophisticated spacecraft. Indian scriptures talk of scientific and spiritual advancement in the same mind. One does not exist without the other. Perhaps spiritualism, modern science and ancient history can inspire ideas so that new technologies can be used responsibly and can become a power enabler for a progressive and a peaceful human race.

ARIEH MIMRAN, VICE PRESIDENT OF QUALCOMM, ISRAEL LTD

The next internet paradigm is here. During the first generation of the internet we've been consuming data from the internet. Reading emails, browsing the internet, reading the news. The second generation of the internet brings about sharing. We started sharing, and not only with one or two people, but with many people who like to read what we write. In the third generation of the internet, devices will speak with each other. This is the 'Internet of Everything', or IOE. It will change the way we live our lives.

Several numbers have been mentioned regarding the year 2020. 25 billion connected devices is an amazing number. It's three times the population living on earth at this year [2014]. It represents the biggest opportunity ever for the internet. The way we will see this realized is in three different spheres. First comes the body and we already see this. We have biometric indicators, we have glasses, devices which measure our heartbeat, pulse, steps, surrounding our body. In the next stage we have the home sphere, our home will be managed in a more efficient way. The next large sphere is the cities. We will be able to manage our cities in a way that will make our life much more efficient. For example, imagine you are in a car, you approach a busy city, you look for a parking spot, you get an indication for a spot and it's reserved for you. You go there, you park. Studies suggest that up to 30% of driving within busy cities is spent on finding parking spots.

Regarding the home front and the environment, each and every one of us has a few devices in their home: gaming devices, lap tops, computers, smart phones. With IOE we will have a mix of all those smart devices and also simple devices. We will have refrigerators and microwaves

communicating with each other. Imagine a case where a light bulb starts flashing when, for example, your kids forget the refrigerator open. Or imagine a scenario where your refrigerator orders for you milk just when you're about to run out of it. Your washing machine will send you a text when it's done with the laundry.

Most of the companies concentrate on the cloud side of security. We heard today many concepts on increasing the security in the cloud, fragmenting it, dividing it, being agile. We now need to have a complimentary shift from the cloud to the edge. What is this edge? The edge is our gateway at our house, our devices – whether they are sophisticated or simple. This gateway at our home stores our identity, it runs services for us that we have purchased.

Let's take a closer look at this light bulb. We see this light bulb, we like the concept. It brings many nice features. It also saves some power. We want to have it. So we go to the nearest store or on-line and we order our light bulb. We get home, and then we plug it into our home network. Now, imagine that this light bulb has a virus that some attacker or some hacker put into it after it left the factory. This virus now starts penetrating other devices. Now our laptop, our TV and our washing machine all become agents of this virus and they start transmitting data outside of our network. Our network today includes our digital identity. We have our passwords stored there, we have all our personal information that we want to use when we purchase things, when we go to have some health care. We have our financial reports there. Everything is digital and it's stored there. When it comes to addressing the challenge, it's no longer the question of 'if we have a problem' but rather 'when and how' a security breach will take place.

We now increasingly more sophisticated machines in our homes, just like big machines in the network and in the cloud, and we need to take advantage of that. The first element of security is authentication. Devices should be authenticated before they can join the network to make sure that they haven't been changed since they left the factory, that the user is the very same user we think should be, that there's no middle man between the device and the gateway.

Then there is detection. With less sophisticated devices we do not have options like the ones we have in our smart phones to run antivirus

that would detect specific signatures of viruses. We need to have in our gateways some sophisticated software and algorithms that will be able to detect the behaviour of those viruses. Once we detect a virus we need to contain the threat, i.e. we can either disconnect the device or reprogram it. Just recently we have announced at Qualcomm the release of the safe switch. Mobile users whose mobile was stolen or lost could remotely lock it using this mechanism. In California and an increasing list of states in the U.S. as of next year [2015] new devices will be required to have a safe switch. In the future we would need to adopt such solutions to simpler things.

When it comes to mobile security, there are two elements to consider: security hardware and security software. Security hardware mechanisms are mechanisms like encryption at a very low level that protect our mobile phones. The software mechanisms represent the upper layers pf security. When we combine those in a smart phone, we can imagine how it's done.

It is a challenge to simplify the solutions for other devices. We need to take a holistic approach to be able to offer a solution which covers all ranges, from clients to the cloud. At the clients level we need to have authentication ability at very low levels. Gateways at our homes will be able to compliment all the parts, for example: an antivirus software can detect the behaviour or things that are misbehaving. Then on the cloud level we would need sophisticated algorithms to make sure nothings escapes from our home to the network.

Our call today is for everyone to wake up. The internet of everything is happening and security is only now catching up. We need to build a common language, create standardization. This common language will allow all the partners in this holistic approach to cooperate in a way that will make things work. Qualcomm announced that it has joined FIDA, an organization that creates standardized authentication for biometrics. Now, we need to take adopt standards to the entire IOE. We need to work together, to build solutions that enables smaller devices.

We are all used to sophisticate computing engines, increasing quad-core, and octal-core. What happens when we have a very simple and cheap light bulb? How do we protect the network? How do we protect ourselves in such an environment? We need increasingly more

sophisticated detection algorithms to allow that. I would like to invite you all to join us to this journey. It's a challenging one.

DANIEL JAMMER, ENTREPRENEUR, NATION-E PRESIDENT AND FOUNDER

Regarding the ' internet of things': I don't see that everything is so beautiful because in everything good there's something bad. By 2020, about 50 billion devices will be connected to each other. The existing Scada system will be challenged more than ever, because hundreds of thousands of new devices are entering the system. One billion smart meters will enter our life by 2020. And as we have seen in the previous talks, our house and life will be inter-connected with solar, battery storage, electric vehicle, wind, thermostats of all kinds. Now, the question is 'are we secured for this amount of innovation?'

Smart meters that are being hacked represent bank accounts and the future of the utilities. Our homes are getting connected and the same threat will appear in this front too. Turning risk into opportunity – that's the reason we developed something new, a new way of thinking. We developed the first energy firewall. It is not a standalone unit, because as a standalone unit it is not possible to win this war against cyber threats. When we started to sort out how to protect N-points, especially N-point of meters, of battery storage, of solar, of wind, or an integration of these things, we set it as if the Scada system is already fringed with hundreds of different kinds of malware. We might also need to develop a new command and control software, what we call 'energy cerebrum'.

All critical infra-structure depends on energy. Water, gas, oil, telecommunications, the financial sector, the energy sector. Everybody talked about 1 billion smart meters, 50 billion smart devices. Who is going to take care of this data tsunami? 50% of organizations today are unaware of the threats. 26% believe that cyber risks in their entity are managed well and only 6% of the employees working in all companies are being trained on cyber. A disaster is around the corner, 68% of utilities believe that they will be attacked. 64% expect that they will be attacked more than once. Therefore, we decided in Nation-E to provide something for you, for our costumer, our energy cyber security centre. In our energy cyber security centre, we offer

utilities, telecommunication homeland security, financial services, gas, oil, data centre a new possibility to detect, to monitor and to learn. In our energy cyber security centre we offer you a complete offering of advisory and auditing.

MAJOR GEN. (RET.) UZI DAYAN, CHAIRMAN, NATIONAL LOTTERY MIFAL HAPAYIS

Mifal HaPayis supports a young group called Magshimim. We currently give a cyber scholarship. Our condition in this field is relatively good, this is a field that the State of Israel had been relatively prepared for. Over fifteen years ago we started discussing a "computer war" in the army. Issac Ben Yisrael was one of the leaders in this field, at it seems that at the time we believed we were sufficiently prepared. The Prime Minister and other high ranking officials have taken the matter into their attention, and there is still much to be done, but Israel is currently in a good and important place when it comes to cyber. I would like to raise a couple of points, a couple of goals, and a dilemma that the young generation is currently facing.

The first goal, a little far from what people like to talk about all the time, is the Hebrew language. It seems that the Hebrew language was born such a long time before the digital age. Only 22 letters. A very concise language, short, extremely suitable for this field. This does not go without saying. The ancient Hebrew writing is 3,500 years old. Later on it became today's Assyrian writing. This is a concentrated language. There are four words long sentences in Hebrew that cannot be translated using anything less than sixteen words. Therefore, on one hand, the Hebrew language is very suitable for this field, and on the other hand, it is a unique language. Many fear that this era turns the language into a meager language, filled with acronyms, takes its soul away. A few years ago, we in Mifal HaPayis announced a competition called Zrazar Payis. The goal was to write a story using 140 characters, and every year the story has a different title. Over the years, tens of thousands of youngsters have taken part in this competition. Two years ago, the winner composed a love letter. In the judges' panel, the writer Meir Shalev remarked, somewhat sarcastically, "you don't have to go very far. Take the biblical verse 'So Jacob served seven years for Rachel, and they seemed to him but a few days because of the love he had for her.' In Hebrew, it's altogether 61 characters." You don't have

oppose, you don't have to move backwards, quite the opposite – one must utilize the language, make use of this age in order to strengthen the Hebrew language.

The second field is not the field of security, as much as we are used to think about a cyber war. This field provides many intelligence gathering opportunities, and some exaggerate in its value, in my opinion. I suggest considering, for example, what were the implications of Operation Protective Edge. How much did cyber contribute to this way? To whomever thinks that this question is insignificant and unimportant, I would suggest to consider if, in the regional war that currently takes place in the Middle East, cyber is the most important and leading matter. In contrast, we have to consider what cyber can do in the social field, and I think this question is one of the challenges that we are facing.

Many speak of closing the digital gap, but even if this gap is to be closed, it doesn't necessarily mean that the weak will benefit from it. A while ago there was a convention here, in Bar Shira hall, which dealt with the issue of cyber. There were about 600 young people there. I was there, and I asked the participants how many of them have already been to the recruitment office for the first time – about three quarters of them answered positively. My next question was how many of them had a perfect combatant medical profile. About three quarters of those answered positively. Now comes the question – in a short while, when they have to face the decision of where to go and what to do in their army service, what will they do? Not all of the young people in the world face this dilemma. I remember that many years ago, my generation didn't have such dilemmas. We had our own dilemmas, but not the question of whether to be a fighter or what is called today a "cyber fighter", which is, in my opinion, an obscene term. There is a vast different between being a warrior and a cyber warrior. These days you can't win a war by clicking on the keyboard, as the war in the Middle East has been proving us. There is an essential difference between someone who endangers their lives and pulls the trigger, and someone who doesn't. They all have important roles, however, today the youngsters are facing a dilemma. I think that the answer to that dilemma is very clear, but we have to be careful. I think it is wrong that there are many hundreds of soldiers in the army who could have been warriors, but are given the option not to do so. And they

gave it the wonderful term I've already mentioned, "cyber warriors". So we are fortunate to have come to a generation that faces such dilemmas. By the way, among all these youngsters there are only 15% young women, girls. This has absolutely no justification. There is not a single Orthodox Jew there. This is completely unjustified. Therefore, this is one of the dilemmas. I choose to say this here, of all places. Obviously, we will continue to support this field. This is a very important field, but please don't consider it the only and most important of things.

PROFESSOR JOSEPH KLAFTER, PRESIDENT OF TEL AVIV UNIVERSITY

This year's conference comes in the wake of a difficult summer for Israel. The country's defense strategies, including in the cyber sphere, were tested, yet they prevailed. More than ever before, we need to nurture the best scientific talent, set up the most advanced labs and strengthen links between academia, government, business towards unified front guard against cyber threats. Recognizing the vital importance of this area, international entrepreneurs and philanthropists Len Blavatnik, has established the Blavatnik Interdisciplinary cyber research center here on campus. Tonight is the festive launch of the Blavatnik center, here in the presence of top leaders, practitioners, researchers and students. And while Len is not here in person, I feel he is certainly here in spirit as we open a new chapter in cyber excellence at Tel Aviv University.

The Blavatnik center will have wide and vary activities. It will draw on the university's deep pool of scholars and experts to advance research, to disseminate findings throughout the highest echelons of government and defense. It will train a new generation of cyber scientists and analysts, expand cooperation between the university and industry, and very importantly, it will educate the general public. The centre's goal is to keep cyber security at the top of the national agenda and to position Tel Aviv University as a thriving go-to place for cyber innovation knowledge in Israel and in the world.

The university has already a solid record in this field. We have hired more outstanding Israeli academic starts in cyber fields than other institutions. The university's breakthroughs have attracted partners such as the US air force, NATO, top Israeli intelligence and defense

agencies, TATA industries, Broadcom and others. On the policy front, the university's Yuval Ne'eman workshop has been providing incisive reports to the prime minister, defense minister, IDF chief of staff and many other decision makers and agencies for the last 12 years. And finally, in a vote of confidence in this track record, the national cyber bureau at the prime minister's office selected Tel Aviv University as the site for a national cyber initiative and has committed major funding over the next 5 years towards this enterprise.

Len Blavatnik has chosen to be a key partner in this venture. He has chosen to invest in our cyber research, but not only that. The Blavatnik center is part of a 20 million dollar Blavatnik initiative which was announced last week, but the Blavatnik family foundation and initiative that will support drug development, computer science, student film production and young faculty recruitment at Tel Aviv University over the next four years. We would like to recognize Len who received an honorary PhD from Tel Aviv University, for his passion for education, for his support of excellence and innovation and mostly, for his friendship towards Tel Aviv University, and his strong belief in us. Thank you very much Len.

And now, I would like to call to the stage Len Blavatnik's representative here tonight, Avi Fischer, who is by the way, a Tel Aviv University Law graduate and also served a faculty member here, to accept a certificate on Len's behalf.

[Content of certificate] "This is to witness that on the 14th day of September 2014, the Blavatnik interdisciplinary cyber research center was launched through the generosity of Len Blavatnik in the presence of Benjamin Netanyahu, prime minister of Israel, thereby, strengthening Israel's national cyber initiative, creating a dynamic framework for generating up to the minute research and analysis by leading scholars and experts, preparing a new generation of cyber innovators and professionals to shape and lead the cyber security field, foster mutually beneficial cooperative ties within academy, industry and government and consolidating the national and international standing of Tel Aviv University as the principal harbour for cyber knowledge and excellence in Israel.

AVI FISCHER; LEN BLAVATNIK'S REPRESENTATIVE

Let me begin by saying that I am very much honoured to be here and even more honoured to represent a good friend of mine and a person I truly admire and cherish, Mr. Len Blavatnik. We have a saying in Hebrew, 'you don't praise a man when he is present', so in this case, in these circumstances, since Len could not make it – I can take the liberty of saying a few words about him. Len is a role model for successful businessmen around the globe and a very warm hearted individual who is devoted to the Jewish heritage and is a proud Zionist. Len, who is a half year younger than I am, succeeded to build in the last 30 years or so an empire; Access industries, a global industrial group that has diversified activities around the globe. In his profession, by the way, Mr. Blavatnik is a software engineer, and therefore, his first donation for Tel Aviv University was the computer school here. He received MBA from Harvard, and most importantly, he's a believer, a man with clear vision in everything he does and a fantastic businessman.

Until recently, Len demonstrated his commitment to Israel and to Israeli society mainly in philanthropy and in very limited business activities. Since mid-2012 under his leadership as the chairman of the access group, he has invested more than a 2.5 billion Shekels to purchase a 100% of Clal industries. One of Israel's most prominent and active industrial groups. Clal owns and leads companies such as Nesher, Hadera Paper, Golf, Clal Bio-Tech, Beit Shemesh engine, Jordan Valley and just this week we announced our renewed commitment to the Israeli high tech industry with new investments in this field. In addition, Clal owns major stakes in companies such as Ta'avura, Yafora, Israel Shipyards, Med-one and others.

We have the privilege and are responsible for around 15,000 Israeli households, not to mention sub-contractors, service providers, advisors and many others. Few of the top CEOs of Clal industries are here with me today. Yohanan Locker, Ruben Krupick and Daniel Shen'ar. Len's investments in Israel are very good news to the Israeli economy, especially at this time, but Len's not only a businessman. His philanthropy around the world is conducted by the Blavatnik family foundation. The foundation is a major sponsor in establishments such as Harvard, MIT in the US and in the UK the University of Oxford, million pounds to the Blavatnik school of Government. It was one of

the biggest donations ever given to Oxford University in its 900 years of existence.

By the way, 90% of English prime ministers in the last 100 years, graduated from this school. Len is a long-time friend of the Tel Aviv University and in a speech given here, last year he said and I quote :" Tel Aviv University has a distinguished tradition of excellence and achievements and I am delighted to help and support the next generation of scientific researchers and innovators in Israel." Len is extremely happy that his gift will be designated among others to a computer science research fund to this cyber research center under Professor Ben Israel and to the medical field, the center for drug discovery. In his words, "this initiative will help support the next generation of scientific researchers and innovators in Israel". In addition, a faculty recruitment discretionary fund will allow Tel Aviv University to make competitive offers to talented researches and bring them back home.

Last but not least, as one cannot leave without art, the donation will create a student film production fund, an industry which is very close to Len's heart. By the way, one of the companies he controls is Warner Music. The fund will provide awards and enable undergraduates and graduate students to transform their ideas from the storyboard to the cinematic work. Let me tell you, and as professor Klafter said, I am not objective about this, I graduated just a few a hundred meters from here and I was a teacher for several years, my wife graduated her and was a teacher also here. And my daughter graduated here, but I think it's safe to say, in Len's view, Tel Aviv University is on the right track to stand side by side with academic institutions such as Harvard, MIT and Oxford. Len as a businessman believes that this donation will turn to be money well invested.

DR. EVIATAR MATANIA, THE HEAD OF THE NATIONAL CYBER BUREAU

I am standing here today three years after the government of Israel decided to establish the national cyber bureau to lead Israel in its journey into the cyber era, and from a comprehensive national point of view to focus on creating a national defense strategy, on developing balance changing technologies and on building an echo system which will position Israel as a leading cyber power.

The bureau was established on 1 January 2012 with one man, myself. We have grown since to more than 30 people. During this challenging period, we have been working with our numerous partners in government on 45 cyber foundations: industry, academia, human capital, international partnerships and many more. Today, I would like to focus on two main efforts in our defensive strategy which are relevant to our work today and the near future. The first effort deals with how we approach operational readiness to cyber threats. At its core, this approach distinguishes between attacks and attackers, businesses and civilians may be curious to know who is attacking them, but their primary concern is countering the attacks themselves through prevention, mitigation, containment and recovery; these are the areas where the attacked parties need and expect our help. At the same time, the defense community is interested in the attackers: identification, exposure, good intelligence, retaliation and so forth. That distinction is of a practical importance given the variety of threats, the scale of the threats, and the capabilities of the government. Combining the two points of view, we are gradually building a national cyber defense center which will work closely with the defense stakeholders I mentioned.

Our national strategy will be the cornerstone of this center, entrusted with much more than the traditional capacity of such centres. First, as a one stop shop, it will serve all the civilian sectors in Israel: citizens, S&B, big enterprises and government agencies. Second, it will promote information sharing on attacks based upon standards of privacy and secrecy. Third, it will guard information through early warning system. It will promote intimate cooperation and collaboration with strategic partners in the cyber security industry. Fourth, it will have the best forensic platforms as well as other technologies to identify vulnerabilities and it will work closely with the intelligence community to mutually forward actionable intelligence for tackling attacks. A move of such complexity and consequences takes time. This center will be built throughout the next couple of years, and I'm very proud to announce that we have already launched its pilot during operation "protective shield". The center will be located at Be'er-Sheva, where it will also serve as a hub for new technologies and will nurture partnerships with the cyber industry and the applied research center in Ben Gurion University, to develop knowledge and technologies of mutual interest.

The second effort I would like to address is the building of our defensive technological capacity. Currently the advanced attackers, definitely those who are state sponsored or states themselves, hold the high ground in comparison with the private organizations trying to secure themselves. This reality points to another role of the government, to come up with technological solutions that will bring about a dramatic change in the balance of power. To this end we are making progress in three parallel alignments: first, game changing technologies for the organizational level, especially for critical networks and systems. Second, technologies that offer unique value when applied at a state level, in contrary to the organization level. This includes information sharing platforms, early warning systems and pro-active tools. Last, but not least, is improving the resilience of our national cyber infrastructure. We are working resolutely with our various partners to realize these essential building blocks, which over time will be incorporated into a strategic program that will provide Israel with a robust digital shield.

I consider these efforts to be of the outmost importance and I believe their magnitude will exceed beyond Israel. I would like to convey my personal greetings to Tel Aviv University, and to Professor Ben Israel, Professor Klafter, Mr. Avi Fischer, on the launching of the interdisciplinary cyber research center which will enable a leap forward in Israel's academic research and professional development in this field.

PRIME MINISTER OF ISRAEL, BENJAMIN NETANYAHU

Thanks to the responsibility in which we have led the Israeli economy in recent years, Israel had not deteriorated to where many other western economies have fallen, economies that in the past have been stronger than our own, and we must continue with this responsible policy. The State of Israel needs a responsible budget, a budget that will provide a response to the security threats that are upon us, and that will not deteriorate the Israeli economy. We need money for Iron Domes, we need money in order to deal with ISIS in the east, Hezbollah and Al Qaeda in the north, Hamas and the Islamic Jihad in the south.

The billions we have decided to invest in economy, or more accurately, in security over the recent years, have saved the Israeli economy. The billions we have invested in thousands of Iron Dome interceptors have

allowed the Israeli economy to continue functioning throughout the last campaign, and have prevented investments from being pulled out of Israel. The billions we have invested in the border barrier in the south have completely prevented the infiltration into Israel, as well as the Jihad members from Sinai, which constituted a threat to the economy, the society and the country. I remember being receiving criticism back then, on the Ministry of Finance, saying that our investment in security had been a seemingly excessive expenditure. I don't want to think what would have happened to Israel's economy, to the State of Israel itself, had we not made those investments. Presently, face with new threats that emerge and form in our region, we need to significantly increase the security budget by investing additional billions once more. And this is important – many billions more. I believe we are able to face these challenges, but only by doing so in a responsible manner, without deteriorating Israel into a state of uncontrollable deficit, with an out-of-control international overdraft. Our challenges are many. They also include, first and foremost, the nuclearization of Iran, or its ability to achieve nuclear weapons within a short time period; the terror threats that surround us; as well as another threat – the threat of delegitimization. This threat is nourished, sadly, not only by a worldwide campaign, but also by factors from within Israel. I would like to make it clear that insubordination of any kind is completely reprehensible. And the political use that has been made lately, while sounding false accusations, is wrong. The IDF, for all of its units, is the most moral army in the world. Alongside that, it performs – in the best possible way – the tasks we give it in order to guard the safety of Israel's citizens. I would like to say, in this forum, that from my long acquaintance with unit 8200, I know that the groundless accusations that have been made of late will not hurt the important work that they do for the safety of the State of Israel. And I tell them – from here, continue going forward.

I want to thank Professor Joseph Klafter, the president of Tel Aviv University and I know that you are today opening the Blavatnik interdisciplinary cyber research center, it's a very important one and I think it has implications for the field and for the state of Israel and I congratulate you for doing that. I want to acknowledge my friend and my partner, major general Professor Isaac Ben Israel. I think he was one of the first to alert me, to draw my attention to the developing field of cyber. I acknowledge Dr. Eviatar Matania who is the head of

the national cyber bureau who is doing a very important work here to continue to transform Israel into a global cyber power as well as acknowledging the presence here of retired general Keith Alexander, the former head of NSA, if you don't know what NSA is, it's the American 8200 unit. Bigger. But these are the finest units in the world. They require great minds and great heart too. Secretary Gordon England, the former US deputy secretary of defense, the researchers who are here, members of the cyber industry and defense establishment in Israel and abroad, dear guests. Last month the state of Israel faced the threat of Hamas rockets and tunnels.

Our enemies, in these various terrorist organizations, Hamas, Islamic Jihad, as they fail in their military and the terror campaigns that they launch against us, they continue to try to attack us through other ways, including in the field of cyber-attacks and that is an arena that is changing, both here and elsewhere in an exhilarating and dizzying pace. The attack by our enemies on Israel's civilian, and I stress civilian, internet infra-structure during the recent operations, these attacks were clearly meant to disrupt the daily lives of Israelis, to harm us, but those same attacks failed exactly in the same way as the terror campaign, as the terror attacks, the rockets and the tunnel attacks failed.

There is a world of difference however, in dealing with these attacks and dealing with rockets and tunnels. With rockets and tunnels you know where they originate. You know who the enemy is. But in the cyber domain there are no clear targets and no instantly recognizable enemies. That's often the case. This is a space in which there isn't a "here" and a "there". There isn't the side of Israel and the side of Gaza that the attacks try to cross. In fact, it's a very board domain which is very hard to define, where does your space end and somebody else's space, including the attackers, begin? The attacks, in a sense, always come from within.

We identified those attacks and we stopped them. The fact is that the cyber-attacks did not affect Israel's daily routine or its economy and they certainly did not affect the IDF's efforts. Those facts are derived from the fact we have the finest minds, literally, the finest minds in Israel's security community and our cyber industry, working to give us those defences. There's an iron dome of cyber security that parallels the iron dome against the rockets and this allowed us the

operating space to continue fighting and of course to continue with the daily life of Israel.

A year ago at this conference I described the threat developing in the cyber sphere against Israel and the actions that our enemies, headed by Iran, are taking against us in that field. Now, we witnessed in the recent operation Hamas's efforts against us, we saw that throughout the operation. What I want to make clear is that the party behind the cyber-attacks against Israel is first and foremost Iran. Including in the Hamas attacks. Iran supports all our enemies, Iran is the source of most of the attacks that are launched against Israel. And we are not their only target in the cyber field. Iran and its proxies take advantage of the security and anonymity of cyber space to attack many other countries around the world. Now, we are unrelenting in confronting this threat. We are increasing our efforts to deal with a range of cyber threats out of an understanding of the importance of cyber security to Israel's continued economic growth and its security.

I mentioned both because both are important. We want to protect the security of our country, the security and privacy of our citizens, but at the same time, we also identify a great economic opportunity. We're currently advancing a number of dramatic actions that will transform the cyber field in Israel. This is a work in progress for us and for our allies around the world, for every country. Cyber is moving very rapidly, changing very rapidly and you have to decide with a certain amount of uncertainty how it is that you are going to tackle a field as complex and as ever changing as cyber security.

It is a daunting task. I would find the most difficult part of any change, structural change, in the economy or in education or in any field, in defense and in cyber defense. I find the greatest challenge to be not the organizational challenge, not the forces that often to clash to competing interest and so on. I find the greatest challenge to be the intellectual challenge. The conceptual challenge – what is right? What is the best thing that we should do? Then you start to make all the adjustments for what is possible, what you can pay for, what is politically required, and so on. You make the adjustments, you trim off the edges of the main conception, but the most important thing in any reform is the conception of what is right, what is necessary. And in cyber, this is particularly difficult. For the simple reason that nobody knows. Nobody truly knows.

It's such a moving target, such an expending and ever changing world that you have to make certain assumptions and go with them and probably you'll have to adjust them as you go along. Whatever it is we do, we have to allow for changes as we go along. Especially in this field. So we are going to make some strategic decisions and we are making great investments in the goal of making a quantum leap forward in the governmental and the national response in the cyber sphere.

We are going to combine two important efforts. One, to transform the government into an exemplar for robust cyber defense, in order to protect our digital assets and also to strengthen the trust of millions of our citizens who enjoy government services. And second, we are going to standardize the cyber defense market, in order to ensure that the entire Israeli economy will have professional people and services in the highest level. The attacks that I've just mentioned and many others that I haven't mentioned, provide additional evidence that the cyber sphere is becoming increasingly a battle field.

Israel feels it from several directions. The principal one originates from Iran, but not only from Iran. We are committed to maintaining Israel's position as a global cyber power, and as such, we have to implement a policy which protects cyber space as an open space and as the basis for global growth. I want to ensure that Israel will always know how to use its unique strengths and knowledge, to protect our country and as far as we can to protect the world's commitment to cyber growth. think there is a tremendous responsibility that comes with power, but also a tremendous responsibility to ensure the economic opportunities that afforded by the growth of the internet economy, the internet world, the internet of things, the internet of people. All of that creates tremendous opportunities for growth and that growth, the increase of productivity for billions of people, instant communications and transfer of funds, the movement of ideas, the movement of capital, the movement of initiative, of enterprise. All of that is under risk by cyber attackers who have the capacity to inflict increasing damage and the attacker always has the advantage as you well know. So we have to work at the same time as we integrate into this modern world as we provide entrepreneurs for this modern world. We have to work at providing security with this great change. I believe that this is a tremendous engine of economic growth.

I don't think there's a person on earth who's not going to need cyber security. I don't think there's a nation on earth that is not going to need cyber security. Some of them violate security, left and right. But every, every country and every citizen of this planet will need cyber security and this will be the century where cyber security will either be achieved or we will lose the tremendous opportunities that face humanity. I think long before the term cyber became known and common placed, Israeli companies developed the first cyber technology, the first firewall, several of the first antivirus technologies.

All these were developed here. And over the past several years, we've seen an explosion of start-up companies that are breaking new ground and dealing with a range of threats using innovative technologies and defense solutions. Over the last nine months alone, 20 Israeli start-up companies have raised more than 170 million dollars. The investors aren't doing this for charity. They know why they're here and I think you know why you're here and we welcome you in that spirit. Because we think that there are tremendous opportunities for real needs for the civilized countries, real needs for their citizens and real economic opportunities that come out of these needs.

People's dependence on cyber keeps increasing and so is the necessity to offer cyber defense. I don't think it's an exaggeration to say that cyber defense solutions will serve as the essential basis for human development and economic growth in this century. I think it's happening before our eyes and everything that you see, these curves that seem to reach into the stratosphere, they're going to continue. They're not going to stop, providing we solve this problem, or at least, control this problem or mitigate it. And in light of these developments, three years ago we determined this area to be a top priority in our nation's future and we're building an Israeli cyber environment with an eye to the long term. Israeli R&D will continue to be at the forefront for many years to come, thanks to the strategic investment in the industry by the government and the private sector, both in human resources and in academia and this event. I think it demonstrates the importance of working together because when you're dealing with cyber you have to deal with the private sector, with academia and with the government. We can fashion this growth by a unique system that integrates the three in a very, very determined and purpose full way.

The research center which is being launched here today is a joint initiative of the national cyber bureau and Tel Aviv University under the leadership of Professor Isaac Ben Israel, and with an investment of tens of millions of Shekels, I think it embodies the understanding of the unique interdisciplinary nature of the cyber field and the significance of the connection between people and computers, between this software, that hardware, it has to keep evolving and changing. We also have a national project, the establishment of the national cyber campus. Now, here is a bit of a copyrighting which is brilliant, it is called 'cyber's park'. It's a cyber-park, it is called 'cyber's park' and it's situated in Be'er-Sheva, we're moving our NSA right into that campus.

So we have academia, government, security and private investors all within a range of 200 meters one from each other, just in the same place. There is still value, even in the cyber world, for people to actually be able to meet one another and exchange ideas face to face, that is still important. And that is, I think, fast becoming the hub of global innovation, Be'er-Sheva will become a very important cyber city in the years to come. We are now establishing a center for applied cyber research at Ben Gurion University in Be'er-Sheva and we're working to establish the national cyber event readiness centre which will become a magnet on campus and it will have its own reverberations into the economic enterprises that are attached to it.

In order to strengthen the industry, just a few weeks ago, the government decided to adopt a resolution regarding special tax benefits for companies that would establish cyber activities in the framework of cyber's park. I think there are other benefits, but I want you to have all the benefits because one of the things we want to see is your partnership. We know that it's virtually impossible to prevent to create delineation of space where our common enemies are operating from and our own space. But at the same time there's every reason to incorporate our partnerships in that same spirit. If the cyber space units all of us, then let's unite to protect the cyber space. And that is why I'm so proud to be here and that is why I welcome you to Israel. I hope you look around, see if what I'm saying makes sense and if it is, invest in Israeli cyber.

THE 5TH ANNUAL INTERNATIONAL CYBERSECURITY CONFERENCE – 2015

23.6.15

OPENING SESSION

PROF. JOSEPH KLAFTER, PRESIDENT OF TEL AVIV UNIVERSITY

The fifth international cyber security conference also marks the one-year anniversary of the ICRC at Tel Aviv University. I would like to take this opportunity and thank the benefactor of the center, Tel Aviv University honorary degree, honorary Doctor Len Blavatnik for his generosity, and thank the Israel National Cyber Bureau for their support and cooperation. This combination by the way of philanthropy and national support is optimal and essential for advancing any research. Research statistics have shown Israel to be a "cyber superpower", accounting for about 10% of global sales in the field. The Israeli academia is at the center of the academic entrepreneurial arena, in which there is rapidly growing Israeli presence, and in particular Tel Aviv University. In any given time we have over 100 cyber researchers and business practitioners working together, leveraging the unique advantages of Tel Aviv University that brings together all the know-how on campus related to security, cyber security, and related topics. These advantages

include a proven track record of innovation entrepreneurship; a wide interdisciplinary scope, which is essentially here for the cyber area; deep-rooted connections with high-tech industry and defense agencies; an extensive national and international network of research partners and partner organizations – some of them are here today; and one more factor which is very hard to quantify – the campus culture of imaginative boldness, of the willingness to not only think out of the box, but to actually throw the box away. This rich and varied conference program highlights these interdisciplinary collaborative and creative strengths, and I would like to thank the organizer and sponsors for really bringing together all these experts from all over the world, and have a high quality global event with previously well-established reputation, trying to bring cyber solutions that will benefit all of us.

DANIEL B. SHAPIRO, AMBASSADOR OF USA IN ISRAEL

I consider it a real honor to have a chance to speak before such an impressive group of experts and policy makers in the field of cyber security. Many of you in this room are directly responsible for or have contributed to in many ways the impressive growth of Israel's cyber industry and its associated technologies. This conference is an opportunity to draw attention to the great progress that has been made in the United States and Israel's bilateral relationship on cyber issues over these past five years. During this period great attention has been focused on cyber issues worldwide, by governments, the private sector, civil society, and the media. Certainly, in both the United States and Israel, our respective governments have created new mechanisms, policies and agencies to better manage our engagement on cyber issues and responses to cyber threats. The United States and Israel are natural partners in working together on cyber issues due to our shared values, and our open and democratic societies, as well as the extraordinary talent and innovation of our technical communities.

Today I want to draw attention to a number of ways in which we cooperate in the cyber and internet field. First, we exchange information on how to best strengthen both nations' national security, and protect ourselves from cyber threats. Second, both countries are promoting investment in cyber and the protection of our digital infrastructure, to create an enabling environment for further growth of the information

technology industry. Finally, we look to partner with Israel to ensure freedom of expression on the internet.

Concerning security, US-Israel cooperation on cyber issues, like our robust partnership in so many other areas, is critical to ensuring the national security of both our countries. Both the United States and Israel are among the world's top targets of cyber attacks, which emanates from foreign governments, terrorist groups, and criminal organizations. Not just our governments are targeted, but also our private sector firms. To respond to these threats there is a rich and mutually beneficial dialog between our government experts, which facilitates the sharing of information on cyber threats. Working together to build and implement the policies, mechanisms and tools necessary to protect our cyber infrastructure is essential to defend ourselves against those who would seek to threaten and injure us.

Many US leaders in cyber policy, such as the department of homeland security, are in regular contact with their Israeli counterparts. Both sides enjoy an ongoing and ever deepening dialog, and information exchange on the dynamic and rapidly evolving cyber issues. Both governments have also taken steps to organize themselves in order to respond to cyber challenges and opportunities. For instance, the 2009 establishment of the US cyber command by the department of defense was a clear acknowledgment of the need to centralize cyber space operations, integrate cyber expertise, and synchronize networks. As such, I take note of the recent announcement made by the IDF to establish a cyber corp. I am very confident that the creation of IDF's cyber corp will allow for even more opportunities for bilateral cooperation between our military cyber experts.

My government has recently taken some additional steps to protect US security, and punish cyber perpetrators. In April, President Obama signed an executive order directing the treasure department to impose sanctions on individuals or entities that engage in significant malicious cyber enabled activities that pose a threat to the national security of the United States. And in response to the recent breach of information at the office of personal management, which has exposed the data of millions of current and former federal employees, the white house stated last week that imposing such sanctions on those found to be responsible is absolutely on the table. It is incidents such as these that propel the United States to work with our partners to strengthen

the capacity of governments to ensure their cyber security. We are working to help partner countries develop national strategies and policies, incident response mechanisms, and other measures to ensure they can defend their networks. We also work with other countries to help us combat cyber crime. An important basis for facilitating international cooperation in this field is the Budapest Convention on cyber crime, which seeks to harmonize national laws, improve investigative techniques, and increase cooperation among nations. My government looks forward to Israel's ratification of the Budapest Convention in the near future.

Lastly, I wish to stress that partnership on cyber issues does not only keep our countries safer, but also drives our economies to job creation, innovation and protection of this critical infrastructure that helps businesses work together. And so, I want to applaud and express my deep appreciation for all of you here today that are involved in expending the robust and active private sectors commercial interactions between our two countries. It is clear that the cyber security sector offers enormous economic opportunities. The cyber center in Be'er Sheva is one of the world's most important high tech centers for cyber security, with collocation of cyber experts in the academia, the private sector and the military, with a strong support of the municipality. In January, the Brandeis University International Business School published its research, ranking Be'er Sheva as the first out of seven global cities forecast to emerge as an important high tech center of the future. I would predict that in five to ten years, and maybe even less, the entire world will think of Be'er Sheva as a global leader in the cyber industry. So much so, that many leading firms, including American companies, may soon discover that they cannot afford not to have a presence in Be'er Sheva. Just think of that.

There are hundreds of successful Israeli startups and cyber security firms making major exits in recent years. One of them, CyActive, is the first startup to make an exit from the CyberSpark in Be'er Sheva. Last year Israeli exports of cyber related products and services reached $6B, second only to the United States. Confident investors have poured more than $500M into Israeli cyber security startups in the past few years. Israel is a true global cyber incubator, and both our countries stand to benefit enormously from the rapid growth in this field.

Businesses thrive when they can work together over an open and secure internet. This is one of the central pillars of our international strategy for cyber space, and one for which we continue to seek partners to ensure that the internet is a stable, multistage holder environment, in which all users have a sit at the table, not just a place where the governments set the rules. Think, for example, what would happen if every country imposed data localization requirements, causing information to halt and undergo inspection whenever it reached a national border. Imagine the negative consequences for commerce under the free flow of information, which would complicate a task as simple as searching online for the answer to a trivia question. The delays would create huge obstacles to multinational businesses, at a time when speed is of the essence and cross border enterprises are major engines of growth. That is not a formula for progress, and it is a way to stop progress in its tracks.

I expect the United States and Israel to continue to work as partners and leaders, to protect the internet as an open, secure, and reliable tool that supports global economic prosperity. Yet, viewing the internet and cyber space as tools for economic growth is not all we strive for. A vital part of our cyber policy is protecting internet freedom. We want the internet to be an open global space for freedom of expression, even as we continue to promote human rights worldwide, and actively oppose those wishing to deny them. Threats to online freedom continue to grow. Nearly half of the two billion internet users around the world live in countries that impose restrictions on content. Our goal is to ensure that everyone, the world over, has access to the internet as an open platform in which they innovate, learn and exchange ideas freely. The benefits of network technology, our ability to work across the internet, should not be reserved to a privileged few nations, or a privileged few within them.

We must pursue a cyber space that is open to innovation, interoperable worldwide, secure enough to earn people's trust, and reliable enough to support their work. We must also pursue policies that seek to ensure the security of our governments, firms, and citizens. And as I have said, Israel is a natural partner for all of these goals. Thirty years ago, few understood that something called the internet would lead to a revolution, and how we work and live it. In that short time, millions now owe their livelihood to the world of cyber space. We

look forward to working with Israel to move towards a future of an open and secure internet, and a future in which the internet protects the security and privacy of those individuals and entities who use it. The United States and Israel continuing to cooperate on these issues makes immanent sense for our national security, for our economic prosperity, and for our shared commitment to protect the freedom of expression of people across the planet.

MAJOR GEN. (RET.) PROF. ISAAC BEN ISRAEL, HEAD OF THE BLAVATNIK INTERDISCIPLINARY CYBER RESEARCH CENTER AND HEAD OF YUVAL NE'EMAN WORKSHOP FOR SCIENCE, TECHNOLOGY AND SECURITY, TEL AVIV UNIVERSITY

This is the fifth international cyber conference that we are conducting here, in Tel Aviv University. Unlike the previous four conferences, that have been organized by Tel Aviv University and Yuval Ne'eman Workshop for Science Technology and Security, this conference is organized by the ICRC, the setup of it, incidentally, was announced last year, at the fourth international conference that we had here. This center is a result of an evolution of the cyber security concept, that has been happening here in Israel in the last 20 years. This is one step in the evolution, and when we realized that in order to have a real living ecosystem that will react automatically, in a way, to changes of various sorts, we understood that we should take care of all the elements. One such element is university centers of excellence in cyber research, the first of which was set up by the INCB, the Israeli National Cyber Bureau and Tel Aviv University right here, in Tel Aviv University, the second one in Be'er Sheva, and there are more to come. We have five research universities, and I guess that at the end of the day most of them will have centers like this as well.

