Enhancing Cyber Resilience in Electricity Systems

International Energy Agency

Electricity Security 2021

INTERNATIONAL ENERGY AGENCY

The IEA examines the full spectrum of energy issues including oil, gas and coal supply and demand, renewable energy technologies, electricity markets, energy efficiency, access to energy, demand side management and much more. Through its work, the IEA advocates policies that will enhance the reliability, affordability and sustainability of energy in its 30 member countries, 8 association countries and beyond.

IEA member countries:

Australia
Austria
Belgium
Canada
Czech Republic
Denmark
Estonia
Finland
France
Germany
Greece
Hungary
Ireland
Italy
Japan
Korea
Luxembourg
Mexico
Netherlands
New Zealand
Norway
Poland
Portugal
Slovak Republic
Spain
Sweden
Switzerland
Turkey
United Kingdom
United States

The European Commission also participates in the work of the IEA

IEA association countries:

Brazil
China
India
Indonesia
Morocco
Singapore
South Africa
Thailand

This publication and any map included herein are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

Abstract

Electricity is an integral part of all modern economies, supporting a range of critical services including health care, the internet and transportation. The secure supply of electricity is thus of paramount importance. Digitalisation is rapidly transforming the electricity system, bringing many benefits for businesses and consumers. At the same time, increased connectivity and automation could raise risks to cybersecurity and the threat of cyberattacks. A successful cyberattack could trigger the loss of control over devices and processes in electricity systems, in turn causing physical damage and widespread service disruption. Using real-world examples, this report offers guidance to policy makers, electric utilities and other stakeholders on how policies and actions could enhance the cyber resilience of electricity systems.

Acknowledgements

This report was prepared by experts from the Directorate of Energy Markets and Security and the Strategic Initiatives Office of the International Energy Agency (IEA). The authors of this report were Edwin Haesen, Enrique Gutierrez, George Kamiya, Grecia Sofía Rodríguez and Jason Elliott. Keisuke Sadamori, Director of Energy Markets and Security, provided expert guidance and advice.

Valuable input, comments and feedback were provided by IEA colleagues including: Dave Turk, Laszlo Varro, Paolo Frankl, Laura Cozzi, Peter Fraser, Aad van Bohemen, Brent Wanner, Nicole Thomas, Edith Bayer, Jihyun Selena Lee, and Clémence Lizé. Anna Kalista provided essential support.

The authors would also like to thank Justin French-Brooks for the expert editing of this report. Thanks go to the Communications and Digital Office (CDO) for its help in producing the report and website materials, particularly to Jad Mouawad, Head of CDO, and Jon Custer, Astrid Dumond, Tanya Dyhin, Christopher Gully, Julie Puech, Jethro Mullen and Therese Walsh.

A high-level workshop on Electricity Security was held in Paris on 28 January 2020. The participants offered valuable insights and feedback for this analysis. Further details at: www.iea.org/events/iea-electricity-security-workshop.

The authors would like to thank the many external experts who provided valuable input, commented on the analysis and reviewed preliminary drafts of the report. They include: Laurent Bernat (Organisation for Economic Co-operation and Development); Stuart Madnick (Massachusetts Institute of Technology); Tim Watson (University of Warwick); Stefano Bracco (EU Agency for the Cooperation of Energy Regulators); Anjos Nijk (European Network for Cyber Security); Avi Gopstein (National Institute of Standards and Technology [NIST]); Louise Anderson (World Economic Forum); Rosa Kariger and Francisco Laverón (Iberdrola); Jochen Kreusel (ABB); Martin Knudsen (Ørsted); Guido Gluschke (Brandenburg University of Applied Sciences); Christophe Blassiau (Schneider Electric); Hannele Holttinen (IEA Wind Technology Collaboration Programme Task 25); Masato Yamada and Tusitha Abeyasekera (MHI Vestas); Stephen Woodhouse (AFRY); Scott Pinkerton (Argonne National Laboratory); Martha Symko-Davies (National Renewable Energy Laboratory); Russ Conklin, Fowad Muneer and Carolyn Gay (United States Department of Energy).

Comments and questions on this report are welcome and should be addressed to EMS-RISE@iea.org.

Executive summary

Digitalisation offers many benefits both for electricity systems and clean energy transitions. At the same time, the rapid growth of connected energy resources and devices is expanding the potential cyberattack surface, while increased connectivity and automation throughout the system are raising cybersecurity risks.

The threat of cyberattacks on electricity systems is substantial and growing. Threat actors are becoming increasingly sophisticated at carrying out attacks. A successful cyberattack could trigger the loss of control over devices and processes, in turn causing physical damage and widespread service disruption.

While the full prevention of cyberattacks is not possible, electricity systems can become more cyber resilient – to withstand, adapt to and rapidly recover from incidents and attacks, while preserving the continuity of critical infrastructure operations. Policy makers, regulators, utilities and equipment providers have key roles to play in ensuring the cyber resilience of the entire electricity value chain.

Policy makers are central to enhancing the cyber resilience of electricity systems, beginning with raising awareness and working with stakeholders to continuously identify, manage and communicate emerging vulnerabilities and risks. Policy makers are also ideally placed to facilitate partnerships and sector-wide collaboration, develop information exchange programmes and support research initiatives across the electricity sector and beyond. Ecosystem-wide collaboration can help to improve understanding of the risks that each stakeholder poses to the ecosystem and vice-versa.

Information sharing can enhance cyber resilience across the system for all electricity sector stakeholders. Stakeholders should be encouraged to share information on vulnerabilities and actual incidents, be transparent on implemented policies, and share information and best practices at national and international levels.

A wealth of existing risk management tools, security frameworks, technical measures and self-assessment approaches are available. Policy makers and industry need to apply what is relevant in their context and approach resilience as a continuous process rather than a one-time milestone. Policy makers and the industry should both commit to an approach based on ongoing collaborative dialogue.

Governments around the world can enhance cyber resilience through a range of policy and regulatory approaches, ranging from highly prescriptive approaches to framework-oriented, performance-based approaches. Approaches that are more prescriptive have the advantage of allowing for more streamlined compliance monitoring, but they could face challenges in keeping pace with evolving cyber risks. Less prescriptive, framework-based approaches allow for different approaches and implementation speeds across jurisdictions, but they raise questions around how to establish a coherent and robust cross-country approach to cybersecurity with tangible and effective impact. Implementation strategies should be tailored to national contexts while considering the global nature of risks.