Looking back, at the beginning cyber was something done by intelligence services, because computers were the main tool for storing information, and therefore the first stage of the evolution was what we called then "information security". Then we realized that information security is not enough, because computers do not only store information, they control other systems in our life, and someone can use the same technique to hack into those computer chips which control different systems in our life, such as power production, and therefore information security is not enough. We went into the second stage, which is cyber security, and

even this is not enough. In the last few years we realized that people talk about the internet of things – home devices that communicate with other home devices through computers with man being kept nearly completely out of the loop, smart cities, Smart Nations, smart cars, etc., and all these wonderful visions will never work unless you can have a certain level of security. Because you cannot really let the bad guys – and there will always be bad guys – use or abuse this new technology in order to shut off electricity, for example.

DR. EVIATAR MATANIA, HEAD OF THE ISRAELI NATIONAL CYBER BUREAU (INCB), PRIME MINISTER'S OFFICE, ISRAEL

In my term at the INCB, there were three major goals we tried to achieve. The first is building the capacity of Israel in the cyber domain, the ecosystem of universities, industry, and human capital in Israel, in order to become one of the powers in the world in cyber security. All of it was based on what we already had, because the Israeli cyber security industry started more than 20 years ago, with companies like Check Point, alongside the capabilities of universities in areas related to cyber security, as well as our human capital in the area of cyber security. We thought that this ecosystem should be maintained, strengthened, and we in the government have to do a lot in order to take it forward and build the Israeli capacity not just to be one of the powers in the world, but also to remain so in the future. We have also begun to establish five research centers – Tel Aviv University and Ben Gurion University research centers, Bar Ilan University and Hebrew University cyber research centers, as well as the Technion research center, which is currently being established.

We also collaborate with the industry, the Chief Scientist and Ministry of Economy, and other colleagues in the government, in order to try and bring more global companies to open their research centers in Israel, to encourage our local startups in the cyber security industry, and help them in their export efforts and all other things which are needed. We have also devised a strategic plan for enlarging our human capital and making it more qualitative.

Our second goal was to develop the Israeli comprehensive national cyber security strategy, the last step of which – asking for support

– ended recently, on February 15th, as the government adopted two resolutions regarding our strategy for the next decade.

The third goal was to succeed in parley of our activities and establish the bureau. It started as a single man in the bureau in January 1st, 2012, and establishing a new and excellent organization in the government was quite difficult.

In the near future, I think our major challenge would be to establish the new Cyber Security authority in Israel, which will be the one and only organization responsible for Israel's cyber defense from cover to cover. We are currently in the first step of this process, but I see it as our main challenge for the coming three years. It is a real challenge, to establish such an organization that will work closely with the civilian market, as well as with the intelligence community, to bring to this organization hundreds of excellent people, and to establish all its methods and strategies.

The second challenge for the future is related to the governmental resolution regarding how to build the market resilience, through working with the current regulators who lead the government, to become a leader in the resilience, as well as take other steps and actions. This we will do in parallel to fulfilling the two governmental resolutions from February 15th, and working according to them.

Yet another important challenge is the international arena. Although we have very good relations and collaborations with several countries around the world, and we are present in several forums relating to cyber security, I think that looking to the future, it is a great mission to position Israel far ahead in the international arena, working much closer with our allies, being more present in these forums, as well as to influence the way the world is going to be built, with its norms, legal issues, and other collaborations in this field. This is yet another major task that I see for the future, and this will take much longer than three years.

I think that the five research centers – and in particular the one in Tel Aviv University, which is an interdisciplinary center – are of great importance to the Israeli cyber security ecosystem. Building these centers was one of the first steps in the process of gaining power in the field of cyber security, in order to become leaders – something that cannot be reached without a strong academic leadership. I think

that the universities should work very closely with the government and industry in order to help them in creating new solutions and technologies that will enable us to better defend ourselves. Secondly, I expect these research centers to also provide us with new thinking directions. I expect the universities to bring knowledge, new breakthrough technologies that will help in balancing the currently unbalanced equation between attackers and defenders in this field, as well as to develop the human capital in this country. I think that they have a major role in these fields, and leading universities also enable us to be a leading country in this field.

As head of the National Cyber Bureau, I see the Israeli cyber security industry as very important to both our national cyber security strategies and the ability to defend Israel, but also for our economy. In cyber security there is a very interesting synergy between our security needs and economical ones. The industry is the one bridging this gap, and we have many new startups and innovative ideas that are currently growing up. I think many good things are happening in this regard at present, but looking to the future, I expect the Israeli industry to succeed not only in producing new startups daily, but also in producing grown up companies, and integrate cyber security technologies and products to services, and to be more present in the world than we are at present. If we succeed in doing that, I believe the future of the industry and the Israeli capacity will be in the right place. With integration services entering into new fields, the SCADA systems, we have everything – we have the startups we have grown up, companies, SCADA solutions. We have many other good things as well, but looking to the future I think that integration and services, as well as our ability to have many more grown up companies, new products and solutions in new areas, are the key to a well developing industry.

By establishing the Cyber Bureau, the government did not mean to replace all the current ministries and agencies working with the market, with the industry and with universities. We see ourselves as those responsible to gather all these ministries and agencies and to point them, as well as ourselves, to the right directions. Viewing cyber as one of the major issues of Israel for the coming decades is a key story in its economy and national security. We currently work very closely with the Ministries of Education, Economy, Science, Technology and Treasury, as well as others, in order to produce this ecosystem.

In my opinion, the role of the government is to enable the market, to support the market, and to help everyone who wants to be there to really succeed in building new industry. For example, the CyberSpark in Be'er Sheva is something based on the industry, on the cyber research center of the Ben Gurion University, but we also have a role in it. First we are going to place the national CERT there in the beginning of next year. I see the role of the government as an enabler – we do the legislation, we will bring what we can bring, we encourage others to do. And I would say that we want to work with the industry, not to replace the free market and the industry or universities, but to be there when needed. This is the way I see it, and this is what we are trying to do, along with all the other ministries, agencies, and the government as a whole, in order to encourage this.

PRIME MINISTER BENJAMIN NETANYAHU

The whole point of cyber is that you have got to question, challenge all the time. This a rapidly evolving discipline, or lack of discipline. It is the fastest going, fastest changing domain in the international economy and security in our world, the greatest force of change and growth is the internet-driven economy with all its derivatives. It is changing by the hour, and we have to be constantly ahead of the curve. I have set a goal, a few years ago, to ensure that Israel is one of the leaders of cyber security. My job as Prime Minister is to make sure that it stays that way. In our time, each year more data is accumulated and created than in the world's entire history. We are in the throes of a great change, moving from atoms to bits, from place to space, and it requires that we be at the edge of innovation all the time.

The cyber needs and the cyber market are not a low-growth market where you can establish a position of dominance, as we have, and rest on your laurels. This is the classic super-high growth market, in which you have to constantly innovate to maintain your position. We have done that now, we are among the top three, but we have to make sure to be there ten, twenty, fifty years from now, because it is not going away. Therefore, we have established two major arms to deal with this. Two government resolutions that we passed a few weeks ago. The first is to create the national cyber security authority in order to build market resilience and define how we approach the question of defense. The second is the decision to create the IDF cyber forces,

and we are eager to build capacities that endure and develop in order to have the cutting edge needs that we require for national defense.

The most difficult decision about cyber is where to draw the fence – around a company? Around an air base, or a power plant? And the answer is yes and no. Yes, because you need it in every one of these installations, facilities or services, and no, because it is not enough. But how far do you go? Where do you draw the fence? And if somebody punctures that fence, what do you do about it? Who do you tell? How do you prepare in advance? Who do you share this information with? What do you do about it? These are exceedingly complex questions, and there are no obvious answers. And so, in the face of this uncertainty, you can basically do two things. You can do nothing, and say "it is too complicated, I don't know what the solution is, it is fast evolving", or you can say "We will organize ourselves by making decisions and moving forward".

We have a saying in the military, "we organize ourselves in movement". This means that you move, you decide where you are going and you get the forces and vehicles moving alongside as you decide which direction to take. We have decided on these two directions, I think these are monumental decisions. We may be ahead of most countries, or all of them, but we are still moving. And we can see the change that is developing once we have decided what we are doing. We learn as we go along. We can share some of what we are doing with governments, with companies, with entrepreneurs, which is important. And Israel is a unique place, because it has a relatively large number of people who excel in this area, and because of our unique culture, that challenges assumptions. This is something that is deep in the DNA of our people. The father of our nation, Abraham, challenged god, that is as big a challenge as you can have. And we have that embedded in our culture throughout, and it is very much something that we see in the development of businesses. Another advantage we have is perpetual investment in this field, and our task is to take this investment and make it not only into a vehicle for national defense, but also a into vehicle for business.

You have government investment of military and security intelligence, an academia that produces and spawns business startups, and that is exactly what we decided to do in Be'er Sheva. We decided to take our NSA and other associated units, put them in Be'er Sheva, right

next to the university, to have our national cyber headquarters, Ben Gurion University, and a cyber park which is rapidly expanding with some of the world's leading firms. This is a prescription of getting the forces that can build the future in one small place, where that culture can grow and thrive.

In addition, we encourage our young people who come out of the military to enter this field, and we will be giving tax breaks, in a few months, to companies that go to Be'er Sheva, in order to further enhance this ongoing investment, because every year we put our brightest men and women through our military and security system, and encourage them to become entrepreneurs. And so Israeli startups have been bought at the rate of about a billion dollars in the last 18 months, we have had hundreds of millions of dollars of investment, in the last year alone, in Israeli startups, and more is coming.

Our job is to make sure that this perpetual motion machine continues to move in a rapid pace, we are committed to it, in everything that we do. We view this as the future – a major thrust of our economic effort, growth engine for the next 50 years. There is a tremendous growth, many people invest in Israel, and this is where the future is built because of this particular culture.

Culture is very difficult to replicate. It is not clear how you repeat something like this, but this has happened here, and we are going to invest a lot in making sure that we have an abundant supply of young people, kids who study math at the highest level. We have special programs for cyber education, both in our schools and in the military, and we are absolutely committed to this domain, because we want to make sure that we are dominant. I said that it is not going to go away, because the problem of protecting the internet-driven products and services is so vast, so challenging, that it is just going to get more and more complicated.

We have hackers and non-governmental organizations that attack us, but the greatest threat comes from governments; and governments who want to protect the privacy of their citizens, their bank accounts, their infrastructures, their economies, have to work as far as they can together, to cooperate against this new threat. Specifically, Iran has been launching attacks against us, against Saudi Arabia, against the United States, against many others. And we are determined to protect

ourselves from these attacks and others, and the way we do it is this combination of government, military, academia, and business. We think this is a potent opportunity. We are moving ahead and we are committed to stay ahead, and I think each of you can have your own opportunity here. I think Israel is exciting, it is open for your business, and I am glad that you are here in the fifth international cyber conference. The numbers, the investments and the opportunities grow each year, and if you are not in Israel, you should be, and if you are, do more.

01

FIRST SESSION: THE SECRET OF CYBER SUCCESS

BRIG. GEN. (RES.) NADAV ZAFRIR, FORMER HEAD 8200, CEO AND CO-FOUNDER, TEAM8

I would like to talk to you about perspectives, motivations, and the people behind cyber security, and I want to do it by talking about three things. The first thing that I want to talk about is the people who are the attackers, and how such attackers have transformed in today's world. The second thing I want to talk to you about is the leaders, or the leadership of today's organizations, and how the leadership must evolve. The third thing is probably the most important one, and that is the talents, the people behind cyber security, who actually do the work.

I would like to start by showing you a boardroom. These may seem to you like executives strategizing next year's work plan in a typical boardroom, but there can be a parallel boardroom located somewhere else, around the world, and in this boardroom there are attackers that act like executives, business people, who are doing exactly the same thing, strategizing, because if you look at today's advanced attackers, they have changed tremendously. If in the past they used to be opportunistic, they are now proactive, and if they used to be tactical, these days they are quite strategic, and if the center of what they did was technology, what they do now is more business-oriented. In fact, take a look at the attackers' ROI, which is something they consider before choosing their next attack vector. They think about their potential reward, about the likelihood of success of their operations, about the

anticipated necessary effort in what they are going to be doing, and then they choose their next attack vector. At the end of the day, it all goes back to ROI.

Now I wish to talk to you about one of the most aggressive cyber breaches or business disruptions, the Sony breach. Let's try to think about the attackers' ROI for the Sony breach. What were they after? If they were trying to make sure that nobody sees the movie that was leaked, the attackers' ROI in this case is probably not so good, because in fact more people saw the movie then there would have if there hadn't been a breach. But what if they were going for something more subtle – what if they were warning the Sonys of the world that they must think twice before they do something that reflects negatively on the attackers' government? Then, perhaps from the attackers' perspective, the ROI here is not so bad.

The question that I want to ask you is: if prior to this attack, Sony executives might have been aware of the attackers' perspective and would think about their ROI, could they have taken a different defense strategy before, during, and after the attack? Moreover, I want to go beyond Sony, to other industries, because in every industry you must think of the attackers' ROI and your reverse ROI in order to understand how to protect yourselves. When it comes to financial services, for example, what if a Sony-like attack would hit a financial service, a big bank, whose main business of such services is trust? Would a bank that has been hit by a Sony-like attack be able to rise from the ashes like Sony did? And what if the attack was on the transportation vector, or on an airline? Could they rise from the ashes?

The message that I want to convey is that the cyber security experts in organizations – the CISOs, as they have come to be known – cannot alone, without the leadership of the organization, understand what the perspective of the attacker might be and what the crown jewels of their organization are. And so, the message is that leadership has to take charge. But I would like to talk about the illiteracy gap, which is very imminent in today's cyber security ecosystem. The business leaders of organizations know a lot about the business, HR, finance, etc. They also know the risks that comes with HR, finance, sales, legal, etc. But they know very little, or not enough, about cyber security. On the other hand, the CISOs are security experts who know everything that they have to know, hopefully, about cyber security, but don't know enough

about the business side of their organization. And this ecosystem is not the environment that will allow the necessary dialog in order to build a reasonable, business-driven cyber strategy or posture. We must close the illiteracy gap by shrinking it, teaching the business leaders the basics and importance of cyber security, and teaching the cyber experts a little more about their organization.

My third point is that organization leaders need to take charge, since at the end of the day everything goes back to the people and what they know. If you shrink the illiteracy gap you can get to what I call the symmetry of knowledge – if the attacker thinks about the reward, you must think about the impact. If the attacker thinks about probability of success, you must think about your crown jewels, and if he chooses his attack vector, you must choose your business-driven cyber strategy or posture. This will allow you to create a reasonable cyber strategy for your organization, which is symmetrical, against what is the non-symmetry of today's cyber security posture, of many of the organizations that we see.

The next thing you have to do is go back to the people, and try to close the scarcity of cyber talent. We all deal with it, and any cyber expert will tell that the biggest challenge in cyber security today is the scarcity of your cyber talent. The current cyber security demand is far from being met, and in the US alone, 300,000 cyber security positions have remained vacant in 2014. This is probably the first thing to take care of to get a reasonable cyber posture in your organization. Nobody really knows how to take care of this problem, but from experience, don't go looking for something that doesn't exist, but think differently, and create your own. If you demand your applicants to have ten years of experience in cyber security, not many candidates would apply for the position, because today's cyber security issues did not exist ten years ago. You have to cast a wider net, and consider transferable skills within your organization and job training in order to create your own cyber experts.

Our unique situation here in Israel allows us to cast a very wide net to very young people, and train them very quickly through the military. I am not saying that this will work for other nations, but you have to find a way to do it.

To sum it up: the attackers have transformed over the years, and currently think about ROI; we must shrink the crossed illiteracy cap between leadership that must understand cyber, and cyber people that must understand business; we have to mitigate the scarcity of top talent, and that is probably the biggest challenge of them all. When it comes to cyber security, we are not on the right course, and we really have to change our course if we want to do it. The rest is up to you.

MR. DEAN BRENNER, SENIOR VICE PRESIDENT, GOVERNMENT AFFAIRS, QUALCOMM

Qualcomm has been in Israel since the early 1990s. We have over 600 employees and we do major innovation in the wireless industry. I can tell you that if you have a cellphone in your pocket, and if that cellphone has 3G or 4G in it, you have a chip inside your phone that has been designed by Qualcomm.

Qualcomm is the world's largest manufacturer of chips for cellphones, and the world's largest inventor of mobile technology, a good portion of which was invented by our colleagues in Qualcomm Israel. Last year, in fiscal 2014, Qualcomm sold 861 million chips for mobile phones, and in fact about 1,500 phones models with the Qualcomm chips were launched over the course of the year, which means that two or three phone models come out every single day with Qualcomm chips inside. Having said that, we are in an ultra-competitive industry, and there is an absolute race to invent new wireless technology embedded into cellphones and other wireless devices and tablets. For these reasons, Qualcomm employees work with a tremendous sense of urgency. One of the core values at Qualcomm is partnering. A major part of Qualcomm's vision is to have humility and know that no single company or part of the private industry has the answer to cyber threats, and we believe that it is impossible to talk about cyber security without talking about cellular technology and cellphones.

At Qualcomm, every employee is familiar with the phrase "The thousand x challenge". This means that globally, every year, mobile data usage is doubling. If this happens for the next ten years, it produces a thousand times increase in wireless usage. Thus, we need to prepare for these contingencies by asking ourselves how we are going to have wireless networks that can deal with a thousand times increase in wireless usage

throughout the next decade. We are going to have wireless devices that can communicate in this scenario. The "thousand x challenge" produces an enormous security challenge. With much of the traffic and the data being mobile, the question that we ask ourselves at Qualcomm is how we are going to secure all of this.

Next, I will discuss Qualcomm's point of view and the execution plan for this vision. The main objective is that in order to develop solutions that are secure, they first must be end to end, they must include the edge of the internet that is in everyone's pocket, and lastly, they must include both hardware and software. Since Qualcomm designs the chip, we are very committed to having hardware and software solutions. We believe that software-only solutions will always be more vulnerable to hacking than a solution that is more deeply tied into the hardware. This has to be done by a wireless ecosystem, and the majority of the solution will begin in the chip.

The first layer of Qualcomm's cyber vision is the authentication. We believe that authentication cannot be just passwords. A system of passwords-based authentication is simply an invitation to hacking, and thus is insufficient. The idea is that for authentication to be seamless, it needs to stay on the device. Qualcomm believes in ultrasonic authentication, where there is no need for the user to memorize the password. Authentication must be continuous, in such a way that the user's device is constantly aware that it is the real user who is using the device.

The second layer of Qualcomm's cyber vision is preemptive protection. The best mechanism to fight threats is through the cognitive technology that Qualcomm has developed with its partners. Preemptive protection centers on the idea that a cellphone can actually learn who its user is. For example, a user is a frequent user of currency converting applications on their mobile device, and doesn't require accessing their contacts through this currency converting application. If the cellphone learns this behavior, it will be able to recognize that a user trying to access the contacts through the app may, in fact, not be "its" user. Qualcomm believes that using the knowledge that the phone holds, and the knowledge that it gains, may hold a promising potential to enhance cyber security.

The third layer of Qualcomm's vision for cyber enhancement is the concept of data protection – having as much of the security protection as possible on the device itself, not in the Cloud. Obviously, Cloud-based solutions will be playing an important role in this concept. However, our concept of data protection implies that maintaining as much of the information protected on the device itself, rather than in the Cloud system, is a strong deterrent to hacking. From the point of view of hackers, they would rather hack into a database in a cloud and gain access to information about 25 million people, than into 25 million individual cellphones. However, devising this concept of data protection cannot be done alone by Qualcomm, or by the wireless industry, and a strong collaboration is required between the industry, government, and academia. It is critical to think about the interaction between the government and the private sector in three different categories.

The first category is regulation. Through command and control, the government is able to tell a particular segment in the industry that they cannot behave in a certain way, and must behave in another. This is the most heavy handed way to deal with security, and as the threats change, regulations should not remain fixed but change accordingly, thus it is imperative to remain ongoing and continuous collaboration between the government and the industry.

The second category is mitigation. The wireless industry and the government deal with threats every single day, which is why it is critical to have good information sharing between the government and the private sector. Examples for such collaborations between the industry and government on cyber related issues is the collaboration between the Federal Communications Commission, and its technical advisory committee called the Tech, and the FCC, in cooperation with Qualcomm and other companies, in developing solutions for mobile device theft; or the FIDO Alliance – a tremendous alliance of different private sector organizations, two members of which are the US and UK governments.

At Qualcomm, we are very committed to doing our part within the complex wireless ecosystem, which requires close collaboration with partners at every level, ranging from device manufactures, OSs, and other software vendors. It requires an endless array of technologies and almost an endless array of different kind of devices, phones, tablets, sensors, smart refrigerators, smart cars, medical devices, and more.

Each one of those requires very robust security solutions that have to be both end to end, they have to be hardware based, and they have to involve close collaborations between government and industry.

MR. AMNON BAR LEV, PRESIDENT, CHECK POINT

I would like to begin by introducing a real-life scenario. The Chief Financial Officer of a US state agency received a phone call from the bank, asking him to confirm a transaction of $5M. The CFO has never encountered transactions of such amount, and started investigating whether anyone knew anything of it. After Check Point was called by the agency, we found a malware in the CFO's computer that has been recording every key stroke that he was making. After broadening our search, we came across 200 additional computers in the agency that possessed the same malware. Now, this scenario is very real. When thinking about the hacker, though, it is safe to say he was very greedy. Had he decided to put forth a transaction of $10K rather than $5M chances are he would not have been caught, the discovery of the malware would not have been made, and he would have been able to continue working under the radar.

What I am going to focus on here is the technology. What is interesting about technology is that what we usually do is to try to block what is happening to us. It is a reactionary model – we have antiviruses to combat viruses, anti-bots to counter bots, and intrusion-preventing systems to fight against intrusions. These things are solved, but the problem is that in the cyber technology industry, we are reactive rather than proactive. The majority of the time, our model is to look for an event that has already happened. If we keep this up, we will never succeed in solving the problems. What we need is to think differently. We need to ask ourselves the questions: can we be just one step ahead of this game? can we actually find and look for threats, and prevent them before they really happen, or at least at a very early stage of them? These questions require a different thinking, and obviously, a different execution plan.

The first problem is: how do we protect against something that we do not know is out there? What is interesting and unique in the cyber field is that many attacks are out there that you do not know about. You do not know that the attack has been made, you do not know who

made it, and you are not aware that you are under attack. We call these types of attacks "zero day" attacks, because there are no indicators to identify them, and there is no signature, hash, or a URL that you know how to block. Check Point did research for a significant amount of companies around the world, which indicated that about 40 percent of these companies download malware every day, and furthermore, there is significant amount of new malware created every minute of our lives. Basically, what people are doing is taking existing malware and putting it into a machine that you can download from the internet that will change some parts of the malware, maybe two bytes of it, and then no anti-viruses will catch them once again. We see a lot more of this going on these days, and it is another aspect of a cyber attack. To use an example from Eastern Europe from last year, an e-mail was sent from Miss World, people opened it, and the documents looked very impressive. What happened there is a download of a bot – a download of a full malware that is looking for specific information. This is common in government and semi-government organizations, nuclear plants, etc. The malware took data, encrypted it, and sent it back to the attackers. To our knowledge we are talking about a terabyte of data, and this malware has been running for a few years.

Let's go back to the question: how do we solve what we don't know? The way we identify these "zero days" attacks is something we call sandboxing, and the idea of it is quite simple. I have a document which I open in an isolated environment and observe how it behaves. If it does not behave as a document should, then it is definitely a malware. This is very straightforward. We look at the system registry, the internet connection, the file activity, etc., and according to these factors we decide if this document is a malware. Today, only about two or three percent of enterprises use this advanced technology, but it is definitely going to be the next big thing. However, even this technology can be problematic because it is possible to evade it. If a hacker puts a malware into a document, but decides that the malware would be activated only in a month or only in a specific infrastructure, then the sandboxing will not work. This makes it a lot more difficult, because the approach that is often taken is that there will be a malware, we will look for it, we will find it and then we will block it, but we actually want to find the malware earlier than that.

I would like to talk about what attacks look like in the real world. The first stage of an attack is vulnerabilities. There are flaws in systems all the time, and because of configuration there will always be bugs. Next we have the exploitation stage. A malware is a piece of code usually executed by its running on the environment. You cannot run it automatically on the environment, because the environment will stop it. In order to manipulate the system, an attacker needs to put a small piece of code that will "clean" the environment, clean the memory, allowing them to get to something called "shellcode", which is a frame that triggers the malware. With sandboxing, we can let the malware do whatever it does, and then we know what we need to do to block it.

Now, let's think differently. For example, instead of looking for malware that runs above the operating system, as previously mentioned, I would like to find it much sooner, at the exploitation level, when it only begins to happen, and when somebody tries to take advantage of a system. If we can figure out how to do this, we can rule out most of the issues in the cyber world. There are millions of malware in the world, comprised of only 6-8 exploitation technologies. If you can manage to find these exploitation technologies and tactics, you can block the issue. This is precisely what Check Point did. We are looking at the calls between CPU and memory, one of the most common techniques for exploitation called ROP, Return Oriented Programing. In this exploitation technique there is a manipulation where the memory "cheats" the CPU. We know that if these calls are abnormal, then this is probably a malware and probably an exploitation attempt. This allows us to block things at a very early stage. Another option is, instead of looking for the malware, we can just clean everything we get, regardless if it contains malware or not. Check Point does this as well, we call this "threat extraction". Instead of looking for malware, we clean what we have, move it to another format, and now we know that it is safe and free of malware.

Another thing I would like to talk about is what we don't control. The main thing we don't control today is mobile devices. Mobile devices are much more dangerous than laptops or desktops, because they go everywhere with us, they know our location, they can record us, and they have business data as well as private data. We basically do not protect our smartphones, because we do not think that it is important to protect our smartphone, and do not understand that there can be malware on our smartphones. It is possible to download

an application on your phone, where a hacker can simply choose to get all of the details stored on the phone and to record the user. This happens when somebody targets specific devices because they want to get specific information from a specific individual, which makes it a targeted attack. Basically, the hacker can choose what he wants to get from that application on the phone. He is able to get the recording of the user's voice, locations, business data, and personal data. This is why it is vital to think about security on mobile devices in a different way, and now is time to do it, before the problem gets monstrous. We need to protect the device and all of its aspects. Most malware take the shape of applications. Another aspect of things is not just to protect the phone itself, but also to protect the data. You can encrypt every document, every piece of data that you create.

To learn more about malware. the first thing we need to be do is to collect all the pieces of knowledge about different malware. At Check Point we have significant amount of research capabilities, and we combine them with threats all around the world from different places, including different intelligence vendors. Once we have this knowledge, we add protection in real-time. To summarize, in order to always look for the best security, we need to be innovative, we need to find a way to protect against what we don't know and what we don't control. It's all down to a lot of innovation.

MR. BOB KALKA, VICE PRESIDENT, SECURITY BUSINESS UNIT, IBM

I live in Austin, Texas, and there is a saying in Texas that is usually applied against barbeque, and that saying is that the appetite is bigger than your belly. In other words, you look at all this incredible barbeque and you say "I'd like to eat the whole thing", but your appetite is only so big. We found at IBM that the same principle applies against information security today. Most organizations that we are working with right now have an appetite to consume things for security that is far greater than their ability to actually do it. I have spent the last 21 years, of my 26 years with IBM, helping to build our cyber security business from almost nothing in the 1990s, outside of the mainframe, where we have always been very strong in security, and I was one of the leaders that made the decision in 1998 that led us to start investing quite intensively in the information security. In the last 16 years we have acquired 26 cyber security companies, including a number of

Israeli companies. We acquired Watchfire about eight years ago, and Guardium and Trusteer just a couple of years ago, so as you can see, we have a huge investment here in this country, in both talent and technology. What I want to give you is our perspective on what is really driving the information security business going forward right now. I chose sort of a "dirty little secrets" theme behind this, because in fact that is exactly what is going on. Through these 26 acquisitions we have gone in IBM from being a no one in the security industry to being the third largest provider in the world – Symantec, McAfee and us – and we are by far the fastest growing information security vendor, according to the *Gartner* report that came out only two weeks ago.

Now that we have gotten so large in this industry, we have many insights. We have over 12,000 clients today, and one of the things that we learn is the dirty little secrets. Let me give you some personal background on why this is meaningful to me. Along with a degree in computer science, I have a graduate degree in group psychology. And in group psychology, one of the most basic things you discover is that every group has something called a "shadow". A shadow in a group is the things that the group doesn't want to deal with or admit that are there. Do you think it is any different in information technology, in cyber shops, today? I would assert to you the biggest problem we have seen in information security today is that every organization has walls, that they refuse to look around the corner, because they know that when they look, they are not going to be able to do anything about what they see – politically, financially, or both. So as a result, what they do is simply not look. The intersection of group psychology with security is very interesting, I think this is what has kept me in this field for two decades.

I want to take you through the four conversations, or topics, that we see driving information security going forward, as well as the dirty little secrets – because by the way, there is at least one for each one of those – what are the dirty little secrets that we either don't want to see, or we are just not looking at? First, before that, a few statistics, the first of which is one of my favorites. We did a survey of some clients, and found that 70 percent of security executives have cloud or mobile concerns, and my question to you is – where are the other 30 percent?

I am around the world every day, meeting clients, and one of my favorite meetings last year was with a very large financial services

company, who said that they were behind on cloud, and wished us to help them do it right, in terms of cloud security. We agreed to run a full day workshop on the topic. At the beginning of the day the CISO and I got in front of the room, about 30 people, and spent seven hours with them, going through very detailed cloud security use cases. At the end of the day, everybody said that this workshop has been wonderful, but once the CISO walked out of the room, the lead security architect told me what was really going on. He told me they did a quick analysis, and about 50 percent of their employees have been using Dropbox to share confidential files. So, they did use the cloud, but the managers chose not to acknowledge it, because they were not looking.

Anyone who has been working at the cyber field for over ten years, knows that cyber was always "buy the best of breed product in each little niche", and now we are in a state where everybody has one or more products from many vendors. I work with an insurance company that currently pays maintenance on 288 security tools from 65 vendors. This is insane. In IBM, we buy a lot of the best security companies to avoid this situation of multi-vendors and many different niche products.

So, what are these four conversations that we believe are driving the information security business forward right now? First of all is optimizing the program, and I know that it sounds like a nice generic thing. What I mean is optimizing the security program and make it truly risk-based instead of complaints-based. This is one of the dirty little secrets in our industry: most cyber shops today are complaints-based programs. A litmus test for that is SIM, Security Information Management. I ask every client, "do you have a SIM?" and almost everyone answers yes, sometimes even more than one. But when I ask them if they make any real-time decisions every day using that SIM, at least nine out of ten people say "not really". SIM is a great litmus test of whether you have a risk-based or a complaints-based security program. If you put it in because you had to have one, and it is a pretty, shiny thing, that's great. But are you using it to make decisions about how you operate your business? The first thing is going from complaints-based to risk-based. Everything you have heard from the other speakers this morning, is that if you just do complaints-based you could throw stuff in, but it doesn't provide any utility other than getting you through of the next audit, and that is not cyber security – that is managing for a job security.

The second conversation is stopping advanced threats. One of the things I love about information security is that there is a subset of decision makers that take a "magic bullet" approach to security, and they say, "all we need is this tool, and if you just give me budget for this tool it is going to be great". Seventeen years ago, in 1998-1999, the magic bullet in cyber was digital certificates, three years ago it was DLP, and now it is sandboxing, and they promise you to "take care of everything". That is silly – sandboxing is important and very useful, but it is an incomplete solution, and everyone that pays attention knows that. So what we realized with stopping advanced threats is you cannot do it by finding a "magic bullet", it's all about intelligence and analytics, taking actionable data from every layer of the stack, if you are a COBIT fan – infrastructure, application data, and people – the users; taking information from all of those places, and making functional analytics and actionable decision based on that. So stopping advanced threats is actually based on quiet quality intelligence and analytics, not finding whatever mouse trap happens to be a better one right now, or the most trendy.

The third topic is protecting critical assets. We, the cyber professionals, are supposed to help our businesses, our agencies, whatever we are a part of, we are all supposed to have established controls over access to our sensitive business data, that is one of the most basic tenets to what cyber is responsible for. But how can you assert that you have proper controls over securing access for your sensitive business data, if you don't know where all of it is? And yet, no one knows where everything is. That is a problem we have as a profession – we don't know where all the sensitive business data is, and we know that this is a target, especially on the unstructured data side, but protecting the critical assets, especially the data, is clearly going to be driving our industry for a while to come. An extension of this thought around protecting critical assets concerns secure app dev process, because a lot of the access to that data is through applications. Do you have a secure app dev process in your business? This is another litmus test, to check if you have a risk-based or complaints-based security program. The litmus test for secure app dev is static source code analysis. If you have a project in place, or at least in the works, for static source code analysis, that is a good sign. If there are no such processes, if you only talk about it or even afraid to talk about it, it means you have a long way to go.

The fourth conversation driving the industry is safeguarding cloud and mobile. Except for the public, private, and hybrid cloud, there is a fourth type of cloud – the covert cloud, the cloud you are doing without even knowing about, or that you choose not to be aware of. There is a difference between the last two types, but they both have the same effect. However, there is another thing around cloud and mobile, especially mobility, that we see with a lot of our clients right now, which is incredibly important. Mobility gives us an opportunity, for the first time, to take IT apps, cyber security and the business, sit them together and figure out how to run the business better, faster, cheaper, more innovatively, etc. So whereas it is very important that we acknowledge what are we really doing in the cloud and protect it commensurately, we should also take advantage of the opportunity we have to take cyber from being "those security people", to literally being able to reshape the way the business operates.

These were the four things that drive the industry. Do you have a risk-based or complaints-based program? Do you have proper intelligence and analytics across the board in place, or a "magic bullet"? Do you protect the critical data, so that you know where it is and have actually taken actions to protect it, and have a secure dev process? And finally – core safe, cloud or mobile? We have over a thousand client using secure cloud right now, and I can tell you that the first five things almost everybody does for cloud are federation, fine-grained entitlement, multifactor authentication, risk-based authentication, and a one-time password.

IBM has gotten to the point where we are literally the fastest growing and largest out there, we have research and stock centers worldwide, and in particular we have and will continue to have a huge investment here in Israel, because you clearly are one of the centers if not *the* center, of cyber security talent in the world, and we take it very seriously for our business. Not only have we acquired companies like Watchfire, Guardium and Trusteer, but we also recently opened a cyber center of excellence nearby, which is also working to have some great research topics.

One of the research projects that our researchers figured out how to do, that you will see from us fairly soon, is how to map the way you move your mouse on your screen, so if you give your machine to someone, or if someone takes over your machine and starts messing

with it, we can tell it is not you. The next step is the way you move your finger on the screen. We have research all over the place, and much of it takes place right here in Israel. The bottom line is that we think we know what drives this industry, we have acquired 26 companies and continue to grow. And now, with over 12,000 clients that we do cyber with, and have a lot of confidence in working with a lot of you, all over the board, we think we can advance the state of the art of what is going in cyber,

02

SECOND SESSION: NATIONAL POLICY AND INTERNATIONAL COOPERATION

MR. BG (NS) DAVID KOH, CHIEF EXECUTIVE, CYBER SECURITY AGENCY, SINGAPORE AND DEPUTY SECRETARY (TECHNOLOGY) IN THE MINISTRY OF DEFENSE

I am from Singapore, a very small country in South-East Asia. It is so small that it is quite common for people to have more than one job. I myself have three jobs – the head of the Cyber Security Agency, the Deputy Secretary for technology in the Ministry of Defense, and I have recently been appointed to be the Deputy Secretary for special projects in the Ministry of Defense, meaning that I will oversee cyber matters in the Ministry of Defense. I am here to talk about Singapore's experience in managing cyber security as we progress in the context of Singapore to a Smart Nation.

This year Singapore is celebrating its 50th anniversary of our independence. Over these 50 years we have transformed ourselves from a third world backwater into a high-tech city state. Singapore's ICT infrastructure is robust and reliable, and we have a very high internet penetration rate of over 80 percent since 2013. This has allowed us to leverage on IT for effective economic and social development. We were ranked as the leader of global ICT revolution in the 2015 Global Information and Technology Report, GITR, and we were ranked third in the 2014 UN E-government survey. So Smart Nation is our vision for the future. Smart Nation in Singapore entails using the information technology to its fullest in order to enable our people to achieve meaningful lives filled with exciting opportunities.

From a social aspect, the building of a Smart Nation is a nation-wide journey. It is not just about technology, but also about engaging our citizens to join in the process of improvement through increased collaboration and implementation of new smart ideas. Everyone has a part to play, and in our view everyone needs to play a part. We need

people to step forward, to contribute, and to spark bright ideas. But all this must be done in a safe and secure manner. From the legal privacy policy angle, there will be significant security concerns, surrounding the protection of increasingly large amount of data that comes with the growth of our proud nation, especially data related to personal privacy and national security. Everyone in Singapore sees the Smart Nation as a great opportunity, but there is so much to do. We have to secure this data and safeguard the rights on how this data is to be shared or used. Policy needs to be in place in order to ensure that data custodians remain responsible for the usage and distribution of the collected data. We will also need to regulate the usage of censures, to prevent any misuse that could expose an individual's behavior or actions in real-time.

Let's talk about the internet of things. Imagine that your smart refrigerator stops buying ice cream, because the smart armchair in your living room simply took your body fat measurements and broadcast it to the surrounding appliances – any appliances interested in knowing how fat you are – including your neighbors' refrigerators. This can have serious privacy implications. As we progress towards a Smart Nation we will see more and more online applications with densely interconnected systems. Our databases will become increasingly interconnected, and our cyber risk exposure will inevitably increase, and If we do not recognize and manage that risk, it will lead to cyber attacks with consequences that can be detrimental to the nation's wellbeing.

Singapore has seen its share of cyber incidents. In September last year hackers breached the costumer database of a reputable karaoke chain, and posted online the personal details of over 300,000 members. In that same year, a major tycoon in Singapore had to suspend an online application due to a potential website breach, after a customer reported that he could hack into the site and access the personal data of its customers. Fortunately, in this case the impact was minimal, and the problem was rectified in time. However, the risk of exposure is real, and the impact could have been significant.

With the proliferation of smart mobile devices, cyber attacks have become increasingly sophisticated and diverse. Malicious mobile applications can be found in both Google Play and Apple Store. These applications allow hackers to steal private information without the

owner's knowledge, or gain unauthorized access to devices. And so, as we push services to these end devices, we have to be aware that they could be unsecured and easily compromised. Cyber space is just too vast, and it is a challenge for every single entity to have complete visibility oversight. Others say that the industry can't do it alone, but from our perspective, we the government can't do it alone as well. Singapore's approach to counter the cyber security challenges extends beyond the efforts of the government, in what is holistically termed as the whole of society approach towards cyber security.

The government lays the foundation by building infrastructure and facilitating different parties to contribute and innovate in the area of cyber security, for example. For example, we have established a Personal Data Protection Commission, PDPC, to enforce the personal data protection act, but also to provide a suit of resources to help organizations implement data protection policies and practices – guidelines on how to manage electronic personal data and data breaches, a legal advice scheme, and even e-learning programs that have been developed to help organizations understand their obligations under the personal data protection act. In April 2015, the Cyber Security Agency (CSA) of Singapore was born, and I have the distinct honor of being appointed the head or chief executive of that agency. CSA provides dedicated and centralized oversight of Singapore's national cyber security functions, and focuses on engagements and partnerships to ensure the holistic development of Singapore cyber security landscape. Through the active engagement of both local and global cyber security thought leaders, CSA aims to set up a robust and sustainable cyber security ecosystem. In October of this year we will be organizing Govware 2015, a conference which provides us with an excellent platform to bring together different cyber security experts in government, industry, and academia.

Academia plays a key role in the development of research expertise and capabilities in cyber security for Singapore. Our National Research Foundation, NRF, has launched a national cyber security R&D program last year, focusing on the development of cyber security R&D capabilities to meet national strategic needs. A total of about $100M will be available over five years to fund cyber security research in areas such as resilience systems, attack attributions, and threat detection. We

make major investments to improve and better assess our effectiveness against cyber and physical attacks.

The academia is also essential in the growth and strengthening of our cyber security work force. Our institutes of high learning provide continuous training and skill development for a wide range of cyber security training programs designed for individuals at both entry and professional levels. The industry, of course, is also an important contributor to our efforts encountering cyber security challenges. It is crucial for us to partner with leading industry players to enhance our cyber capabilities development and widen our cyber defense mechanisms. For instance, Asia pacific center of excellence, in collaboration with the Infocomm Development Authority of Singapore, provides manpower training programs at the expert's level of skills in the area of cyber threats intelligence. The collaboration also covers the development of the next generation on its application programs and interface platforms.

In Singapore, our aim is to recast and reframe our mental models, and to position cyber security as an enabler to leverage on technology. We see cyber security as the crucial enabler that will allow us to confidently progress towards our vision of a Smart Nation. And we can only strengthen our cyber security foundations through continuous efforts in technological development, and active engagement with both local and global cyber security professionals.