Cyber resilience policies need continuous review and adaptation. Further decentralisation and digitalisation of the electricity sector – especially at the distribution level (smart meters, connected consumer devices) – shifts the risk exposure to the grid edge. Effective policies need to look beyond bulk utilities and consider the entire electricity chain, including supply chains.

Supply chain security is an international issue. To demonstrate security preparedness, certification or other similar mechanisms based upon existing international standards need to be institutionalised and interoperable at the global level, where deemed appropriate.

Recommended actions

Many countries and companies are developing and implementing policies and strategies to enhance the cyber resilience of their electricity systems. While differing contexts require tailored approaches, several overarching action areas can serve as the basis for achieving more appropriate electricity security frameworks for the future. These are: institutionalising responsibilities and incentives; identifying risks; managing and mitigating risks; monitoring progress; and responding to and recovering from disruptions.

Institutionalise

Policy makers need to set appropriate responsibilities and incentives for relevant organisations within their jurisdiction.

- Policy makers: designate responsible authorities to set objectives, give direction on measures and assess their implementation.

- Policy makers and regulators: implement co-ordination mechanisms between responsible authorities (both within and outside the electricity sector) to avoid conflicts between various regulatory levels.
- Policy makers and regulators: incentivise or oblige regulated and non-regulated entities to implement cybersecurity safeguards. Measures should aim to improve outcomes, rather than relying only on compliance-based processes that risk becoming a box-ticking exercise. The level of enforcement needs to relate to how critical the organisation is to wider system reliability. Positive incentives need to be considered to foster transparency, co-operation and co-ordination.
- Policy makers, regulators and industry: increase the level of awareness of the need for cyber resilience across the sector, including in electricity-related agencies and authorities.

Identify risks

Policy makers need to ensure that operators of critical electricity infrastructure identify, assess and communicate critical risks.

- Policy makers and regulators: ensure designated organisations regularly conduct system-level risk analyses to identify key threat scenarios and system vulnerabilities.
- Utilities and operators: identify and classify assets, systems and interfaces according to their risk level (likelihood and impact) and assign security measures according to level of system risk.
- Policy makers and industry: facilitate public-private cyber risk information sharing.

Manage and mitigate risk

Policy makers and industry have to collaborate to improve readiness across the entire electricity system-value chain.

- Policy makers and industry: provide accessible tools and guidance on cyber resilience best practices.
- Utilities: implement proper risk management strategies to identify capabilities and risks of their systems from both information technology (IT) and operational technology (OT) perspectives. Establishing a clear risk management strategy can help prioritise areas of work and investment decisions to maximise benefits.
- Policy makers, standards bodies, industry and researchers: develop facilities to test and validate effective implementation of cybersecurity measures and controls.
- Policy makers and standards bodies: consider certification of products and services by carefully analysing criticality, enforcement options and market impact.
- Policy makers and industry: develop capacity building for cybersecurity to ensure skills and resources evolve appropriately. This involves achieving buy-in and a

basic understanding across the entire organisation. Mandatory training and certification of critical staff should be considered.

Monitor progress

Policy makers need to ensure mechanisms and tools are in place to evaluate and monitor risks and preparedness, and track progress over time. This is important at the operational level for individual utilities, as well as at the level of policy makers and regulatory authorities who need to understand if strategic objectives are met.

- Policy makers and regulators: develop or provide mechanisms and tools to continuously monitor preparedness.
- Policy makers and regulators: develop mechanisms to monitor and build knowledge around emerging threats. This is an area where partnerships and communication with the intelligence community is essential.
- Policy makers, the intelligence community and industry: develop and support active threat hunting and cyberthreat intelligence mechanisms to prevent or limit the damage from high-end attacks.
- Equipment providers and utilities: conduct active monitoring of the supply chain to detect vulnerabilities.
- Policy makers and industry: develop mechanisms to share incident reports and other information.

Respond and recover

Resilience must go beyond preventing incidents to include effectively coping with attacks. Policy makers need to enhance the response and recovery mechanisms of electricity sector stakeholders.

- Utilities: implement robust response and recovery procedures that help maintain operations in the event of a cyberattack, with clearly allocated responsibilities to all main stakeholders.
- Policy makers and utilities: execute regular response exercises and capture lessons learned and adapt practices.
- Policy makers, regulators and industry: stimulate information logging and sharing to facilitate analysis of actual incidents.

Introduction

Digitalisation and decentralisation are changing the nature of cyber risks in electricity systems

Electricity systems – particularly network operations – are becoming increasingly digitalised, bringing many benefits to electricity consumers, utilities and the system as a whole (IEA, 2017). However, the growth in connected devices and distributed energy resources is expanding the potential cyberattack surface of electricity systems, raising cyber risks. The nature of these cyber risks is also changing as a result of increasing connectivity and automation, a shift to cloud computing and the replacement of sector-specific IT with open-protocol standards.

The electricity system is interconnected with all other critical infrastructure and services. Cyberattacks on electricity systems are therefore a critical threat to every aspect of modern societies. Policy makers, regulators, system operators and industry across the electricity value chain all have important roles to play in enhancing the cyber resilience of the system.

This is a guide for decision makers in response to the substantial and growing threats

The following pages offer practical guidance to energy policy makers and other stakeholders on increasing the cyber resilience of electricity systems. Using real-world examples, this report aims to address the following questions:

- What are the greatest cybersecurity risks to electricity systems today? How are they evolving?
- What strategies and actions can electric utilities and other key stakeholders develop and implement to identify and manage cyber risks and recover from attacks? What sector-specific characteristics need to be considered when tailoring general cyber resilience principles and measures to the electricity system?
- How can collaboration between stakeholders help to maximise effectiveness and optimise efforts? How can responsibility best be assigned and shared?
- How can policy makers and other industry organisations encourage a more proactive integrated risk management approach?
- What are the lessons to be learned from different jurisdictions' regulatory approaches to cybersecurity in the electricity sector? Which approaches have so

far proven to be most effective, and how can effectiveness be measured in advance of actual incidents and failures?