MR. HOWARD A. SCHMIDT, FORMER CYBER ADVISOR TO PRESIDENTS BARACK OBAMA AND GEORGE W. BUSH; FORMER CSO AT MICROSOFT; FORMER CISO AT EBAY

I would like to share with you my comments on issues of national information sharing and all the things related to the international side. This is not a new issue. In 1998 President Clinton signed a presidential executive order that mainly stated three things. 1) The vast majority of these critical infrastructures is owned and operated by private industry; 2) The government at the time did not have enough interaction with them to worry about where we stood when it came to critical infrastructure; 3) the private sector was not organized to share information about the protection of critical infrastructure. However, while the presidential executive orders can direct the US

government to do something, they can only recommend these actions to the private sector.

In May 1998, during a speech at the US naval academy, the President talked about three things. The first was encouraging the private industry to share information in what they call ISACs, Information Sharing Analysis Centers. The reason that it was so important, was because at least the vast majority of what we depended on, in terms of critical infrastructure, had the ability to share information. And bear in mind, for those who followed the tech industry, my old boss Bill Gates, Scott McNealy from Sun Microsystems, and Larry Ellison from Oracle were not exactly the best of friends at that time. But yet Mary Ann Davidson, the Chief Security Officer for Oracle, Whit Diffie from Sun Microsystems and I worked very closely to help create the ISACs. Creating the IT ISAC involved the financial services, and this has paid tremendous dividends. But it only gave us a part of what we needed.

After 9/11, President Bush appointed Richard Clarke as the chairman of the PCIPB, the President's Critical Infrastructure Protection Board; I was the vice chairman until his retirement. We put out a national strategy to enhance cyber security, and I encourage you to read it – it is still available on the White House Homeland Security website. But it had the same key components: reducing vulnerabilities, both in the government and out of the industry; looking for cooperation concerning international issues; looking for the education. That national strategy was the tipping point in establishing the things that we needed to do as a nation. And I am very pleased, in a number of aspects. We have worked with other nations to develop strategies that are very similar to ours, but fitted to their culture and their nation. Some of the things there were the issues about vulnerabilities, the exploitation of such vulnerabilities, nation states, criminal gangs, activists, and how we can protect against all that.

After President Obama was elected, he asked us to put out three national strategies. The first was the national initiative for cyber security education. Looking to develop this, we asked: what are the necessary skills? Because we knew we would not have enough people to fill the positions, but we had to figure out what the positions were. And it is interesting, from both my private industry and government experience, that when you talk to someone about what is a cyber security expert, they say "people that understand security". But there

are different technologies, mobile devices, internet of things, television being the center of your existence, let alone the network devices and the identity management, and all these are parts of the bigger cyber security. So we had to find out what are the discrete skills that are necessary – as a nation, for the US government; but just as importantly for the private industry, because the vast majority of the people that protect us are indeed of that sector. We wanted to give them a vehicle by which they can have careers.

The second strategy commissioned by the President was a national strategy for trusted identity for cyber security – basically identity management. When we look at the vast majority of the intrusions that take place, they all circle around using user ID and password. And I would imagine that many of the people in this room, and the ones that I know, have dozens of different passwords for different user IDs. I have 57 different accounts – airlines, hotels, universities that I am a part of. We need to move away from that – all of us, including the government – and build an identity management ecosystem owned by the private sector, not the US government. But when you look at all the bad things that have happened recently, including many incidents within the US, they all boil down to clicking an e-mail that gives an intruder access to a system. Which is the second part of the digital identity – because if you receive an e-mail from a digitally-signed entity or individual, you have a higher level of trust. You can filter out the bad things, the phishing e-mails, the pieces of malware. So it was very important for us to develop this national strategy.

The third strategy, and probably the most important one, which affects all of us today, is the national strategy regarding international cyber space. Noticed that the word "security" is nowhere in that title, because cyber security is just a single piece of cyber space – we need it, we need defense, we need the military, we need the law enforcement, we need the security from within the companies, and we definitely need the universities to train our next generation; but it is much more than that. When I served for President Obama it was interesting, because on the security side we want to lock everything down, protect it, make sure people are not getting into the systems, and even if they would get in they would be found immediately. But on the other side we want an open society, an open internet, and we had to find that balance. Israel, Singapore, Japan, Germany, many of the countries that I work

in, are looking at the exact same thing, trying to find out where is that balance. What we do know is that the international cooperation is key. I've seen it in many areas, and the cooperation is vitally important. We need to execute; we need to start trusting our friends and colleagues, to not keep information only available in the United States or Israel or Germany or anywhere. Because even though we have national interests in this, the internet is much bigger than that.

We want to have a protection against countries like North Korea and Iran, that, as we have seen recently, are looking to cyber attack us either as a retaliation or to get ahead of us. We need to protect ourselves against them, not to destroy the internet in doing so. Our privacy protection is critical, it is not just something that consumers need to worry about through businesses. When you look at a situation where you have four million victims, it is something that could have been prevented by doing the things we need to do, by sharing the information, by looking at the technology beyond our borders – because when I look at the technology here in Israel, or Singapore, or India, or other such places, it should not be discounted. Even though the big companies, the multi-companies around the world, work very hard on solving this issue, there are also many companies that can provide the same technologies. Don't label them by saying, "this is a foreign country, and it is a foreign software, therefore we can't trust it". We have to learn to trust. If the governments can't do so, then we at the private sector have to take the lead, and make a difference in what we do. Because all of us, anywhere in the world, are citizens of the internet. We may have our national citizenship, but the internet is what makes us work in everyday life. So while we have problems – and we will continue to have problems until we develop the technologies – we develop the business processes, and we develop the relations between governments that are willing to stand up and say, "we will cooperate with each other to stop the bad guys, but also to improve life through internet".

My last point is that if you have an opportunity, the national strategy for international cyber security is an invitation for everyone in this room to do their part, to secure their part of cyber space. And that, indeed, makes us all more secure.

DR. KYUNG-HO CHUNG, VICE PRESIDENT, KOREA INTERNET & SECURITY AGENCY

Over the last few years our country has suffered a series of very serious targeted attacks meant to compromise the critical infrastructures. One of the most important lessons that we have learned about this kind of attacks is that we need to align our cyber security strategies and framework to fight these kind of attacks as a whole. Additionally, international cooperation between CERTs is needed more than response to attacks. Our efforts should extend to defense intelligence in order to prevent and identify the prospective attacks, and we need to be proactive rather than merely respond to attacks. I will talk about the recent shift of our cyber security strategies, and about the subsequent changes that happened this year.

In the last few years we have experienced various attacks. The first major attack was on internet banking, in 2011. The Nonghyup, the National Agricultural Cooperative Federation, is one of the biggest internet banks in Korea, and they reported damage to their servers. They lost all of the account information, and could not run the business for 18 days. What happened was that an employer used his laptop to log into the system and download movies from the internet, his computer was affected, and the hacker successfully downloaded some hacking tools, as well as eavesdropping software. So the hackers could identify internet works and even listen to conversations inside the bank. When we recovered all of the evidence and analyzed the malicious code, we found that the attack originated from North Korea.

Another major attack happened in 2013, and was an attack on the media – newspapers and broadcasting companies. This attack took place at a similar time as the attack on the Blue House. The President's oval office had made homepage placements containing internal data, and the hackers posted them online.

A third major attack was on our critical infrastructure, as the hackers attacked a nuclear power plant. The attackers suggested they would compromise the nuclear power plant, and fortunately they only compromised some of it and failed to penetrate the control system, but they managed to obtain the blueprint and some information from the computers, and posted the information on the SNS social network and on the internet. They exposed this information little by little and over

six times. At that time it was critical for our government, because our government had a contract with East Asia to export our nuclear power plants. Even though the attackers did not manage to compromise the plant, it was a big issue in our society. That is how the cyber security has become a national security matter. One of the main concerns during this kind of incident was the plant's control tower. In Korea, KISA, Korea Internet and Security Agency, is in charge of the private sector, the National Intelligence Services are in charge of the critical protections, and the government's Cyber Command is in charge of cyber defense against terror. And the question was – in times of peace, who will be in charge of coordinating the all the security-related activity? After these incidents, President Park appointed two people to serve as a cyber security special advisor and a cyber security secretary, and these two people report to her directly. So the Blue House took responsibility over the nuclear plant's control tower.

Last year we experienced another severe attack on our broadcasting networks, which surprisingly did not originate from the PC, but from mobile wireless devices. There are more than ten million mobile wireless routers currently installed in Korea, and the problem is that these devices have no security measures installed by the users. Most of them are controlled by the users, but these users do not know how to fix security problems. We found that there are over 200 different models out there, some are not supported by their manufacturers anymore. In that case, who can handle this kind of issue? We dispatched people to fix the problems, but there were too many devices without any security measures. This year we have had similar attacks on the CCTV – there are more than 10 million CCTV cameras installed in Korea – and these attacks will not stop in the future.

The KrCERT in Korea takes responsibilities to protect our internet, and we believe that our role is bigger than the typical type of the sort. We dispatch the people and we provide the technical and legal support, and we advise the companies that have encountered any kind of attacks. One of our main activities is cyber security monitoring. We monitor the networks and internet nation-wide, all the information coming from the ISPs, and look for any symptoms of attacks, any kind of flux in the information. We monitor them 24 hours a day. Another activity is our malicious code finder. It is kind of a house check of homepages. Nowadays, malicious codes can be installed via "drive-by download",

and infect websites and homepages. In Korea there are more than 250 million homepages, all of which are being checked daily. Each homepage is reviewed every two hours to see if any of them has been infected by a virus. And if we find an infected homepage, we call its owners and ask them fix the problem, and sometimes we dispatch our members to resolve the problems. We also block the malicious IPs and provide some technical services to the users.

A third activity of KrCERT is securing systems. We also provide some alarm services; if a PC is infected then the user working on the computer receives a message saying that his computer is infected, and refers them to KrCERT or an anti-malware company to download updates and patches. We are also thinking about making similar applications for smartphones. This kind of service will be started this year. The final activity I would like to mention is the cyber fraud alert. In our organization we have traps such as a spam trap and a honey pot, and we collect all the data from the ISPs and distribute blacklists to the service providers. We also have emergency telephone numbers – like you dial 199 for emergency calls, you can dial 118 for cyber emergency calls. That way people can contact us, and if they need any support, we will provide the necessary services.

I mentioned some of the attacks that happened over the last couple of years, and their frequency continues to increase; it looks like we are losing the game and need another approach, since the current approach is not working at all. We work very hard, but we have not achieved any result, and therefore we think about changing the rules, adopting a new strategy. We call it the KICT security strategy, and it consists of five parts.

We require commitment from our cyber security industries; this is the main concept. We try implementing push and pull strategies to create big opportunities for the industries, and encourage them to produce better products and to commit more to cyber security. Risk assessment is another part of KICT. We currently have about 400 critical infrastructures, and we will reach more than 1,000 critical infrastructures by 2019. We are currently building an information sharing system called CTAS, Cyber Threat Analysis System, and because we have much experience in the area of cyber security we have immense amounts of data. We collect the old data, put it into one system in the platform, and we ask the industry, the academia

and online game companies to also put their old data there, like the malicious code, attackers' IPs and older information. Then we try to share that information with government agencies and cyber industries, in expectation that it will present them a great opportunity to identify the hackers and improve the performance of their products.

The third part of our work is the security investment. Our government is highly concerned about security investment, because we found that many small companies do not invest in cyber security. Our goal is to reach a state where 10 percent of asset investment is in cyber security. We are considering incentives to encourage these cyber security investments, such as tax exemptions for the companies.

The next part is R&D. In Korea we spend more than $200M every year on cyber security. We are working with the cyber security industry and the academia, and our goal is to make the best cyber security products. The last part of KICT's activity is training workforce and talents; our goal is to educate 7,000 white-hat hackers until 2019. Here I explained our five main goals and strategies, but if you think about this as a scheme, this is a cycle we call "the chain", which, we think, holds some value. Because of that we make the link, trying to improve and increase the demand for cyber security, and give the industry a better chance to compete and benefit in the area of cyber security.

Finally, another goal is the implementation of sharing and cooperation. In case of an incident, what is the most important issue? The question is who is the attacker, or the attribution problem. In most cases it is very difficult to identify the hacker. We work with many different organizations, but in many cases it is very difficult to get the right information. Last year, at the same period of time where Sony Entertainment suffered a cyber attack from North Korea, we suffered a cyber attack originated there as well. That was the attack I mentioned earlier, on the nuclear power plant, and we found that the attackers were related to the groups that attacked Sony. We identified over three groups working together, we collected evidence and shared that information with the US-CERT. We discovered that there was a close relationship between two groups, and successfully found the attackers. But these are very rare cases. We work with the Chinese CERT, CNCERT, we work with JPCERT, and we all work better on cyber crimes when we cooperate with each other. But when it comes to cyber terror, it is very difficult to get the right information because the hackers use compromised

servers, and not their own IPs. We can trace the attackers' routes, with some help from other countries, but we need to build some trust-based cooperation. And we have done just that.

MR. RAJENDRA S PAWAR, CHAIRMAN & CO-FOUNDER, NIIT GROUP & FOUNDER, NIIT UNIVERSITY, INDIA

I represent the industry, and the first part of my talk is about how the industry is looking at this whole situation as an opportunity, while the second part is about international cooperation. It is reassuring to see that many recognize that the problem is not a national problem or a company problem, but a global one. On the 25th celebration of our association, Nescom, our Prime Minister, Mister Modi, gave an outstanding speech, in which he mentioned cyber security. However, he did not talk of protection alone, but when he spoke of many of the heads of government he had met during the first year of his Prime-Ministership, he said that most of them see this as one of the top three problems, and he challenged our industry association to look at that as an area where we can serve and do something meaningful, and a task force, which I have had the honor to chair, was formed just a little over a month ago. This is all a work in progress, and I have heard many comments saying that it will have to evolve on a daily and even hourly basis. However, the first thing we did was to say that our industry has to respond to this situation, and that we should think of defining the scale of the opportunity.

The worth of Indian IT and business process industry was $146B last year, and we have an aspiration, as an industry, to reach $350-400B over the next ten years. Within this, the share of cyber security companies is very small, about one percent, but it could be as much as ten percent of the size of the industry. As an industry, we are looking for an opportunity to build a subsection of our growing industry, and – more importantly, in a country like India, which has 1.25 billion people with very high unemployment – it can create jobs. So we expect that such a skill would also generate, directly and indirectly, about a million jobs by 2025.

In our thinking, the task force has defined this large charter, and has created four work groups, and by end of July we will come up with a recommendation to the government and the Prime Minister. The first

work group of the task force handles industry development, which involves all the planning within the industry association on its various subsectors, how do we build a road map to reach that skill and size. The second and third groups handle two enabling factors that have come up over and over again: the question of building new technology, where we see a very big role for academia, and skill development – an issue which has come up in virtually every presentation. The fourth group handles policy development – not the national policy on cyber, handled by the government on a larger scale – we only examine supporting policies that will help the industry agenda to be met, as well as existing policies that are getting in the way of developing the industry. Our trust and our analysis will be restricted to that aspect of policy. Everyone on this task force is an expert, however they are also new to the subject, in a sense.

This mission is fundamentally different than anything we have done before. The first and perhaps most important difference is that we are talking of all the bits, not of all the atoms. And so, when we talk of identification and attribution, we can recognize that there are difficult bits to recognize. They also travel at a very different speed than atoms or light, and a very important part, for me, is that this is a concept on which very little is understood. We live in a world of atoms, and the economics of atoms has created a whole body of knowledge which is predicted at best, on the scarcity phenomenon. If there is one kilogram of something which I want to share equally with someone, each of us gets a half kilogram. If you want to share it among ten people, each one gets one tenth of a kilogram. But with bits, at a marginal cost, if there are a thousand people who want to share a megabyte, each one gets a megabyte, with almost zero marginal cost. So the underlying economic theory has to be predicted on abundance rather than on scarcity. Many interesting phenomena, such as the .com bubble, cannot be explained by normal economics, and we do not yet have a better economic theory, based on abundance.

The second difference is that we are dealing with a situation of fundamental asymmetry. We talk about the fact that we are currently only responding to threats, because the thieves are free and the cops are restrained by laws. And thieves are far ahead of cops. We all know that people try to put a value such as $3-4 Trillion of losses in a year, and there appears to be an underestimation because no one knows

exactly what the loss is, and whatever we know is underreported, because people don't want to share that they have lost something. So these two reasons are causes which have to get us to think completely afresh.

Now I want to talk about the reason why I am here, with the delegation from India, which is that we see an outstanding opportunity for collaboration between our two countries. There seems to be a very natural opportunity to collaborate based on good positive emotion and trust, and I am talking about scope and scale. Israel already has a track record of being a startup nation, and there are many reasons why your history has created this culture. You have defense expertise, every citizen here, and your youth have a great sense of discipline and purpose, serving at the very formative stage, before you go to college. This has a deep impact, which I think it has been translated into building a base capability that is very important for the sector.

And of course, Israel has a very special condition, which is difficult to replicate anywhere, with defense and industry and academia that work so closely together. This is not something most countries will be able to do, and that is why a deep collaboration with India is what we seek. So you have the scope of activities, and what India brings to the table is skill. Our IT industry is very young, and was built from mostly nothing in the early 90s. We have three million IT professionals already employed directly, and perhaps one and a half times more than that additional jobs that the sector has created, and at this point in time we currently have four million students on their way to obtain their engineering degree. This gives us about a million new engineers per year, many of whom look forward to getting better and better jobs. The new government under our Prime Minister, Mister Modi, has announced a digital India agenda, where the motive is to work the focus on the individual citizens, however poor and challenged they may be – and India has a very large percentage of people living well below the poverty line. So the digital agenda of India is not a money making agenda, but rather a social agenda that deals with helping the poorest of the poor in leading a better life. That translates into massive investment in IT, which will therefore require building a strong underlying cyber security infrastructure.

The Indian IT industry has the largest number of companies certified to the highest levels of quality in software development in the world, even

as a percentage. So India brings skill, and we believe that Israel builds scope. I heard that in Israel, young entrepreneurs build companies and sell them. It is a very different mindset than ours – in India we build companies and want to stay with them. For example, I started my company in 1981. The mentality here is interesting, building a company like a product that you can sell, which can create value. So, the ability to generate new ideas, working with Indian companies who take them to scale, could be something that could be done as an activity. We do have a very interesting young and fast-growing product ecosystem, but it is still very small, and therefore I can see terrific opportunities for interactions between our small companies as well as many companies here, and I think the opportunity exist for us as two countries to create a new value chain; this is my central idea. But we should think about it together, plan it together, because we don't want to end up just eroding value, we should mitigate value erosion, we have to think at policies at a national level, which incentivize cross-border M&A. It has to become much easier than it is today.

I have to admit that in my opinion, in India we have very poor collaboration between the three key players – academia, government, and industry. I am simply astounded and deeply impressed by the contrasting picture here, in Israel, of how closely your three entities work, and it is a part of your culture, of your national system, of how young people grow here. Having spent a little time here, I feel deeply encouraged that for many, many reasons, rather than just economic ones, there is a scope for a lot of collaboration and cooperation.

03

THIRD SESSION: BEYOND INTERNET

MR. PATRICK M. DEWAR, EXECUTIVE VICE PRESIDENT, LOCKHEED MARTIN INTERNATIONAL

I want to reflect on what we at Lockheed Martin are doing to safeguard our future, and take us beyond the internet. The internet has been a great catalyst for change, and look at how things have changed in the last fifteen years. The internet takeover of global communication was almost instant in historical terms. It only communicated one percent of information flow through the two telecommunication networks in 1993, and then 51 percent by 2000, and more than 97 percent of telecommunicated information by 2007. Today the internet continues to grow, it is driven by ever greater amounts of online information, commerce, entertainment and social networking, as we all know. And paired with the rise of the internet are the political, economic, technological, social and cultural changes that we have experienced. It is clear today that the landscape is being reshaped, and this includes the rise of digital technology, and the risks associated with the increasingly connected world.

I would like to talk about the risks posed by the challenges, how they might threaten our security, and what we should be looking at. Here, in Israel, Lockheed Martin, with our partners, develop processes to take us beyond the internet. We have been partnering with the defense establishment for many years, but we are relatively newcomers to the IT and cyber areas here in Israel. Last year we set up an operation in Be'er Sheva, and the location was specifically chosen in appreciation of the innovative Israeli technology ecosystem in that area. Our business in Be'er Sheva allows us to focus on enabling a combination of academic engagement with Ben Gurion University, actively participating and leading the efforts to build an internationally renowned cyber security hub in the form of the CyberSpark initiative in the Negev, and to build support for small and medium enterprises located at the campus that are building many of the world's foremost emerging cyber security

technologies. There is also a great amount of joint academia industry research studies that we are proud to be part of, and supporting the development of plans to recruit and develop the talents of local cyber specialists. Attracting further local and national investment in the region particularly, but not only, in the context of Israeli defense forces move to the south initiative. I am pleased to say that our work in the Negev not only stimulates growth for the Israeli work force, and further develops and trains in-country talent to become cyber industry leaders, but our presence also supports Israel and their aspirations to be a highly advanced information technology hub in the south. We want to continue to play a key role in establishing Israel as a global respected cyber venture, via a significant contribution of skills, experience and inward investment in jobs, and we are looking forward to some exciting times ahead.

Cyber security is not new to us. We have been delivering security services and solutions across the world for almost 30 years, and in everything we do, every program and every product we develop, cyber security is at the core. But with that comes the increased risk of cyber attacks. And it is important to invest in people, technology, facilities, and best practices to ensure networks remain secure. So as we all know, the volume of sophisticated cyber attacks continues to increase. We, as a company, see growing demand for cyber services and solutions in both the public and private sectors, and to answer that demand we use the capabilities that we have developed in protecting our own networks, in order to help secure our costumers' assets. But we have learned that ongoing vigilance is required to safeguard sensitive business and personal information, and we are determined to continue delivering our capabilities to our customers, so that they can benefit from the same level of protection that we have used for the past several decades.

We live in a world where developing nations, rogue nations, non-state actors, and even individuals, are more and more able to influence global events. The internet means that vast sums of money can cross the world in a keystroke, a drought in Australia can lead to food crisis in Haiti, and a virus in Africa can unleash panic in North America, and in such a world, strength flexibility and adaptability are at the premium. So we must be innovative and agile to keep up with these ever-evolving challenges and emerging threats. The rise of digital

technology has created huge opportunities as well, but it also brings with it unprecedented risk. In this era of Big Data we can build tools that look beyond the world we see, using data to anticipate more accurately than ever what is over the horizon. Sophisticated analytics help us to predict everything, from stock market trends to the next disease outbreak. Worldwide demand for smartphones is estimated to increase by six times over the next six years. Mobile data traffic will grow by more than eleven times in five years. And much of that demand is coming from developing nations, which are simply going to skip a generation of technology, and fuel their economies with smartphones and digital solutions.

The exponential rise in digital demand has created an extraordinary demand for capacity and the satellite systems that enabled it. All of these advancements come with new challenges and threats. Society's increased independence on digital networks has made us more vulnerable to digital disruption. It seems that every week we hear of a new data breach or a new cyber threat. Hackers have struck organizations as varied as large retail stores, film studios, and health insurance companies. Quoting from a recent US pentagon report: "cyber adversaries have become as serious a threat to US military forces as the air, land, sea, and undersea threats represented in operational testing for decades".

Lockheed Martin actually started the cyber business before anyone called it cyber business, because we had to. Given our line of work, we are often a target ourselves for advanced persistent threats. We faced 50 such coordinated and sophisticated campaigns in 2014 alone, and that number is sure to keep growing. So we have made significant investments to protect ourselves, our information, our forces, and our shareholders. We have used our knowledge by forwarding, anticipating, and averting these intrusions to help our customers secure sensitive information, protect business interest, and stay ahead of the threats that technological advances bring with them. We are the cyber security providers for more than 200 customers around the world, supporting critical infrastructure for the energy, oil and gas, chemical, financial services and pharmaceutical industries.

One of the greatest strengths we can bring to our cyber customers is our multilayered intelligence-driven approach to defend against these threats. We have more than twelve years of intelligence about

these advanced persistent threats, where they may be based, how they operate, and what tools and techniques they use. This deep pool of intelligence allows us to predict, identify, and respond to threats for our customers. As we look ahead, we focus on how we can help shape the future and continue to grow our business and that of our customers in the long term. We now live in a world where both man and machine can obtain information on almost any topic at any moment. Documentation of our world happens in real-time, through a constant autonomous torrent of ones and zeros, and research and recall of that information have been reduced to mere mouse clicks. Who hasn't gone to dinner, had a question, and immediately pulled out their iPhone and got the answer to that question, just like that?

With all the data available at all times, opportunities and adversaries can also move in real-time. So we should ask ourselves, how do we move faster? This is a domain of predictive analytics, a concept that is not new, but the potential of which in a new world, not limited by data and power processing, is expanding rapidly. Our investment in predictive analytics primarily serve the goal of anticipating threats, emerging from dynamic environments, and being able to do so faster than others. What is new, however, is that they are no longer limited, this is no longer limited by data and processing power. Data is enormous and available in real-time, and we are now, as many have observed, firmly in the era of Big Data. Processing power, meanwhile, is now so immense that we can capitalize on this abundance. It might seem that more data would increase the unlikelihood of finding the proverbial needle in the haystack, but this challenge is largely overcome by the sheer processing power available in modern computing platforms. The true value of expansive data is in the enablement of analytic prospecting, quickly identifying and recognizing patterns and connections within the data. We can look beyond finding the needle to finding the patterns that might indicate the presence of a needle. We can truly start going faster than real-time. The same multidisciplinary approach and computational ideas used to simulate airflows or fighter jets, or predict missile trajectories, can now be applied to harness data and unearth actionable intelligence in previously intractable areas. For example, data analytics has been employed to assist in this, the discovery and identification of criminal networks responsible for producing and distributing counterfeit drugs. Using essentially the same tools we use to make sense of political and military turmoil,

we are able to discover the true identities and aliases of key players as well as the flow of money through the illicit network. The power and applications will only continue to grow and spread. Big Data will only get bigger. The more computing devices we connect to, what is now the internet of everything, and the more areas to which we apply complex algorithms, will only expand the information we have prior to making decisions. As data and processing power cease to be a limiting factor, such analysis will revolutionize the way we interact with the world, and measure the risk of our decisions. Meeting the challenge that they represent will always be a matter of staying ahead.

In a world not limited by data or processing power, real-time awareness will not be sufficient. We will need to be faster. Indeed, it has been estimated that the world's data store will grow 40 to 50 times by the year 2020. This exponential growth sounds frightening and intimidating, so how do we ensure we harness this data and not drown in the deluge? However, for organizations, large and small, not tapping into the Big Data trend can easily translate into a missed opportunity. But that, in safety, security, intelligence or business change, that is our challenge.

MR. BRENT CONRAN, CHIEF INFORMATION SECURITY OFFICER, INTEL

In 1974 Intel started with six employees, and today we are more than 10,000. We have had a long and prosperous relationship, and we see this continuing to grow. Today, as we look beyond the internet and the internet strategy, we see that the traditional infrastructure that we have broadly across our global infrastructure is no longer relevant and it is crumbling pretty quickly, and this is our challenge. With all the pressures, on which you have already heard, about social, mobile, analytical, the internet of things that are coming, the deluge of information, the traditional model of computing has been turned upside down. And the fact that we are moving into a model where most of our data will live external from our traditional environment, means that we have to think about how we secure data elements that are specific to our intellectual property, or our ability to keep this information safe. We see that with cloud technologies, and the Cloud First strategy, the cloud is where the sensors are. It is no longer a question of whether or not you are going to the cloud, but how fast

you are going there; we see this as a tsunami, in the way that we compute, and the different and various ways we use it.

We talk a little bit about the amount of data that is coming and ask how do you cut through all that information to offer services, to find out who is this person that is going to get your services, and how you can collaborate in a global environment. This is our challenge, and this is what we need to do in the future to be successful. So some of the enablers to that challenge how we think about what we need to do in the future, and the framework that we are thinking about today, partnering with our friends and trying to figure out the right technology strategies to build that infrastructure. We see a lot of enablers along the way. The way people compute today – my children, for example, they don't even use a computer anymore, they only use a small hand-held device, and they want to compute, and contribute to the corporation, they want to contribute to university. They think and consume information very, very differently, and our systems today are not prepared for this new computing model. We have enablers for the enterprise, our application and our data, how do we get our data into the right model, all of the things that are out there that can help us be successful, build better technology, and provide better services. This is our challenge: how do we get the data out of the sensors and turn it into actionable intelligence? So we have come up with a conceptual design, which is essentially everyone on the outside of our environment. We think about how someone can consume resources, and the crack of that framework is that we think about how to secure data elements, and no longer how we are going to secure the enterprise.

Everyone says that the traditional security model, which we have enjoyed for the last ten years, is collapsing, and I would say that the perimeter just moves. In my opinion, the people are now the new perimeter, and the data that they produce is no longer the data that the corporation produces, but data that the individual produces, and it is important to put the right policies around that data and data element. Data will live in the cloud, data will live in your environment, on your premise, on laptops, it will live in different countries and in different regions, and different laws and regulations would apply to that data. And it is important that you think about the security controls around that data, this is where we will have to go in the future. And then, how do you access that data? Today it is very simple. You come

in using a name and a password, and we believe that you will have to think about access to that information much differently in the future. There is going to be context around the access to information. Where you are, what you are, how you use your devices, important things. Down into the hardware, all the way to the software application, and adapt authentication methods, based on the criticality of that data. And in the middle of that, we believe, there will be policy enforcement points, policy decision points, and policy information points. That may happen in your environment, and that may happen externally to a data element. But you are going to have to think about how people can access information, and never get back into your global infrastructure.

So, information will live in the cloud. How are we going to get someone, from their small firm factor, out to access that information in the cloud? It is going to come with the context on how that person interacts with that data. This is what we think about as we move forward, and we think that most of the information and the context should relate to how people are going to sum these attributes, or how these people are going to be authenticated, in this vast sea of information. Once we have gone through that process of authentication, then we have to make decisions – once I know who you are, what is it that you are going to access in that environment? And that is what these policy and enforcement engines of the future need to be. We are going to take mass quantities of data from the internet of things and from individuals, and from that develop the right algorithms to create a policy to know for sure that this is the person who needs to consume this information. Once we get through that policy and decision point, we have to provide enforcement – in addition to whether or not you should have this information, can you copy this information? How do you consume this information to drive business forward, and make sure that the advanced actors are not people consuming this data?

These policies and forwarding points are gates, and these gates will be how we are going to think about people accessing this information. It is clear that the context that we are going to receive from the internet of things, from the cloud and from how we interact is very, very different, and the traditional model is going to change. We envision a day where our employees go into our Intel facilities and are able to compute and participate in our business, and always be on the outside of that infrastructure. If you think about that model and how that flips, and how

the advanced hackers can take and use that against our environment, naturally you will have to go to the data itself, and think about how you want to secure that data. Also, if you do it that way, where the data lives becomes much less relevant than it is today. Today we build massive databases and massive security apparatuses around that data, and tomorrow we think the data can live anywhere – in the cloud, on-premise, off-premise, on your laptop – it doesn't matter, as long as you put the right security and security model around it. So this is our design, this is our thought. We believe that the data wants to be free, and we think that if we build this model, this conceptual framework, we will be able to compute in a much cleaner and much more efficient method, and into the future.

MR. ASAF ASHKENAZI, DIRECTOR OF PRODUCT MANAGEMENT, QUALCOMM TECHNOLOGIES, INC. (QTI)

I am going to talk about the human factor, and how we address the problem of the human factor in security, as well as how cognitive technologies and humanizing the interface between machines and humans can improve security. When we look at what is cognitive technologies and how we humanize interfaces, in a nutshell, you have the perception, and this is where the device or the machine gather information – it can hear, it can see, it can use other sensors on the device, to realize what is going on in the environment. And then it learns. This is the reasoning part. It learns, and it anticipates what the user will do. Then it takes action, and it acts upon the information and the processing that it got. For example, let's look at how an IT manager, when he comes home, plays with his kid. His son wants to play ball with him. But how can he know that this is his son? He asks, of course, "hey son, I cannot be sure that it is really you, I want to have your password. What is your password?" and the poor kid says, "I forgot my password, I don't know what it is". And of course, well, no problem, he asks when was the last time that they had ice cream together, and he will reset your password. Of course this is not how it is being done, but this is how we are communicating with machines, and it is not intuitive at all.

So how does the human brain authenticate people? If you think about it, it is quite amazing. We know, very seamlessly and automatically, to authenticate people that we have met in the past, and we do it very well

and immediately. We do that by observing – we look and we recognize their faces, and we know very well to distinguish between a video or a photo and a real person. This is not all – we can hear, our brains can recognize voices very well. Even on the phone, when you talk to somebody you can sometimes recognize who you are talking to. And then we also look at the contextual recognition. If, for example, I am on a business trip to China, and in my customers' meeting room I see my son, there is probably something wrong. So we know where we will see different people, or in what situation we will see them. And it has been working very well, for millions of years, so why change it?

All this is part of how the future of authentication will look like. It will use biometric information from the device that you are holding or using. It starts with the fingerprint taken when you swipe your finger. But this is history; the future will have the sensor embedded in the device, so when you hold it, it will automatically take you fingerprint. It will also use voice identification when available, when you talk the microphone will listen and identify you. And then, the camera can take a snapshot of your face or your iris to authenticate you as well. If you have a smartwatch, the device can also capture your heartbeat, which can be used as biometric information. All of this information will be gathered into a processing machine – not just the biometric information, but also the behavioral information, your typical activities and ways to do things. The machine will learn and get to know you, so it will have the contextual information. In most of the phones today, you have accelerometer. You can measure how I hold the device, or how I move, so the device can now recognize me by just picking up the device, just by walking, because everyone moves in a different way. And then I can use other devices – your smartwatch, and other devices that we have tied together – or take other two devices together to increase the reliability of their authentication. When you get into your car you will not have to pull your mobile phone, and start authenticating yourself. The mobile phone will know from your palm, it will know that it is you, and it will open your car or your house, when you get home. Or when you launch an application, it will already know that it is you, so you don't have to use any password or swipe your finger.

This is an example for how humanizing the use of cognitive technologies can resolve some of the problems we have, such as authentication. But there are other ways we can use these technologies. If you have

observed or learned about the recent big attacks on data centers, you will learn that most of them started from a targeted phishing attack or a targeted device of individual contractors or employees in the organization, which allowed the attacker to get into the IT system. And a lot of these attacks today are based on phishing attacks. As our security solutions become more sophisticated, attackers go after the human factor, trying to trick people into giving them information that will be used to attack the organization. It can also be used to get their passwords and other information that allows the attackers to, for example, drain your bank account, or do other fraudulent activities. How do they do that? How do they trick us?

First they need to get information about you, to make it very reliable, and a good way to do that is by using your mobile phone. Applications – we all know these applications that are free and wonderful; except that you usually don't get free meals. You download the application, it is free, it is great, but the question is what this application is doing. It doesn't have to be defined as malicious, because a lot of these applications are up front. They say, "if you download me, I want to have access to your calendar, your photos, your e-mails and your location", and guess what – most people don't even read this, they just press "accept" and install the application. And this is where the attackers start the attacking, by gathering information about you. The application reads your e-mail and calendar, and lets the attackers understand what your role in the organization is, who are the people you are interacting with, and what projects you work on. Then they use this information to their advantage, to launch the targeted attack. In this example, the attacker learns who is the executive manager in the organization of this employee, and he know that he is working with Jennifer Lu, so he uses namedropping, something like "hey, I just bumped into your teammate", to make it reliable, and then he puts in some sense of urgency, saying "hey, I'm in a very important customer meeting, and please send it to me immediately, and by the way, have some problem to access my e-mail, so if you can send it to me to my private e-mail address". This is where the employees get tricked and send information.

How does the future look like, in terms of preventing this kind of attack? The solution is to teach your device or machine to think like humans – only not just like a human being, but like the user himself.

That way the machine can learn and look for the typical behavior of the user: what application he is downloading, at what time he is using this application and in what context, when he is likely to share photos and other things. Then, instead of trying to look for malicious applications running on the device, based on the pre-knowledge this application has, the machine simply observes the things that happen on the device. For example, I downloaded an application and suddenly in the background it decides to share contacts. If the machine is smart enough, it knows that the touch screen is off and the device is not moving, so probably nobody holds it, meaning that the user is not using the device, then why does this application need to send the contacts? From the situation it understands that something is wrong, and it will block the access of this application to these resources. Which means that in our case, if you download the application, and this application wants to send information in the background, the device will block it and will not allow thee application to send the information, without knowing whether the application is good or bad. The device is not looking at that. Similarly, your machine can learn how you behave, and recognize when it is not you. It can know the device has been stolen, and it will shut it off or kill it.

There are many examples for how we can use this technology of machine-learning and cognitive technologies to learn or teach our machines to behave like a human, and to get security benefits by doing so. Until now this technology was mostly used for other purposes, however, this is the time to get this technology and let it help us with security. Every one of us has a super-computer in his pocket, and we can use it to provide better security using these technologies, which may look like science fiction, but they are not. It will all come pretty soon. And the team at Qualcomm, especially the team here in Haifa, is working on this kind of exciting technologies that will improve the security, but also make it easier for us to use security.

MR. OPHER DORON, GENERAL MANAGER, MBT SPACE DIVISION, ISRAEL AEROSPACE INDUSTRIES, LTD. (IAI)

When I have been asked to speak about Beyond the Internet, I thought how far could we go beyond, and space is pretty much as far as we can go. So we well talk a bit about space, and then a bit about cyber space, and then a bit about how cyber can be used against space. We

are extremely dependent on space in our everyday life; you may not know or feel it all the time, but you all know you have GPS and some of you navigate by Waze, but lots of other things come from space. You know what the weather is going to be because we have satellites up there. Your maps that you navigate on come from space. Many of you communicate using satellites, even though you don't know it, not just your television, but also the phones that you talk on. Also, in many regions of the world internet can only be delivered by space, they are never going to get fiber optics too far off in regions of small countries, so space is crucial for almost everything that we do nowadays.

Space is an unpleasant place. Satellites have difficult lives, it is cold and hot, there is vacuum, it is difficult to do the thermals. There is radiation that wreaks havoc with electronics and software. Distances are huge. Orbits are fast. And after you have spent hundreds of millions of dollars building a satellite, and hundreds of people work on it for a few years, you put it on a huge explosive device called the launcher, send it off, and hope it doesn't blow up on the way to space. So you invest heavily in making a satellite work, satellites are very sophisticated but very conservative at the same time. All of you have updated a software on your computer, most of you have crossed your fingers hoping that it would reawaken when you finish doing that. Now imagine doing that to your satellite in space, and hoping it reawakens.

Israel decided to get into space at the very beginning of the 1980s. It was a crazy strategic decision at the time, in fact it would be considered crazy by many now as well. We are the only small country in the world that has full capability in space, to build, design, launch and operate satellites. The others are all huge – Russia and Japan and America and Europe, and China, of course. So it is a big deal for a small country to go into space, this is probably one of our most successful startups. It has become quite a large startup since then, it has become a big business – the space industry is about a billion dollars in Israel now, and the satellites are a few hundred millions of those. We are sort of going back for the startups soon, for actually starting off a small incubator, a startup center for space technologies, to get some more startup entrepreneurship in there. But space is a daring thing always. And for Israel it is a strategic decision, so that we can look and talk far away and see what the bad guys are doing all over our very, very challenging and interesting neighborhood.

Since we started this space program we have launched fifteen satellites that have been performing fantastically. You can't do everything when you are such a small country, so we specialized – we do very high resolution, very small satellites for Earth observations, so we basically take pictures from a few hundred kilometers away. Our preservation satellites fly in about 500 kilometers altitude and take pictures with fantastic resolution. So you can see people and you can see cars and you can see buildings, you can see the bad guys doing what they want to do. We are getting better and better at resolution, and we keep them very lightweight, so they are relatively cheap to launch, but also very agile so you can take pictures wherever you want to look at them, which is very important in space. And because guys like working at night, and they like working under the clouds, then we also have radar satellites, which can take pictures that are very similar to optic pictures, but they take it through the clouds and through the darkness; it looks slightly different, but it is enough to tell us what the bad guys are doing day and night. And we have some of those up there as well. We launch them the long way around: You have all learned in bible class why Moses decided to pick this place, after 40 years of wondering around the desert – but it is the wrong reason. He chose this place because this is the one and only place in the entire region where you have 2,000 kilometers of open sea over which you can launch a satellite and crop off boosters without getting the neighbors worried. The only problem is that you have to do it westwards, and everyone in their right mind launches satellites eastwards, because that is the way the earth rotates and you give it initial speed, but there this theory that if we launch eastwards it will cause some problems, so we do it westwards. We also develop, build, launch and operate – well, we don't launch them, but we operate them – the communication satellites, these are much bigger ones. And they are further away, 36,000 kilometers away, so I think that is pretty much beyond the internet, though much of the internet does go over communication satellites. The largest satellite we are currently building is called Amos-6, it weighs almost 5.5 tons, and we will be launching it in a bit less than a year.

We are actually going out for smaller satellites that are smarter. It isn't trivial, making smart communication satellites, because while they are very sophisticated, communication satellites try to be transparent to the users. You spend a few years deciding what your satellite is

going to look like, then a few years building it, and then you launch. It has to live for 13-20 years in space, you can't fix it or anything. So the operators who are now buying a several hundred million dollar satellite for 20 years want it to do its job in 20 years. Can you predict what communication is going to look like in 20 years? I doubt it. So satellites are pretty stupid, they receive and transmit back down again, without understanding or doing any processing up on there. We are actually starting to do processing up in space, we have a couple of space processors up on our communication satellites, and we are going towards smart processing and communication satellites, where you are actually going to be uploading application to the satellites. That is sort of an internet of things stuff, when you sort uploading applications to satellites 36 kilometers away that you can never reach.

So, if satellites are so important and so sophisticated, somebody must want them not to work. And the bad guys have been trying to take care of satellites, more or less since the time satellites have started working. The first thing people ask is, "well, can we shoot them down?" and the answer is yes, but it is very difficult, and it is quite unpopular. It is unpopular because when you blow up a satellite, you get thousands of satellite pieces floating around in space, and those pieces can start running into other satellites and colliding with them, and when you travel at 7.5 kilometers per second, if you get hit by a small piece it is end of story for you, and then you get hit by a thousand pieces. So space debris is a big problem, people don't like it when you shoot satellites. The Chinese did it to one of their own satellites, just to see if they could, and to show the world that they could. And the US had a faulty satellite of their own, which they shot down in 2008, just one year later, from a navy ship, so they showed everyone that they could too, and they are probably not the only ones. And theoretically you could fly up to a satellite with another sort of satellite, from this one design to refuel it, and grab it and take it away, and move it from its orbit. But that is really difficult, and it is also very, very expensive.

It is easier to interfere with satellites, so interfering with communication satellites is extremely popular in this region. Everyone is doing it, the Iranians very obviously block all sorts of propaganda coming from the US and from BBC and from any other radio. The Libyans and the Eritreans and the Chinese are jamming satellites, and there are even press reports, god forbid, saying that Israel put on propaganda during

the 2006 Lebanon war in Hamas or Hezbollah channels, so maybe we do it as well, I don't know. You don't even have to go to the Middle East to see that, someone jammed the playboy channel in the US a while ago because he was a Christian devout. So it happens everywhere. And you can probably blind and jam observation satellites, although it isn't so easy to do, but this is all for the experts – you need big equipment, big antennas, and once you get caught it is unpleasant. But there is another way in, and the other way in is cyber, which is why I'm here today.

At the other side of the all the computers up on top of the satellite, there are large ground stations with tremendous infrastructure. These do everything from controlling the radios that talk to the satellites and decode and encode and sending commands, to the stuff that transmits to the satellite, with the actual information that goes up and down, and then it goes from there to data storage and to data distribution, and to sending the TV signals everywhere and to customers' CRM systems, etc. So you go from very specialized equipment all the way down to mundane storage and internet stuff, and if you take out the ground control system, then you start making some interesting headway. There has been quite a lot of activity in cyber, it is not talked about very often, because space people are sort of closed, they don't like talking about their vulnerabilities very much. But there are reports from the US that in 2007 somebody, allegedly the Chinese in origin, interfered with a couple of the NASA satellites by hacking into a ground station in Norway, and just about two months ago General Hyten, the commander of the US air force space command, which is also a space in cyber command, said: "outside groups around the world are constantly targeting the satellites network of the US air force, accounting for millions of probes every year". Somebody is trying to fool around with the networks there, and he has a small cyber force of his own, 4,600 cyber people and another 10,000 in reserves. That is what he writes in his website, so I don't know how many he really has. And you have to protect it.

Cyber protection of space assets is something we have started dealing with very seriously over the last few years, as the risks have become clearer and clearer. It is a huge challenge. Not only are we dealing with the normal routine IT stuff, but also with dedicated equipment and embedded controllers and RF devices, which are distributed

all over the world, because we have stations in several different countries around the world, talking to our different satellites. All of these stations have specialized equipment, and you may have to fool around with the software in space to do it well, and you really, really don't want a software to go offline for a while, because it is unpleasant to have a satellite up there when you can't control it. So you have to do extensive and complex testing, and connect all these proprietary systems, and protect them even without having other problems at hand. We have been coupling our space expertise with our cyber expertise, first of all to protect our station, and then to start working with other potential satellite users, to work on their systems as well. It is a layered approach, where you deal with the IT and the communications and then with the dedicated satellite stuff, hardening every type of equipment specifically, and finally go to the sophisticated stuff and to that anomaly detection situation awareness, etc. It is a growing business, with more and more satellites, the operators are becoming aware of it, and we hope that we manage to stay in front of the trend. It is a huge challenge, especially with systems that have to live for so long, and are so very sensitive to off-time.

04

FOURTH SESSION: ISRAELI CYBER SUCCESS STORIES

MR. CHEN BITAN, GENERAL MANAGER, EMEA & APAC, CYBERARK

Our company, CyberArk, went public about nine months ago. It was an exciting moment for everyone, all of us, who joined the company 16 years ago, when we were a team of five people with a dream and a vision, but also for people who joined CyberArk two years ago, and even several months ago, because they feel like part of the organization. However, we see the IPO only as a milestone – an important milestone, yet still a milestone – because we truly believe that market opportunity for cyber is huge. We are turning to the team, to the partners, to the customers, and now to the investors, and we truly believe that we are now starting our story.

The IPO impacted us in many aspects. First, it allows us to continue to do what we did in the past as private company, but in a much higher, wider and deeper scale. Now we focus on activities that allow us to continue to grow our business even faster than what we had in the past, and to really bring expanded offering and higher value to our customers. Another aspect is that the IPO actually opened an opportunity for us to do some activities which are harder to do as a private company. Because of the new position as a public company, we are now looking into more strategic and global partnership processes, including the ability to combine our internal growth with some inorganic growth. We will only do it when it is needed, and we will be very careful in what we do, but it definitely opened us the opportunity to look for more such activities.

There are several approaches to having an idea and getting acquired by a large company. I think CyberArk's story is very different than that of other Israeli cyber security companies, and any approach is valid, of course, but I think it starts from the beginning. When we founded the company it was April 1999, it was the peak of the High tech .com bubble,

and most of the young companies then had a dream, an attractive, sexy idea, and they looked for the shortest path to be acquired by a large company. At the starting point of the company, our dream was very different. We dreamed of creating a real and sustainable company, an Israeli flagship in our industry, and we were targeting this idea. I think that when you build a company with the initial goal to become a large company, you don't look for shortcuts, everybody is unified in the long term goals, and this is what helps us to build the company's foundations, and to become a larger company as we are today.

There are many factors that contributed to the success of CyberArk's success, and I will try to touch some of them. The most important one, which we truly believe in CyberArk, is the people – the amazing team we have created, and the unique things we were able to create. I don't speak only about the most professional people in what they do, but also about people who bring their personality and fit into the culture that we would like to create as an organization. After all, there are many small decisions which are made by companies every day, by a lot of people in the organization. Only if you have the right team, a unified team that work in an open atmosphere, and any individual on the team understands the company goals and examine how the individual can impact them, only this atmosphere can create the ability for small decisions, made together, that can impact the organization and create a successful company. So the first factor is the team and the culture. The second factor is to have the right offering at the right time, something the market really needs, and it must be backed up by the right technologies – technologies and products that are considered the best in the market. In addition, the company has to aim to leading the market at all times, and we believe that to be a leader is not just to be able to do the best you're doing today, but also to collect all the information from your activity in the market, to analyze all this information all the time, continuously, and to know how to lead the market to where it should be in three to five years, and always to work on offering, which should firstly meet the market needs today, but also meet the future market needs. This is about leadership. Two factors, in short, are continuous innovation – CyberArk releases a new product or offering to the market almost every year, which actually expands the value; and continuous improvement, which means that no matter how good you are, always look to be better, always look for the gaps that you should improve.

We are an Israeli company, and are very proud to be as such, and we see it in many aspects as a great advantage and strength of CyberArk. I'll have you know that CyberArk's entire research and development center, as well as our cyber lab research, is located here in Israel, and we are very proud on it, and see it as an advantage. The ecosystem in Israel helps us pick the right people to lead the cyber development, the ones that will actually allow us to be much stronger in the market. And we are proud of it. When you are an Israeli company in the cyber security area, it is obviously good, because Israel is considered to be the capital of the cyber security area, and our CEO always says that you should buy watches from Switzerland, and security products from Israel. So this actually helps us. But it definitely also brings challenges, because there are territories in which we are not allowed to sell, but we try to make the best out of it.

MR. MARK GAZIT, CEO, THETARAY

Last year there were four companies here, 75 percent of them were JVP companies. This year there only have two companies on the stage, but it makes it 100 percent JVP financed companies, CyberArk and us. It is actually a good point to start with, because while CyberArk is about fifteen years old, we are only two years old as a company. We are lucky to have quite a nice market recognition, we were covered by Gartner, and won the Frost and Sullivan best company for cyber security award, and what we do is uncover the unknown. This means that there is enormous amount of data, coming from enormous amount of sources, and there is a need to find this needle in a huge haystack of data.

Why is it relevant to the cyber security, this whole idea of Big Data? Because we face the new world. And the world of attacks has changed during the last years. The hackers are not necessary looking to deface your website, or not even stealing credit card numbers. Yes, it is nice to embarrass people by putting pictures on their websites. But actually the hackers would like to cause real damage, to shut down physical infrastructure and nuclear programs, you might say, to steal real money. There were many discussions about it, and the barriers disappeared. So there are no outside or inside organizations anymore – people with mobile phones are inside the organization, and when the

organization go to the cloud, the organization is, in a sense, outside the organization.

The first phenomenon is that perimeter and rule-based solutions do not work anymore. A second phenomenon is, if you would like to measure the data created by devices, the data becomes unlimited. Take a single airplane as an example. In a single flight this airplane creates about 20 terabytes of data. In a few flights, you fill the entire library of congress, almost every day. And somebody needs to analyze this data, because we believe that in order to catch the bad guys, that would like to steal money, the best way is to look at the financial transactions. In order to catch somebody that would like to take down an airplane, the best way is to look at the engine information, to look at the steering information, the flight information of the airplane, and there is a need to do it in the real-time. So thanks to the works of two distinguished professors, Professor Kaufman and Professor Averbuch – who, by the way, is from Tel Aviv University, so if there are TAU people here, thank you very much for financing the development of the company – we developed a solution-based idea on how to take data from many sources and analyze it in real-time. And that is what we do: we take data from different sources, analyze it in real-time, build an automatic model of the system, and tell customers if something wrong is going on in real-time. It is actually a software black box, which allows the customers to protect themselves against unknown attacks, and make them future proof in a way.

Here is an example, to convert the theory into practice. A financial institution that installed our system felt that they have a level of fraud that they can't identify. Our system analyzes the data automatically, without any human intervention, builds a model of behavior, and when we get a transaction, we tell the customer in real-time if this transaction is problematic. In this case it was loans, and the system found that three fields raised suspicions concerning some loans. The first suspicious field was age, 16-19 years old loaners, which is legal age for financial institution. The second field was transaction size, which was actually less than average. Still totally fine. The third field was transaction type – mortgage. Again, a valid one. So existing systems could not catch this problem. But if you look at the combination of the fields, suddenly you see that these are mortgages given to minors. It was a fraud, and within 50 seconds we saved the bank 9M€. By the

way, in the past such a thing could not have happened. Without cyber you had to get your physical ID, sit in front of the clerk, who would check your age, and then sign physical papers. But now the system is on the internet, and the bank allowed people to get small mortgages over the internet. Suddenly you could change the rules, so somebody broke into the system, changed the age detection rules, and got mortgages for minors. We all understand that if you get a legal loan, or if a bank gave you a loan, legally they can't claim it back. Luckily for this bank, we found it very quickly.

We have other examples with industrial organizations, where we can automatically detect behavior of systems caused by abnormal commands coming to the system. But I think it is all about the value we bring to the customers. Because having good technology is not enough, it isn't enough to become a successful startup. We believe that we give our customers value that they just could not get from anybody else. Not only do we have very high level of detection, because we use machines and we find things that people can't even imagine they should be looking for; but we do it and with an extremely low level of false-positives. We all come from the cyber business, and we understand that there is this tradeoff. If you want to be very sensitive you will get a lot of false positives. For example, an organization with an over-sensitive threshold found themselves dealing with 12,000 alerts, which is an impossible amount to deal with. And if you would like not to have false positives, then you will definitely lose some of the attacks. In our case, the better the action rate is for us, the lower is the level of false positives. For financial institutions, for example, we detect seven times more frauds, but the level of false positive is 95 percent less. The secret is that we don't use human beings – we use machines to build those models, and automatically update it, so the system is always up to date. You don't need to get experts to change the rules, time after time, it is automatic and very easy to deploy, and it is disruptive, mathematically-based.

The best way to position us or to think about us is similar to what you would think about medicine. 20 years ago, people really thought that we will eliminate all the viruses and consume a lot of antibiotics, and then people will only die from obesity and heart attacks, because there will be no diseases. Now we know that this is not true, today there are still viruses, and antibiotics don't work. The same has happened

in the world of cyber security. Today it's impossible to build a system that will be totally immune for all the viruses, worms, etc. Instead, we strengthen the immune system of the organizations, the same way as today, the best way to fight unknown diseases is to strengthen your immune system. And of course it not only reduces operational costs, because we discover attacks very quickly, but it also mitigates potential damages.

Except for the fact that we built this company to look for this needle in a haystack, we believe we should behave as if we were our own customers, and listen to them. And our customers told us: you are not looking for a needle in a haystack, you are actually looking for a needle in a stack of needles, because they all look the same, but one of them is dangerous. We believe that this new world of connected devices creates infinite threats, but also infinite opportunities, and we currently focus on financial organizations and industrial internet organizations, but of course the system can do much more. To summarize, we face real need, where the rule-based systems are just not enough.

MS. MARIA LEWIS KUSSMAUL, CO-FOUNDER OF AGC PARTNERS & PARTNER IN THE INVESTMENT BANKING GROUP

I am not a cyber success story, but I have had the privilege of working with more than 73 entrepreneurial teams that did represent cyber security success stories, including the Israeli Safend, Aladdin, and also Finjan. I am going to try and give you some of that collective experience of twelve years and 73 cyber transactions, in terms of what does it take to be a cyber success story.

We are going to look at four areas. The first is the market backdrop, because part of your success is going to depend on market psychology, investor enthusiasm for the space, as well as fundamental demand. We will also look at some of the micro factors, such as what you need to do with your teams as individual entrepreneurs to achieve success. We will look at some of the common pitfalls, things to be wary of; and finally we will talk about a couple of cups, as we like to say in investment banking, or some cyber success stories that we have had the privilege of participating in. So let's take a quick look at the market. This is a very active and growing capital market. Looking at the number of security M&A deals over the last 5 years, in 2014 we

had almost 200 reported transactions, and in the first quarter of this year alone, we are at 73. So there is an insatiate appetite on the part of global acquirers for security DNA – not just security companies, but digital companies, telecommunication carriers, MSP software companies.

Everybody needs security DNA, and investors are only too happy to foster the growth of that DNA. We had seen almost 200 security transactions in 2014, these are financing realms from early stage to late stage, and 40 transactions in Q1 of 2015 alone. I look to collect the dollars that have gone into cyber investments in the trailing twelve months – this is the accumulative amount of reported investment. As everyone here knows, many times there will be a gap between when funds that get raised and when they get reported, but this is in the twelve months ending in March 2015, and if you add that up quickly, it amounts to about $2.75B – a total of $7.2B over the last five years. A billion dollars to cloud, almost 500 million to network and data, 300 to identity management, and you can see some of the active investors here.

There is an unprecedented amount of capital going into the cyber space, so that may beg the question, is the market overheated? Is it frothy? In 1999, at the peak of the NASDAQ bubble, the NASDAQ trailing 12 months, revenue multiple was 8 times. The peak of recent security IPOs was around December of last year, when FireEye bought Mandiant, and I think was trading in about $80, and so you'll see that those revenue multiples are equivalent to the peak of the NASDAQ bubble. I look for some other signs of the market. The RSA trade show in San Francisco each year is the industry's largest conference. In 2009, after the 2008 global financial meltdown, there were 53 exhibiting companies there, and most of them did not call themselves security companies, but compliance companies – because that is where the budget dollars were. Compare these data to the number of exhibitors this past year – 501, and they were companies who had raised series of $30-50M, with boost the size of vendors, who had ten or fifteen or even 50 times their revenues. Because in many cases they did not have revenues. And in the last corner are the unicorns – private companies that achieve a billion dollar evaluation. Unicorns are also mythical creatures, and so you don't necessarily know whether they will sustain that evaluation at the end of the day.

What does it take to be a cyber success story? First, prioritize the mission – it is about what you are building. Solve the problem you set out to do, and the rest will follow. Tackle the hard problems: web security, DOP, insider threats, APT. Operationalize the solution, since you cannot expect to drop your new platform in an ecosystem filled with a workbench of security tools, you have to make it synergistic with these tools and operational. Match capital to milestones, don't raise more than you need, and know what you are going to achieve with the capital that you raised. Choose your advisories and your mentors well. They are the source of your relationships, customers, and experience.

Recognize the capital is a means to an end, don't treat it as an end to itself. Just as CyberArk said, you don't celebrate the IPO or the $15M round, but utilize that capital and celebrate the milestones that you achieve with it; and recognize evaluation only matters when it becomes cash – those billion dollars unicorns remain as such only until somebody buys them or they go public and realize that their return, it is a meaningless number. Pilot customers, banks and government agencies who will try one of anything, they are great, except a lot of that stuff ends up as shelf-ware – what you need is real customers that will really deploy your product in scale. Lastly, comparisons are odious. What I mean by that is, just because the company that your cohort in 8200 founded had no revenue and got sold for 200 million, doesn't mean that your company is worth 200 million. Your technology may be as good or even better, but you know what, life is not fair. It is worth what somebody is willing to pay at the time an offer comes.

Lastly, a couple of the success stories, to show how a number of these companies have used capital wisely. A good one is Mandiant, we helped them raise $70M in 2001 and get a $145M in valuation. KP came in, as did One Equity Partners, helped advising and growing the company, and 2.7 years later they sold at twice the multiple, and made a billion dollar exit. So, concluding thoughts: cyber threats are endemic; industry leadership is clearly in flocks; there is a tremendous opportunity to jump to the top; demand for effective countermeasures is high and rising, capital availability is unprecedented, valuations are high, and cyber talent is scarce. So it is a great time to be a cyber entrepreneur.

What I love about Israeli startups is that, first of all, you are pragmatic in your approach, energetic in your execution. My advice to Israeli

startups would be: number one, don't lose that. Number two, think globally, not only in terms of customers, but also in terms of capital and business development context. It is very important to leverage the ecosystem on your behalf. Whether it is finding go-to market partners, technology partners, or ultimate acquirers, you should be getting those, that vision of who you are and you value out early. Number three: don't sell out early. There are opportunities to build great new leaders out there; platforms companies that can deliver in this next generation of technology, what the protective and preventive companies did in the first generation. So I would say, use your capital wisely, grow globally, but build something sustainable, and I would rather see you as a source of cash, buying the companies that I am selling, rather than selling you early.

05

FIFTH SESSION: CYBERSECURITY AND PRIVACY – VIEWS FROM GOVERNMENT, INDUSTRY AND ACADEMIA

MS. MAUREEN K. OHLHAUSEN, COMMISSIONER OF THE FEDERAL TRADE COMMISSION, USA

The FTC is a bipartisan law enforcement agency in the US, with authority over commercial practices. We don't play a role in national security issues, but more in issues of how companies collect, secure, use and share data about their consumers. We are also an antitrust agency, and later I will discuss that in connection with sharing cyber threats information. What is the FTC's role in the cyber field?

We have two types of authority in the consumer protection area. The first is deception: if you have made a promise to consumers about how you are going to collect their information, share it and secure it, and you don't meet that promise, you can be liable to the federal trade commission. But most of our work in the cyber security area is focused under another type of authority we call "in fairness". If you have sensitive consumer information and you have failed to secure it, in a way that raises the risk of harm to consumers, and the FTC can bring an enforcement action against you, if you operate in the US. We have probably more than 50 data security cases against some of the biggest companies like Facebook, Google, Twitter, HTC, etc., anything that has an impact on consumers. Sometimes it can be a third party in the chain.

If you have failed to take reasonable precautions to protect the data that you hold for consumers – and there can be precautions against outside threats or even against insiders, when someone unauthorized in the organization has access to the data – the FTC can bring an enforcement action. We have also brought many cases involving spam and spyware. We try to keep up with the evolving threats that all of you are facing, and try to counter them.

The data privacy and cyber security are part of the larger privacy mission at the Federal Trade Commission. If you have information from consumers and you fail to secure it or protect it appropriately, that can certainly have a privacy impact on consumers. One of the things that companies have said they would like to do is to be able to share some of the cyber threat information, so that they can take better steps to protect themselves, and one of their concerns is, could that raise any trust concerns? When you have competitors getting together and they share information, often that is something that any antitrust enforcer looks at with great suspicion. One of the things we have done in the US, was to make the Federal Trade Commission an antitrust enforcer, much like the US Department of Justice. Last year we issued joint guidelines to give companies some comfort about getting together to share this kind of cyber threat information, to tell them that we don't perceive it as commercially sensitive information, and that we would not be concerned about competitors sharing in this regard. We stated that we are trying to allow companies to have room to get together and to try to take steps to better protect consumers. I think our discussion will also talk about this. As I mentioned, we see data security as a subset of privacy at the FTC, but sometimes privacy and security can be in tension with each other. Sometimes security means that we want to know more information about consumers, we want to know more about who is using this service, who is taking these steps. And that can sometimes be in tension with privacy concerns. Certainly there are other concerns about liberty, public discussion, and freedom of expression, that all come into play. I think this makes privacy data security a particularly interesting area for debate, and I look forward to our discussion.

Concerning the issue of "reasonable data security" in the absence of specific regulatory statutes, this has really become a topic of great interest lately, because the US congress has been considering whether there should be specific data security in breaching legislation. In the US we have some sector-specific regulation in privacy, so for financial and medical information there is a certain level of privacy requirements, but for all the rest of it, it is the federal trade commission. A question we get is, should the FTC be writing specific rules for actions and protocols that need to be taken, and we try to resist that. This sector is incredibly technologically fast-moving, so it would be very difficult for a government agency like the FTC to write a specific rule. Instead,

we focus on whether companies take the right precautions – more of a process-based kind of approach. Do you know what information you have? What promises have you made to consumers? How do you secure it? Who has the access to it? Are you checking that the third parties with whom you are sharing it are doing what they told you that they would do with it? And do you have trained your personnel on the types of cases that the FTC have brought in this area? We focus on what we consider very basic failures of data security, so in failure to train, you allow your employees to install file sharing software on their computers, which contain people's medical information along with the pirated movies that people download, and there are backup tapes that are just stored in somebody's car, and someone's network password is "password". Those are the kind of things that seem like a low-hanging fruit, but we brought a lot of actions in that area. Again, we don't have a specific rule that says "use this, use PCI compliant", etc., it is more like, are your precautions reasonable, given the sensitivity of the data that you have, the size of your organization, and the cost of taking those precautions? This is what is important to us.

Sometimes there are attacks businesses just can't deal with. There are parts of the US government that may give advice or guidance, or have requirements about network security and such things, but the FTC actually investigates many of these data breaches. One of the things we look for is systematic failures. It is not a strict liability standard – you have had a breach and therefore you are liable – because I am not sure that it would be an appropriate standard of companies to be subject to.

Some of these threats and attacks, like in the Sony case, are Nation-State attacks, you can't necessarily assume that an individual company can withstand that. So, when we do these investigations, we look to see if you have taken appropriate precautions, trained your staff, kept up with the patches and the well-known threats, or disabled certain features, and then failed to re-enable them. One of our cases was against a well-known app called Fandango, that had disabled cell to cell certification while it was going to data testing and then never re-enabled it, which allowed man-in-the-middle attacks. This is the kind of things we look for. But for every investigation that we bring a data breach enforcement action against, we have closed about two and a half investigations without any such action. So it's not a strict

liability thing, but more of a spectacular failure of protection, like systemic kinds of approaches, that we look for.

The other thing we try to do is to give guidance to companies. The biggest companies have lawyers and security experts to guide them, but many of these breaches happen in medium and small-sized businesses, and they can have consumer harms as well. So we try to give advice to businesses, and particularly to reach out to the startup community, because they usually try to create something so quickly and sometimes overlook some of these basic precautions. We feel that consumers are better off if we can give companies some information, so that they can take the appropriate precautions to prevent such consumer harm from happening. That is a better investment of our resources.

If companies share cyber threat information, it seems unlikely to me that they would need to share the personal and identifiable information of their customers, such as their names and credit card numbers, for example. But I think that in cyber security there is also this issue of authentication, we want to make sure that the person accessing this service or database is the right person. And how do you do that? Often by collecting additional information about that person. Once you have that information, collecting even more information can help serve privacy. It is somewhat counterintuitive, that sometimes you collect more information to better protect privacy and security through data security. But the issue is safeguarding credentials, safeguarding the kind of authenticator that has been used in that regard. Every time we collect more information to authenticate it is indeed you, we check how that information is stored; this is a challenge that we discuss and we do a lot of policy work about at the FTC. Once we go to biometrics, it would be harder to change than your password and hack into your account. But so far it is a challenge, a little bit of an arms race.

We can't have perfect privacy, perfect security, open commerce, free innovation, all of it, we can't maximize all values at once. There will always be tradeoffs. But I think that there are tools that can be used to minimize some of the effects of privacy. You mentioned using machines to do that, and we certainly have anonymization, hashing, differential information, or techniques – none are perfect, though. There is no perfect solution for everything, but there are reasonable steps that can be taken to balance between the concerns of safety

versus privacy. One of those steps is de-identification of information. However, as I said, there is no perfect de-identification. With enough computing power thrown at it, you can probably re-identify everything, and I think that the question is always compared to what you lose versus what you gain. I think that everything can be re-identified, but it would be extremely difficult. Also, are you sharing it with others who have made a promise not to re-identify it for their uses, and is their promise enforceable? That's often what we look at, at the FTC – have you de-identified the data, how have you used it, have you re-identified it in a way you promised not to, or have you shared it with someone who has not made a promise not to re-identify it? It often comes down to more of a contractual kind of approach, saying you are going to have access to the data, but you have to promise you will not try to re-identify it.

Judging by the number of very well-known technology companies that we currently have under order for privacy data security violation, I don't know whether we have been successful or spectacularly unsuccessful, but we definitely got their attention. Our approach has been that you don't need permission from the FTC to do things, but you need to keep the promises you made to your consumers, and make sure that your practices do not cause them substantial harm. We define substantial harm as a risk to a consumer's financial information, medical information, health and safety information about their children, and we recently put out an internet of things report. We did a workshop on that, and we didn't recommend any new internet of things legislation. What we said is that the basic rules still apply in this new world, and that companies should make sure to take steps to protect consumer information and consumer privacy in this space, particularly in an emerging technology, and make sure that consumer and market confidence can continue to grow in this new area.

MR. AMIT ASHKENAZI, LEGAL ADVISOR, ISRAELI NATIONAL CYBER BUREAU (INCB)

What the National Cyber Bureau has been doing is similar to the question and the policy issues faced by many democratic states in this space. We see more cyber attacks, more advanced potential damage, and sometimes damage happens in the private sector, and countries ask themselves: what is the role of the State here? And specifically

for this discussion, what is its policy role in legislation, regulation, facilitation of what is going on in the market?

When we approach this issue, we have to take note of two things. The first is that before it was called cyber, this domain – the internet, our smartphones and our social networks and everything else which is now cyber – was a type of a sacred domain in the eyes of the law, in the sense that the law and its institution and government basically stepped aside, and let innovation and information flows and financial transactions go on without the government bothering them. Many western countries, including Israel, had a policy of non-intervention, so to speak. The other issue that is important to set the scene is that in this space, the State, its organs, cannot do effective defense without cooperation of the organization, because the cyber defense "battlefield" happens within organizational networks. So if Sony was attacked, it doesn't matter what high facility type of team would be sent in. The amount of man-hours that were invested in networks before this attack requires any type of sensible defender to do this defense exercise with the people that manage the network daily. There was no override of the defense scene, and this is not the case in other security areas, where the police or the army comes and closes the area, and conducts the battle without people interfering.

With these two problems, the policy fashion in Israel, which was numerated in two government decisions from February 15th, includes two elements. The first is something that we see in a lot of western countries, dealing with the State's offline role. We call it "offline" because it is the straightforward incentives regulatory roles, telling organizations to become more resilient, mapping to information security standards, and this policy process is based on several concepts. The first is government leadership – everything we want from the private sector, we apply to government, maybe even government by example. In our cabinet decision 2443, for instance, we want ministries to spend at least eight percent of their IT budget on cyber security, and we set up an institutional mechanism within the ministries to manage the cyber security issues, which are out of the IT department; these are management issue of buying from the top. This type of accountability scheme is important in order for the government to say, "this is how I see cyber security resilience going on in practice". The other element of this decision is that we are not appointing a new regulator, but expect

each regulator in the government to deploy cyber security insights within its existing regulatory functions, except for the regulator of cyber security services market, in which we see a vacuum at present. In this area, more work needs to be done in order to make the service security market more efficient, because if all this pressure is on firms to buy cyber security services, there may be a lack of understanding by clients and service providers about what the services, their nature and quality are, and then some of the spending for cyber security may be inefficient.

The second element of the policy is the online role of the State, or the fire brigade metaphor. The fire brigade comes to help and to assist and to locate fire even before we catch the guy who set the fire, and in this context we need something to mitigate attacks even before we mitigate the attackers, so we need an online role for the State. One of the major elements of this concept is CERT, Cyber Event Response Team, which acts in the online world. But we bring governmental assets into this operation, and it is going to be within a national cyber security and defense authority. This mission, of creating a legal authority for cyber security defense, has two advantages in this space. One of them is that this space is not an extension of something that has happened before, so you need somebody that looks at this space, coast to coast, if you like. It is not a legal issue, that this space requires a totally new doctrine. We look at things strategically, and this of course is a very valuable thing in the cyber security civil right intersection, because we have an authority that is focused on what is going on in the machines, and they are not interested, at least at first, at what their users are doing. In this sense, we are different than other agencies that are interested in the cyber domain.

When it comes to the State's role in cyber security, we believe the online and offline defense models are complementary; you need both capacities. Of course organizations have to put in defenses in order to manage their daily security. but then I think one of the most illustrative examples is the infamous Target breach in 2013. Target was PCI-compliant, and PCI is quite a tough standard to be compliant with. This is what the INCB head calls, "not the advantage of being big, but the advantage of being small" – being a smaller country with a smaller administration may be an advantage that we can leverage here, in Israel, and put these functions within one body.

The government, on the other hand, has a role as a monopoly of legislation and policy making. There are many things that companies can do to better protect themselves, while government can create a more facilitating legal environment. An offline action, something that says, "this is legal, this is something we can do and you can do", immediately enables companies to better defend themselves. I think one of the most successful operations in this area in the US is the FS-ISACs, which shares information between financial institutions without the government, but the government said it was okay, so government has a role here in creating a friendly environment. We see it in other areas of the law as well, where the government doesn't have to do anything directly, but it has to move aside obstacles or engineer the law in order to enable more effective defense.

On the issue of cyber threat data sharing, and legal obstacles to that, there are antitrust issues about which the FTC and the DOJ issued a joint statement; they want to pursue this type of sharing for cyber security purposes, and there are impediments, and I want to focus specifically on the tension here between data security and privacy, to lay out the arguments. From the data security side, you want to collect as much information as you can in order to see the correlations and trends, and detect this needle of a threat in the haystack, and to be able to deal with it. On the other hand, from the privacy side, the more information you collect and analyze, the more privacy risks you create. I wonder how you see a solution or mitigation of this tension, considering what happens if you can't find the needle in the haystack, or if you don't create the haystack. On the other hand, inevitably, if you have the haystack then you sometimes have serious threats to civil liberties.

This discussion which has become very heated in the recent years, but it is a bit more simple in the cyber security domain, because we focus on how our cyber ecosystem functions, and our major aim is not what people think and do, but what machines and other things do, because this is what our forensic analysts are looking for, and this is where we see the signs and the trends that trouble us. The other thing that we have at our aid is the fact that we have a specific mission, which is focused on the cyber security, and as mentioned before, in many areas cyber security promotes data protection and privacy. Some of the major cyber security events are actually data

breach privacy events, so these areas merge. Another thing is that we have to utilize what we know about smart designing of systems and mitigating these risks. Indeed, many things can be collected, but then, the access is by a machine process, the algorithm is calibrated in a certain way, and further uses of the information are strictly regulated by processes. Therefore, it is not just a big haystack that anybody can go on looking at, but technology can help us in streamlining the way we use this information, and again – remember that we are looking for cyber security-related information, and not other things, and this helps us. Of course, it will be naïve to say that this is a black or white solution. It is a gray area, where we have to develop policies smartly, and each side – data protection, privacy, and cyber security – has to look realistically at what technology wants, and what are the actual risks, at the end of the day. I think we should do what we can to mitigate privacy risks, and do the cost-benefit analysis at the end.

One of the questions is how to make this distinction between data about the machine, as opposed to data about people. One of the things that came from the cabinet decisions, which set up the authority, is that the national CERT has to operate according to the principle of taking into account basic rights; and the attorney general in the ministry of justice, which is the highest legal authority in the Israeli executive branch, is looking at it from a human rights perspective – they sort of check on what we are doing. I think the answer here is in the details; not every time we need everything from the content, and a lot of information sharing is really technical and does not relate to content. So this is something we can work with, and if you add to this the ability to calibrate machines to do most of the scanning, then the event when you need to look at content will be triggered by something. I will get a bit more technical here, saying that it depends on whether you are looking at revealing a trend, or actually investigating a cyber event. When you investigate a cyber event ex-post, after something bad had happened, you obviously need access to everything, but we are talking about things you want to do in order to mitigate things in advance. You want to have some sort of radar for cyber space, and look at where the bad things are coming from and where they are going in your systems. At this point, you don't always need to inspect every bit of content by a human. Basically, we can differentiate between information that is not privacy sensitive, metadata, and things that may be privacy sensitive, but we try to create an algorithm or funneling

system in which these events are very minimal, and then you have to escalate in your permission list in order to enable things. Of course, when such a process happens it leaves traces, so you can perform an audit about who did what and why. I think these are the basic mitigation practices in any type of system that deals with sensitive data.

Basically, we have two tools we use – technological, i.e. good-enough de-identification, as well as a commitment not to re-identify and downstream obligations that we impose on our service providers, business associates, etc. To take the discussion a bit further in the technical sense, let's look at the ICO, the Information Commissioner's Office in the UK, who is also the commissioner for freedom of information – the law that makes you want to publish things, and today we are talking about publishing databases. They have a conflict of interest between publishing things and protecting privacy. They published a very good manual on anonymization, with many tools, the utility of which is contextual – in some cases it would be anonymization, in other areas it would be tokenization. I guess what you would look for in the specific context is to answer the questions: what would be a reasonable attack be against this type of de-anonymization technique, and is it reasonable in the context use – because if it is not reasonable, I don't see it as a problem. Also, you always have to carry a big legal stick for everybody who accesses the data, in order to create penalty, so that people won't try anything silly. It is also symbolic. I think that in the cyber security context we can be more optimistic than in other areas, since here the privacy and the value dilemmas that we face every day – as consumers, as parents, as people, what is privacy on social networks and so on – are a bit simpler. Because the context of the use is security, it is something that people basically want, and if you can give assurances that you are focused on security and not on other things, such as marketing to people, which is the basic use in data, maybe there is less danger of conflict of interest, de-identification, etc.

The approach of the bureau is "very light touch". When we talk about doing the online activities, we build partnerships with firms, and in this space we will have to be very attractive, and convince firms to share information with us, to trust us. This is an issue that will have legal implications, what we promise and how we create their trust, that is why we will have robust privacy protection in our processes, and we will also apply them outside the domain of PII, Personally Identifiable

Information, but also about the company's sensitive information, so we apply the same processes there in order to create trust. In this context, I think that on the one hand, bad thing are being said about government, and some of them are true, but on the other hand, in this space we see more and more calls for the government to come in because of the amount of risks, calls for governmental intervention and assistance in order to help firms deal with the challenges of cyber defense. And the government has to do this very carefully.

24.6.15

OPENING SESSION

DR. GIORA YARON, CHAIRMAN OF THE EXECUTIVE COUNCIL, TEL AVIV UNIVERSITY

I want to focus on leading the next frontier for cyber security. We believe that in Tel Aviv University we basically have all the essence to lead data revolution and data frontier. In Tel Aviv University, like any university, we are primarily being measured by research, and we research areas where we feel that we are either number one, or have a great opportunity to become number one. However, in Tel Aviv University we have taken upon ourselves another charter: we feel that we don't only need to lead in research, but we also need to lead in making an impact, on both the economy and national defense. In most countries it is good enough if you create an impact only on the economic systems, but unfortunately, and with our friendly neighborhood that we live in, we need to make an impact in other places, and we set the bar relatively high.

The impact we would like to make, is similar or even better than the impact Stanford University has had on the US economy through the Silicon Valley. A very high bar, if you will. How do we think this should be done? Looking at the computer revolution that is in front of us, there are three phases. The first phase, which now looks very simple but at times may seem very complicated, is when you have a computers center and a variety of software, CRM, ERP, that are used to manage the company. The second phase, in which we live today, is the internet, where we have hundreds of millions of contact points, customers, companies, individuals, connecting the cloud, and as Facebook has reported, this number now exceeded 1.4, or let's assume even 2 billion contact points. The phase that is coming in our direction is the IoT, the Internet of Things, or the Internet of Everything, where we are going to have anything between 25 billion to 50 billion contact points, which means that every one of them can service a window, a door or a chimney for malware for Trojan Horses. If you want to look

at another way, there will be 25-50 billion contact points over which there is a layer, not of Big Data, but Very Big Data. And you want to run analytics on it, on quality data.

In this respect, we can and should come to play at three areas. The first one is educating the next generation, so that they are better than we are. I always used to say to organizations I ran, "I am happy to report that if they had to accept me as an employee, most likely they would have not", i.e. we want to continue raising the bar, and the first chapter is to educate the next generation. In Tel Aviv University we have, for example, industrial engineering, computer science, electrical engineering – each field includes another several sub-disciplines.

The second area is the primary objective of an academic institution, to conduct research. We have research in a variety of areas: mobile, cloud, image and video recognition, critical infrastructure, etc., and it has been supported by the Blavatnik Center with a variety of financing means. But to conduct research you also need a roof over your head, and indeed, Check Point has contributed the Check Point building for computer science, so not only will we have the research, the students, the programs, and the money, but also a roof over our heads to conduct that research.

After studies and research, the question is: how do we create an impact on the economy? We have raised a fund called the Momentum Fund, where two major investors, Tata and Temasek, have invested $5M each, to get the visibility to the next generation innovation. That allows us to breach the gap between end of research and beginning of commercialization.

The last of the three areas I mentioned earlier is the Innovation Entrepreneurship Center, led by Professor David Mendlovic, which focuses on teaching, mentoring, and acceleration modules, all in order to lead the entrepreneurs to better work. Generally speaking, it enables the entrepreneurs to make the first steps towards commercialization. Basically, you have the science side, and our industrial partners, VCs that know how to build companies and help in building and running companies, provide guidance on the business side, and all that is recorded by the Tel Aviv infrastructure, which had allowed that to happen.

Why do we believe that we win? Very simple. Tel Aviv is ranked on the 9th place among universities worldwide in the numbers of companies created by entrepreneurs who came from academic institutions. We are the only academic institution in Israel that got to the top-ten list. Last but not least, when you look at economies from several months ago, you see that little Tel Aviv is second only to the Silicon Valley in terms of density of startups, while other big cities like Chicago, London and Moscow getting the 10th, 7th and 14th place, respectively. I believe that if we do it right, we have the chance to take both the economic ecosystem and the national defense in Israel to the next level.

06

SIXTH SESSION: REINVENTING CYBER SECURITY

MR. DAVID KEREN-YA'AR, SCIENCE ORIENTED YOUTH

My name is David Keren Yam, I am fifteen years old. Seeking challenge in math, I joined The Scientists and Inventors of the Future program. As part of the program we study various topics, such as Python and C programming, Discrete Mathematics, Linear Algebra, Extended Introduction to Computer Science, etc. I have many friends in the program and outside it, and we plan to build a world together. The program taught me to appreciate computer science, and I want to deal with artificial intelligence and human machine interface when I grow up.