Various terms and concepts are introduced and discussed in this chapter. The following table defines some of the principal terms used. This report uses the "cyber" prefix to discuss digital security and resilience issues related to intentional and malicious attacks and incidents on the electricity system (e.g. cybersecurity, cyber resilience, cyberattack, cyber risk). The report does not cover unintentional incidents or broader digital security issues such as data privacy. The intent of this report is to provide broad guidance to energy policy makers and companies to enhance resilience in the electricity sector, and does not go into technical details or cover national security issues.

Table 1. Key terms and definitions

Term	Definition
Cybersecurity	Broadly refers to the ability to prevent or defend against cyberattacks and cyber incidents, preserving the availability and integrity of networks and infrastructure and the confidentiality of the information these contain. Commonly also refers to the safeguards and actions available to do this.
Cyber resilience	This report does not explicitly cover digital security issues that do not directly impact electricity security, such as data privacy and protection issues. Cybersecurity in fuel supply chains or nuclear facilities is also outside the scope of this report.
Cyber incident	The ability to anticipate, withstand, adapt to and recover from adverse conditions, stresses, attacks or compromises on systems that use or are enabled by cyber resources.
Cyberattack	An event that could jeopardise the confidentiality, integrity or availability of digital information or information systems. Such incidents could also result in the physical disruption of operations.
Cyber risk	A cyber incident with malicious intent. Cyberattacks are conducted via computer networks for the purpose of disrupting, disabling, destroying or maliciously controlling a computing environment/infrastructure, stealing controlled information and potentially impacting physical operations.
Cyberthreat	The potential for financial losses, operational disruption and/or damage as a result of cyber incidents and the failure of the digital technologies employed for informational and/or operational functions.
Information technology (IT)	The threat of a cyber incident occurring, such as a violation of computer security policies, acceptable use policies or standard security practices.
Operational technology (OT)	Software, hardware and communications technologies used to store, retrieve, transmit and manipulate data.

Sources: IEA (2017), Digitalisation and Energy; Gartner (2020b), Information Technology Glossary; Costantini and Acho (2019), NARUC Cybersecurity Manual; NIST (2020b), Computer Security Resource Center Glossary.

The electricity system faces unique challenges compared to other sectors

The fundamental principles of cyber resilience, such as embedding a culture of cyber hygiene and implementing risk management strategies, are generally applicable across all sectors and industries. However, the application of these principles needs to be tailored to account for sector-specific characteristics and needs. In the electricity sector, these include:

- Real-time requirements for and expectations of very high availability.
- Interdependencies and cascading effects within and across systems.
- A mix of new technologies and legacy assets with long lifetimes.

Electricity systems operate in real time, prioritising availability and reliability above all. Electricity industrial control systems must react within fractions of a second, thus requiring cybersecurity procedures like authentication to operate seamlessly and to support the underlying industrial control system functions. The real-time nature of electricity also means that common cybersecurity operations, such as installing patches and rebooting, are more complex compared to the same operation performed on less critical environments, which are easier to take out of operation temporarily.

Electricity systems are also prone to cascading effects across both digital and electrical systems. As utilities increasingly interconnect their systems for the sharing of operational and planning information, an attack could cascade across their digital networks. In addition, if the operation of an electrical network depends on IT located in another network region, an outage there could spill over because of the outage of the IT systems. As with most electricity security risks, a single incident can also cascade across the wider electricity network, causing large-scale outages.

The impacts of an outage can then also affect other critical services that depend on electricity. For example, an insurance company has estimated that an extreme but unlikely scenario of a malware attack on power plants in the northeastern United States could cause economic losses of around USD 250 billion as a result of impacts. These would include direct damage to assets and infrastructure, decline in sales revenue to electricity supply companies, loss of sales revenue to business and disruption to supply chains (Lloyd's & University of Cambridge Centre for Risk Studies, 2015). Cyberattacks on London's electricity grid could cost GBP 21 to 111 million a day (Oughton et al., 2019).

The majority of electricity infrastructure – such as power plants and transmission and distribution systems – have long operational lifetimes, often lasting over fifty years. This means that most electricity systems today include a mix of recent highly digitalised technologies and analogue legacy assets deployed decades earlier. Older, unprotected OT was often designed without the intent of connecting to networks (i.e. they were "air-gapped"), but are being increasingly adapted and connected to IT networks through standardised protocols and additional interface devices. Without adequate security measures and integrated cyber resilience approaches, these connections risk introducing new vulnerabilities to the system.

Policies therefore need to effectively address the specific risk exposure of the electricity sector to build system-wide resilience

Cybersecurity experts believe that there are three necessary conditions for a major cyberattack: opportunity, capability and motivation (Madnick, 2020). To date, disruptions to electricity caused by cyberattacks have been limited. As the opportunity to attack (i.e. existing unresolved vulnerabilities) and the capability of attackers continues to grow, it is clear that electricity system stakeholders must continue to be well prepared and resilient. For countries around the world, cyber resilience of the electricity system is becoming a matter of national security.

While full prevention of cyberattacks is not possible, electricity systems can become more cyber resilient to attacks – by designing them in a way to withstand shocks and be able to quickly absorb, recover or adapt, while preserving the continuity of critical infrastructure operations, or a large part of it. The capacity to adapt to new technologies, as well as to new risks and threats, is key.

However, the uncertainty and the evolving nature of cyberthreats make it difficult to justify large expenditure on staff, tools or cyber insurance policies.[1] For industry, cyber risks should be integrated across all departments (e.g. operations, procurement or innovation) and reported with other business-critical risks. Establishing a cyber-resilient culture and strategy are key – beginning with ensuring that cybersecurity efforts are not confined to the IT department or the "cyber risk board".

[1] The NIST Framework for Improving Critical Infrastructure Cybersecurity provides an approach to assessing risks as they relate to the operating environment of the system, and then prioritsing mitigation and response resources. For policy makers, the NIST Cybersecurity Framework Smart Grid Profile provides a set of written considerations for each cybersecurity function, category and subcategory that can be used as an initiation into cybersecurity concepts in the context of the electric grid.

Policy makers and regulators have an important role to play in encouraging cyber resilience efforts. Regulatory requirements can help to ensure that minimum necessary investments are made, for example, adding cybersecurity criteria to the rate base for regulated electricity grid operators, or qualification criteria to stakeholders participating in the market or connecting directly to the grid. However, compliance with regulatory standards does not, on its own, guarantee that infrastructure will be or will remain completely secure and resilient. In general, regulatory standards, due to the decision-making processes and the need for stable and inclusive governance, may struggle to keep up with rapid technological change and emerging vulnerabilities.