MS. SHIR VELTSMAN, SCIENCE ORIENTED YOUTH

My name is Shir Veltsman, I am 14 years old. I started my way in science at high school. I chose to learn computers and physics. I study at the MOFET program in the scientific technology reserve. Two years ago I learned math in a special program for children in Bar Ilan University. Last year my teacher sent me an e-mail about the Scientists and Inventors of the Future program in Tel Aviv University. We chose several courses, one of them was cyber. I chose to learn cyber because I thought that this subject is interesting, fascinating and innovative. This program is also a place to meet friends. This year I had the honor to meet smart and lovely students in my age. In addition to the two days a week that we study together, we also hang out on the weekend and have a great time. In my first year, I learned to program in C, Python, and Assembly, as well as Discrete Mathematics. When I grow up and join the military, I want to help defend our country in a cyber unit. In the future I hope to learn and work in the field of cyber and the human mind. I hope that next time we meet I will tell you about my new research.

MR. GIL SHWED, FOUNDER, CHAIRMAN AND CHIEF EXECUTIVE OFFICER, CHECK POINT SOFTWARE TECHNOLOGIES

I think Israel has a great ecosystem with many good ideas and great entrepreneurs. I think the challenge that entrepreneurs face, all over the world, is that there is too much "us or them" – too many good ideas, too many companies, and if you just look at the ability of the buyer – in most cases the head of the IT department in any company – to absorb all this new technology, it is almost impossible. When I started Check Point, every year there were one or two new big trends in technology, and in each area there were three companies competing to be the best. Every company, every idea, got the chance, and every company that was really good got the chance to lead. Today there are thousands of new companies every year, technology buyers cannot look at everything, which makes it very hard for both the startups and the largest companies to promote completely new products or categories. From the macroeconomic perspective, the amount of invested money has to be divided not amongst the top 20, 50 or 100 companies, but amongst 5,000 companies, which makes the share of everyone smaller. I think that is a global challenge, and that the market powers have to take care of it.

We have programs and collaboration with many small Israeli startups, and we think that they are a great base to kick up abilities in our products; but at the end of the day we have to remember that startups have to fight for their future. It is not just collaboration with other people that will take care of them. Every entrepreneur has to understand that they are going to go into a big struggle to find their unique place in the world, to prove themselves to the world, and be winners on their own.

I think that in general, large Israeli companies in the field of cyber that buy companies outside Israel, try to keep their intellectual property and their people abroad, so they are not forced to work according to the regulation in Israel. That is not a good phenomenon in Israel or anywhere in the world. It is better for the country to have a little control over having no control at all over what is being done. One thing that the governments have to remember today is that in the internet world, companies can move everywhere they want very quickly, and there are no physical boundaries anymore to where a company should be. Israel should become a much more attractive place for companies that want to base their people, their intellectual property and their

profit there, because the world is open, and Israel is not the only place in the world.

I think that the future definitely holds challenges for us. We need to have more students for computer science – take a look at the big universities in Israel, where the number of computer science students has not changed in the last 20-30 years, with the exception of Be'er Sheva. There are only a few hundred students every year, but the demand in the industry is bigger, and if we can get these excellent universities to double and triple the numbers of students, that can have a big impact on the universities and mainly on the economy, with better supplies of excellent people that universities have. Another thing that can be done is to attract companies to Israel. A few years ago there was an initiative in the government to simplify the rules in order to attract companies to Israel, but in the last three years this initiative has been neglected. As a company in the industry, we feel that while there are many government officials that understand the need to attract new companies, in practice the government tells companies to leave the country, or not to come here. In this situation, companies will either move all or some of their operation from here, and growing companies might simply leave the country altogether.

On a more personal level, I would like to believe that we will continue to lead the market in the future, perhaps sometime maybe create new markets. 20 years ago we created the internet security or the Firewall market. Today we invest in mobile security and in all the new technologies in threat prevention, and we believe that we have the best products and the best architecture and the best solutions, but it is still for us to prove it, and that will be our journey for the next 20 years.

MR. AVI HASSON, CHIEF SCIENTIST, MINISTRY OF ECONOMY

Looking at this industry growing from year to year, I think it shows the great potential we have. From our perspective, 2014 was a great year for cyber, mainly integrating startup raising money. Looking at what Check Point and other companies do, 2015 is shaping up to be just as good. But we are in Israel, and as the former president Peres says, the biggest contribution of the Jewish people to the mankind is dissatisfaction. We are never satisfied. I want to talk about the challenges, the things we see as problematic. The fund raising is

strong, and many companies raise money – which is obviously good, because venture capital is the fuel to the technology industry – but this still does not reflect in sales. We see many small companies now find it hard to penetrate to the customers, to create a scale deserving to ramp up.

I believe that the most important word in the world of innovation today is collaboration, and many challenges can be overcome by collaboration – primarily between industry and academia, which is relevant to this place, but also between companies. Big companies can work with smaller one because they can both benefit from it.

We in the government can do a lot to reduce some of the risks, because we want more people taking on that important challenge. Multinational companies come into this country to set up R&D centers, leveraging the innovation ecosystem, but we also see some Israeli companies that go the other way around. Focusing on the role of government, we have the OCS incentives that take off some of the financial burden, and we know that many times our R&D funding is an essential consideration for companies when they make a decision. We also have regulation, which is important in the world of cyber security, and includes export control policies as well as intellectual property limitations, and as such can be meaningful. As Chief Scientist and promoter of the industry, I think that we should be as open as possible to promote the industry without harming national security, and there should be balance. But apart from national security, there should be no other factor impacting the regulation.

In Israel we have a very strong ecosystem, and a lot of what we do is to worry about the next 20 years. From our perspective, the last 20 years were all about creation. It started with the forefathers of the Israeli high-tech here, in the late 1980s. There was very little high-tech in this country back then, and in these 20 years – and I believe the government played a positive role in that – an ecosystem was created with factor capital and human capital, with stronger industry-academia collaboration, and with great support for entrepreneurs. I think that the next 20 years are going to be about keeping our leading position, because we worked hard to get there. We also ask ourselves how we can increase the economic impact, and in the field of education, how do we increase the number of students, both in high schools and in academia? We also wish to bring that innovation notion to larger

sectors within the industry and the country in the next 20 years. This is one of the reasons for creating the new national administration authority for technological innovation, because we realize that we can't keep doing what we have done.

07

SEVENTH SESSION: RETHINKING INNOVATION

MR. MATT THOMLINSON, VICE PRESIDENT, MICROSOFT CLOUD & ENTERPRISE SECURITY

I want to start by talking about innovation in defense – how to make sure that as we have an innovation, we can actually roll it out into the fabric of the internet and cyber space? I call that "persistent security". Over the years I have seen many proposals, many ideas, many technologies, startups, pitching ideas about how to secure the platform. And I have seen some common failure modes for some of those ideas, which I want to highlight here. I think that talks to what sort of innovation we need, and what sort of problem we need to solve when we think about new technologies and innovations. But first I want to talk about the opportunity.

Do we have too much innovation in cyber? I think it is hard to argue that we have just the amount of innovation we need today, that we have solved the problems. First, the problems that we are trying to solve for are changing, it is not static. 50 billion devices will comprise the internet and cyber space by 2020. Data volumes are surging, all these devices are going to emit and consume more information, CIOs are looking to move their enterprises to the Cloud and take advantage of that, platforms are changing, it gets harder for enterprises to contain and manage the systems that they have. I think that there is a big change here, and a challenge for us. The attackers are not static either; over the last few years we have seen that it is not just about a single vulnerability, it is about cross-industry vulnerabilities.

When a vulnerability comes out, whether it is in Apple, Google, Microsoft, etc., everyone responds in the same time frame to try and close these issues. We also see attackers going up and down the stacks and various layers. We have seen destructive attacks, we have seen the APT, the slow and low attacks, and we have nations investing in

offensive capability and bringing the might of leading militaries to bear against commercial entities. Attacker trends are also concerning, which captures the attention of the industry, CIOs, CEOs, boardroom conversations – nobody wants to be the next target, the next Sony. This drives investment and interest in this area. So in my opinion there is a need and a market for new defensive capabilities.

In my work, I am most interested in solutions that can be adopted broadly, and I call that Mega-scale. How can we make sure that when we do have an invasion we can roll it out, in Microsoft's case, to hundreds of millions of billions of endpoints, or billions of consumers? Historically, our focus has been on protection. We worried about how we would keep adversaries out, and if you look five or ten years ago, it was all about how do we keep cyber criminals from going after consumers and enterprises. We used things like economic models to put pressure on the cyber crime ROI. How do make sure that their investment cycles are longer and more expensive? And how do make sure that they only get to use it a few number of times before it's taken away from them. That was reasonably successful, against cyber criminals. You can look at the rates of attacks and successful attacks against consumers, and it is a step change from where we were a decade ago. But things are changing.

The types of systems people use, the platform diversity, the edge disappearing, all force us to go look at the other areas of the circle, and at detection. How do we detect at scale? How do we respond? How do we recover? That is going to require more innovation in those areas. A few examples of some of the past innovations that have worked are trusted platform module, protection down in the hardware, and EFI making sure that we can secure the boot. If you buy a consumer PC with Windows 8 today, you have secure boot. We put exploit mitigations into Windows since Windows Vista, which makes it harder for an attacker to go leverage a vulnerability, if such exists. The consumers don't have to be aware of that layer of protection, but it increases the cost for attackers. Recently we deployed the Control Flow Guard, in Windows 10.

Discouraging of passwords – how do we get to biometrics? We made some significant progress over the past few years, and we are going to take steps in that direction. It is a particularly interesting field, but there is some friction involved. Application stores are also included

in security innovation, since the rise of application stores gave us a way to manage the entire application life cycle, in a way that we could not before. We can actually keep applications up to date, and curate them before they get into consumer stores. These things allow us greater ability to control the experience.

Another step change is coming as we look to the cloud. Small and medium companies struggle with things like patching or monitoring access control. How does a local furniture store deal with managing their IT on a daily basis? We are talking about one PC sitting in the backroom, probably not updated and unmanaged, at least probably for the level at which we can do in the cloud for them. Those are very important basics, but there are whole areas of innovation that are going to come online and give the small furniture store some advantages – everyone gets to leverage the expertise, the relationships, the threat intelligence that we have built over the years, and so, the assets that Microsoft has, the relationships with companies, where we get information that we can go act on, enable us to protect billions of customers, including the local furniture store.

Another thing is cross-company detection and mitigation. If you run your own exchange server, you might detect a phishing attack, and you might be able to go back in and make sure it doesn't hit you again. If you do it across many customers, as we do in the cloud, we see one phishing against a single customer, but can protect all customers. And so we get that level of scale, that multiplication, and there are more technologies and techniques we can use like that, and then everybody can access advanced capabilities. You pay a couple of dollars, you get an account, and you have all these tools available to you. I think those are some of the modes that are going to change the game in cloud.

I think it is important to keep in mind what the innovation space looks like. Why have some innovations succeed over the years, and what barriers do we have to overcome to see them succeed at scale? I put together a list of some of the common failure modes, I call it the eight great barriers to getting defensive technology succeed at scale. Some of them may seem obvious, but I have examples for companies, even major ones, that have failed at some of them. The first is solution barriers – your solution has to survive the first encounter with the enemy, you have to be resilient to the next round of attacker innovation. We need to make sure that the barriers that we put in place are going

to be resilient. A niche product might work just fine, but as soon as you deploy something a million or a billion times, it is going to be targeted and worked around. The second barrier is protection and detection – these must be effective, high signal, actionable. That means things like high distinction, high discrimination, as well as driving down false positives and false negatives. If you don't do that in real usage, then it is going to be too noisy to use and to deploy.

The next issue is consumer barriers. The first barrier is to get it into the customers' hands at scale, and by default. We learned this one the hard way. A famous example would be Windows Update. Windows Update existed long before XP service pack 2, but that was the time when we turned it on by default for the first time, because we found that people did not update the system for themselves. The simple act of turning on the updates by default, making sure we had default protection in place, is actually very important. In contrast, today we have iterated enough on the solution to just turn on updates by default in some of our protection technologies, such as Reference ASLR or the secure boot example I used earlier. It is on by default, I don't have to tell my parents to go in and configure something.

The next issue is impeding consumer usage. If you do, the consumers will turn it off, or will not adapt your technology. A good example is ad blocking – a great ad blocker that also blocks embedded YouTube clips will simply not be used. One of the reasons we didn't turn the Firewall on by default in Windows XP was that we were worried about the consumers, about applications that would not work correctly, leading to rejection of the idea that the Firewall should be on. The last issue is that you have automatically protect things, and don't involve the users in the decision making. User decision making is notoriously poor, not because users are dumb, but because it's difficult, and the bad guys are going to try and game that. That is what phishing is all about, trying to trick the user. If you ask a security critical question, the users probably don't have the necessary context to answer that correctly all of the time.

On the enterprise there are a few barriers as well that are separate form consumer barriers. The first is, "first, do no harm". These people struggle to maintain their systems – they have legacy systems, era 2000 systems, they have partners and relationships, they have business apps on their hands, etc. They try to move into the cloud. Adding

more cognitive load to the enterprise admin is a non-starter. The second barrier is that it has to be manageable and flexible. Adding another pane of glass not only increases cognitive load, but other things you never anticipate can happen. I have been astounded by some conversations I have had with customers. I have had technology pieces that I have written, as well as conversations with governments and militaries about how they work, because they are worried about how they can use that technology in the battlefield to communicate between tanks, and make sure they can actually revoke a tank should it be overrun. That is not something I design for, but it needs to be manageable and configurable to the point where they can actually use it in enough scenarios.

Finally, the last barrier is scale down and scale up. When we deploy something in a Windows server, we are not only serving the Windows enterprise, the Fortune 500, the financials, who might have high viability clusters and large numbers of admins and machines; we are also focused on the single server under the desk, the furniture store. You have to make sure that your solution can scale to both of those ends. I hope you take these barriers into a counsel that can see more of these defensive solutions deployed at scale.

MR. HUDI ZACK, SENIOR VP AND HEAD OF CYBER BUSINESS UNIT, VERINT

Some feel that there may be too much innovation in cyber, and that organizations can't keep up with the rapid pace of emergence of new technologies. I am going to talk about the shortage and the need for another type of innovation – innovation in convergence and orchestration – which can help with this, as well as with a few other important problems. Many capabilities that used to require a standalone tool only a decade ago, have now all converged into a single unified platform, which we know as the smartphone. This innovation was first introduced eight years ago, in late June 2007, and since then it has changed our lives in a great number of ways.

The reason I bring this up is to explain that the power of convergence is actually threefold. First, it is the convenience of having to deal with only one tool instead of a few dozens of gadgets. Second, some of the capabilities have become much more effective in the process. Think,

for example, how much more useful a smartphone camera is, as opposed to a standalone camera which is never there when we need it. Third, and maybe most importantly, this integration enables new capabilities to emerge, which could never have happened when these capabilities were separate. For example, only when you can connect mobility, GPS, and internet connectivity on a smartphone, you can get Waze, which enables us to choose a driving route based not only on the distance, but also on the actual traffic state.

Back to cyber, we all know the attackers' side has great innovation, which the defenders are having a hard time trying to cope with. This is a drill in concentration, these attacks are planned and executed like military operations, they are focused on key strategic targets, they are persistent, using multiple tools over long period of time. In essence, these are multi-phase, multi technologies processes that require a lot of manpower and funds to execute. And despite huge investments, these high profile attacks continue and even accelerate. We have been talking to many customers over the last couple of years, all of them high-end enterprises who invested a lot in cyber security products, recruited security teams, built security operation centers, and we hear the same thing from almost all of them. Basically, they are lost. They have too many tools, which they can't align into coherent defense strategy, and the advanced malware manages to get through the gaps between these different tools. Their systems create too many alerts, and they can investigate only a small portion of these alerts, but have no clue which ones they should focus on. This makes them miss many of the high-risk attacks, as was the case in the famous attack on Target, where an alert was given, but was ignored.

Even if they do manage to identify an attack and initiate an investigation, these organizations lack the ability to understand the full scope and consequences of this attack in a timely manner. It takes them weeks and months to complete their investigation and start taking corrective actions. For example, in the JPMorgan Chase breach, the malware was active within the bank's network for two months, and took more than two weeks to be completely cleaned once it was discovered.

It is clear that a new paradigm is needed, and we believe this paradigm needs to involve a platform that will enable integration invisibility across three dimensions – functionality, coverage, and time. Today each of these three dimensions is served by a disjoined set of point

tools. In contrast, this platform needs to combine capabilities and unify work flows within and across these three dimensions.

The first dimension is functionality. This type of platform has four basic functionality aspects: detection, the ability to create alerts; prioritization, the ability to decide which alert you want to focus on; investigation of the high priority alerts; and protection against the attacks that have been identified. These are served by four different tools sets, which create a lot of incoherency and inefficiency. We believe there is a need to integrate these four functions in order to streamline and expedite the entire incident handling process. The ability to share information across the different functions and move smoothly and automatically from one stage to another is imperative to achieve this convergence, which – like in the smartphone case – cannot only make each function more effective by itself, but enable new capabilities to emerge through the synergies within them.

The second component, or dimension, is coverage. Today systems are fragmented and siloed. Each tool is looking at a certain area of the organizational assets – one is looking at the endpoint, another is looking at the network, etc. This was okay with the old, simple, one-dimensional attacks, which usually addressed a certain asset in the organization. So if you had an attack on the endpoint, you investigated it with an endpoint oriented tool. However, today attacks are multi-dimensional, multi-technology, and evidence related to a specific attack can be found in different places in the organization. You need a more holistic approach, to have an integrated set of detection and analytics sections that will speak to each other and cover all the potential attack vectors, since the attacker may try to infiltrate your network, endpoint, payloads or files. Through that you can create a comprehensive view of the attack to the analyst across the organization.

The third dimension is time. Today there is a clear dichotomy between real-time detection and post-breach investigation. Again, this was okay with the old, short, monolithic attacks, where you either caught the malware in real-time, or if you missed it, the damage was done and you had time to investigate, repair, and prepare for the next attacks, whenever they come. With the advanced attack the situation is fundamentality different, because these attacks are long, multi-phase processes, and the malware can reside within the network of the victim for months. The separation between real-time and post-

breach is blurring, and you need to constantly maintain and enhance the intelligence picture related to an attack, on an ongoing basis. You need to be able to move freely back and forth in time, reevaluate older information in light of newer findings, and even try to "go" to the future and wait for the attackers' next move. All this in order to be able to bring to the analyst at any given time the more insightful picture about the attacks, so that we can take action as soon as possible and minimize the damage.

So far I talked about integration within each of these three dimensions, but we believe there is a need to take it even further and connect these three dimensions. We believe there is a need for a sophisticated orchestration automation mechanism, which we call the brain of the system, that will connect capabilities across the different domains and invoke the different engines to work in the right sequence in the right context, related to the specific attack. Basically, this means that each incident will be handled differently and automatically. This platform should be highly integrated, but it also need to be kept very open. First, in order to enable to integrate and leverage the existing assets the organization already has in place, like the perimeter tools or a SIEM. But more importantly, you need to have that in order to be able to easily add new capabilities and algorithms as the threats and the mitigated technologies continue to evolve. If designed properly, this can significantly ease the pain organizations experience today, trying to add new capabilities and keep all of the systems up to date on a daily basis.

The existing security paradigm, involving dozens of loosely coupled point tools, is failing against the new advanced attacks. We in Verint have worked to create the vision of this three dimensional integrated platform, and in the last couple of years we have been working diligently to bring it to the market, which on one hand is saturated with so many point tools, but on the other hand is starved to get new ideas and new approaches. With our recently announced Threat Potential System, or TPS, which was built based on the concept highlighted in this presentation, we believe that we are one of the pioneers, and that many others will follow. In this case, what you saw here will become the prevailing approach organizations use to protect against advanced attacks in the very near future.

DR. DORIT DOR, VP PRODUCTS, CHECK POINT

In my role at Check Point I meet many customers, partners, and vendors – small vendors, such as startups that are trying to innovate, and bigger vendors that are still trying to move fast within the space. At Check Point, one of the key elements that we think of when we talk about cyber is collaboration and partnerships, because we think it is a big problem. I will talk about ways to move from thinking about point innovation to understanding the whole point in innovating, and to present how can bigger companies such as Check Point can help innovators bring their innovations to market and make them more successful through collaboration.

Every discussion about cyber involves attacks. In such attacks, the attackers share information, ideas and exploits, that is common knowledge. One of the attackers' advantages is that point innovation is really good for them. They only have to find a certain sequence of holes in order to make their attack successful. The problem, however, is that this point innovation turns very quickly against the defenders. Look at attacks such as Stuxnet: from the moment it was published, the world learned about few new zero day events, with few new attacks methods, that in a single moment turned from being a nation grade attack, to something everyone can activate, an open source attack on the wire.

This sort of thing only happens in cyber. In other technologies, such as nuclear plants, even if everybody knows how to build nuclear plants, it doesn't mean that anyone can just build one. But in cyber, it really turns to be an open source attack very quickly, and so, unfortunately, the problem and the need for defense are accelerated. That doesn't mean that the nations or organizations can stop doing what they do, because that is part of how you run a war. However, we have to acknowledge that, and we have to run faster in order to address it, because everything that is invented nationwide very quickly becomes our immediate commercial and even consumer problem.

Moving on to the problem and the needed innovation: we have the next generation of malware – it is hidden, polymorphic, and very sophisticated. That calls for innovation on our part. We can use point innovation, identify unknown malware, look for a specific problem and find its solution. The problem with point innovation is that people

approach it as attacking a specific issue, even successfully – each of these point innovations can successfully detect three malwares that nobody else found. However, that doesn't really help the customer, because, if every company can detect three malwares, and they need to protect against all malware, how does it turn into being a solution? Even if there was one company that would say "I know everything about malware, and I will solve all the malware problem", a sophisticated attack comes that is unrelated to malware. These attacks start with lateral movement within the organization, as the attackers go from one point to another, and attack the whole organization without having malware.

By creating a solution to every attack we find ourselves with many point innovations that are very hard to prove. You can't see the forest for the trees. The customer has to see a very clear picture, which is impossible with many products, and they can't afford to implement all these products. The vendors have the same problem; they are not being noticed. RSA is one of the biggest conferences and all the companies show there, and when you walk from booth to booth, they all have the same message; it is very hard to highlight yourself and prove that you have something completely different than the others.

We need something a little bit different, and it all starts with the customer. What is the customer's problem? Even if the customer knows they have a problem, they're not sure how to fix it. In most cases the customer doesn't work for security – maybe they sell shoes, maybe they have a successful pharmacy, etc. They don't deal with security, they have their other business to take care of, and they want solutions that will help them have peace of mind and create a defense system where they could focus on the rest of their business. This defense system has to follow some operational guidelines, so it will be deployable. Also, from one of the researches that we have done, we learned that even if we told customers that they have a bot on premise, they didn't know what to do about it. Maybe they fixed it for a while before it came back, but in many cases they simply don't know how to approach it, they lack the tools. That means that we still need innovation, because the problem is really not solved, but we need to think about innovation not as just point innovation – we need something a little bit more comprehensive, to help customers resolve the challenge.

An example I can bring from Check Point is the CPU level protection – a method to identify an exploit by looking at the behavior of the CPU. By looking at the CPU you identify a whole family of exploits, and the exploit phase is a narrow phase during the attack. Few tools have become standard ways of defense in system, such as ASLR. If in the past the attackers would find a buffer overrun, overrun the buffer and simply implement their code, this is no longer possible thanks to ASLR and other protections. These days the exploit phase has become very narrow, and that is our time window to identify it. Generally speaking, one of the problems is that once a problem is solved, we are left with the problems that follow it, which requires more and more point innovation, and that is one of our challenges. However, we are able to identify all the newest exploits thanks to the ASLR narrowness of the exploit phase. It operates quickly, so it helps us in prevention and not just in detection, and it plugs into our whole architecture and is a part of the full solution, not something isolated that the customer has to operate. In this case, it is part of a sandbox that the customer could plug into the environment from any gateway.

If we look at the solutions that customers implement, very small part of the money goes to these point solutions, and if you look at the number of startups around the world, many offer such point solutions. But at the end there is a lot of money at the security space, and not much is being spent on these point solutions because they are very hard to implement and feed into a whole bigger picture. Hence, if we want to innovate, we need to innovate across this space, or we could innovate in the smaller cycle, but create it in a way that is connected to the bigger cycle.

The customers have a big problem, but they are unable to address it. We need creative thinking, a way to look at the same problem and to do something different. This could mean one of two things. We could wait for a moment of spirit until we can say "we have X, and X solves everything". Maybe such X will be found someday, but there is none I know of today. The attackers do whatever they can to find and "anti-X" for every X, and so the battle continues. A better way to think differently about the problem is to think about the system and how you could live within an ecosystem and serve the customer there. And so, I would like to discuss how Check Point brings a platform that you could collaborate on top of, as an example for other, larger customers.

We try to collaborate with all the solutions out there, but it is also possible to collaborate with other architectures and technologies.

When we come to a customer, the first question the customer asks us is, "how would I implement these security measures?". We have had this discussion with many customers, until we realized that we have to present a proposal of an architecture to them. We came with a proposal of software defying protection, that has an enforcement layer, a control layer, a management layer, we created plug ins for each layer, and explained how it connects to the environment and to the other solutions. When we come to the customer we picture such an architecture, this is our proposal to the customers, and they find it very useful. However, wherever you go as an innovator, you need to find out what is the architecture of security the customer has implemented, and to live with that environment.

The other opportunity for collaboration, and for thinking about the problem as a whole, is actually in our threat intelligence, called Threat Cloud. We get information from gateways, from endpoint, from mobiles. We have sensors out there, we have analysts and researchers with automatic tools and manual tools that look at this data, and we operate this for our purpose with our intelligence. But in the same way we could collaborate with other vendors, and we do – with startups and other innovation companies – in order to use the same infrastructure, whether it is manually or in an automated way, to plug in everything to the same environment and to protect the customer at the end, by creating a holistic solution for the customer.

DR. YANIV HAREL, GENERAL MANAGER OF THE CYBER SOLUTIONS GROUP OF EMC

We are talking about cyber, about information technology, and we all agree that it is becoming bigger, much more complex, ever-changing and more and more connected. At the same time, though, we find that there is danger ahead – the cyber security. This challenge, that used to be a matter of information security, is much more than just information security today. It touches every part of our lives and our technological lives, and this is really a challenge to keep it secure and to live our regular lives. We try to create global capabilities, to better know the threats, to be protected and to control it, but it will take us

long take until we are able to say that every part and every threat is being identified from the beginning.

Over the last year we have seen several important trends in this field. the first one is the automation. We have invested about a decade to create greater threat identification, alerts and inputs that enter our systems; but with these immense numbers of information and alerts, who is going to take care of it? Even if our analysts are the best in the world, and even if they work more hours, it is not enough. We are going to see a trend of taking to automotive capabilities, and more and more we will expect our machines to process before our analysts should make any decision or understand what the threat is. We are going to invest much more in automatic capabilities.

The second trend is collaborations. We don't need to only defend our company or our organization; the fact that everyone sees threats and don't share it with others is not the best way to defend ourselves. The collaboration should not be solely between organizations, but also between functions inside the organizations. We are going to invest more in creating collaborations between companies, segments and sectors, in order to be better protected as a society in this area.

The third trend concerns virtual and shared resources. We all talk a lot about the cloud, the change to get things as shared resources, the changes in application and every part of our technology, so in that sense, this is one of the changes that we are going to find. And it is not just the cloud, but also the mobile, the IoT, etc., that are a part of this revolution.

The fourth trend is fighting the unknown, which is one of the challenges that also requires a great level of innovation. In the last few years we could plan our defense on understanding and knowing the threats against which we tried to defend. We knew the signatures, the behaviors, but today we all know that in sophisticated or very advanced attacks, we cannot count on familiarity with the signature of the attack. We have to find other ideas to fight the unknown threats or attacks, and we do it. We invest a lot in anomaly detection, we try to prevent the damage, shorten the reaction time, etc.. One of the ideas we have come up with is the simulation idea, which is something that we believe is a part of the answer for the challenge of fighting the unknown. We

believe that with the simulation capability you can think of an attack before it is launched, and predict something that has not happened yet.

In this simulation, we have a specific file server with important files in it. We have someone create a drop site outside of our organization and wait for a specific file, and there is a compromised computer inside our network that someone is controlling from outside with Command and Control, controlling this computer. On a specific day, the command is being given, and now a specific file is going out from our file server to a drop site. This is sort of DLP or stealing information for our company or organization, not something very sophisticated, but if it uses specific tools it can be an activity that we would really like to stop from happening, to eliminate it. And if we can run this scenario on a simulation machine before it happens, this becomes something we can prevent, perhaps, from happening in the real world. And if we have a repository of many scenarios, we can prevent many of possible attacks that we don't want our company or our organization to face.

We have developed this capability as a service and as a key project, as we, in EMC, believe that this is one of the ideas that we can bring to the table in order to stop such unknown capabilities. EMC and the other companies in our group – VMware Pivotal, RSA and VCE – develop cyber solutions and develop holistic solutions based on the building blocks we obtain and on our R&D group, located in Be'er Sheva. We believe that collaborations with big companies, as well as small ones and startups, are part of our R&D capabilities. We also believe in investing in research, and we do so with Ben Gurion University and other universities. We believe that part of this holistic concept also includes involvement in the SOC and CERT parts, and we see it as part of all the holistic idea involving in SOC, in specific global view, and in CERT for the sectors and for the national level. We believe this is also part of solving this problem as a nation, not just for the companies, but also for society as a whole. And we believe that today, as we all move to the cloud, or to cloud architecture even in our databases, this is our time to bring solutions, become involved from the architecture level to risk management, segmentation, and simulation is a part of it.

To conclude, we believe that the cyber bring us a very interesting and important challenge, we have to fight it, and to fight the unknown as part of this campaign. We believe that simulation is one of the tools

we should use, and invest in this capability, as well as in SOC, CERT and cloud security. We collaborate with other companies as well as startups, and we invite them to collaborate with us. We also think that Be'er Sheva, which was announced as the Cyber Capital of Israel, is the right place to do this job.

08

EIGHTH SESSION: CYBER SECURITY – TREND SETTERS

MR. NICHOLAS J. PERCOCO, VICE PRESIDENT OF STRATEGIC SERVICES, RAPID7

First I would like to provide some background, some things that I have going on in my day job over at Rapid 7. I run a group called Strategic Services, which provides security program guidance to organizations, executives and board members, to help them line their programs for the future. I also spend a lot of time doing cyber con investigations, studying data breaches to understand how attackers think and how they navigate within those environments. Outside of Rapid 7, outside the cavalry, I run a hacker conference in Chicago called THOTCON. Finally, personally I enjoy thinking about the evolution of technology, where technology is going, where we will all end up in 10, 20, 30 years, and rearing that with what the security implications of that technology are.

We have a group called "The Cavalry", which sparked into existence a couple of years ago. A Colleague and I and a friend, Josh Coreman, who at the time was working at Akamai, had many conversations about the future of the Internet and technology, the implications of security and how those all intertwine. We also wondered what was the impact going to be on our family members, our children and their children, as technology advances. We bound it all together and tried to come up with ideas and ways to get in, catalyze researching other activities to get ahead of when these problems will exist in the future. And we did. We could have gone and twitted about it, or produce a blog post and put it out on the internet and hope that someone would read it, but instead we took a risk and we submitted it to one of the most hostile hacker conferences on the planet - DEF CON in Las Vegas. Fortunately, we were accepted, and we were slated in the largest room at DEF CON, which could hold 2,500-3,000 people, but unfortunately we were given the time slot of 10:00 AM on Sunday, when most people

only come back from the vendor parties or actually go to sleep. We expected to see no more than 50 people in the room, but then to our surprise as we walked into a full room.

The conversations we had about the topics that worried us really helped spark this movement into existence; it was the people in that room and the media that attended that really gave our ideas life. So we started thinking and speaking about everything that revolves around two statements. The first one is "technology is advancing faster than our ability to secure it"; the second was combining that with the idea that technologies impact on human life and public safety is actually increasing. When you combine those, it is clear that we can end up in a bad situation in the future. And so the idea around the Cavalry is to collect existing research, collect researchers, and connect between them.

In the Cavalry movement we don't do a whole lot of research ourselves, we facilitate conversations, we take people who do automotive hacking, and people who do medical device hacking, and put them in a room together, allowing them to collaborate. We also cross-collaborate with people outside of what we consider the hacking community. We have people who contribute to the Cavalry that are lawyers, marketing people, PR people, and we have folks from the media who often collaborate as well. The whole idea is to catalyze security research that would otherwise not happen, unless we were actually pushing it forward and trying to get in front of these problems.

Last year we spent clambering, working with organizations, talking to people, and we produced a paper called the Five Star Automotive Cyber Safety Framework. Essentially, we designed it to help align the automotive manufacturers along a comprehensive set of rules that they would have to follow and could attest to, and to show not themselves, but the consumers, that they are aligned with cyber security safety. There are five areas within that framework: safety by design; third party collaboration, which talks about collaborating with security researchers; evidence capture within those vehicles, so when there is a cyber safety issue, there is some evidence that can be captured in and understood; security updates – many cars are smart cars today, how do those update when there is vulnerability in those cars deployed within the systems? The last area is segmentation and isolation – if I was to hack into the entertainment system, can I cause

problems with the controls, the steering, the breaking, the other things that were in those cars?

We released this paper last year, and we have been having conversations with various automotive manufactures to various people behind the scene. Unfortunately, not many automotive manufactures really earned very many stars on this list, the only one that really has been working to improve here is Tesla. They currently have between 3 and 4 stars, depending on how you slice and dice it, but they are definitely leading the way when it comes to cyber safety and cyber security within the automobile industry.

The next topic I would like to talk about is risk based exercises. These exercises are meant to get people thinking about the risks that exist in some of the technologies from the past or the future. For example, take some products from the past few decades, things that consumers would have purchased years ago, and think what are the risks that exist today, that could have existed within those products – a microwave oven, a walkman, an old mobile phone, etc. The risks range from mere electrocution to radiation, damage to other objects such as cassettes, hearing damage, etc. Now do the same risk exercise, only for the next 40 years.

If you think about the 2020's elastic transportation systems, these are devices that are going to combine things like Uber technology and self-driving cars, and allow going all over the place around the world without having someone drive it. As I go through these technologies I think about this from both the consumer and an IT security professional standpoints. Imagine the 2020's, when you have a whole fleet of these within your business and your executives are actually taking this around your city. In the 2030's we have things like social robots, the best example here would be like autonomist physician assistance, which would essentially help to create a consistency of care within the hospital, instead of getting different nurses and physicians every time, which is very disorienting. In the 2040's we have digital telepathy, something called carbon hacking. These are brain-computer interfaces, and the prediction is that we will have a breakthrough in that area in the next 20-30 years. If you move beyond that, there is sleep working – we all run out of time during our day, and if we have the ability to do brain-computer interfaces, and we combine that with technology like lucid dreaming, why can't we take advantage of things that are

still too difficult for computer to solve and computers to perform, but we can do them while we are sleeping?

Looking at the future, we can try to make another risk analysis for all those different types of technology. Looking at the 2020's, there are software stability and logic flaws in those vehicles. Instead of turning left they turn right, into a brick wall. Remote compromise may also exist – imagine someone hacking into a self-driving car, and causing harm to the occupants that were in that vehicle. We have an autonomous business system or social robots that will be in our lives. Here, there could also be logic flaws; they can give us wrong information and create privacy concerns, since all those devices have cameras in them, as well as voice recognition, and they will be embedded in our lives. Malicious diagnosis can happen in the hospital robots. If these robots make those types of decisions, there could be some malicious injection or diagnosis that can cause harm to the patient. Concerning digital telepathy, when we will have perfected that brain computer–interface, there will be obvious privacy concerns. If someone could actually tap into your thoughts, maybe they can also perform some malicious control, combined with augmented reality or other types of heads-up displays. And then, of course, think of ransomware – someone can take over your life and limit your ability to connect and communicate with the world around you. Sleep working is also an aspect of that: taking advantage of systems, similarly to Bitcoin mining that takes place on random machines around the internet, through botnets. Imagine a psycho stealing people as they are sleeping and making them perform tasks for themselves.

It all comes down to human life and public safety. We are going to stop hearing about data breaching and Personally Identifiable Information compromises, and instead we are going to hear more about cyber safety and the impact of cyber on the world around us and the people that we love, in our own lives. We also need a revolution, and this goes back to the Cavalry and to discussions revolving around what we can do to change this. And there are some things we can do. We have the community approach; we have whole auditoriums full of hackers in places like DEF CON and others around the world. We have the Cavalry movement, as well as organizations like Build It Securely, that can try to overcome of the lack of knowledge in those communities People build new types of Internet of Things devices, and these organizations

help them, educate and give them tools and frameworks to be able to build more secured products that they bring to market. There is also the government approach, the idea of new legislation that can be introduced. These new laws may seem scary, but we can influence them, and have been doing it through the Cavalry, as well as by trying to educate law makers.

Software liability is another thing that will be tested in the future, when we get devices that are going to impact public safety and human life, because we have compliance regulations for that as well. People have different opinions about when you actually introduce compliance, and if it is even effective, but those things may come about when we get some of these new technologies. There is the informed consumer approach, and this is where all of us can contribute. Even if you don't want to contribute to the grassroots movement, to the hacking community, to the research, this is a very simple thing. Teach people how to update their devices, for example. If you teach them and show them how simple it is, they go and tell other people and that will spread, and they will have more knowledge and accessibility to doing things, such as performing a security update.

We can also take our children to places like hacker conferences, which exist for children as well – not only school age children, but also very young ones. There are also places like Kickstarter and Indigogo, where you can donate money to security-minded projects. Finally, we can hack new technologies. Those who have the ability to do that can find vulnerabilities and actually contribute back to finding new issues.

For the future, the Cavalry has several things that we are working on. We are working on forming a global education foundation; we develop a five-star library; we are going to launch a medical device, and we also work on producing an industry summit. But we need people to contribute, we can't do this without them. This isn't going be just me who will solve these problems; it is not going to be some other people out there. This falls on me; this falls on all of us to try to get to in front of these issues.

MS. AVIVAH LITAN, VICE PRESIDENT DISTINGUISHED ANALYST, GARTNER

At Gartner I follow security analytics, and this is what I wish to discuss; and when I think about revolution, I think about rapid evolution. The pace of change in security is getting very fast, and the new thing in security these days is machine learning. The machines are getting so smart, that according to an article I just read on artificial intelligence, computers these days are about as smart as insects, but in less than 20 years we will have a computer as smart as Albert Einstein. And about half an hour after inventing a computer this smart, it will probably invent ten computers that are even smarter. The possibilities become a little frightening and scary, but hopefully we will make these computers work in our benefit, for security.

I wish to talk about behavior analytics, with intention to help a guy. Welcome to a day in a life of a security officer who is buried in point products. Today every single breach generates an alert, but the alert is buried in one of many terminals. How can you expect this person to know which alert to look at, when there are thousands of them going off at each of these point products? Hopefully, with the advent of machine learning new analytic techniques, we can help this person, make his life easier, and hopefully automate much of the detection. There are two key issues: who is attacking us, and how are our security methods being defeated. Then we will look at the user in entity behavior analytics and see how that helps secure our assets.

There is a whole range of attackers, some are low-tech, some are high-tech, and they defer by their motivation. But their techniques are largely the same – even though some have much more sophisticated techniques than others, the basic modus operandi – whether the attackers are cyber criminals or a Nation State – is to just get the malware in the system, use it to get into an account, escalate privileges. The cyber criminals try to get money, low-tech insiders like bookkeepers try to pay, take invoices, hacktivists try to disrupt services, spies try to take intellectual property, and the Nation States that we're all concerned about are interested in a cyber war.

To deal with all of these attackers, and start solving our problems, we need strategic technology, and I put that into three buckets. First, you want to protect your data and software. Self-protecting data by

tagging hasn't worked very well in the past, but it is getting smarter. The protection is built into the data, as well as the codes; self-protecting software, encryption and tokenization to scramble the data. These days we see more sophisticated methods like polymorphism of the applications that are scrambled on demand, and obfuscation of codes. We also see deception, and the Israeli companies are best at this; but especially in this category, companies have developed ways to deceive the adversary when they come in so you trip them up, whether it is with honeypots or software defined networking. Finally, the area I am going to focus on is stronger analytics – looking at user behavior, looking at entities like machines, and reducing the signal noise ratio.

I believe this is a rapid revolution, Machine learning has been around for a long time, in fraud detection, in credit risk, in trading, but it hasn't been in security until a year or two ago. Security has always been based on what you know, which means what happened yesterday. It is very hard for us to predict the future, so we end up with thousands of rules and many false positives, and that is changing with behavioral analytics. We currently use machines and models that get smarter all the time. This solves quite a few problems. First, it improves the life of that fellow in front of the ten terminals and all the alerts he has to look at. Now, instead of looking at thousands of alerts every day, hopefully there will only be ten important alerts per day that require that person's attention, and they will be prioritized.

The second problem this revolution solves is investigation efficiency. When you get an alert, you have to go talk to quite a few different departments and all your colleagues in these divisions, and figure out why this alert was generated and what happened. With behavioral analytics, the data has already been brought together, and the reasons for the alert are readily apparent in the data. Thus it improves productivity with alert management and investigation efficiency, and we have certainly seen this happen.

Third, you find the bad guys, that needle in a haystack, and hopefully you don't disrupt the business. After the Target breach, there was a big front page story of how the FireEye alerts went off, and they were negligent because they didn't pay attention to these high priority alerts. Well the truth is that systems generate a lot of high priority alerts today, and those fellows in the security operation center probably got a thousand such alerts that day, and didn't necessarily have the time

to look into it. Hopefully, behavioral analytics with machine learning is going to rapidly detect and prioritize what you need to look at.

The rapid evolution in this technology has two sides, data and analytics. We can finally bring together data from any type and any source and make sense of it quickly, and that is what Big Data is all about. We don't have to go through these structured ETL processes; the data is now ratably available for analytics. Now work flow data can be translated into information instantly, which wasn't the case before. The analytics has also changed quite a bit. We have always been able to correlate, but not to baseline and profile before. Now it is possible to correlate information across users, IP addresses, devices, applications, and create a baseline of all these entities. You can know what every user does every day, how applications are accessed, how each endpoint behaves – and you can detect anomalies against that baseline and profile. That is where the rapid evolution is, with those models.

How does the framework that we have developed at Gartner fit into the context of looking at security solutions? These are layers four and five of the seven layers stack. The first layer is endpoint centric – detection and response systems are part of this layer, and some of them go a bit into the second layer, which is network centric. Here we look at network behavior and search for anomalies. Layer three is for specific use cases, like data loss prevention, database audit and protection, and typically it means looking for one type of breach. But when it comes to layer four and five, we look at users and entities across all these different domains and activities. This means correlating what happens in the endpoint protection system with what happens in the data loss prevention system, as well as with what happens in database audit and protection, or just looking at network flow data.

If you look at network flow data, you can be inline to the transaction and actually block it. If you look offline at layer five, you have to be based on log files or Big Data, you are not inline to the transaction but it is starting to become real-time. The time from logging to analytics has been reduced to five seconds, in some cases. But the bottom line is that we are looking across our entire enterprise, baselining, profiling and doing anomaly detection with machine and models.

The target state is to have the source systems; you may take it from network flow, or from existing systems. You enrich the transaction

information coming in with contact, device location and behavior, and you build these profiles. You constantly profile and analyze and find anomalies using the systems that bring all these data together, through common alert management, and incident response that can go all the way to immediate remediation. And you bring in external identity and threat intelligence as needed.

The key findings are user and entity behavior analytics; it is really transforming security management. It is much easier for enterprises now to get visibility into what is going on, and get their arms around the information. The platforms require some tuning, the products don't run off the shelf, but some of the vendors are much more off the shelves than others, and they are getting quicker and quicker, sometimes no more than a few days. They augment existing systems like SIEM with advanced profiling and anomaly detection. Most companies use this type of technology to investigate events, but we are starting to predict and detect bad things as they occur. According to our prediction, today about 20% of the breaches are self-detected, and around the year 2018 almost half of them will be self–detected, a third of those will be self-detected using these technologies.

I would like to share a few success stories from this field. I will not name the companies that had the breaches, but the vendors. Exabeam are UEBA vendors that have implemented at a national grocery chain, which was concerned about a breach of the point of sales systems. Exabeam detected a bad guy who got in through an HR employee account, got into the VPN, bypassed the two-factor authentication, put some malware on that employee's account that bypassed the authentication, and started doing reconnaissance on the point of sale credit card systems. When the alert went off, they killed the malware before it could propagate to the payment systems. Another bank put in the Exabeam system and saw the system admin was backing up 3,000 servers from his home account in the middle of the night. That last example shows you that sometimes the problems is not malicious behavior, but sloppy behavior on the part of the security team or the IT team.

Another vendor, Comcast, was getting a half a million alerts a day, they put Bay Dynamics and got down to a thousand alerts per day, which were very clearly prioritized. A bank we worked with also put in this software, and they had been trying to make sense of DLP alerts

for a couple of years, and they weren't getting anywhere; there were 150,000 DLP alerts a day at that bank. They put in Bay Dynamics and afterwards we ended up firing three people within two weeks for leaking data and it was very effective. And then, the Israeli vendor Adallom, a cloud access security broker, applied these techniques for cloud applications. One of their customers found an account that was accessed in Office 365, which was really a malware coming from ToR. They also found that a user accessing Google Apps were actually hackers that had compromised the user's authentication. So there are many success stories in security, and there are also success stories with fraud. An interesting example was a big hotel booking company, and there was a process coming in form from Amazon Work Services. The hackers came in through the Amazon IP address and the hotel company couldn't block them. They couldn't use traditional means to stop them, but using behavioral analytics from a company called New Data they were able to see these low and slow distributed attacks, using 5,000 compromised credentials to try to see which ones would work at this travel company. The vendor was able to model the behavior by IP and device, and the way it was moving, so that even though the hackers only use one IP twice a day, and the attack was distributed globally, they were able to see similar behavior across this population of the attackers' botnet.

The attackers are usually a step ahead, so they've been slowing down their attacks and then distributing them, in order to look like normal human beings. But with really good behavioral analytics they were able to isolate the population they needed to block. So the direction of the market years ago, you had to hire a vendor to write the analytics for you, now we're seeing off the shelf analytics products, the machines are getting smarter, and now you can bring all the data together, and as the machines get smarter it is easier to do this quickly. I know there are a lot of Israeli vendors that are participating in this; vendors like Fortscale for example, they have a good product that does this. Exabeam came at it and Imperva, so you know some of the Israelis and the Israeli companies really understand how to do this.

To summarize, my recommendation is: these things really work; the models are getting smarter and smarter, you don't have to disrupt your entire infrastructure to be successful. You want to augment what you have, companies have spent millions and billions of dollars on

security, and you don't want to just throw it away, but if you put machine learning and smart models on top of your existing infrastructure, your existing monitoring systems, you can actually salvage what you have and make your systems much smarter.

09

NINTH SESSION: SONY – LESSONS LEARNED

MR. BRUCE SCHNEIER, INTERNATIONALLY RENOWNED SECURITY TECHNOLOGIST, THE "SECURITY GURU" ACCORDING TO THE ECONOMIST

I would like to talk about cyber attacks in the 21st century, and I want to start by talking about Sony. I think the Sony attack last year illustrates many problems and challenges with cyber attack moving forward.

This story has two preludes: the first is in the fall of 2010. There were two NSA operations to penetrate North Korea, including what they call a "fourth party attack": South Korea was eavesdropping on North Korea, and the United States was eavesdropping on South Korea that was eavesdropping on North Korea. The other prelude takes place in June 2014, when North Korea threatened Sony not to release the movie "The Interview". The President of Sony consulted the US Government, and he was told that the threat was an empty one. Sony concluded that there was some risk, and decided to release the movie anyway, but take off some of the names from the credits.

The attack started in September 2014. We believe this was a phishing attack against someone within the company, some kind of Zero Day exploit. There are some forensics teams in Sony that are still looking at what has happened, but the details are not public yet. The attack was undetected by Sony, and the attackers quickly obtained administrative credentials and spent a lot of time in the network, mapping the Sony systems, downloading files. The hacker brag says they managed to obtain 100 Terabytes of information. The attackers spent a lot of time downloading files, planning their attack; they were very careful and very patient.

The public attack began in the morning of November 24th. The destruction of the hard drives and servers was done to both destroy data and cover the tracks of the attackers. Here the attackers made

their first mistake: when they started deleting data off the computers, a picture of skull and crossbones appeared. A little tip: if you are going to erase someone's data, put the scary picture on after you are done, because any smart user would immediately yank the plug, and thereby save a lot of data. On that same day, November 24th, there was a Reddit post attributing the attack to the Guardians of Peace, an organization nobody had ever heard of. No motive was given in the initial announcement; they just said: this is us. Within the US government, work on attribution began immediately, both from their extensive firewall with its detection systems and from their implants around the world.

On November 26th, the first publication for the previously unreleased movie showed up on BitTorrent, and was the first inkling that this attack is about more than leaking data, but North Korea was still not linked to it. The first time someone publicly talked about the possibility that North Korea was behind this was on December 1st. This link between the attack and the movie was made by US news organization NBC News.

On December 1st we saw the first major leak of Sony data, 26 Gigabytes, including employee data and executive salaries. The attackers released those data over the course of several days and weeks, and tried to put interesting details out there that will embarrass Sony. Executive salaries can be embarrassing, especially if you pay your women less than your men, which was on the news. On December 3rd the second major leak occurred, including passwords, payment information and accounting information. On December 7th, the attackers released budget financial reports, banking statements, license agreement, employee contracts, and how much Sony was paying its stars, where we could see another gender gap. Basically, they released a lot more details that the news media liked.

On December 8th was the e-mail leak, e-mail correspondences by the Sony executives insulting their stars and the US President. On that same day we got the first message from the Guardians of Peace, and I quote: "Stop immediately showing the movie of terrorism which can break the regional peace and cause the war". On the next day the US director of the FBI cyber division said there was no attribution to North Korea at that point, only speculations. On December 10th, 13th, 14th, and 16th there were more leaks of data. Also on December 16th we had

what was believed to be a terror threat about the movie: "remember the 11 of September 2001". Not really explicit, but at this point we had movie theaters that did not want to show the movie, since they were afraid that there would actually be something behind that threat.

On December 19th, three weeks after the initial public attack, we finally got something out of the FBI, and I quote: "As a result of our investigation, and in close collaboration with other US governmental agencies, the FBI now has enough information to conclude that the North Korean government is responsible for these actions". President Obama also made a statement: "We cannot have a society in which some dictators someplace can start imposing sanctions up here in the United States". But the security community did not believe him, there was a widespread distrust. All of the evidence in the FBI statement, the similarities to the 2013 attack attributed to North Korea and network use, all of this can be faked. The FBI statement alluded to other US government departments and agencies, most likely NSA, meaning that there is some secret evidence involved, which they can't reveal. What we know now is that the intelligence was partly based on a human source in the North Korean government. However, at that time there were many skeptics, who believed it was not necessarily North Korea. For one, it didn't make sense – why would North Korea do this over a movie?

There were many alternative theories, mostly that these were hackers. The last time such a thing happened was in 2010, The target was a US company called HBgary federal, and the attackers were the hackers LulzSec. But someone did a linguistic analysis of the Guardians of Peace messages, which implied a Russian speaker. Some people thought it was unaffiliated North Korean nationals, what we call cyber malicious – you see a lot of them in China and Russia. These are not people from within the government but other people trying to help, for example the Syrian electronic armies.

On December 22nd and 23rd, North Korea was a victim of a DDoS attack. Some people thought it was Unites States, but we don't know what happened; North Korea's link to the internet is tenuous on the best of days, so it certainly could have even been natural. January 2nd, though, is when the US administration imposed sanctions on North Korea in response to this attack. On January 7th, the FBI director, James Comey, was at an event in New York, and gave more evidence concerning the attack – how the attackers got sloppy, and didn't hide their tracks well.

What finally managed to convince the skeptics, in the end of January, was a New York Times article by David Sanger, which talked about the progression of what happened within the administration to identify the North Koreans and the process. However, the forensics investigation and lawsuits continue to this day, and I have seen estimates of costs of $100M to Sony, but I believe the costs are going to be much higher.

This is interesting because it encapsulates many of the themes of cyber conflict. We have had a lot of hyperbole in the US about how this is cyber war and we need to go to war over it. But the target is interesting, because it is not critical infrastructure. Who would have imagined that the first major attack against the US by a foreign country would target a movie company? And the objective was theft, destruction, coercion, which is very different than what you would expect; and we are all vulnerable to this.

I always think of attackers along two axes – skill and focus. Your low skill, low focus attackers, what we refer to as Script Kiddies, opportunists, kind of the background radiation of the internet. High skill, low focus – those are identity theft attacks intended to exploit more; they are the fancier ones. Low skill, high focus is traditional target attacks. High skill, high focus is APT, Advanced Persistent Threat, which is a buzzword we have been hearing a lot recently.

The difference here is absolute vs. relative security. In a low focus attack, for example the Target breach, the attackers just wanted a big block of credit card numbers. They didn't care where they got them. If Target security was better than that of the next retailer, Target would have been fine. But in high focus attack, the attacker wants you, specifically. And on the internet, the attacker has the advantage. Officially funded, motivated and skilled attackers will not fail to get in, period.

How do we deal with this? On one hand, Sony had very bad security, as some of the leaked documents showed. There wasn't even a coherent response plan for the attack, and they had no real way to figure out what to do or even what happened, because their network was so badly destroyed. The cyber war rhetoric says we are fighting a cyber war, but that is not true; what really happens is that we increasingly see more war-like tactics used in broader cyber conflicts. Technology spreads capability. Once, you used to be able to determine the attacker by the

weaponry – if we saw a tank, we knew the military was involved – but that doesn't work in cyber space. Everyone uses the same tactics, techniques and tools. We have legitimate and serious debates about whether a cyber attack was the result of a foreign power with a $20B military budget, or two guys sitting in a basement somewhere.

Last year the hackers of Anonymous offered to take out ISIS for us, and in 2010 another arm of Anonymous warned NATO not to threaten them or mess with them. Regular people do not get to warn NATO, that is not the way the world is supposed to work. But in cyber space we have this blending of Nation State and non-Nation State actors, and politically motivated cyber attacks. And politics is very broad here against nationalistic, ethical or religious corporations, governments, institutions or individuals. This means that attack attribution is hard, much harder than in the real world. Packets don't come with return addresses, it is easier to hop through other places, and you don't have the same geography that you have in the real world. It took three weeks before the US was able to announce that North Korea attacked Sony. You want to get this right, because there are major problems with potential misattribution. So we have this arms race going on, between attribution and deception. How do we figure out who did it?

In 2012, the US Secretary of Defense said in public: "the US has made significant advances in identifying the origin of the cyber attacks". We don't know what that means – whether the NSA has some new technology, or simply very good espionage. Strong attribution leads to deterrence. In the past year and a half, the United States has been far more aggressive in saying "we know who did it". We indicted five Chinese nationals in absentia last year for hacking US corporations, for example. The attacks on the White House, earlier this year, were quickly blamed on Russia. I think what the United States is doing here is saying to the world, we are good at attribution, don't try anything. But you have to provide evidence, otherwise this gets tricky. What happens if you announce "North Korea did it", and nobody believes you? In the US there is broad mistrust of the national security community. There is a lot of history of the evidence not really being there, or sloppy evidence that was given – Iraq, for example.

There are several levels of attribution. The first is the easiest, saying "I know you did it". The second is saying "I know you did it, and I can convince you I know you did it". The third level, and the hardest one,

says "I know you did it and I can convince the world I know you did it". With the Sony case we did level one, maybe two, but failed miserably at level three, mainly because the evidence was secret, and based on NSA surveillance. If our government wants to convince the world of the legitimacy of its retaliatory action, it has to provide evidence, and if that evidence is based on secret sources and methods, that is going to become difficult. This makes it very hard to figure out who is in charge of defense.

Scott Charney at Microsoft once said that when you are attacked, there is a variety of institutions you call to defend yourself. In the US, for example, you can call the police, the military, the Department of Homeland Security, you can call on some commercial products and services or your corporate lawyers. What matters is that the legal framework in which your defense operates depends on two things – who is attacking you, and why. When you are attacked in cyber space, these are the exact two things you don't know, and you might not know them for a while. Duqu, attributed to Israel, took a little less than a year to figure out. The Anthem attack in the US, attributed to China, took a few weeks. So whose job is it to defend Sony? If it is hackers, you can argue it should be the police. If it is North Korea, you can argue it should be the military. But the real question is, whose job is it to defend Sony *before* you know whose job it is to defend Sony? What is the default legal framework in which your defense operates? It depends a lot on the country. In the US, the NSA wants to be the default. I personally think a law enforcement default is better. There are countries in which police and military are more integrated, and there will not be that much of a distinction. In many cases, though, it is Sony's job to defend itself without attribution. As soon as the Sony attack happened, the big question in the media was who did it. However, within Sony, that probably was the one question they didn't care at all about; because it doesn't matter to them, they just had to figure out how to recover, how to get back security, how to defend themselves.

We need fast, flexible incident response without attribution, and that is difficult, and there is some blurring between attack and espionage. In the US, the term for espionage is CNE, Computer Network Exploitation, and the term for attack is CNA, Computer Network Attack. CNE is the NSA's job, and it is under one set of legal rules. CNA is in a separate government branch, the military US cyber command, and answers

a completely separate set of rules. From a policy perspective, these two are very far apart, even though technically they are very close. This is why in both CNE and CNA, the NSA and US cyber command are headed by the same General, and are located in the same building at Fort Meade; because as a technical person, you know that there is an enormous number of steps involved in these things. Infiltration, reconnaissance, getting privileges, doing all that work. And that is all the same except the very last step, which is to either copy or delete the files. As a defender, you have no idea what is going to happen until that very last step, which also makes defense difficult. This is why you see some policy proposals to treat espionage as an attack – because from the victim's perspective, it basically is an attack.

There are three basic types of attackers when you talk about governments, and I think it is important to distinguish them from one another. There is what I have been calling APT, which is the major governments in the world with cyber attack capabilities: the US, UK, China, Russia, Israel, some other European countries, maybe down to India, Pakistan, some of the BRIC countries. Under that you have customers that buy cyber weapons off the shelf from cyber weapon origin manufactures, for example the governments of Ethiopia, Azerbaijan, Syria, and Saudi Arabia. Under that you have the cyber militias, which are people either working for the government, or just tolerated by the government, who use hacker tools. Many of the things Syria does are based on normal criminal hacker tools that have been repurposed. There may be several types of operations in tandem – for example, China does APT and also has a cyber militia. Then, below that, you have all of the Non-Nation State actors. They range from criminals to nationalists, politically motivated hackers, who do things for various reasons. Sometimes they write their own tools, most often they use tools that are out there.

My fear is that we are in the early years of a cyber war arms race, that we are witnessing a large build-up of cyber attack capabilities by a variety of countries. And like the previous arms race, there is not a lot of defense involved, since attack is easier than defense. There is a phrase saying that the best defense is a good offense. It is actually not true the best defense is a good defense. But on cyber space, good defense is hard to do, and we have to start paying attention to what defense looks like, because as these offensive things continue

to happen, we are increasingly going to be in the blast radius. These days, when North Korea gets mad it attacks a movie company. The US attacked the Brazilian oil company, Iran attacked the Saudi oil company, Stuxnet caused collateral damage outside the intended target. Earlier this year, China attacked GitHub, and we are seeing more Nation State attacks against Non-Nation States. That is going to be very interesting to watch in the future, as countries realize that they may deliver their best punch using cyber attack, by going after an easy, sometimes civilian software target, instead of a government or military target.

Many companies do and say things that they really wish they didn't, and in the Sony case, many data and conversations were exposed and embarrassed the company. One of the things to be learned here is, don't pay salaries you'd be embarrass to see in public; don't send e-mails you'd be embarrassed by. But this doesn't only go to companies. In Saudi Arabia, for example, many diplomatic secrets are being leaked to WikiLeaks, and it is stuff they wish they didn't do, or at least that the world didn't know they did. The solution in the world where secrets are harder to keep is, do things that when they are exposed, you are not going to wish they weren't.

When public shaming comes out to an institution that people would like to trust – a bank, for example – this is a serious problem, and we see this more in the personal space, not in the corporate space, individuals have their information published. The term for it is doxing, and it is being used as a tool of power. We also see it in the public shaming of individuals who say things that are unpopular. How do we, as a society, deal with that? It is still very much in flux, and I think we currently see companies being pulled into that. It is a kind of forced public release, a way for the less powerful to obtain more power. The motive can be someone who behaved badly and angered the attackers, or a political motive of someone who wants to get even with their government.

In my opinion, Sony should have had a better response, which means not drilling the actual incident, but rather training and drilling and practicing so that people know what to do, have communication systems that do not use the network that is currently under attack. There is a lot that could have been done to make that response better. This is a place where a company uses its reputation capital, but Sony was a company that no one trusted even before, and the attack only made it worse. Compare that to what happened to Apple last summer, with the

leaking of the celebrity photos. This was a very embarrassing incident for Apple, but they managed to weather it a lot better, because they are inherently a more trusted company, and so their response will be more trusted, more people believe that they did their best and it just failed – as opposed to Sony, where everyone thinks they just didn't care. This is very interesting to see; it really shows who you are as a company. You invest in this reputation capital that you are going to spend like crazy during such an attack; but if you have enough of it, you will be able to come out the other end well as opposed to poorly.

Security has always been a combination of protection, detection and response. I think that as an industry, we have matured over the decades. We spent the 1990s selling firewalls and antivirus to build barriers and keep the bad guys out. In the 2000s we started using detection systems such as IDS, trying to detect attacks as they happen. In this decade, I think we finally see response coming to its own, and products and servers are built around responding. Response moves very quickly from the technical to the political. From the IT team, very quickly it moves to the lawyers, HR, PR, all of these departments. Coordinating that is a huge and vital thing.

I both like and dislike the notion that companies are going to have to become their own Nation States, when it comes to cyber attacks and defense. Companies have to defend themselves, but we really don't want to repeat the cases of Dutch East India Company or the United Fruit Company, where companies had private armies. We have to think about attack vs. defense, and how that works. I think that as some companies realize that they cannot rely on their governments to defend them, we will see more calls for what is called "strike back". Companies want to attack back, and I worry about that. I think there is a real reason why we don't allow private entities to have sanctioned violence, and this is a really interesting policy discussion.

We need to get to the point where we know we may not be able to prevent attacks, but that we can survive them; that we have some kind of resilience in our system. This means different things; Apple Pay is a really great example of turning a credit card system, which is very vulnerable for those big databases of credit cards that the retailers keep, to a one-time number system where that database becomes less valuable. That is a resilience measure that makes the cyber crime less effective by creative thinking, and I think we are going to

see more of that kind of thinking in corporate networks. Maybe we won't be able to prevent this attack, but against massive attacks that publish all of our information, we are going to have less information that needs to be secret. We are going to be more open as a company, have reputational capital that we can spend, and we will be more resilient against this sort of attack. I think we are finally going to start looking at the whole, and come up with strategies that let us survive. So far, the NSA survived Snowden, Saudi Arabia is going to survive their leaker. We all seem to manage; we just have to make it less painful.

MR. RICH BAICH, CHIEF INFORMATION SECURITY OFFICER (CISO) & EXECUTIVE VICE PRESIDENT, WELLS FARGO

Cyber security consequence is what drives many different behaviors. It is really about how you handle the incident, rather than the incidents themselves, that matters. From an organizational standpoint, most organizations try to prioritize their assets, and around those assets they choose different deployments of defense to protect them. In reality, security incidents happen everywhere, and the question is how the organizations use it, respond to it, and what are the facts associated with it. This is really about reputational management. If you look at many of the cases that have been in the news, and how organizations deal with it – that is what drives customers' confidence. I think that today, individuals understand that organizations are doing their best to protect your information, and often times can fall victim to a potential Nation State threat or an attack. When an organization unfortunately falls victim to such an attack, and maybe didn't take appropriate action, or doesn't have sufficient controls, there could be a backlash from their customers. I think what really matters in how you deal with an incident, and the consequential management of the incident itself.

In today's environment, an incident is as much a corporate event as it is a cyber event, because you will have your legal team and your crisis communication team involved; you are going to be liaising with law enforcement and potential National Security agencies. You are going to look at forensics, or even engage your fraud teams; and you will obviously engage your IT infrastructure teams, all of those come together in a time of crisis. But there are learning curves, and good response requires practice. From a leading practice standpoint,

organizations probably do table tops, at least quarterly, revolving around real incidents. In addition to that, sophisticated organizations have their own red teams that test their own systems, validate it and try to see if they could break in and raise alarms in systems and controls within their own organization. The art of information security is about "trust but verify", and a good information security and cyber security team includes testing their own controls, a part of which is how you deal with an incident.

Then, there is the question of the difference between information security and the new term, cyber security. From my viewpoint, information security has been around for a very long time, very much a silo discipline domain construct, and what cyber security has done in the last several years is to take that practice, operationalize it, and try to make it proactive and preemptive, in terms of risk management. From a corporate standpoint, you are going to see organizations move a lot of their information in cyber security functionality out from a traditional IT infrastructure, and into the risk office or the operations office, because you want to have that segregation of duties between traditional IT practices.

Good information security and cyber practices greatly depend on technology and technology teams that maintain their infrastructure at a very high level, creating good defense. It also depends on the security operation center, and many of those are being merged into cyber threat fusion centers, where you can say that it is not the offense of the company, but the ability to be proactive and preemptive through analysis, whether that would be open source, partnerships, or engagements with law enforcement and national security. The emergence of going into cyber security and the emergence of the reporting structure moving out from the CIO is something we are going to see a lot in the industry in the next few years.

From a financial services industry standpoint, specifically to the US, there is strength in numbers. We have a governing body called the FISIC (Federal information security incident center, or the US-CERT) that helps policy with the government; and we have a tactical operational body called The Financial Services Information Sharing Analysis Center. Those things are put together because normally, no financial institution is the only one to experience exploit or other consequences in a potential attack. Thus, by sharing information, the

financial institutions can potentially respond in a coordinated way, to understand when a particular attack is being launched across the industry. The government also has a part in it, they have to set the stage as far as the ability to get the proper information out to the right individual, so that appropriate actions can be taken. Speed is critical, and I think that today, an effective organization can demonstrate the shortest lapse time between identifying an incident and being able to isolate it, retain it, detect it, and then respond to it. I think lapse time is a term we are going to hear a lot more about soon.

BRIG. GEN. (RES.) NADAV ZAFRIR, FORMER HEAD 8200, CEO AND CO-FOUNDER, TEAM8

In an organization, if you are protecting everything, then you are basically protecting nothing. If you don't know what you are protecting, and who you are protecting yourself from, then it doesn't really matter how you protect it. I think organizations have to identify what their specific crown jewels are, in what context, and versus what adversary, and only then they can narrow it down to a small percentage of their data, of their infrastructure, of their personnel, and it is a hard job.

I think that specifically in Sony's case, it was almost impossible for the CEO to do much better than he did, because he was not prepared for this. And once you are hit, that is not the best time to start preparing or training for it. But concerning the issue of what could be done before such an attack hits an organization, I think there is a lot to be done. There is a learning curve between attackers and defenders, between offense and defense, and we are obviously behind in the learning curve, in terms of defense. It might get worse before it gets better, but it will get better, because like other domains, offense emerges first, but defense eventually catches up with it. Even before cyber, in previous centuries, there were ways to hurt and kill people; this is just another means to achieve the same goals, and the learning curve for the defense will balance itself.

Regarding asymmetrical warfare, I think CEOs and top C-level managers of larger organizations are going to have to start thinking like leaders of small nations. These days some of these corporations have more impact on everybody's lives than the national leaders of their Nation States have anyway, so I don't think it should be a surprise for these

leaders and CEOs that they have to deal with a globalized asymmetric warfare situation, with a strategic planning just like leaders of nations had to do in the 20th century. The world is changing, but it is not impossible to get a decent cyber posture for an organization if you know what you are defending and who you are defending yourself from, and if you prioritize and segment the things that are really important.

If in the past the norm used to be that mostly everything is private, and the fragments that you chose became public, today mostly everything is public. Our generation finds it difficult to comprehend, but the next generations are going to born into this reality, and there is going to be very little that remains private – it might be a specific transaction for some kind of firm, a specific vertical at a specific time of the year, at a specific geography, that is super-crucial and you will dedicate substantial resources to protect that.

The next step is that organizations, just like Nation States and militaries have done in the past, are going to have to prepare for an incident becoming an event, which will happen every once in a while. And when it does happen, the aim is to shorten the time to bounce back. I think that in the future we are going to see organizations leveraging their reputational assets and their ability to thrive in the cyber age. This is not just going to be a threat, but also a competitive advantage. If I am leading the bank or the law firm or the e-Trader that has the best security measures for my customers, that is going to be one of the things I sell to my customers. So the whole notion of cyber is not just about the threat, but also about an opportunity, for cyber vendors but also for everybody else, and it is going to become everybody's problem. I think there will be collaboration between Nation States and corporations. Someone said, not long ago, that cyber is a team sport. So even though we don't expect companies to take violent actions, we do expect them to be able to protect themselves well.

10

TENTH SESSION: BRAIN & MACHINE LEARNING

PROF. LIOR WOLF, FACULTY MEMBER AT THE SCHOOL OF COMPUTER SCIENCE, TEL AVIV UNIVERSITY

I will discuss using deep learning in order to automatically annotate images. Deep learning is the study of neural networks with many layers, much larger than what we were able to train before. There is a lot of excitement about deep learning, because it holds the promise of making computer perception as good as human perception, and this applies in various fields. We apply it in voice analysis, understanding what the person is saying and identifying who is the speaker; image analysis, understanding what is inside the image; text analysis, which is the new front of natural language processing – as input we get large texts, and we want to extract all sorts of insights. We also apply it in robotics and related fields. You probably heard about it, because it is really everywhere in the news. There is a lot of excitement around deep learning, and it is evolving very rapidly; it is now like a sport, who is getting the better AI system faster than the other groups. There is a very fierce competition, all the major tech companies and universities invest many resources in this domain – the leaders in the academia are NYU, Toronto, Stanford and Berkeley.

I would like to give you a self-centered view of artificial intelligence in general. In 1996 I built Deep Blue, which was better at Chess than the best human player at that time. Since my computer Chess is much better than human Chess, human Chess is really no competition anymore for computer Chess. But that was almost 20 years ago, what happened since? Did the promise of AI materialize itself? Do we see AI systems everywhere? Not that much, nothing really exciting happened, there have been many advancements, but not the huge science fiction type of dreams. However, this is changing, and I will show examples from our labs.

Last summer we were able to present the first computer vision system that could perform facial recognition better that any human, a computer vision system that performs better than humans. This was work done jointly with the Facebook AI research group and here, the school of computer science at Tel Aviv University. This year we are presenting a system that is able to take as input an image it has never seen before, and create a description of that image. This is the dream of artificial intelligence, of computer vision. We want to get an image as input, and we want to be able to describe what we see in that image. The reason that it took so long is that AI today is not about searching, as was the case in systems like the Chess computer. It is about learning – just like humans learn from examples and get better and better, so do machines. Machines today are able to learn from data much more effectively than before.

What is image annotation? The input is an image that the machine has never seen before, and the output – for example, two girls playing soccer – is a sentence the computer generates after seeing this image. This is, schematically, the way that this is done. We have technology that can put together images and text in the same neural network. We start by giving the computer the image that we want to annotate, and the computer's neural network creates the first word. In this case the word is "two". Then we take the word two and feed it to the same neural network, and the neural network thinks just a little bit, and then produces the next word, which is "girls". We take the word "girls", feed it to the neural network, and we get the word playing, until the computer tells us that this is the end of the sentence. So we started with an image, and got the entire sentence automatically generated by the computer.

A few examples of sentences created by the computer for images it has never seen before are "a dog with a ball in its mouth", "a basketball player in the uniform is running in the air", "a man in black helmet, he is riding bike on the road", "a boy is jumping into pool". You can see some of the limitations of the system, the system selects what to present. Some visitors came to our lab, we let them play with the system and they selected an image, and the computer said, "two dogs are playing in the water", while it actually showed bears. It actually makes a lot of sense, since we trained the system with a limited

number of images; it has never seen a bear before, and a dog is the closest it could find.

Of course the system is not perfect, it is unable to solve the problem completely, and sometimes it fails miserably – especially when they are shown different types of images than what it has been taught. There is still a lot of work to do, and the human brain is still much better than the computer brain in this task. The specific task of annotating images is probably the most popular, hardest task in computer vision right now, and there is a lot of competition from all the major companies, like Google, Baidu, Microsoft, as well as all the major universities. We like the results that we get, there is place for improvement, but we like that our system is a little liberal and creates new sentences and do not rely on old sentences.

In our lab, the deep learning lab at the school of computer science at Tel Aviv University, we study all domains related to deep learning, whether it is robotics, text analysis, image analysis, or voice analysis. If we compare results on the related task of selecting the most appropriate sentence, given an image, out of a huge number of sentences, our system has a significant advantage over all results of the current systems, which were published in the last half a year by major research labs in the world. Right now we are expanding the system, we want to work with video, we want to be able to form complete discussions, chats around the images, and these are the next steps that we are currently pursuing.

DR. ODED MARGALIT, CTO OF IBM CCOE

I am going to talk about the usage of cognitive computing for cyber. My alma mater is here, Tel Aviv University, and I worked at the industry in Machine Learning, detecting anomalies and other things. I am the current puzzle master of IBM research, and the CTO of CCOE, the Cyber Security Center of Excellence. I am involved in all kinds of cyber competitions, for example Cyber Night last year and IEEEXtreme.

What is cognitive computing? I will give an example. The first age of computing was the tabulating system – doing the census, repeating, doing very repetitive task again and again, but slightly faster and without getting tired. The second age, the programming era, included computer programs that were programmable, could do different

things. The current age is the cognitive one, where you actually don't exactly tell the computer what you want it to do, but it actually does it. This is the difference between computing of the second age to the third one. The second stage just says "gives me an exercise, I will compute it and give you an answer", but the third one is a cognitive computer, which actually has some "ha ha" moments, of realizing that an answer is strange or interesting.

An example of cognitive computing capabilities, one of many, is Jeopardy, or you can give speech to text machine translation, using language. I will give an example of a personality insight. From the cyber week conference, I took the description and entered it into an API. When you give this API a few paragraphs of text, it gives you personality insights. For example, our conference is very self-disciplined and outreaching, according to the system. This is an example of how we use cognitive systems in healthcare – we took a lot of information, internal and external, such as lists of chemical compounds and all kind academic papers in medicine journals, some blood test results and other lab notes, and we take all of these Terabytes of information into a cognitive cord that is able to ingest all of it and help the physicians come to some interesting conclusions.

In the cyber domain, what we are going to do is make use of this kind of technology but convert it to cyber, so instead of reading medical reports we will read some X-Force or CVE or Microsoft or any other kind of reports, and instead of using the X-ray results, we will take SIEM reports and use the same mechanism to combine the things together, and help SOC operators or whoever wants to use the system.

The real question concerning cognitive computing in cyber is, what are we going to do with it? We have several use cases, a possible one is a CISO asking who is attacking me, what is going on? Another use case is, if for example you are Sony or another big company, and you want to know in advance what would happen if all your data would leak. You can ask the system to find the embarrassing information in your textual data. It is a good use case, because what Watson does best is read a lot of information that is written in human languages, by humans, for humans, but its size is too big, so that no human can read it all, and come up with interesting results from that. There is another use case, where you want to connect the dots. Read some blog posted on the DarkNet that connects some BotNet to a Twitter

handle, connect these dots from another source using the IP, and check the IP reputation, go back to the DNS, connect all the dots together, and find out what is going on.

To summarize, we have a very powerful tool, Watsonognitive system, and we are looking for use cases, especially in the cyber domain, a matter in which we are always happy to receive help from cyber experts and professionals.

CYBER REVOLUTION IN MILITARY AFFAIRS

BRIG. GEN. (RES.) YAIR COHEN, INTELLIGENCE AND CYBER ELBIT SYSTEMS

Recently it has been decided by the IDF to create a new branch in the military, specializing in cyber. Unit 8200 will undoubtedly be a substantial pillar in the implementation of this decision, which will be executed over the next several years. Even without knowing the full details and content of this decision, I believe that it makes sense, because we need to look at cyber as something that will be very crucial in the future battlefield. On the other hand, if 8200 will indeed constitute a substantial pillar in the implementation process, it will require changing some aspects of the unit, and this needs to be done very carefully. I think that 8200 is a very successful organization from the intelligence, technology, and other aspects. It has immensely influenced the Israeli Hi-Tech industry, and making changes in such an important factor could have major implications on the entire Israeli market. That said, I believe we do need to adopt offensive capabilities as well as defensive ones, which is one of the required changes.

There are many variables that contribute to the success of 8200. The failure in the Yom Kippur war; the decision to bring the best young people to the organization; the luck; the great decision to include R&D within the unit; etc. But one of the main variables in this equation is undoubtedly the combination between the gathering of intelligence and R&D, which are carried out together in the same unit. I'm not claiming that there is no need for change, but for the reasons mentioned above, it needs to be done with caution and extra care.

Winston Churchill allegedly said that after the First World War we realized how crucial the air dimension will be in the future battlefield, but we didn't realize how crucial and to what extent. I think that we can say the same for cyber at present. If we take the opening of the 6-Day

war as an example, which was Israel's most successful war from the military aspect (although not politically), within less than three hours since the first shot was fired, the Israeli Air Force jets destroyed 180 aircrafts of the Egyptian Air Force, thus ensuring the outcome of the war. Such swift victory is not achievable now, but I think that this must be the goal; that by a press on a keyboard button we will achieve the same result without sending pilots and risking human lives.

However, this goes both ways. I think that cyber brings the competition between strong and weak to its highest peak in favor of the weak – not the regular armies, but the guerilla groups and terror organizations. I think Israel was lucky so far not to have suffered major attacks with destructive outcomes. This is not the case for the US, for example – the NSA, CIA, and FBI are suffering many such attacks, and are referring to them as a Pearl Harbor. Some would say that this is not luck, but people who work very hard, but in the US they also work very hard, and still got hurt. A colleague of mine, former head of the NSA and CIA, told me once that we have built our future upon capabilities that we haven't learned how to protect. In the ever-lasting war between strong and weak, cat and mouse, from an asymmetric point, the current situation is 100% in favor of the attacker and not of the defender.

Because of the asymmetric equation, I think that there is almost no deterrence regarding cyber to our enemies – whomever they may be – since it is very difficult to identify cyber attacks. Moreover, even after identifying such an attack, it is very difficult to understand that this really is, indeed, a cyber attack, If you are lucky and you manage to identify that you are under a cyber attack, it is extremely difficult to know its source. A good example for that is the hacker who identified himself as a citizen of Saudi Arabia while he stole hundreds of credit card numbers from Israeli citizens, a statement that had later been proven false. The problem is that following his initial claim, Israeli "patriots" started to attack the stock exchange in Saudi Arabia – a dangerous move to make, especially when the attacked party, such as in this case, is innocent. Another aspect to be aware of is the financial one – if the stock exchange in Saudi Arabia falls, it will have direct impact on the global market, including the Israeli one, with unexpected implications.

This state, where identification and attribution are almost impossible, and deterrence is almost non-existent, makes it very appealing for

organized crime and various countries to attack other organizations and countries. Look at the famous example of the Stuxnet, the attack on the reactor in Natanz in Iran. The Iranians declared, very clearly, that this was a blue and white operation, with or without US cooperation. The question of whether or not this was indeed an Israeli operation is under debate, but the general global reaction indicates that some cyber operations have more legitimacy in the global community than physical attacks.

That said, I am mostly relating to isolated attacks. When it comes to an all-out cyber war, Israel maintains its deterrence, among other things, because of our physical strength. It has been clearly said, by both the UK and the US, that if someone attacks them in cyber, they will attack not only in cyber but also in physical weaponry, and Israel takes the same position. This is, in all probability, why Iran never retaliated, even though they are sure that Israel is behind the Stuxnet attack.

Recently in the news, it was published that someone installed a malware in a Swiss hotel hosting talks between the Iranians and the West regarding the Iranian nuclear project. Kaspersky claimed that they investigated the malware, and that they found that it had the same footprint as the Stuxnet worm. We don't know if it's true or not. I believe that if Stuxnet was built by a super-power, as Kaspersky claims, and that its development cost $100M, the super-power in question would have enough money to change the code so that it wouldn't be similar to the Stuxnet in such a discernible way. Obviously, many intelligence communities were interested in what happened behind closed doors in the hotel, but there is no evidence and no sign that Corporal Shoshana from 8200 wrote her name in the code; attribution is difficult, at best. Unfortunately, these days hacking is almost a commodity. It is relatively easy to track targets by opening microphones, reading their e-mails, tracking usernames and passwords, etc. You don't need 8200 or the NSA to do such a thing, as these tools are available on the free market and the dark net.

REAR ADMIRAL OPHIR SHOHAM, DIRECTOR OF DEFENSE RESEARCH AND DEVELOPMENT

There are two things worth mentioning about the announcement by the Minister of Defense regarding the creation of the new military cyber arm: the first is that he reminded us that this decision is by no means

a new one, but that he first pushed towards this process over a decade ago, when he served as the Chief of General Staff. The second thing is that he views this change as an evolution of the IDF. I agree with this notion – this may be a speedy evolution, but it is an evolution nonetheless. Many talk about the cyber domain in terms of revolution, but in many aspects it is also an evolution. There are similarities between cyber, EW, and SIGINT. One can imagine cyber as a better, modern, more capable tool in the race of ECM, ECCM, and other intelligence and offensive electronic capabilities. Without going into details, I believe this decision is very balanced and its goal is clear. On the one hand, this decision will allow the IDF to move very quickly towards becoming a dominant force in the cyber domain, using our unique qualitative edge. On the other hand, it makes sure to keep the important pillars that we have in both the C4I directorate and the intelligence corps, in a way that allows building new capabilities without ignoring important values.