Cyber resilience efforts require action in other related sectors such as telecommunications and manufacturing as well, complicating the regulatory oversight process. Cyber resilience in the electricity sector should be considered within the broader context of enhancing resilience across all critical infrastructure and services, including water, transport, communication networks, health and finance.

Governments, utilities and other stakeholders across the electricity value chain need to be proactive in finding solutions that can adapt to evolving cyberthreats. An ongoing commitment to co-operation and collaboration will be necessary.

International co-operation is particularly important due to the global and instant nature of the internet – an attack against a particular asset can rapidly spread across the world. International organisations and policy makers play a key role in fostering collaboration at the international level. This should include collaboration across all relevant stakeholder groups, from senior policy makers and regulators, to individual utilities and suppliers of electricity and equipment.

Box 1 IEA work on cyber resilience

Cyber resilience is a growing challenge for governments and energy companies around the world. The 2019 IEA Ministerial underlined the role of the IEA in electricity security, with a particular focus on cybersecurity.

An underlying objective of IEA work in this area is to support countries in mainstreaming cyber resilience in government policies and strategies, as well as providing a platform to exchange experiences and establish new focal points. The IEA's collaboration with industry and the launch of high-level events at ministerial and senior business representative level are designed to help governments and energy system operators work together to manage the increasing complexity of

risks and threats. Operational aspects of cyber resilience, such as specific threat assessment and monitoring, and incident management and response, are matters of national security outside of the scope of IEA analysis.

The core IEA work on energy security increasingly covers raising awareness of new cyber risks among countries within a wider context of planning for resilience over the short, medium and long term. The IEA conducts in-depth policy reviews of its members; these reviews investigate, among other topics, whether members have robust national governance arrangements for both internal and international co-ordination and information sharing on resilience to a wide variety of risks. These reviews have now been expanded to include governance of cyber resilience.

The IEA also organises emergency response exercises on a regular basis to test the preparedness of the IEA and its member countries to respond to oil, natural gas and electricity disruptions. These exercises expose participants to various disruption scenarios assessed by the IEA Secretariat, which may include potential high-level impacts on energy markets and electricity system operations, particularly those resulting from cyberattack.

Trends in digitalisation and cybersecurity

Digitalisation brings many benefits to the electricity system, including greater efficiency, lower costs and shorter outage times

The electricity sector has been using digital technologies to facilitate grid management and operation since the 1970s. Electric utilities have steadily adopted increasing levels of automation and control capability, as costs for digital technologies have fallen dramatically in recent years. Since 2010, internet connection speeds have increased tenfold while the costs of data storage and Internet of Things (IoT) sensors have fallen by 70% and 54% respectively (McCallum, 2020; Microsoft, 2018; Nielsen Norman Group, 2019; The Economist, 2019).

Across the electricity system, digital technologies offer an array of opportunities to improve performance for the benefit of individual companies, the system as a whole, energy consumers and the environment.

For example, sensors in power plants and electricity networks can gather and share real-time information on components to help optimise plant and grid operations. Ubiquitous connectivity, the IoT and automation increasingly enable automated and remote operation of electricity assets and systems. Artificial intelligence (AI) and machine learning can help improve real-time renewables forecasting, and improve grid stability and reliability (IRENA, 2019). Digitalisation also enables shorter market closing times, helping to mitigate the increasing dynamics that result from higher shares of variable generation. Digitalisation of the transmission grid is already at an advanced stage, and these trends are progressively unfolding at lower distribution grid levels.

Potential savings from digitalisation in the electricity sector could total USD 80 billion per year to 2040, or about 5% of total annual power generation costs today (IEA, 2017). Savings can be achieved through improved efficiencies in generation, transmission and distribution, reduced operation and maintenance costs, reduced unplanned outages and extended operational lifetime of assets.

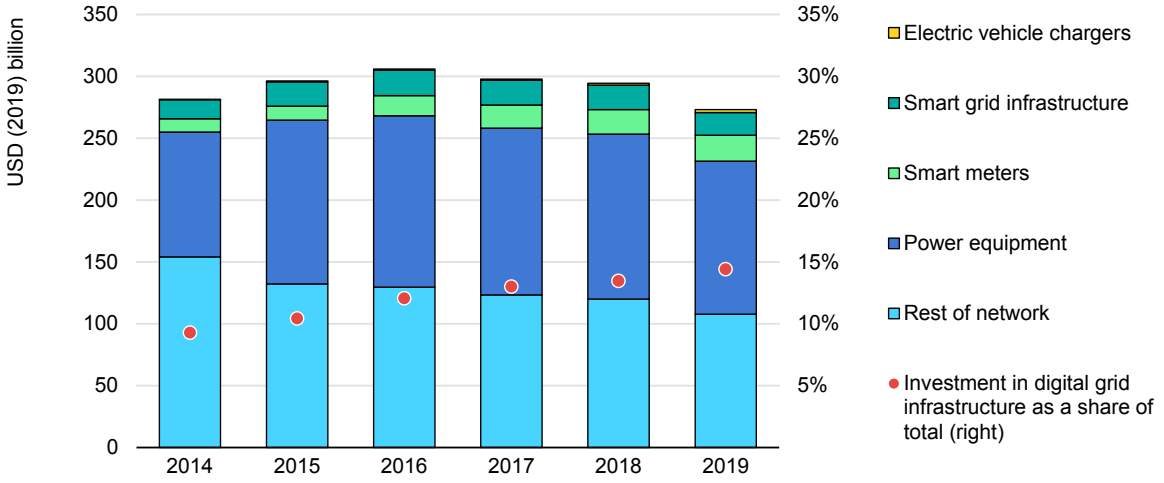
Crucially, digitalisation also supports clean energy transitions

Digitalisation can help to accelerate clean energy transitions by unlocking more demand response opportunities, integrating greater shares of variable renewables, and facilitating the smart charging of electric vehicles (IEA, 2017).

Some digitalisation trends such as home automation and aggregators are arising from "market pull", while others are the result of a "policy push", such as mandatory remote control capability of distributed generation (PV and wind) and in future possibly for electric vehicle charger applications.

Smart grid investments and deployment of enabling technologies will be critical to accelerating energy transitions. Investment in digital grid technologies rose by 14% to USD 40 billion in 2019, mostly in smart meters and grid automation equipment (IEA, 2020). Spending on digital grids now makes up nearly a fifth of network investment.

Figure 1. Investment in electricity networks, 2014-2019

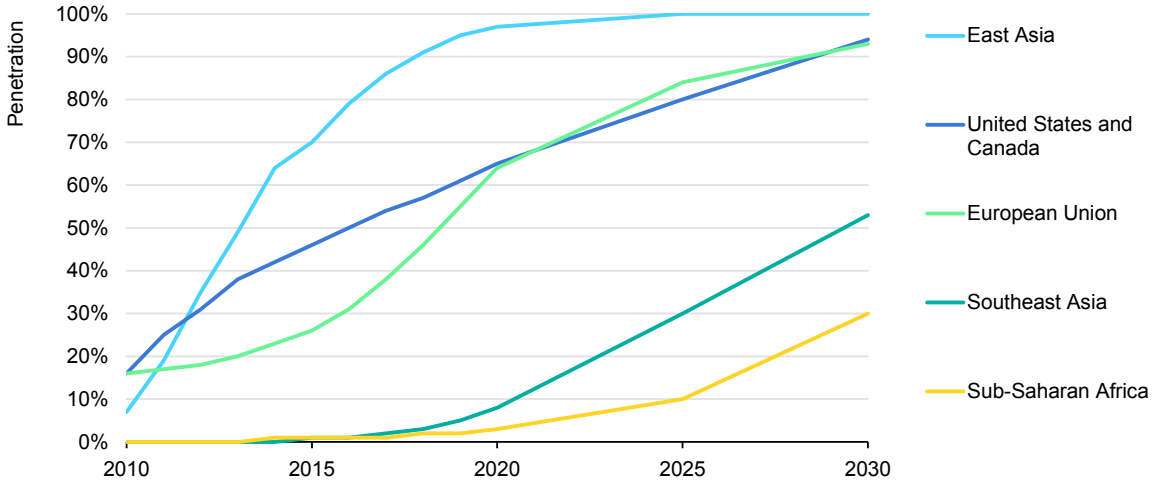


Notes: Smart grid infrastructure comprises utility automation equipment at substation level. Power equipment corresponds to transformers, switchgear, power systems and substations.
Source: IEA (2020), World Energy Investment 2020.

Smart meter deployment has advanced considerably in recent years in several key regions, and is expected to grow from around 1 billion installed meters in 2019 to nearly 1.3 billion by 2025 (St. John, 2020; Wood Mackenzie, 2020). The People's Republic of China is approaching full deployment, and Japan, Spain and France are poised to achieve full roll-out in the next few years (BloombergNEF, 2018). However, there can be a wide disparity in the real-world capability of smart

meters deployed in different regions and at different times (e.g. data granularity, communication frequency, use of dynamic tariffs, interoperability with behind-the-meter distributed energy resources), making deployment alone a limited indicator of smart grid progress globally.

Figure 2. Penetration of smart meters by region, 2010-2030



Source: BloombergNEF (2018), Smart Meter Market Size.

Connected devices, together with other smart grid technologies, can unlock larger demand response resources, enable more energy efficiency initiatives, and facilitate the integration of higher shares of variable renewables in a cost-effective and secure manner. The number of connected IoT devices (e.g. smart thermostats and appliances) is growing rapidly, with the global stock projected to double between 2020 and 2025 to 25-42 billion devices (Gartner, 2017; GSMA, 2020; IDC, 2019a). Of the estimated 5.8 billion business and automotive IoT units installed in 2020, utilities account for the largest share (24%) at 1.37 billion units (Gartner, 2020a).

But digitalisation could also raise concerns over new cyber vulnerabilities to the electricity system

While digitalisation offers many benefits, increasing connectivity and automation throughout the electricity system can also increase risks to cybersecurity across the electricity value chain.

For example, a typical power plant uses computing systems and software to control a range of devices and processes (e.g. SCADA). Historically, these systems were thought to be protected from cyberattacks through physical

separation from internet networks, i.e. air-gapping (Guri, 2018). But as operators have increasingly automated these systems and connected them to IT systems and the internet, access by attackers has become a possibility. An attack would trigger the operator's loss of control over devices and processes, in turn causing physical damage and/or service disruption.

Cyber risks also present barriers to further digitalisation. According to one survey of executives, cybersecurity concerns are a major barrier to further IoT adoption, particularly in the energy sector (Bain & Company, 2018). Of respondents from the energy and utilities sector, 57% expressed significant or extremely significant concerns with IoT cybersecurity risk.

As new systems and technologies are rolled out, critical infrastructure can often rely on fall-back procedures and manual overrides in case of issues. A crucial consideration for further digitalisation of the electricity sector is whether such fall backs can continue to be implemented in an increasingly digitalised grid that is operated in real time with a focus on continuous availability.

Cybersecurity is garnering greater attention from governments and businesses, particularly for critical infrastructure

Cyberattacks are among the top ten global risks in terms of likelihood and impact according to the World Economic Forum *Global Risk Report 2020* (World Economic Forum, 2020b). More than three-quarters of respondents expected the risk of cyberattacks on infrastructure to increase in 2020.

Governments are paying more attention to cybersecurity, particularly for critical infrastructure (ITU, 2019). Nearly half of national cybersecurity strategies globally have been developed or updated since 2017 (CIPedia, 2020; ITU, 2019).

Businesses are also increasing their focus on cybersecurity threats. Worldwide spending on information security was an estimated at USD 100-125 billion in 2019, growing at around 10% per year, outpacing overall IT spending, which is growing at around 3% per year (Gartner, 2018; IDC, 2019b). However, among economic sectors, cybersecurity spending by utilities lags behind other sectors such as government, finance and telecoms (Malik, 2018; McKinsey & Company, 2019).

Electricity sector investment in cybersecurity is difficult to identify

Expenditure on cybersecurity could be used as an indicator to track the action taken by utilities to ramp up cybersecurity capabilities. However, it is difficult to assess the investment electric utilities make in cybersecurity, let alone identify what is optimally needed. There are challenges around disclosure, as well as determining what actually constitutes “cybersecurity spending”.