In the next war and those that follow it, I think the cyber domain will become more and more significant. This has already begun – we can look back at Operation Protective Edge, in 2014; Israel was attacked by cyber attackers from states like Iran, as well as terrorist organizations and various hacker groups and individuals. Although no significant damage had occurred due to these attacks, this does not guarantee that it will not happen in the future, if we are not properly prepared. In my view, since being able to have cyber capability is not reserved only for super-powers, and various indications show that countries and organizations hostile to Israel are actively trying to acquire such capabilities, we should not underestimate them. I believe that the cyber domain will be significant, and that the evolution of such a force and operational capabilities is very essential to the IDF and the overall security organizations.

Israel has many enemies with various capabilities in the field of cyber, without going into specifics. However, Israel's main advantage was always our qualitative edge, in terms of human resources, technology, and the combination of the two. Therefore, we should continue to invest in that edge, and specifically in the cyber domain, while always remembering that this is actually a race, and in a race you should never underestimate your rivals.

Over the years, one of the means that served Israel in maintaining a state of relative quietness is deterrence. Such deterrence is much more

complicated in the cyber domain than it is in the physical one, a domain in which the rules are not clear and definite. It is hard to specifically identify attackers, and it is hard to define what is considered an act of war. Moreover, some areas of this domain are very unpredictable. That said, we must have the capability to retaliate for any identified attack that may happen. If the attackers take into account the possibility that they will be identified, perhaps it can affect their actions.

Modern warfare requires us to cope with new challenges all the time. Cyber is a major threat to be dealt with, and specifically the possibility of a cyber attack compromising weapon systems. As defenders, we should make maximal efforts to protect our weapon systems; however, we don't have unlimited resources, and therefore must prioritize our defense efforts. Defenders always have the more difficult task of closing all the gaps, while attackers need only one weak point in order to penetrate. That said, we have to remember that cyber is not everything. In many cases, the most cost effective way to disrupt military operations is still not cyber, but rather kinetic war and physical damage to antennas, command posts, etc. It is important to decide how and where to use cyber capabilities.

BRIG. GEN. (RES.) DR. DANIEL GOLD, CEO AND FOUNDER OF GOLD R&D TECHNOLOGY AND INNOVATION LTD. & HEAD OF THE ISRAEL NATIONAL COMMITTEE FOR COMMERCIAL/ CIVILIAN CYBER R&D

Many discussions about the new cyber arm in the IDF revolve around the topic of organizational structure and the place of unit 8200 within that new order. However, these are not the important part. What is important, though, is the potential effectiveness of that arm, and the effectiveness of the IDF in general as a result of its establishment. The integration of cyber intelligence and cyber defense in one place has a great potential to increase the overall military defense capabilities. This combination of cyber, kinetic and non-kinetic capabilities should improve the IDF's ability to deal with threats wisely and efficiently.

At present, I believe that more damage can be done with a one-ton bomb than with a cyber attack, but that might change in the near future. Cyber attacks have the potential of controlling kinetic instruments, including tanks, aircrafts, etc. This is not to say that it will be an easy task for attackers, due to advanced shielding and

protective mechanisms installed on such instruments, but it is definitely possible. However, while cyber is a tool that can possibly be used in a lethal way, it is often aimed at interfering with operations and affecting public opinion, which are mostly a PR effect. Cyber is sexy, and can have moral effect, beyond the military aspect, on the general psychology and public perception, by serving as a tool for propaganda or damaging critical infrastructure. Cyber will not win the war, but it can definitely be a powerful tool. That is why, when discussing the new cyber arm in the IDF, we have to remember that it is not only the army that requires defense against cyber attacks, and that in order to achieve their goals, the enemy might go after civilian, government, and financial targets as well.

I think that deterrence is one layer of defending your country, be it cyber or not, but it is full of uncertainty – you never know whether or not what you do will indeed deter your enemies or have been deterring them. Even if you have deterrence at a certain point in time, you don't know how long it will last, or how would your enemies' capabilities change. Potentially, Israel or any other major power has the cyber capability to significantly impact the utilities and critical infrastructure of their enemies, including electricity, water, etc. However, as we have seen, this has not prevented enemy cyber attacks, nor has it stopped Iran, for example, from continuing advancing their nuclear efforts. Another aspect of this is that it is very difficult to accurately identify the source of an attack. Kaspersky claimed that the malware found in the Swiss hotel hosting the talks between Iran and the West had the same footprint as the Stuxnet worm, and by conjunction this attack was attributed to Israel. However, as pieces of the Stuxnet code are available to those who know where to look for them, the Swiss hotel code could have been developed by anyone, from a 16 years old kid to a Nation State. Therefore, I believe that cyber, by itself, is not a deterring force.

What we need to do in order to defend the country from cyber attacks is to create a defensive array, sort of a "Cyber Dome", similar to the Iron Dome currently active in Israel, which will cover the military, civilian, and government sectors. This array should combine all the defense layers – deterrence, prevention, intelligence, etc. – and in addition to passive defense, it should also implement proactive defense, in order to push attackers into a defensive mode.

BRIG. GEN. (RET.) PINCHAS BAREL BUCHRIS, PARTNER, STATE OF MIND VENTURE

I have been pushing, behind the scenes, the establishment of a new cyber arm in the IDF for almost five years, and I am very pleased that this decision has finally been made. This step indicates upcoming major changes in the army. In the last two years, the high command of the IDF, as well as the Ministry of Defense, have begun to understand that cyber is a weapon; it may be a completely different weapon than what we are used to, but it is a weapon nonetheless. This is the fourth dimension of warfare, alongside the three classic dimensions – land, sea, and air. Cyber can kill, cyber can create a great deal of damage to infrastructure, economy, etc.; bombs are not the only way to cause damage to a country. Using cyber you can mislead weapon systems, or penetrate sensitive systems that connect to the net. This decision was made by the Chief of General Staff in his first few months in office, a bold move in which I support. As to the implications of this decision on 8200 and other units, it is all a question of implementation. It is possible that it will take time to implement this decision, and that it will involve some trial and error, but I believe that eventually this is the right decision, and that the army will succeed in implementing it correctly. Such correct implementation should allow the intelligence units to continue doing what they are used to do, but the development of offensive cyber capabilities requires more than just intelligence. This means that the work of the new arm should not only include the military and the Ministry of Defense, but also other organizations, such as the Shin-Bet and the Mossad.

Cyber capabilities are going to change the world. This is a non-physical war that has no borders, and everybody has to protect themselves. I see it as a balloon, which you have to protect with your hands, and the cyber attacks are pins that try to go through between your fingers. There is no system, military or not, that can be 100% proof. Currently, there are no more than 20 countries worldwide that have nuclear capabilities, and as such are considered to be a threat to other nations. However, cyber capabilities are available for everyone, and almost every country in the world has them. Moreover, this is not limited to nations, but also includes various organizations, and even individuals.

Some may claim that cyber warfare is different, as it happens in an asymmetric battlefield. However, in my opinion, since the Yom Kippur

war in 1973, Israel has not participated in a symmetric war. Versus terror organizations, this is always an asymmetric war, and the power is not equal at all. Our enemies' goal is to create the largest possible impact on civilian life; this is why they launch rockets on civilian targets, and now they see cyber as another attractive target. The Ministry of Defense, the Administration for the Development of Weapons and Technological Infrastructure, and the Israeli Military Industry have already taken care of "stupid" missiles, using the Iron Dome. Such missiles, and other "stupid" weapons, can't be neutralized by cyber. Other, "smarter" threats, require a different and more sophisticated solution. We have to take our enemies very seriously; they are very smart and capable people, and they have developed many cyber capabilities.

There is no 100% protection against cyber. However, I think that what our country is doing so far is not enough, and we need to invest a lot of money and efforts, not only in the military, but also in the civilian sector. We need to protect all the layers – from the basic infrastructure all the way up to the most sensitive computer systems. Putting a patch on one part of the system is not enough. The way to deal with cyber security in order to protect yourself is a strategic way – every layer in the organization or the country needs to be protected, and all the strategic layers should be well coordinated with the other layers. It will take time, but I think that our leadership is in the right direction.

CARMI GILLON, CEO OF CYTEGIC AND FORMER HEAD OF THE SHIN-BET ORGANIZATION

There is no doubt, in my mind, that the new cyber arm declared by the IDF is necessary. Cyber has existed for many years in the IDF in various forms and within various units, and so this is not a new thing for them. However, the way it is done today is uncoordinated, and I think that a centralized cyber arm would make it more effective. The big question, though, is – will it work? Our previous experiences in the security community are not good indicators for these type of projects. Israel is known for its innovation, which, among other things, stems from inner competition. There is a possibility that a centralized bureaucratic structure would impede such innovation and talent. The new cyber arm should act only as a coordinator, and not as a manager.

This is especially important, as I think that in the 21st century cyber warfare is going to be second only to nuclear weapon. Today the

battlefield is completely computerized; even the combat team that located Bin Laden had a direct digital video connection to the white house. This is the future weapon; it already exists, but in the future it is going to change the battlefield completely, and for that reason every country is going to invest a lot of resources in it. Take the 9/11 terror attack, for example. Using cyber, one can achieve similar results without risking any of the attackers; this can be done from anywhere and by anyone. You don't need suicide terrorist anymore when you have cyber. If you attack a control tower using cyber, you will have the same number of casualties without the risks involved in a physical attack. But cyber can do much more than that. The terrorists' goal is not necessarily to kill people, but to terrify the population. They don't care about ten people killed in a bus by a suicide bomber; what they would like to see is that every Israeli is afraid to go on the bus or to stand next to a bus in traffic, and the same goes to flights and so on. To stop traffic, you don't need to attack the towers, you can attack the X-Ray machine instead. No security officer will authorize a flight, the passengers in which have not been checked before boarding the plane. Every computerized system can be a target, and you don't have to attack the most critical ones to maximize the effect. This is not a future prediction, but something that can be done even today, and we know that terror groups, such as Daesh-ISIS, are already recruiting trained computer science engineers for this task.

The problem for us, as defenders, is that it is easy for us to prepare for the last war, but not for the next one. In the last three wars in the southern border of Israel, rockets were the main threat to the Israeli population. However, as it has already been proven, Iron Dome made these rockets less effective. This means that the next war will be different than those we have seen so far. I don't have enough knowledge regarding the abilities of Hezbollah, for example, but I am sure that they have prepared themselves for this new kind of war. The IDF is a completely computerized army, which, in a sense, is a weakness.

It is very easy to be an attacker in the cyber war, and as such you will always be ahead of the defenders. The defender will always need to get into the shoes of the attacker in order to understand what will be the next generation of attacks. However, the difference in cyber warfare is that thinking outside the box is much more difficult for the defenders, as it is hard to imagine what the next thing may be.

Moreover, you can't ask the Chief of General Staff and other generals to come up with a cyber-strategy, as they have experience in moving tanks and units, but not in this field.

In addition to these difficulties, there is also the matter of deterrence, or the lack of it. If we take, for example, the Sony case from 2014, it included two countries with nuclear capabilities that were involved in a cyber conflict. Following a movie that mocked the ruler of North Korea, the country initiated a cyber attack on Sony Pictures, which is an entirely civilian target. President Obama immediately assigned blame to North Korea, and ordered a cyber-retaliation. In response to that, North Korea did the same. Eventually, however, the entire conflict dissipated without much consequences. There is a moral to be learned here – it seems that the Kissinger policy from the cold war still stands today, meaning that the fact both super-powers have similar cyber capabilities provides a system of checks and balances, preventing an all-out cyber war.

Another thing to remember is that cyber is the new tool or weapon of choice, but the targets remain as they always were. Sixty years ago, the KGB dug a 1km tunnel in order to wire the Israeli Embassy in Moscow. These days we can simply use cyber to do that. But the fact that all countries have these capabilities makes attribution much harder. Is Israel capable of doing some of the things attributed to it by other countries and entities? According to the history of the intelligence community of Israel, as formally published, it is very likely. However, none of it can be proven, and it just might be the US, France, or any other country.

In order to properly protect a country from cyber attacks, you need to protect every layer because they are all connected. For that, the administration has to issue instructions and regulations regarding cyber security, such as regulation 361 that was lately issued by the Bank of Israel. Among other things, this regulation not only obligates banks in Israel to maintain a high level of cyber security, but they also have to demand it from all of their suppliers and distributors. Another example is the Executive Order issued by President Obama in the US, urging businesses to report any attack or incident they experience. Such regulations are going to play a very important role in the future of cyber field.

TECHNOLOGICAL TRACK

MR. INBAR RAZ, HACKER OF THINGS, VP OF RESEARCH, PERIMETERX

I am going to talk about ethical hacking, also known as "white hat hacking". I started doing computer science related things when I was nine years old, and started reversing when I was fourteen. At eighteen years old I found myself in the tank core in the army, and from there I ended up in the military intelligence, where I spent a large part of my career. Later on I went to work at Check Point, I started the malware research and the vulnerability research group, spent there three years, and now I am the VP of research at a new web and cloud security company called PerimeterX. In parallel to all that I am a volunteer member of the Red Team – we do coordinated and collaborative Red Team attacks on the large companies and corporations, that in our opinion, should they get compromised, the damage will be countrywide, and not just local to the company.

Our world is vulnerable. We are surrounded by software that is being made by so many vendors, and while on one hand we have curious hackers, who just play around and end up breaking things, on the other hand we have the professional hackers, the criminals, people that monetize on crime. The name of the game is now monetization; how can I make money out of stealing things. In the middle we have all kinds of "hacktivists" – the Syrian Electronic Army, Anonymous – and I left out the Nation States, because this is a game we don't want to play, and out of the scope of this discussion.

Someone needs to be the first to find those vulnerabilities. What happens if we are the first to find the vulnerability? We can get it fixed, and then there is one less door for the bad guys to walk through. But just going and looking for vulnerabilities, even if you are a good person, is a little complicated. There are three stages to the process of finding vulnerabilities – finding the vulnerability, reporting it, and publishing

it – and each stage has some points that we need to consider. For example, in the "finding" stage, was it deliberate or accidental – did we go looking for vulnerabilities, or did we accidentally try something, and ended up somewhere we shouldn't have? Did we use specific technique and hacking tools, or were we just playing around? Using professional hacking and penetration testing tools is not like simply playing around with some URLs, or manually typing what we hope would be SQL injection strings. Data access and extraction – do we access sensitive data? Do we extract it? Do we make copies of it? What happens if we cause damage? We are pen-testing somebody else's computer, and we did something, deliberate or undeliberate; what are the consequences? That needs to be thought of. Also, what is the victim's point of view? We know that we are the good guys, we know that we are trying to make things better, but what does it look like on the other side? When they are looking at the same situation, what are they thinking?

When it is time to report, and how quickly do we report? Do we take our time, or the minute we got something we give them a call or we write them the disclosure? Who do we report to? Is it some guy at the IT security? Is it the CISO? What language do we use – an offensive or mocking language, or a polite phrasing? You have to be neutral; if you tell someone "you have a problem, and we have just the product to help you", that may be perceived as extortion, perhaps also according to the law. You have to be neutral; say something like "Hi, you have a problem, it is your problem, you have to solve it. We are not going to help. We will give you, though, all the information that we have". And lastly, do you mention that you going to publish the vulnerability? Because that gets people into a defensive mode, which can sometimes even involve lawyers.

At the last stage, the publishing, you want to publish what you did. As a researcher – especially an academic one – you know that if you don't publish anything, you don't exist, your CV is empty. But when to publish? Do we wait for the vulnerability to be patched? Do we wait for the patch to be deployed? What sort of patch is it? What forum do we publish it in – is it in a local blog post with my company? Do we go on stage at a conference? Do we spill it all over the internet? What is the level of detail – do we publish a proof of concept? A proof of concept is a loaded weapon, so unless the vulnerability has been patched,

you don't want to issue one, because that means that everyone can now use a loaded weapon to make the attack. Also, do you get credit when you report a vulnerability? Because people like to be credited for their work.

Next is the vendor response. Do we include the vendor response when we publish? Do we wait for the vendor response to be published? And if we don't do that well, there is a law at the US, called the Computer Fraud and Abuse Act, which causes many strange incidents. For example, a guy in the 8th grade is going to jail because he changed the background on his teacher's laptop, using a password that was given to him by the teacher, or shown to him. Another guy used an open interface to extract e-mail addresses of AT&T, without breaking into anything or using any vulnerability other then ask a question and get a response, but he published it in the wrong way, and got sentenced to 41 months in prison. The most famous example is for that law is Aaron Swartz, who ended up committing suicide because he was facing a ten-year jail sentence and maybe even more, just because he was doing a service to the community, or at least that was his intention.

The solution is ethical hacking, and this is where we come in. An ethical hacker is a guy that looks for vulnerabilities in order to report them and get them fixed. We like to make the world a better place, and I know that many companies say that, but this is a purer semi-altruism – we want to get it fixed, we also want to get the credit for it, but these are not the reasons we do it. I like to give my dad as an example – if there is a vulnerability somewhere that is not fixed, then some hacker is going to use it, and my dad is going to get damaged in any way. I want to fix that because no one else is protecting my dad – or any dad, for that matter.

Some people say, "what about 'bug bounty' programs?". A bug bounty program is when a vendor says, publicly, "please find bugs, report them to me, and I will pay you money for that", which is a good incentive. But even the most famous bug bounty programs, like Microsoft's or Facebook's, leave out some things. For example, how exactly do you report a vulnerability? Can you just do whatever you want as long as you report it? Because hacking can also cause damage, as I mentioned before.

Last year Jeroen van der Ham, a Dutch professor in the University of Amsterdam who teaches ethical hacking, gave a talk called "Hacking Ethics and Education" in the CCC conference in Hamburg. In his lecture, he explained how they teach hacking ethics while giving a hacking course. He also explained that there is an ethics committee for every project framework that his students write, and phrased the "traffic light protocol" – and the following terminology and quotes come from his presentation. The color green means that there is no ethical consideration involved. For example, if we are working on an open software or on an offline database, we are not touching anyone, there is no harm done, and we can do whatever we want. The color yellow means that we make it into contact with personal data in a very confined way – for example, if we do some research and get somebody's address. But this is just an address, not social security numbers, ID numbers or credit card numbers. It is personal information, but not of the confidential type, and if we cause any damage it is going to be insignificant. The orange stage is when you might actually stumble upon, or get access to, large quantities of data – for example, if we facilitate a hack into the database of a credit card company, or the Target breach, we get credit card details of many people, which is significant. If we get their social security number, like in the OPM hack that happened in the US recently, where all the personal information of all the federal government's employees were stolen, this is serious. If we caused damage while doing that, it can have serious implications. The last stage is red, which means a project that crosses the line, but it is still important to do it anyway. An example for that is the OPM. If someone had done ethical hacking on the OPM, and discovered that they were vulnerable, that would have been highly significant, and maybe even worth the risk of getting into trouble, because it is such a big problem.

In April I was invited to participate in a panel in a conference called GCCS, Global Conference in Cyber Security, in The Hague. The conference was organized by the Dutch government, and the participants there were actually representatives of governments; We had foreign affairs ministers, ambassadors, Chief Information Security Officers for governments. The conference lasted two days and covered a lot of ground. I participated there in a panel about ethical hacking, where we talked on ethical hacking, how to do it right, what are the problems that we are facing, etc., and at the end of the conference we decided

to have a follow-up meeting. Eventually we created a workgroup, with the purpose of formalizing the process of coordinating disclosures, and called it the Organization for Coordinated Disclosure, or OCD. We wanted to create a process that lets you do it the right way, without hurting anyone or getting hurt.

We reached many resolutions, but I will mention the three most important ones. The first resolution is to create a safe environment and protections for vulnerability finders. We are very vulnerable ourselves, and if I report to someone and they don't like it, they can sue me, even though I just notified them about a problem that they had. The second resolution is to emphasize the maintenance of privacy protection for user and personally identifiable information. Wanting to find a vulnerability is a good thing, but you cannot create a new risk that did not exist before. Stealing the entire database just to prove that there is a vulnerability is the wrong way to go; if you can hack into the database and steal just two passwords, it is good enough to prove the point. The last resolution is to reaffirm the principle of doing mutually no harm, when researching and responding to a finder. I will cause you no harm when I look for the vulnerabilities, you will cause me no harm when I report it, because I am doing it in both our interests.

Sometimes things don't go as planned, even when hacking ethically. Last week, we at PerimeterX performed such a research, and we did it by the book: we created an ethical hacking project framework, identified the sensitive information, declared what must not be done and how to take the data from the server, do the processing, and immediately dispose of it, in such a way that cannot be traced back – and yet, somehow we apparently crashed a server. Once that happened we immediately sent out the disclosure, and three days later it turned out that the company that was giving the service was actually using a third party, so what we crashed was not the website to which we reported, but a third party vendor. So we contacted them as well, and sent them an updated version of the disclosure. I called them to ask if they got the report we sent, and they replied that they were on the way to the police, because we stole their information and crashed their website. I was shocked. Then I immediately contacted the company lawyer, of course. To make a long story short, it was a misunderstanding. The vendor felt that we were stealing information and wanted to cause damage. However, as we explained ourselves,

it all went away. So, even when you do it by the book, you never know who you are dealing with – maybe they don't like the attention, maybe they really think you are lying. Things can always go wrong, so be prepared, and have an attorney.

MR. YUVAL NATIV, R&D TEAM LEADER FOR NICE SYSTEM. CEO OF MORI.R.T

I would like to discuss the Internet of Things. It is a buzzword, but we will try to see what is inside it. The Internet of Things is the concept that one day everything will be on the internet – you will be able to check your refrigerator, your garage door, etc. But that also means more software and more components, and therefore more bugs. Usually software is more important than hardware. There are interesting combinations such as in the iPhone, but that is an exception, because most vendors don't have access to both software and hardware to combine them. I am going to talk about a few concepts that we saw, and then get into a bit of embedded device hacking, which is mainly a big word for an extract.

Instead of talking about regular smart items, such as the smart TV, I will discuss routers, a technology that is a bit more mature. These devices are basically the same thing as all Internet of Things devices – little hardware pieces with Linux running on them.

We chose routers for several reasons: they are common – everyone has them; they are very mature – they have been worked on for ages; they are manufactured by very big companies, and you can find them almost everywhere. The specific router model we chose was TP-Link TD-W8980B. We chose it not because it has something special on it, but because it has a huge bug that can be located within minutes.

When you download a firmware you just get an image, a file that has multiple sections in it. Using easily available tools you can extract the main section, and then you are just looking at regular Linux file system. There is nothing special in it, and it has no encryption – we can just start researching it. In the worst case scenario, you might need to do a bit of reverse engineering on some binary files, but nothing extreme. In one of the firmwares I analyzed I found out that in the login process of the Telnet protocol it kept comparing the authentication for a user name which is hardcoded – either "admin"

or "user". I couldn't figure out where it gets the password from, until I scrolled down a bit and noticed that it does the string compare again on exactly the same strings. Both the admin and regular user were hardcoded in the binary, and in both cases the same phrase was used for the username and the password.

Coming back to the firmware of the TD-W8980B, I found very disturbing things, and the first time I saw it I thought that the developer had to be drunk. However, looking at other firmwares I saw that most of them have the exact same issues. For example, when you take a look at the HDPD binary, the web server that is installed on the devices, most of them have all the configurations and the htmls hardcoded in the binary.

When investigating a firmware, we have to ask ourselves where to start looking for vulnerabilities? In other words, given a regular Linux system, where would the "juicy stuff" be? The answer is the Etc. As we mentioned before, the image is just a regular Linux file system. And so, if you look at the Etc folder, you see that there is a passwd file and a .shadow file, just as you would expect. Cracking the passwd file took me five minutes, using widely available tools, and I found out that the password for the admin user is "1234". Due to the fact that most of these devices have Telnet or SSH open by default, this basically meant I had acquired admin access to all of these devices. Looking further, there is also a VSTP passwd file, which is not very different, and you can just continue on to see all the things that are automatically enabled, which interface they are listening to, which port, which directory they give you, and of course, all the passwords are exactly the same.

One could argue that such an attack could work only from inside the LAN, but it is simply not true. For example, take the UPNP implementations in most routers. Most of the time it looks like a fourth-grader implemented them. It binds to all devices; it doesn't differentiate from where it gets the UPNP request. You can just send the UPNP XML request from the WAN, and it will map a local port out to the world.

This knowledge is easily accessible via search engines, it is very easy to download firmwares and firmware modification tool, and that is basically all you need to start hacking. In the worst case scenario you use IDA to open some binaries. Again, they are never obfuscated, and they are never checked in any way.

In summary, things don't look good in terms of IoT security, but there is hope, because now things are getting a bit more intimate. Once people get a bit more intimate with their devices, and see where they are and what they can do if malicious attacker attacks them, I think it might lead to a bit of an upgrade in security, which is, at this point, non-existent.

MR. TOMER TELLER, SENIOR PROGRAM MANAGER, MICROSOFT AZURE CYBER SECURITY GROUP; MR. GIL DABAH, CO-FOUNDER & CEO OF NORTHBIT

We would like to demonstrate a vulnerability that we have researched and found in Windows 8.1, allowing to move from user mode to kernel space, and from there run malicious tools. One of those tools is Mimikatz, a Windows post-exploitation tool, usually used by hackers after they compromise a machine, whether it is on disk or in memory, using meterpreter, metasploit, etc. Once they get their tools into the compromised machine, they would likely extract some sensitive information from the computer, such as clear text password (previous to Windows 8), password hashes, Kerberos tickets, etc., and use it to move laterally in the network using "Pass The Hash" or "Pass The Ticket" techniques.

When attackers manage to compromise the machine, how do they manage to grab the hashes and move laterally inside the organization? In order to understand where the hashes are stored, we need to understand a little bit about the LSASS process. LSASS, Local Security Authority Subsystem, is responsible for the overall security policy in the system whenever a user logs in. It also manages the SAM file that contains all the local users. Most importantly, though, it is there to support the Windows Single Sign-On – the feature that allows you to type your password once, and then log into any resource available to you in the network without typing your password again. To make this work, LSASS has to store the hashes, the credentials encrypted in memory, in order to present it to the resource, saving you the need to type in the password each time.

Imagine this scenario: we managed to compromise a computer network, tried to move laterally inside the organization, but failed to do so; Mimikatz failed to extract the hashes from the LSASS process.

The reason for this was we compromised a hardened Windows 8.1 computer, running Protected Process Light, a new security technology from Microsoft. This technology that doesn't allow even a system administrator, with the highest privileges, to access critical processes. Microsoft added it because it is obvious that the "least privileged" model failed; people abuse it too often, and everyone is assigned admin privileges because they don't want to use the "run as administrator" option all the time. Because of that, Microsoft wanted to have a more granular protection level for each process. They marked critical processes, and now, even as an administrator on your own machine, you can't access them. On top of that, they removed all the plaintext passwords from memory, but the hashes are still there, in order to support Single Sign-On.

Why are the hashes important, if the plaintext passwords are gone, and how can we move laterally in the network? In order to move laterally inside the network, you don't actually need the clear text password. You only need the hash, because protocols such as Kerberos and NTLM leverage those hashes in order to communicate in the network. Our goal is to obtain those hashes, which are potentially stored in LSASS memory. However, we cannot access it from user mode anymore, because of Protected Process Light.

When looking at the Task Manager in a computer with Protected Process Light, we can see that when trying to perform a memory dump on the LSASS process – where all the keys are stored – we are denied access, since this process is protected. Mimikatz fails to do that same thing as well, when trying to add the debug privilege into the process. This means that if you are an attacker, you won't be able to penetrate a hardened Windows 8.1 with your regular tools using that method. In order to get in, we need to define three objectives. The first objective is to infiltrate the kernel, since we can't get those hashes from the user mode. Once we are inside the kernel, we move laterally inside the process memory, the kernel memory, looking for the LSASS process, and attach to it. Once we're inside the LSASS process, we work linearly, looking for a specific signature, extract the hashes, the keys, and decrypt them.

Our first objective, getting inside the kernel, is not as easy as one may think. Attackers have had a hard time recently, because Microsoft is investing substantial resources in order to secure the kernel.

For example, data structure hardening is something that Microsoft added in the last couple of releases and patches. They listen to the attackers' community, and whenever attackers use a specific object in memory in order to exploit something, Microsoft changes that object to make it even harder to exploit. We also have ASLR, Address Space Layout Randomization, which means that every time the system boots or a process loads, at least in user mode, all these models are randomized in memory. This means that an attacker doesn't know where the addresses are located, so when they are trying to do their return-oriented program jumps, they won't be able to write to fixed addresses. Microsoft ported the same technology into kernel space, making it even harder to understand addresses and models inside the kernel. Same goes to DEP, Data Execution Prevention; users give the operating system data, which it can't trust, and can't place in an executable place, because attackers will pass a shellcode and then execute it. This barrier is enforced by DEP, and the same technology is ported to the kernel.

Last but not least we have the SMAP, a new technology enforced by the CPU. In order to exploit kernel vulnerabilities, the hackers have to allocate their shellcode in user mode, and eventually exploit the vulnerability in the kernel to make it run from within the kernel, transferring the control back into the shellcode in user space. The reason for this is that usually, when we hack into systems, we come from a user mode process, e.g. a browser. To mitigate privilege escalation, the processor can detect this kernel space to user space mix.

In modern operating systems, such as Windows, we use virtual memory, which is technically done by page tables. Each and every virtual page is described by a PTE, Page Table Entry. A PTE is a set of bits that contains or describes the virtual page characteristics, such as whether it is writeable and/or readable, and what is the physical page that it actually maps to. One special bit is the owner bit, indicating whether the page is in the user space or the kernel space. All that the CPU has to do is compare between the CPL and the owner bit. The CPL is the Current Privilege Level. It means the processor is running inside ring0, so CPL is 0, and then if there is a mix between the owner bit and the CPL we know that is should not be run, and the exploitation is busted. Starting with Windows 8, this feature is enabled once Windows boots, and it simply sets the 20th bit in Control Register 4.

We are going to present a few techniques that the security community has developed in the last two years. The first technique is a kernel rope, jumping into a code snippet inside the kernel that will disable this exact bit. Once this bit is disabled in the CR4 register, the processor will stop detecting kernel space to user space mix. The problem with this technique is that it is very nice in theory and in the lab, but in reality, hackers can't use it. This is because in different Windows versions, patches, and updates, the offsets inside the kernel change all the time. Another technique that used to work until Windows 8.1 was to maliciously craft a special object in the kernel, containing the shellcode. Because the object is already inside the kernel, and because it used to be inside an executable pool, that code wouldn't be detected or stopped by SMAP. We took another approach: instead of manipulating CR4, we circumvented SMAP entirely by changing the owner bit in the PTE containing our shellcode.

In NorthBit, we researched a new technique, which is supposed to be much easier and much more robust – a very important thing if we want to use exploitation in real life, for example in pen-testing. Imagine that we manage to find a kernel object that gives us the ability to write user-defined data into it – in our case, the shellcode. We copy the shellcode into the kernel, and the kernel can't stop it. This should not be possible, because you are not supposed to be able to copy anything into the kernel; the operating system shouldn't allow you to do it. We found that in one simple API, insert menu item, you can add a string literal, which we can use to write our shellcode. By calling this API – which is completely documented – you trigger a syscall, which copies the data from user space to kernel space. Once in kernel space, we don't even need to change the owner bit of the PTE, because it is already marked as kernel, thus bypassing SMAP. However, there is another problem we have to bypass. Starting with Windows 8.1, the kernel was hardened again to separate pools of memory, and now DEP is blocking us. In the past, kernel drivers used to be able to allocate any object to anywhere in the kernel, but now they have to allocate each object to a specific pool; some of these pools are executable and some are not. This means that we need to find a way to not only manipulate an object in the kernel, but we also need it to be in an executable pool.

What attackers do, as we have seen in researches on the internet, is to manipulate the PTE, where the shellcode is located, and change bit number 63, i.e. the NX bit – No Execute. When this bit is active, everything mapped inside that PTE is non-executable, and DEP is enforced. The attackers locate that PTE in memory, and patch that single bit. Once this is achieved, DEP is disabled and the object becomes executable. Once again, locating the PTE's virtual address in memory is not an easy task, because of KASLR and other mitigations in the kernel. However, research showed that there are some fixed locations in memory, what we call ncores or base addresses, existing across all versions of Windows. This means that even if ASLR is enforced, the attackers can still manage to get to the ncore and jump to the place they want, circumventing KASLR. All they need to do is form a simple formula, comprised of the PTE base address and some other objects, in order to find that PTE in memory: PTE_VA = PTE_BASE + ((kOBJ_VA >> 12) << 3)

There is a missing link in the formula, though, since we don't know where the object is located in memory. To find it, we need a vulnerability, such as the one found in the Win32 kernel model, responsible for all the graphical user interface in Windows. Because this model is in the kernel, every time a user space process performs actions related to graphics, the process is switched from user mode to kernel mode, what is known as context switching. This switch takes time for the processor, and in order to make it faster, the designers of the operating system mapped some of the kernel mode objects into user mode. They gained performance, but this created a security problem, because now some pointers to kernel addresses are revealed to the user mode process, where the attackers work. In our proof of concept, we use a "use after free" command of a MenuState object, inside the Windows kernel, that is already patched. Imagine that there is a thread A, and it wants to show the user a simple menu. But suddenly comes thread B, which somehow references the same MenuState object of thread A. If thread B manages to kill thread A, it has to kill all the objects it owns, including the MenuState object. However, at this point thread B still points to unallocated or garbage memory, effectively creating a kernel crash.

The first objective has been accomplished, we managed to infiltrate the kernel and get it to crash. But that is not enough. Next we need

to access LSASS memory from the kernel itself. For that we need to transfer control to our shellcode. Using the techniques mentioned above, we can patch DEP, which means that the object is now executable. Now we only need to make sure that something jumps into our shellcode and starts the execution. In order to do that, the 1-day vulnerability was coded in a way that once its code runs inside the kernel, it is going to patch some callback pointers, and then you can call a function from the user mode, that in turn calls a function that calls a system call, which eventually floats inside that callback and calls our shellcode, and executes it.

Usually, the first thing we want to do in a shellcode is to locate NTOSKRNL, where all the code of Windows kernel exists. If we find it, we can use the APIs exploited by this model. Once we find it, which only takes a single processor instruction, we need to find the APIs themselves, the ones we would use in our next steps. To do that we use a simple home-made GetProcAddress code that helps us do it, and then we only need to locate LSASS itself. But every time you boot your computer, there is a new ID for the LSASS process, meaning that we need to scan all the processes in the system in order to locate the right one. There are many techniques to do it, but they are not as robust or as stable as we would like them to be. What we can do instead is to simply read the PID of LSASS from the registry – this is an uncommon property LSASS possesses, since not all processes have this information stored in the registry. Once we do that, we can attach to the LSASS process. Attaching from kernel means that we changed the virtual address space of the user space, to that of LSASS, and now we can access it from kernel mode, from our shellcode.

The next thing we want to do is to start implementing our shellcode, jump into it, and scan the memory. We have already seen that we can neither dump the memory, access it, nor use Mimikatz, but coming from the kernel side, it is a different game. Once we manage to access the memory, we want to extract the hashes from memory, which is quite easy. There is also a lot of research done by teams, such as the team behind Mimikatz, showing that credentials are stored in memory in a reversible way, in LSASS address space, which means that now we have access to the hashes. We also have access to the keys that rely on the same memory space. All we need to do is scan the memory linearly, looking for a specific set of signatures based

on the operating system version. Then we can dump those keys and hashes, decrypt them using the algorithm that was used for their encryption, whether 3DES or AES, and reveal the password. Once we managed to get the hashes, we managed to get in, and our goal has been achieved.

A short recap and a summary: Windows 8.1 security improved significantly. They added many security mitigations, such as protected processes, and the hardening of data structures. There has been much news coverage in the last couple of weeks concerning many attacks that target memory, such as dump persistent malware – malware that only resides in memory, which means that when the process is done, everything is wiped away. We recommend that you focus on live memory forensics, which is going to be the next big thing. Everyone is talking about it, but no one is doing it well just yet. "Pass the *whatever*" is still here to stay, as long as Single Sign-On is still here, and we make substantial efforts to make sure that no one gets into those hashes. And while you think that kernel access is over, things are going to change drastically in Windows 10, introducing a lot of new technologies, such as vContainers, which make getting those hashes extremely hard and sometimes impossible.

MR. EZRA CALTUM, SENIOR SECURITY RESEARCHER, AKAMAI'S CLOUD SECURITY INTELLIGENCE

I would like to discuss the topic of full SQL injections. The data I present here is not theoretical, but based on an analysis made in Akamai on real traffic that we encountered. But before we can begin, I need to explain why can we speak about attacks in a global scale, and how can we carry out this kind of research? First of all, Akamai's main priority is to bring content from point A to point B in the fastest way possible. To be able to do that, we have more than 160,000 servers in more than 2,300 locations, which means that we have presence in more than 750 cities, 92 countries, and 1,000 networks. This translates into about 2 trillion hits per day, enabling us to see around 780 million unique IP addresses every quarter, 13 trillion LOCs (lines of code) per day, and 216 terabytes of compressed daily LOCs, constituting 15-30% of all the web traffic.

Much of what happens on the internet is attacks; therefore, from that corpus of information we have, we decided to take a look into the SQL injection attacks. We took seven days of research data to be able to look into 2,000 applications, and there we saw something like 8-8.5 million different injection attacks. The first question that we as researchers had is, what are the attackers trying to do? Our first objective, therefore, was to try and categorize what the attackers were actually doing. The first step in an SQL injection attack is to try to identify if the application is actually vulnerable, which is as simple as the equation "1 = 1". It is something that the computer will always accept as true, and this is a very simple way to identify if the application is vulnerable. Searches are the most common form of attack that we see – about 5 million out of the 8 million attacks that we saw included probing – roughly 59 percent of all attacks. This is a very big number, as most of the attacks we see include this particular kind of strings. Therefore, for the next statistics I am going to present, I will take a normalized approach, where we will present the ratio of these attacks, and the same ratio without these particular probing attacks.

The intention of injections that we see in the majority of attacks is probing in order to try and understand which back-end data the platform is running – MySQL, Oracle, Microsoft SQL, etc. We saw roughly 1,300,000 such attacks (15.5% full ratio; 38.42% normalized ratio). This is very useful as an attacker – if you know that you are attacking a MySQL database or an Oracle database, you will be able to optimize your SELECTs or your UNION SELECTs to that particular platform. You will be able to try to find particular hashes or exploits for this particular platform, and that explains why we see so many attacks in this category.

The next category that we saw, which surprised us a little, was database content retrieval – what we in the internet used to see as the dumps. Whenever the attackers managed to hack into an application using SQL injection, one of the things they tried to do is retrieve the entire database. UNION SELECT is one of the many techniques used in order to do that. There were about 129,000 such attacks (1.5% full ratio; 3.8% normalized ratio). Why do we see so few of these attacks? Our analysis has shown that attackers prefer credential theft over database content retrieval – there were nearly 2 million such attacks (23% full ratio; 57% normalized ratio). When attackers can connect to the back-

end but can't get credentials to the back-end, UNION SELECT and all the techniques used to gather the content of the database make a lot of noise. On the other hand, an admin can see everything and do anything quietly, even with platforms like Drupal or WordPress, for example. Additionally, an admin can inject code, among the rest, which is probably one of the reasons that most of the injection attacks try to get credentials from the system.

Another interesting kind of attack that we saw is the login bypass – when you are presented with a username and a password, and the attacker puts as the username the phrase "admin or '1 = 1'" (or an equivalent phrase). Since 1 is always equal to 1, and this statement is true, the attackers get access to the back-end. In this particular category we saw only about 5,000 attempts (0.06% full ratio; 0.16% normalized ratio); we couldn't explain why there were so few attempts of this type. In the old days, when you were doing an SQL injection, you were able to run commands in order to try and read system files, such as "etc/passwd". As this attack technique became more and more common in the industry, the default configurations of most of the database platforms would not allow to read system files. This is one of the reasons why, out of 8 million different attacks, we can only see 24 injections (0.00028% full ratio; 0.0007% normalized ratio) trying to use this particular attack technique.

The next type of attack that we saw in the wild is attempts to shut down the database – a type of denial of service, although it is not as malicious as what we are going to see next. In this particular scenario, the only thing that the system administrators would need to do is to reboot or restart the particular instance of the server. And we can see that only 326 injection attempts (0.0038% full ratio; 0.0095% normalized ratio) have been trying to use this particular attack. Another type of attack that we saw more of is attempts to corrupt the data: to drop tables such as the users table, drop the LOCs, or simply drop everything. In the Stratfor hack in 2011, once the attackers stole the entire database, all the usernames and passwords, they just dropped everything. In our data corpus we encountered 2,238 such attacks (0.0265% full ratio; 0.0657% normalized ratio).

Next we can see attacks of defacement and content injection. Once the attackers steal the entire database and drop all the tables, what other mischief can they do? The answer is – they can inject content.