This is a challenge even for regulated entities, as cybersecurity-related spending is often part of various infrastructure or operational spending categories. It complicates the ability of regulatory authorities to set effective policies, and runs the risk that cybersecurity spending is kept down to minimise overall capital and operational expenditure. Utilities may also be reluctant to reveal cybersecurity-spending figures to avoid misperception by customers, shareholders and possible attackers.

Recent estimates show that overall “energy IT and cybersecurity software and services” spending globally is expected to rise from USD 19 billion in 2020 to USD 32 billion in 2028 (Business Wire, 2020; Navigant Research, 2019). Only about 7% of this is security-related, representing around USD 1.3 billion in 2020, though this component is proportionally growing faster (Walton, 2020a).

Almost no robust data is available on cybersecurity expenditure by specific type of organisation, size or region. There are benchmarks for IT-related cybersecurity costs in various economic sectors (e.g. percentage of revenues), but not for the OT domain of electric utilities. Overall cybersecurity spending remains a small percentage of total utility investment, but many organisations see an increasing trend for cybersecurity investment relating to IT and OT. A 2018 survey of energy company executives found that over half (57%) had increased spending on cybersecurity over the past 12 months, and 68% planned to spend more over the next 12 months (EY, 2018).

Threats and incidents

The threat of cyberattacks on electricity systems is increasing

The threat of cyberattacks on electricity systems is increasing. In his testimony to the House Committee on Energy and Commerce in July 2019, the President and CEO of the North American Electric Reliability Corporation stated that the threat of cyberattacks on grids is at an all-time high (Robb, 2019). More than half (54%) of utilities in one 2019 survey expected a cyberattack in 2020 (Ponemon Institute & Siemens, 2019).

According to the Edison Electric Institute, large power companies can face thousands to millions of potentially malicious network "attempts" each day (Sobczak, 2018). RTE, the French transmission system operator, was subject to over 10 000 "attacks" every month in 2018, while the California Independent System Operator reportedly faces millions of "undesired communications" each month (Nikolewski, 2019; RTE, 2019).

However, such quantitative measurement of threats, attacks and incidents should be interpreted with caution, and comparisons should be avoided. There could be major differences in scope or definition, such as what constitutes an "incident" or "attack". In addition, many incidents may not be reported, and some attacks may not even be detected.

The vast majority of attempted attacks are phishing email attacks and automated scans, which are in general some of the easiest and most defensible types of cyberattack. While these attacks are often detected and stopped without operational impacts, their sheer number highlights the intensity of the risk and that weaknesses in the system (where they exist) are likely to be exploited. Other common attack types include malware and denial-of-service attacks. More recently, attackers have combined multiple methods, such as the MAZE ransomware incidents (FireEye, 2020a).

Table 2. Common types of cyberattack on IT systems

Type	Description
Phishing	**Phishing** is the practice of sending fraudulent communications that appear to come from a reputable source, usually through email. The goal is to steal sensitive data like credit card and login information or to install malware on the victim's machine. Phishing is an increasingly common cyberthreat. **Spearphishing** is a type of phishing that targets specific individuals. **Whaling** is a specific type of spearphishing targeting key senior-level individuals such as CEOs. Attackers will masquerade as someone senior or influential at the organisation to directly target another senior member of the organisation.
Malware	**Malware** is a term used to describe malicious software, including spyware, ransomware, viruses and worms. Malware breaches a network through a vulnerability, typically when a user clicks a dangerous link or email attachment that then installs risky software. Once inside the system, malware can block access to critical components of the network, install additional harmful software, or covertly obtain information by transmitting data. **Ransomware** is a type of malware that encrypts user data, asking victims to pay a ransom in order to obtain a decryption key.
Denial-of-service (DoS) attack	A **denial-of-service** (DoS) attack floods systems, servers or networks with traffic to exhaust resources and bandwidth. As a result, the system is unable to fulfil legitimate requests. A **distributed denial-of-service** (DDoS) attack uses multiple compromised devices to launch the attack.

Sources: IEA (2017), Digitalization & Energy; Cisco (2020), What Are the Most Common Cyber Attacks?

Threat actors are becoming increasingly sophisticated at carrying out attacks on electricity systems, both in terms of their destructive capabilities and their ability to identify vulnerabilities (Ponemon Institute & Siemens, 2019). In addition, attackers may need fewer skills themselves, as strategies, tools and other skilled resources become more available to exploit common vulnerabilities (US Government Accountability Office, 2019). For example, in the Ukraine power grid attack of 2015 attackers used tools and techniques that were readily available on the dark web, including tools previously stolen from the US National Security Agency (Madnick, 2020).

The capability level of hackers varies substantially. Most organisations can prepare for attacks by amateur hackers or even larger, more advanced persistent threats by diligently applying the most essential cyber resilience measures (also called "cyber hygiene"). This should be the foundation for any organisation, be it large or very small.

Some organisations may need to conduct effective threat hunting and cyberthreat intelligence activities to prepare for threats from highly capable and motivated attackers. High-end threats from professional attackers with possible state support need to be taken very seriously by policy makers; they require concerted action across the sector and beyond, including collaboration and co-ordination with the intelligence community.

Various best practice overviews are available detailing cybersecurity measures specifically for application in the electricity sector. Early guidance and a leading reference source are the NISTIR 7628 Guidelines for Smart Grid Cybersecurity (NIST, 2014), and the related NIST Cybersecurity Framework Smart Grid Profile (NIST, 2019) (see Annex A).

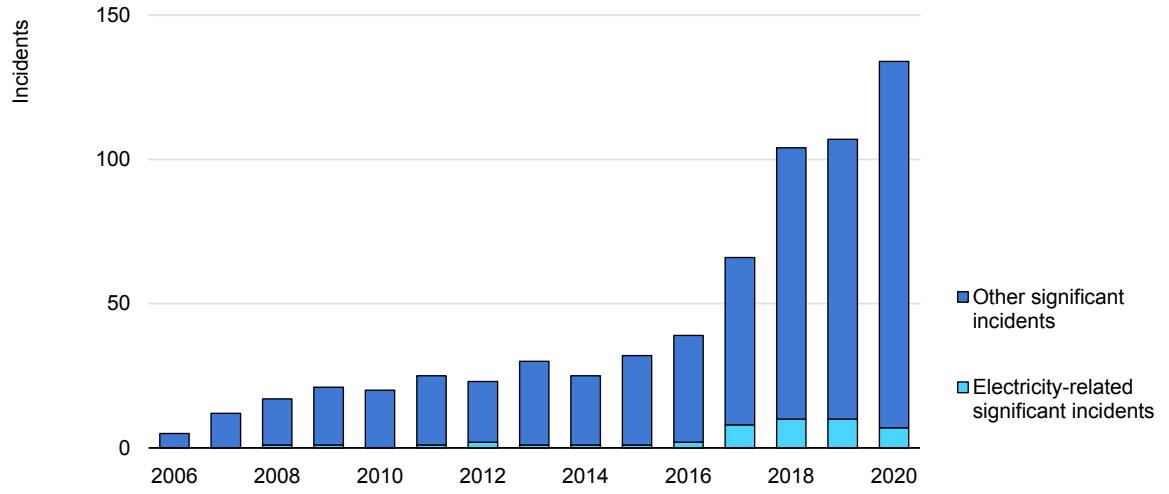
But publicly available information on significant cybersecurity incidents is limited

Across various sectors, most cybersecurity incidents may not be publicly reported, or even reported at all to regulators or other authorities. In one survey of industrial organisations, two-thirds indicated that they did not report cybersecurity incidents to regulators, even if they were legally required to (Kaspersky, 2019). Exposure to liability and loss of customer confidence in the event of a data breach are major business concerns that contribute to under-reporting. It is also likely that there are attacks that go undetected (Ponemon Institute and Siemens, 2019; Tripwire, 2016).

The number of "significant"[2] cyber incidents reported globally has risen dramatically in recent years. Of the 134 incidents tracked in 2020, seven were electricity related (CSIS, 2020).

[2] Cyberattacks on government agencies, defence and high-tech companies, or economic crimes with losses of more than USD 1 million.

Figure 3. Significant cyber incidents worldwide, 2006-2020



Note: "Significant" cyber incidents are defined as cyberattacks on government agencies, defence and high-tech companies, or economic crimes with losses of more than a USD 1 million.
Source: IEA analysis based on CSIS (2020).

In terms of the average cost of cyberattacks in various sectors, utilities had the second-highest average cost in 2018 (USD 17.8 million per company per year, up 18% from 2017), behind banking (USD 18.4 million, up 11%) (Ponemon Institute & Accenture, 2019). These costs include internal costs related to dealing with the cyberattack (i.e. detection, investigation, containment and recovery), as well as costs related to the consequences of the cyberattack (i.e. from business disruption, information loss, revenue loss and equipment damage). Tools such as Blackout Simulator 2.0 can estimate the potential costs of blackouts (Reichl et al., 2020).

Disruptions to electricity systems caused by cyberattacks can result in significant harm, but have so far been relatively limited

Cyberattacks on electricity systems could result in significant harm to safety and the environment, the utility and its customers, the broader electricity system and the economy (EPRI, 2015).

To date, disruptions to electricity systems that have resulted from reported cyberattacks have been small compared to other causes, such as power outages from storms, equipment failures or operational errors. The 2015 attack on the western Ukraine power grid was the first confirmed cyberattack specifically against an electricity network with impacts on system availability. Attackers accessed and manually switched off substations, resulting in 30 substations going offline and

225 000 people losing power (E-ISAC, 2016). Other reported electricity-related cyber incidents since 2015 are summarised in Annex B.

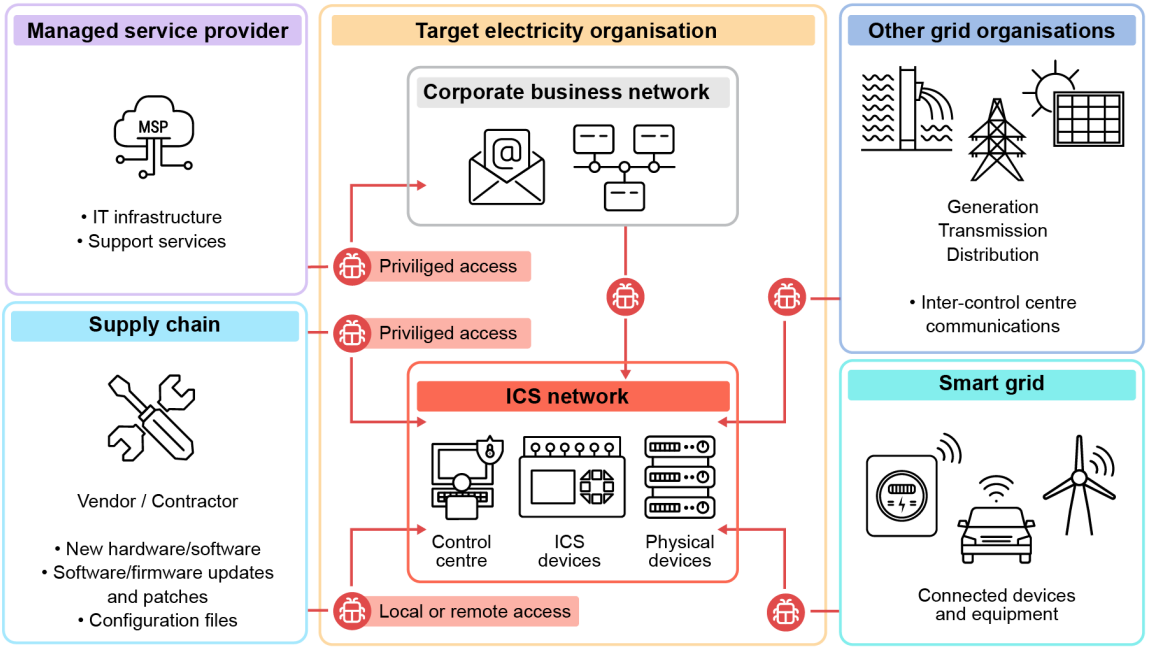
Cyberattacks on fuel supply infrastructure can also affect electricity systems that depend on these fuels. In February 2020 a natural gas pipeline system in the United States was the target of a phishing and ransomware attack (Buurma & Sebenius, 2020; DiChristopher, 2020; O'Flaherty, 2020; US Department of Homeland Security, 2020). While the attack only impacted OT systems at a single gas compression facility, the pipeline system was shut down for two days to restore the affected systems from backup files. US gas pipeline operators were also attacked in 2018, but gas service was not interrupted (Krauss, 2018).