For example, the attackers try to inject a stored XSS to the website, in order to send its visitors to a "watering hole", where they will be redirected to an exploit kit. Attackers don't only hack and pound the web servers, but rather, they also use the servers they attack as platforms to infect users. Our analysis found 8,156 attacks of this type (0.0967% full ratio; 0.2394% normalized ratio).

The final objective of an attack is to try and get remote command execution. Looking at the statistics, the number we get is small, only 794 of them (0.0094% full ratio; 0.0233% normalized ratio). This could be explained by the fact that nowadays most of the databases are secured by default against this kind of attacks. Since we switched to more default installations of platforms, most of the system commands that allow to actually execute activities in the system are restricted, and we don't see that sort of attack very often anymore.

To summarize, malicious attackers use a variety of techniques, and there is not only data execution that we see in the wild, but also attempts to elevate privileges, to execute commands, to infect or corrupt the data, to deny service, to use these platform servers, watering holes, etc. Attackers continuously become more advanced, and we, as defenders, need to take into consideration these kind of activities.

MR. NETANEL RUBIN, VULNERABILITY RESEARCHER, CHECK POINT

I would like to discuss the RCE (Remote Code Execution) I found at the very popular eCommerce platform Magento. This is the kind of platform companies use when they want to open an online shop, and Magento – currently owned by eBay, after being purchased in 2011 for $180M – is the most popular platform of its kind in the world, with over 30% market share. In all aspects, this is the eCommerce platform to use if you are opening an online shop. It is flexible, reliable, and very corporate-oriented. This is why hacking it can be very significant.

What we found in Magento was an unauthenticated RCE attack, meaning that an attacker can take over any Magento store without any prior conditions. The vulnerability was in Magento's core, so we don't need any specific plugin to be installed first; and it is not an XSS type of attack, where admin intervention is needed for it to work. If you are interested in the full white paper, please have a look for the "Analyzing the Magento vulnerability" blog post at Check Point blog.

As mentioned above, Magento is very flexible, and it allows anyone to develop new custom features. In order to provide that interface, Magento is made out of several small pieces of code, each providing a different functionality. At its base, Magento is made out of modules – packages containing codes for different parts in the system. For example, there is a module responsible for the purchasing system, one for the customers, one for the product, and so on. Modules are made out of controllers, which are PHP classes providing specific functionality for different parts in the module. For example, there is the login controller, a product view controller, a forget password controller, etc. These controllers, in turn, are made out of actions, which are methods inside the controller class, that contains the actual code from the controllers' functionality.

Looking at the structure of a regular HTTP request, for regular and unauthenticated users, it is composed of the module name, then the controller name, and then, if needed, a specific action. For administrators it looks exactly the same, except this time an admin prefix is inserted at the start of the URI. As attackers who want to exploit the vulnerability, first we need to bypass the admin authentication. Admin privileges can gain us access to powerful controllers and expand our attack surface. When Magento encounters an Admin request, it first checks it for an active session. If it can find any, it then checks for a login attempt. If both have not been sent, all the supplied credentials are invalid, and Magento changes the controller we requested into the default login controller – basically, overriding our controller. That is important to note, because Magento doesn't block our request, it just changes the controller.

How does Magento decide when to change our controller and when not to do so? The code contains a line that is responsible for changing our controller. However, the line prior to that line checks if a certain parameter named "forwarded" is false, and only if it is indeed false does Magento change the controller. This means that if that parameter was set to true, the controller change will not be executed. But how can we control it? Magento made a false assumption, and treated that parameter as an internal property, set only by the system, when in reality, this parameter is part of the HTTP request instance, and can actually be controlled by the HTTP parameters as well. So if we are to send this request, setting the "forwarded" GET parameter to "1",

the check will fail, and our controller will not change. This means that we can now access the admin panel unauthenticated.

The only problem with this bypass is that some controllers are also checking for specific privileges, and as we are unauthenticated, we of course don't have any. One of the controllers that doesn't check for privileges, is the "What You See is What You Get" controller (WYSIWYG), which is responsible for displaying images using a user imported path. We control the directive variable of this controller through our HTTP parameter. This code contains a "filter" line – this is actually a method inside the admin template parsing class. As we provide the input for that function, we are actually treated as an admin template file, and thus can use any template directive we want. One of those directives is the block directive, which allows us to create a block class and execute a method inside it, bringing us deep inside the internal system mechanism, and giving us access a lot of code. Blocks allow us to filter their data, using an SQL WHERE statement. Because we are treated as an administrator, we can control the field on which this statement is executed on, and the field is considered safe, and escape characters are not being added to its content in order to protect against an SQL injection.

Now we perform an SQL injection, meaning we can alter the database as we like. So we will be using this injection to insert a new file record into the database. Our file is considered by the system as an image uploaded by an administrator. Due to performance issues, Magento only stores the file in the database first, and creates it on the actual file system only when someone tries to access it. We do that by using the get.php script, which extracts images from the database into the file system.

Now our file exists physically on the file system. Unfortunately, our file has been created in the media directory that contains the images for the system. Because it is an image directory, CGI scripts located there can't be executed. We don't want to override the .htaccess, because it is too suspicious, but we still want to create a valid image file and execute any PHP code we would like inside it. For this we will use LFI (Local File Inclusion). LFI is an attack used to execute files that are otherwise non-executable. Looking around, I came across a function that includes any file that we want. We can control the path being included, thus we are able to include our file. But in reality things

are not this simple – a forward slash is appended to our file, making our file path into a directory path, which cannot be included by PHP. To handle this situation, we will use RFI (Request For Information), because we control the entire path prior to that slash, and the stream wrapper as well.

PHP has many stream wrappers such as HTTP and FTP, but unfortunately for us, those wrappers cannot be used in PHP versions greater than 5.2, which came out in 2006, nine years ago. This makes LFI seem useless for us, but we are not done here yet. There is a wrapper called "phar://", an almost hidden stream wrapper that acts as a JAR for PHP files. It is actually an archive containing PHP files and code. If a Phar is included, its PHP stub code is executed. When we try to include a Phar file with an ending slash, like in our case, the system treats the ending slash as the root for the Phar file as if Phar was really an archive. This hidden, unknown wrapper allows us to execute our LFI.

We finally managed to include our file and execute it via the system, which allowed us to completely compromise and control any Magento store, and get what we like for free. Who uses such a vulnerable system? Well, eBay does, as well as Samsung, Lenovo, Olympus, Vizio, Nike, the New York Times, and about 250K other stores. Hacking a Magento store is very significant for several reasons, mainly because the platform stores the customer credit card numbers, allowing an attacker to steal any future card being used, and in some stores, even the ones previously used. It also handles the purchasing process, allowing an attacker to change the owner's bank account to theirs, for example. And if they want to, attackers can even "buy" things for free. On a more corporate level, the vulnerability allows an attacker to steal customers' full data, including addresses and phone numbers. The most surprising fact of all is that Magento stores worldwide handle over $60B per year, a staggering amount for a system so unsecure.

We reported this vulnerability to eBay security contact, and provided a full technical description. This granted us $20K as a bug bounty reward, which we donated to charity. Have they fixed it? The simple answer is yes. Magento released a patch to address the flaws. However, while the patch blocks the described attack, it is still not perfect, because they left several non-critical flaws unattended. It is important to emphasize that we published this vulnerability only after we made sure there is a patch, after a total of 96 days after the private disclosure.

In conclusion, even if we are dealing with an eCommerce system that handles $60B per year, and even if it is owned by eBay, it seems as if no code is completely secure.

MR. YITZHAK VAGER, VP CYBER PRODUCT MANAGEMENT & BUSINESS DEVELOPMENT AT VERINT

I would like to talk about lateral movement today. There are not many solutions in the market today that try to detect lateral movement, even though lateral movement does something that doesn't make sense in the network: If I try to access a computer next to me, or directly access the data center or another resource in the network, it doesn't make sense in the regular way that the network operates. Despite this case, there are not many solutions to this issue. We will look into it and try to see what is going on inside.

The first example is an operation supposedly revealed by Kaspersky, although Fox IT from the Netherlands actually revealed it earlier; The malware in question is mostly known by the name given to it by Kaspersky – Carbanak – even though the Fox IT team called it Anunak. Kaspersky claimed that nearly $1B have been stolen from various banks using this malware, mainly by a group of hackers from both Russia and Ukraine. They did most of the work in Eastern Europe, but not all of it. They started by sending some spear phishing e-mails to everyone they could, and then tried to move laterally within the network, trying to get to some interesting resources, and to obtain admin credentials. In some cases they managed to get into the Oracle databases, where they created new accounts, got into existing accounts and increased the cash balances, then wire-transferred the money to other accounts, sometimes in other banks. They managed to activate the ATM machines to give them money. They did something truly amazing.

Looking into the details of that attack, once the attackers compromised the first machines, we can see their tool box. This includes everything that a system administrator's tool box may include, as well as additional tools. The first set of tools is aimed at remotely connecting to machines and executing command. These include tools like Ammyy Admin 3.5 – a remote admin tool used by every administrator, a Telnet/SSH client, PSExec, etc. Other tools are meant to exploit weaknesses and vulnerabilities. In this case, the attackers used Mimikatz, which

enables attackers to harvest credentials and hashes from memory, allowing them to execute "pass the hash" or "pass the key" attacks, allowing them in turn to log on to another machine.

Looking into fifteen different such attacks that are covered on the internet, we see that no matter where the attackers come from, they all use similar tools, be it an Iranian attack on Saudi Arabian assets, or even professional pen-testers. Unlike the exploitation and infiltration phases, and the resources invested by attackers in order to keep a more permanent control over the machine, lateral movement usually involves standard tools. Not so many detection tools are available for lateral movement these days, which is very surprising. It also means that, unlike the common assumption that attacks are mainly automated, they are not so. The first phase is automated, but in later phases there is a man behind the machine, moving around the network, trying to get into something more interesting and powerful in order to steal information, steal money or create damage. Therefore, there is a lot of potential in protection from lateral movement.

What is the process of lateral movement? The assumption is that first you have any kind of a compromised machine with access to the network, either within the network or outside it, and you use that in order to, first of all, try to escalate your privileges, i.e. get local or domain admin rights. There are many ways to get admin rights – sometimes there are mistakes you can exploit, or you can use a "zero day" attack to obtain those privileges. The next stage is trying to move laterally from one computer to another, until, hopefully, you get a golden ticket – perhaps Kerberos tickets – of a domain admin, and maybe even the ability to do things in other domains that are within this network and jump between domains.

The challenge of both the attackers and the defenders is to try detecting the lateral movement. It is like trying to cross a river – you need to find the narrowest place to cross, then you need to make sure that the current is not too strong, and find stones to step on without falling down. Attackers will try to do many things: port scanning or IP scanning; ARP spoofing; rerouting the traffic via their machine, to serve as a man in the middle to other traffic within the network; finding some network share, in order to get the credentials and jump to another machine. They will try to use any kind of remote protocol to get into the next machine, to get a full hold of the network.

On the other hand, the challenge for the defenders is to try and detect these different methods. The defenders could be in the end points along the network, they could be in the network, passively monitoring the traffic, and they can even fake an end point, using the "honeypot" method, and then try to get the attacker to jump into that honeypot, and catch him over there. You can also combine methods and work from both the end points and the network. When you are at the end point, trying to detect lateral movement, you try to collect forensics for the different activities such as the above mentioned. You can do so by simply looking into the operating system log – some logs are very comprehensive, and you can get a lot of information by viewing them. Otherwise you can implement an agent at the end point, and run it in the device level, on the application layer, or on both, in order to try to detect all that was discussed earlier.

Another way to detect lateral movement is by passive monitoring of the network. To be able to detect lateral movement you cannot just monitor the gateway of the network, you need to go into the internal network segment, between the different machines, where all the network switches are, and monitor from there. This is easier said than done, though. The network managers may tell you not to go there, but this is the place where you can see everything; the attackers will not know that you are there, but you will be able to see all their lateral movement activities.

The next technique is improvising a fake end point, which can be located on a virtual machine in a centralized place in the network, connected by kind of a VLAN to that centralized place, and it needs to look like a regular machine. You need to leave some honey tokens on the compromised machine to try and persuade the attackers to move into that fake machine. If this works, the attackers would try to take over the fake machine, and you can catch them. You can also catch the actual weapon, because one of the things the attackers may do is to compromise that honeypot in order to go to another place in the network. These are our three defense techniques against lateral movement.

One of the ways to detect lateral movement from the end point perceptive is to look for these specific tools from the attackers' tool box mentioned above. You can look for signs and traces of them in different files, actions of privileges escalation, or look at all the processes within

that machine and search for malicious processes. It is also possible to look into all remote accesses from a monitored machine to machines that were not supposed to be accessed. All these can be done using an agent at an end point.

Each method of defense against lateral movement has its advantages and disadvantages. The end point is usually very cost effective; you can deploy it from a centralized location, it runs on the end point, you don't need additional machines or additional devices to deploy it. You can gain high visibility, because you see everything, including many things that cannot be seen from the network, such as harvesting of credentials. On the downside, this method is intrusive; not everyone likes that invasion to their privacy, and the attackers may be able to detect you, because you are running on the same machine as them. The lateral movement could also be between different platforms, for example from an iPhone to a Linux machine within the network, so you need to develop something for all platforms and operating systems in your network, which is complicated.

The network based approach gives you full transparency, no one knows that you are there unless you tell them. You have a sniffer over there, and it is in a fully promiscuous mode. There is a clear isolation between what you are doing and what the attackers are doing. The lateral movement protocols over the network are always the same, it almost doesn't matter what device or OS you are using, so you don't need to implement the method in multiple ways for different operating systems. The high cost is a disadvantage, though. To deploy something in each segment of the network, you need now to go to all of these segments – whether on another floor, building, city, etc. It is more complex to implement such a defense. In addition, some of the protocols are encrypted, meaning that it will be very hard to decode them and enable network monitoring.

The deception approach, or the "honeypot" method mentioned above, is a more proactive method than the others – you try to persuade the attackers to do something. The deception is an emerging field in the industry. Many customers push to try and do something more proactive, make the attackers' lives more difficult. The cost is medium – you need to install a device in the network, or you can do it at an external location, and still you need to access or manage all those switches in all the different places within your network. On the downside, this

method is highly intrusive; you are doing something in the network that was not supposed to be there, and people – especially customers – don't like it, because this means changing their network, adding things they are not sure that will not affect their business. You have partial visibility, depending on how good you implement the honeypot. Sometimes sophisticated attackers will be able to detect the honeypot, if they see something that doesn't make sense to them. Then there is the complexity in deployment.

These are the pros and cons of all the different methods. There is no single winning method here, it is just a matter of advantages and disadvantages. In Verint, we don't do just lateral movement, but offer a holistic solution that is mostly network and end point, and does both detection and forensics in both ways, as well as combine all the information into a complete incident response system. This system allows you to move in time, so you can look back and see what happened in the network, as well as tell some of the detection engines to try to detect a specific incident. This allows us to see information through a complete network, not just a specific location, as well as to automate the steps of the investigation. This a special product that we just launched recently to the enterprise environment to try and defend from lateral movement.

MR. OFIR ARKIN, VICE PRESIDENT AND THE CHIEF ARCHITECT AT MCAFEE, INTEL SECURITY

I would like to discuss the topic of a holistic solution approach rather than a specific product. Being in a startup company for nearly eight years, you always think that the problems you are trying to solve are the most important problems in the world, only to realize that this is not really the case. Only when you start working for a bigger company, and get access to larger customers, you understand that in most cases customers are dealing with yesterday's issues. These are customers with 100,000-200,000 end points, numbers that Israeli startups don't usually get access to.

Our way of thinking about what we do and how we design the architecture of our solutions sometimes significantly suffer from that mentality, of not really looking at the overall problem and trying to solve it from a solution perspective. When I served as a Chief Information Security

Officer, the easiest way for me to go and persuade my CIO to buy a product was to show him that the product is in the upper right corner of the magic quadrant for Gartner. Doing that got me the money for that product quite easily. The problem that we created by buying best-of-breed products, is that those products don't communicate with each other. With each product we bought we added another dashboard, another screen, another silo of information that cannot be shared. For example, if the Firewall managed to find a new attack, blocked it and log it, that knowledge might be useful for the end point as well, when it hits the same type of an attack.

We can see that organizations that bought the right solutions at the time, ended up in a situation where instead of getting better at their return on investment in their operation and automation, they are getting worse. They have complete lack of visibility, they cannot connect the dots between the different solutions, and it gets harder and harder for them to continue leveraging the products, compared to the pace of change in the attackers' community. The latest Verizon report showed an interesting graph that describes the pace of change, or how fast an attacker can compromise an organization, and how slower the organization itself reacts to it. Organizations don't usually have infinite funds, so they are lacking some of the manpower, expertise and processes to deal with this.

Looking at these things, the end result is very clear – we see a shift in how the industry looked at cyber security management before and after the Target breach. The reason is that everyone in Target that were responsible for security, from the CISO the CIO, even the CEO. left the company because of that incident. That incident showed us that we have an issue, which is one of the biggest problems in security, and it is called automation. Many people get a bad feeling hearing the words "automation" and "security" together, when you try and explain to them that with the amounts of information that we have to process, generated by different solutions and products to operate in their own silos, there is no way whatsoever we can have a successful security operation. With that, we try to look at the world and to describe this problem in an even simpler way. As mentioned above, one solution or product might detect something; however, as long as they don't share that information with the rest of the security estate, your ability to better defend yourselves against that specific

threat, or new or old threats that may share the same characteristics, is basically non-existent.

The whole idea is to try and understand how what you detect may have future effects or may already have an effect over your security posture, by researching better, by understanding what this smoke signal tells us. A good example is a Firewall that detects an evasion attack. We'll assume that the Firewall blocked this evasion attack, and that a file was used as part of the evasion attack. According to our logic the Firewall did a great job blocking the attack, but there are two interesting parameters that are usually left alone and not touched. The first is the file that was blocked, and the second is the context at which we can use in order to understand how we can take this indicator and transform it into an indicator of attack. So for example, if we know the target of that attack, and their role in the organization, and if we find similarities in the attack towards additional folks in the same department that were a target at the same timeframe, or across a certain timeframe, we can sanitize that and use it in order to declare this as an indicator of attack, share this information with the rest of the security estate, and make sure that either this file or derivatives that produce the IOC for this file are not capable of doing anything in the organization.

Today, the way it is usually is done, the attack might or might not be blocked, depending on the Firewall that is being used, and that is it. There is no continuation beyond that point. If I can take that information and share it with the rest of my estate, I can say to the web gateway, e-mail gateway, end points, my application sandboxing – "be smarter". Because now I have more knowledge about this attack: I took the file and detonated it in an application sandboxing; created an IOC; understood what are the malicious parts of that IOC; shared that within my infrastructure; looked for that with the information I have collected with my SIEM; understood whether or not I have been susceptible to this attack before and what were the results, and blocked future attacks. We will be able to use that block to adapt to that threat, and understand whether it had any effect whatsoever over our infrastructure. Today this circle does not exist in the solutions out there, because, either companies are looking at each component separately, or the linkage between the different components is missing.

When we looked at the problem, we tried to view it in a holistic approach to solve this issue. The innovation that we applied here was to look at the different parts, either coming from us or from the industry, and trying to remove ourselves from the game of APIs. Some companies offer solutions that connect between one product to another and have to connect to different APIs. Every time the API changes or the product is upgraded, you have to try and understand whether that integration still works. When you want to share the information across a wide variety of products, you want to prevent the need to chase the API change; assuming you have n products, you might end up with n^{n-1} integrations between those products.

The easiest way for you to share the information would be to use a single API that would allow you to consume literally anything you want. This sounds like a fantasy, it doesn't exist; but looking at past solutions, you see that these problems were solved by messaging, allowing various applications to connect, even though they had no idea they needed to communicate with each other. By using this means, we enabled a connection between different solutions, either created by us or by a third party. Using a single integration that doesn't care whether you upgrade your product or not, you are able to consume and produce information that you are seeing, and then react to what the rest of the infrastructure is contributing to you. For example, when the firewall or the sandboxing application detect something, everything is adaptive to that detection, and your entire infrastructure is being immunized as soon as that piece of information is shared between the different solutions connected to that messaging fabric.

We also tried to find the line between where automation makes sense, and where a manual operation is needed, because now our detection capability is much better. Now, for any block or suspicion, we have the ability to send that information to one or multiple application sandboxing mechanisms. We can look at the results, and use the IOC that was produced to scan the information we have previously collected in the SIEM, and try to understand if a machine in our organization communicated with a malicious URL, executed something related to the malware that we just found, etc. Our ability to communicate between the different solutions, and having one solution that can actually be adaptive and bring more value to the customers, has actually been delivered to the market. The idea is to think about what will be most

beneficial for the customer; the customer went and bought security solutions with their hard-earned money, but at the end of the day it was hard to manage everything. They needed to make sense out of this mess,that was created, while the customer thought that they were doing the right thing, investing in best of breed. However, the real innovation here is linking between those different products, and get a holistic approach to fight cyber threats.

I refer to SIEM solutions today as librarians. If you want to find something that happened in the past, they will do the job. However, it already happened, and in most cases there is nothing you can do about it. One of the things that we can see today is the shift of security to a real time state, rather than what had been done in the past. We still need the SIEM and the information it provides, because we need to understand how an attack started, among the rest. In our solution we added capabilities to mark all the files that went in and out of our web gateways and e-mail gateways, because we want to build a visual trace route. This helps us answer questions such as: what came through this gateway, and was not detected? What attacked it? Did we hand over the file to someone to look at its detonation or not? And what was the path this malware took until it hit something that generated another alert?

We connected the SIEM to this real time fabric as well, and changed some of the products, including some of our partners', to share critical events with the SIEM in real time. The big problem with SIEM is not the processing or the correlation, but the inability to operate in real time, receiving the data as the attack happens, so it can use those mechanisms in order to react to what is being done. Therefore, we connected the SIEM to this real time fabric, and now we can detect things and have workflows in real time, that other SIEMs cannot.

This mental shift needs to occur in the way that the SIEM operates as well. It still needs to get the logs from the traditional sources in the traditional manner, but things that can be done in real time should be done in real time.

MS. TAMAR SHAFLER, SR. PRODUCT MANAGER, IBM SECURITY

What we are here to discuss today, is how we can overcome and fight this growing sophistication and advanced threat landscape. To

illustrate the immense costs of this battle, based on a survey that we did with Ponemon, we found that on average, the cost of a breach per lost or stolen data record is about $154. That number represents an increase of 23% over the previous year. For example, last October eBay had 150 million records stolen; multiplying that number by this average cost, we can understand why they cited that breach as the main cause for their decrease in revenues.

It is not surprising that organizations spend more and more money on security, and according to the IDC, over the previous five years there has been a 35% growth in the spend on IT security, and Gartner doubles these estimations. That said, we still see a growth in successful attacks. According to the website Hackmageddon, which lists all the main breaches that occurred week by week, in the first five months of 2015 there have been 440 breaches, which means 22 breaches per week, on average. That average is 48% higher than the average in 2014.

The reason to the increase in successful attacks, even though more money is being spent on defense, is the growing sophistication of the attackers. In February the health insurance company Anthem was breached, and personal information of several millions users was stolen. Interestingly enough, one of the destinations of command and control used in this attack had the name We11point.com. A few months prior to that breach the company was acquired, and changed its name to Anthem from Wellpoint, which is quite similar to We11point. That way, when they reviewed logs in their SIEM solution or other security controls, it seemed like a legitimate address. Another example is the Carbanak malware, that was used to steal nearly $1B in a very evasive and sophisticated attack. However, it started with phishing e-mails sent to bank employees, which then led them to download the Carbanak RAT (Remote Administration Tool). Another interesting example is the TV5Monde attack, allegedly performed by the ISIS hacking group, which caused a 4-hour blackout of 11 public television channels, and included taking over the company's social media channels. This attack also started with phishing e-mails sent to all journalists in the TV5 network, and it took only three of them to click the attachment in the e-mail, and download the RAT that infected machines, later allowing the attackers to black out the channels.

Another reason for the increase in successful attacks is that the basic premise of our environment remains the same, and sometimes

even becomes more complicated. On one hand, we have vulnerable systems. According to X-Force, in 2014 over 30,000 vulnerabilities were disclosed by them, not including some mobile vulnerabilities. On the other hand, we have a growing sophistication in attack methods. The Verizon data breach report cited that 70-90% of the breaches in 2014 were carried out using a malware unique to the attacked organization. According to a survey by Lastline, in 2014 there was a growth of 300% in evasive malware.

In the existing situation, as mentioned above, the weakest link is always the user. In 82% of attacks in 2014 there was a human factor involved – either by phishing, social engineering, or a combination of these factors. In the majority of the attacks, the entry point would be the user – according to Verizon, 23% of the users would open a phishing e-mail, and over half of them will click on the attachment. This can happen even in security aware companies, when users expect a certain e-mail, or they are sent a spear phishing e-mail that is highly targeted to attack that specific company. The combination of these factors leads to a successful attack.

But it is not only about phishing e-mails. During a news coverage of the TV5 breach, an office in TV5 was filmed, and in the footage you could see usernames and password posted on the office wall. Moreover, it has been revealed that the password for the station's YouTube account was "lemotdepassedeyoutube", literally meaning "the password for YouTube", a very easy password to crack. What can we do about careless users, then? We can educate them, but that only will take us so far. That ignorance of the users is a very important component of a successful attack. If we look at the attack life cycle, how an attack is being carried out, the process starts with one of two points. The first is sending a weaponized attachment, containing an exploit of a vulnerability, such as a Word document, a pdf file, etc. The malicious piece of code will exploit the vulnerability to get out of the context of the exploited application, writing and executing code to download malware, install it on the infected machine, and ultimately reach sensitive information and exfiltrate it to the attacker's command in control.

Alternatively, the attack can be carried out by sending an e-mail enticing the user to click a link. In one scenario, the target website will request the user to provide their credentials. For example, a user

may get an e-mail pretending to originate in their IT department, saying "you need to change your password", and to do that they need to enter their original password. Another scenario is of an e-mail that redirects the user to a malicious or a legitimate yet exploited website, and behind the scenes, a "drive-by download" will install malware on the user's machine. Our research found that at least 1 in 500 machines, in organizations that we surveyed and monitored, is infected with a sophisticated, evasive malware.

The Carbanak attack started with e-mails that were sent to bank employees, which contained word document or CPL files containing an exploit. Once these files were opened, the exploit downloaded the Carbanak RAT to the employees' machines. From there it moved laterally in the network, and transmitted video captures, screen captures, and loggings of key strokes from the employee's machine. This was a part of the reconnaissance phase of the attack, and there was a human on the other side, watching these videos and analyzing the actions that they were taking in order to carry out this sophisticated attack, ultimately leading to $1B stolen.

Only this month, there was a major breach in the Japanese National Pension Fund, resulting in stolen records of about a 1.25 million people covered by the fund. The trigger of the attack was a very convincing e-mail message that contained a notice of health insurance, so very relevant to employees in the Japanese National Pension Fund. The e-mail contained a self-extracting, executable ZIP file that once opened, pretended to be a legitimate document that can be opened with Ichitaw, the Japanese equivalent of Word. Usually, when one opens a malicious document, the exploited application will crash because it is not a legitimate document. In this case, the self-extracting executable launched Ichitaw after the exploitation, the user actually saw the document, so it seemed completely legitimate, while behind the scenes it downloaded a RAT, called "Blue Termite" by Kaspersky. Next, the malware utilized lateral movement, and ultimately sent files, sensitive information, e-mails, and browser information from users to a command and control server.

Cyber security is a cat and mouse game, and as attacks become more and more sophisticated, so do the security solutions. The evolution of solutions from being based on prior knowledge, such as signatures or pattern identification, is now shifting over to identifying anomalies

and analyzing the behavior of applications. We mapped the number of samples required to correctly identify a malware. At the entry and exit points, countless samples are needed to generate different signatures; it is very easy for the malware to change a signature, using, among the rest, polymorphism and dynamically generated addresses of command and control servers. However, we identified certain strategic choke points where the number of patterns, the number of possible variations, is the smallest. For example, in the cases of Carbanak or the Japanese pension fund, the exploit tried to perform certain operations that are abnormal to that application; it was trying to get out of the application context and execute some code. We identified these strategic choke points, mapped this abnormal behavior, and that is where we can lock, identify and block the attack. In a similar manner, if the attack didn't start with an exploit but with a user-initiated action, eventually the attack will try to communicate outside of the network to send sensitive information. Evasive malware does not communicate outside directly, but rather tries to inject code into other processes, and to write on the memory of other processes. We identify these abnormal operations, and that is where we block the attack.

To summarize, there is no silver bullet or one magic solution to the problem. We need to have a defense in depth; a layered approach; real time, not just monitoring. It is very important to have visibility, but we also need to be able to prevent the attacks in real time.

DR. ALON KAUFMAN, DIRECTOR OF RESEARCH AND INNOVATION, CTO RSA ISRAEL

I am going to talk about how we at RSA see data science as a key technology in transforming the way security is done. As is known in the cyber world, the third landscape is getting more complex, aggressive, destructive, and disruptive. On one hand, we have been attacked on and from any platform, and this is our reality. On the other hand, we have the security operation model, where all the relevant technologies fall into four main buckets – collection, detection, investigation, and response – which is true for any kind of security. We collect evidence when something looks bad; we detect something that look abnormal or creates an alert; we investigate it to learn what happened and validate

it was really an attack; and based on these we respond, stop that from happening again, and try and implement new controls.

That is what everyone has been doing for many years, and the situation looks bad. We are losing this battle. More than 90% of the breaches happen within less than a day from the initial attack, but in terms of the detection, the minority of them is detected in less than a day. Moreover, this gap between breach and detection is continuously growing. We have the technologies, we have the money, we have the brains, and for some reason we are still losing to the attackers. We have to ask ourselves, what is the nature of this battle that we are losing?

First of all, the attackers know exactly what are all the parameters. They decide when they are going to attack, what they are after, and what the target tools are, since we, the vendors, publish our tools all the time. For them the world is much clearer, more predictable, and they have the ability to plan their actions, making their lives much easier. In contrary, our lives as defenders are unpredictable; attacks can come from anywhere, anytime and on any kind of system. The attackers just need a small hole in our system to get in, and we have to patch and close all these holes, leading to the fact that our security operations today, in that model, are extremely slow, and reactive by nature. One could even say that we essentially wait to be attacked in order to investigate it and put the remediation for the next time.

Another thing is that our current security methods are heavily based on security specialists. There are not enough such people, and the existing ones wear out quite quickly, creating a huge gap between demand and supply. The fact of the matter is that we simply don't make the attackers' lives hard enough. We all make compromises, and even as attackers attack an organization using a specific vulnerability, others don't hurry to patch themselves against it, allowing the attackers to use the same attack methods across different organizations.

The question is, why do we continue using this reactive, slow, human dependent operation method? In the 1960s, the radar was introduced into F-4 fighter planes, allowing, for the first time, to widen the pilots' viewing range from 5-7 miles to 20-30 miles. However, early versions of this technology required a skilled operator on board the airplane, in addition to the pilot, to manually operate the device. Over the last 50 years, our technology evolved to the point where the viewing range

increased, and moreover, modern systems, such as the TSD (Tactical Situation Display) automatically display strategic information on all nearby objects – all this without requiring any human operator. Taking this analogy a step forward, for the last 100 years, drivers and pilots were needed to actively steer their vehicle. These days, however, we are witnessing a transformation where smart cars and airplanes receive orders from their operators, and execute them autonomously.

In security we are probably still in the manual era. Looking at common security operations, people spend most of the time manipulating and fine-tuning the systems, and not really operating based on their skills. We are slaves to the systems, and in many senses we do not fully utilize them. This is a critical part of the reasons why we are in the situation mentioned above. We have point solutions, these so-called radars, each of them giving us additional visibility, but each of them is now a solution that you have to fine-tune, etc. Some solutions are better than others, but there will always be a next generation of solutions.

The idea behind using data science is to take all of these point solutions, and combine them into a much broader system that can better leverage what they have to offer, in a holistic manner. The biggest complaint regarding some of these systems is false positives and the likes. However, by combining these systems and helping them learn from one another, this nuisance is significantly reduced. That way, in cases where one or two of these systems raise false alarms but others do not, the holistic system can overcome it. Ideally, what we would like to achieve is a combination of all of these solutions into one big system that provides a much more comprehensive and accurate view of the world, enabling a much more efficient use, and also allowing it to learn by itself.

Our goal is to build a system that prioritizes current events and incidents, allowing security experts to focus on the most important task at hand. All of the relevant information, including risk and impact analysis for each threat is consolidated into a single screen, instead of dozens. We want this radar-like concept to be there, along with all the supporting evidence around it. Instead of a bottom-up approach, that tries combining alerts into a single event, we want our analysts to work from the top down, providing a much more comprehensive view of the world.

This doesn't change our detect-investigate-respond model, but rather moves it to a different level. We are not interested in detecting independent single points, but in detecting attacks, or the "kill chain". We don't want to have small alerts and pieces of evidence, we want to have everything prioritized and aggregated, so everything that is related to a specific incident would be combined together, and maybe even predict the next move of the attackers. Obviously, investigations have to be a top-down concept, and every time an analyst investigates something, the system should learn how to do it by itself for the next time. Whenever an investigation ends the right way, the system should learn from it. Alternatively, if an investigation ends in a non-sufficient manner, the system should also learn what should not be done. We don't want our analysts repeating their work over and over again. As for the response, we should automate anything that can be automated, teach the system anything that can be learned, and use human intelligence only when these are not possible.

For me, data science is about one simple thing: you have a goal, you have a problem, you have data, and data science is the art of connecting them. In most places you will see data science only in the detection phase, for example user behavior analysis and anomaly detection. However, we at RSA are expanding it to all levels, from finding indicators of compromise, combining them into attack models or detections models, combining them into higher levels of detection models, combining these, in turn, with the investigation phase, and of course crowd-sourcing and so on, in order to eventually reach high-level indicators and operational information. These points are not singleton alerts, but attacks predicting how impactful or risky they are to the organization, and how long would we have until we solve the problem.

The key is not to look at any element as a singleton element, but to chain things. So many IoCs are part of detection models, and many such models are parts of an attack. Consider a scenario of detecting a suspicious VPN login. In our specific case, we have a system with 30 different IoCs, for example: what country the attackers came from, what device they used, what was done, etc. For each IoC we build an anomaly detection engine, which detects how anomalous it is, and gives that IoC a risk score. In our case, the user owning the credentials always came in from a specific country, and then a sign-on came from

a new country, which we consider an IoC. The device was different than usual, and so was the volume of data, etc. All of these IoCs already have a priority, and we combine them into one final score, showing how risky the VPN connection is.

This VPN detector, by itself, can be a nice model, and better than many other systems in the market, but this is not enough. When the user logs in, you want to continue monitoring their actions. In our example, the user not only logged in from a VPN in a very suspicious way, but then we started to see lateral movement in the network. They start traversing different devices, from different people in different organizations across the network. In our system, the risk will go up as the attacker traverses the network until they reach the highest score. In this case, we don't stop here, but rather monitor the attacker's actions when they go into new device, as they scan and look for passwords, etc.

We need to chain IoCs, detection models, and so on. You can also introduce crowd-sourcing into the chain. Anything you find within your network is great, now you should ask what the rest of the world thinks about it as well, and start to chain these things together. That way we can get our visibility across the board, enable all these point solutions provided by startups and companies to fit into a single holistic system that can learn and assign the right weights to the different products.

To summarize, there is a great necessity to build such holistic systems, which can learn automatically and drastically change the daily work of analysts today, from tuning and finding these things to actually operating on a much higher level, going top-down and really addressing the attacks. And this is basically the approach we are taking at RSA.

MR. YAIR SHAKED, CLIENT TECHNICAL PROFESSIONAL AT IBM ANALYTICS

There is an intelligence gap between the current cyber security products and solutions and the capability of investigation. IBM's i2 aims to close that gap, and I will illustrate it by providing a theoretical investigation scenario.

In the past we mostly dealt with known vectors, such as cross-site scripting and DDoS. We are still concerned about them today, but we currently have another spectrum of technology that we need to

cover – the mobile or the cloud, with attacks coming from both known and unknown vectors. The big risks in the future will be related to sophisticated or unknown vectors, revolving around technologies such as IoT, SCADA, etc. Studies say that by 2032, the average person on the street will be surrounded by 5,000 devices that transmit data to the internet at any given time. This translates to an immense potential for hackers to penetrate and steal sensitive data.

Another issue is Social Engineering. The hacker Kevin Mitnick said that this is the most effective tactic, and that it should be in every attacker's arsenal. The reason for that is that we are all human, and while we hear a lot about phishing, not everyone is tech-savvy. If someone gets an e-mail telling him that they need to change their password, for example, they may eventually end up providing their password to the hacker on a silver platter.

The scenario I present will show how to use i2 to combine data from a SIEM system with external data in order to give the analyst or the investigator a broader picture, and help them understand what happens in a specific attack.

In the i2's investigator desktop, we can visualize relationships between different entities. An entity can be an event originating in a SIEM, it could be a machine with an IP, a domain, etc., and link between these entities to get a broader picture and visualize their relationship. We begin by exploring the repository, and run a visual query. Not all analysts or investigators have SQL skills, and can run SQL queries easily. To bypass this issue, we provide a tool that visualizes linkages between the entities. All the investigator needs to do is drag the first entity, which is the event, into the canvas, and assign this event to a category called "virus detected". Then the investigator adds the source into the canvas in order to understand the links between the events and the infected machine, and draws a line to mark that they are linked. They also need to specify the relationship – source and event; and add another event to see what happened on the other end of these machines, so we might identify the attack.

The next step is to run a search, and refine the results. We found two events in our system: the first event, that we were aware of, came from the SOC, alerting that a virus was detected in our network, and the second one is a possible Command and Control connection. The

search results also show a list of all the infected machines. At this point the investigator can select all results and create a chart showing all the relationships between them. All of these results came from our SIEM system, but we can also use external sources. In our scenario, the external sources are represented by ZeuS Tracker, a website that records all the history of malicious IPs and URLs, binary URLs and configuration URLs, as well as the drops URLs, the latter of which are a part of this scenario.

At this point the investigator can extend what they know about this Command and Control server by clicking "filter expand". This feature allows the investigator to filter what they want to see in the chart. In this scenario, the investigator chooses to see only "event to destination", which in our case shows only one specific IP to which the infected machines in the organizations send their data. This can be extended even further, to view the destination to the command host, in order to see all the domains. After another expansion, the investigator can see several domains, probably the hackers' attempt to try and hide their identity. A careful examination shows that the IPs are the same for all domains. The investigator chooses one of the domains that bear the same IP, and expands it to show its command and configuration URL, command and binary URL, the drop URL, and the malware. This shows a linkage between the selected domain, the ZeuS malware, and the latter's drop and configuration URLs.

The process is now at the point where the canvas shows the investigator the full track between their internal system and the external one. There is also an option to use geospatial data, giving longitude and latitude coordinates for each IP. The solution allows using services such as Google Earth to visualize the location of a certain entity on the world map.

In conclusion, investigators or analysts don't need to know SQL in order to start their investigation. Using the information given by the system, the system administrator can harden the network and the infrastructure, avoiding such attacks in the future.

Interdisciplinary academic research has a crucial role to play in cybersecurity. The first 2011 Annual Cyber Security International Conference at Tel Aviv University has attracted top political, industry and academia leaders and experts from Israel and the world, on stage and in the audience. The following annual events saw the line-up extended, dedicated tracks added, and enjoyed attendance of over 5,000 participants each.
The Proceedings of the fourth and fifth Annual Yuval Ne'eman Workshop for Science, Technology and Security Cyber Security Conferences publication will enhance the global impact of the work presented at Tel Aviv University.

The Blavatnik Interdisciplinary Cyber Research Center (ICRC) was established at the Tel Aviv University as a joint initiative with the National Cyber Bureau, Prime Minister's Office.
The Center is based on researchers from Tel-Aviv university and emphasizes the importance of interdisciplinary research. Currently, there are 50 faculty members and over 200 cyber researchers from different faculties such as Exact Sciences, Computer Sciences, Law, Engineering, Social Sciences, Management and Humanities.
The Center aims to become a leading international body in its field and to increase the academic efforts and awareness in the field of cyber security.
Research topics at the Center include key issues such as security software, attacks on hardware and software, cryptography, network protocols, security of operating systems, and networks as well as interdisciplinary research such as the impact on national security, the impact on society, regulation, and the effects on the business sector.
The Center operates a research fund which is supported by the National Cyber Bureau.

The Yuval Ne'eman Workshop for Science, Technology and Security was launched in 2002 by Prof. Isaac Ben-Israel in conjunction with the Harold Hartog School of Policy and Government and the Security Studies Program at Tel Aviv University, to explore the nexus of science, technology and security, and to addresses policy-relevant issues with rigorous scientific research. The Workshop engages topics of international relations, strategy, cyberspace and cyber security, space policy and space security, precision weapons, robotics, nuclear energy, homeland security, and the interplay between society and security. The Workshop organizes a range of conferences, panels and expert meetings, and maintains working relationships throughout the academia, business, policy and defence circles.