There are plausible scenarios where cyberattacks could cause significant harm to electricity grids

Understanding past incidents and their causes can help to prevent reoccurrences, but does little to address new types of attack. Preventing and recovering from new types of attack – including the use of multiple attack mechanisms – requires exploring and understanding plausible scenarios that could have major impacts on electricity grids.

This requires knowledge of the vulnerabilities of assets, as well as strong situational awareness to understand the various ways in which an attacker could compromise IT and OT systems, such as by gaining access to industrial control systems.

Figure 4. Potential ways an attacker could compromise industrial control systems



Source: Canadian Centre for Cyber Security (2020), Cyber Threat Bulletin: The Cyber Threat to Canada's Electricity Sector – Canadian Centre for Cyber Security.

There are numerous potential cyberattack scenarios resulting in a range of impacts on electricity systems. Several scenarios are described in detail in Annex C, including:

- A virus infiltrating an industrial control system through USB flash drives.
- Compromised firmware updates of OT assets.
- Supply chain vulnerabilities resulting in compromised equipment.
- Malicious firmware update of smart meters triggering a mass disconnection.
- Manipulation of a large number of high-wattage connected devices.

These and other scenarios are discussed in further detail in EPRI (2015) and Fischer et al. (2018). Various public knowledge databases exist which outline cyberattack tactics that can be applied to specific types of system, such as the MITRE ATT&CK framework for ICS (EPRI, 2015; Fischer et al., 2018).

Emerging threats and vulnerabilities pose risks to all stakeholders in the electricity value chain

As the scenarios above demonstrate, there are vulnerabilities and threats across the electricity value chain – from generation to end users – as well as along the supply chain (i.e. hardware and software vendors).

Every segment of the electricity sector sees many benefits emerging from digitalised solutions. Each of these segments needs to adopt proper cyber resilience measures to avoid attacks that may have operational impacts on larger parts of the system.

Table 3. Opportunities and cyber risks from digitalisation across the electricity value chain

	Generation	Transmission and distribution	Consumers and distributed energy resources
Opportunities	• Improved efficiency • Predictive maintenance • Reduced downtime • Lifetime extension • Renewables forecasting	• Improved efficiency of assets and wider system operations • Predictive maintenance • Reduced downtime with faster fault localisation • Lifetime extension • Grid stability monitoring • Enhanced local flexibility options	• Demand response, including vehicle-to-grid (V2G) • Demand forecasting • Energy management • Smart buildings
Cyber risks	• Loss of control • Physical damage	• Loss of control over substations • Physical damage • Blackout • Cascading effect on connected systems via power system or IT communications	• Breach of data privacy • Impact on customer processes and support • Mass attack on distributed devices via common vulnerability

As the electricity system evolves, some threats may subside while others emerge. For example, many OT systems today still use customised processes and hardware, unlike in IT systems. This means that it takes attackers more effort and reconnaissance to build effective malicious software. This heterogeneity of OT also blocks attackers from replicating and scaling attacks. But as electricity OT systems become increasingly homogeneous – shifting to open-source protocols and industry standards – these potentially mitigating factors are deteriorating (Dragos, 2019).

The grid edge and emerging digital technologies

Consumer IoT devices, such as smart appliances connected to the grid's distribution network, also pose a new and growing cyber risk. Industry analysts project upwards of 40 billion consumer IoT devices connected by 2025 (GSMA, 2020; IDC, 2019a).

If an attacker is able to compromise a large number of high-wattage IoT devices (such as air conditioners, heaters and electric vehicles), they might be able to turn them into a botnet to launch a co-ordinated attack that causes large demand fluctuations and imbalance across the distribution grid, ultimately triggering an outage (Acharya et al., 2020; Raman et al., 2020; Soltan et al., 2018; US Government Accountability Office, 2019).

However, due to its technical complexity, experts have a range of opinions on whether such a mass attack via many small grid devices is a high or low probability risk. Historically, cyber resilience strategies developed by utilities and regulators have typically been based on the assumption that most plausible critical attacks happen at central nodes of the system, such as the control centre of a system operator or large plant operator.

Another emerging vulnerability arises from the use of global positioning systems (GPS) to monitor and control generation, transmission and distribution functions (US Government Accountability Office, 2019). A malicious actor could spoof GPS signals, which could result in localised disruption to grid operations.

Emerging digital technologies like AI hold promise in improving threat detection and thwarting attacks, but could equally boost the capability of attackers who may rely on decisions taken on predefined algorithms and with limited knowledge and information.

Supply chain security

Significant cyber risks are associated with the supply chain that supports electricity system operations with critical hardware and software. For example, malicious code could be inserted into software at an early development phase. Back doors could be built into the hardware to enable remote access once installed, allowing attackers to steal data or disable systems (NIST, 2015). Remote firmware update communication channels themselves can also be compromised. This emphasises how the resilience of the wider system or individual grid users also depends on the level of cyber resilience of stakeholders other than those directly accessing

the electricity system. This creates substantial questions regarding liability, trust, interdependencies and effective policymaking. In addition to all this and probably most important, even when vulnerabilities in IT or OT software are identified and fixed early by the original equipment manufacturer, the user needs to implement this fix as soon as possible.

Insider threats

Many cyberattack techniques target personnel (management, staff and contractors) with the aim of exploiting their privileged access to enterprise networks and files. One study estimated that half of all breaches had a substantial "insider threat" component, of which the majority were not intentional (e.g. negligently opening a malicious attachment) (Bailey et al., 2018). Therefore, increasing awareness at all levels and building an organisational culture that is "cyber hygienic" are fundamental in reducing cyber risks. Other cyber hygiene practices include secure configuration of equipment and networks, keeping software up to date, avoiding giving staff and users unnecessary system privileges or data access rights, and training to establish a security-conscious culture throughout the organisation.

The technologies and systems being used by utilities are constantly changing, as are the vulnerabilities of these systems and the capabilities of potential attackers. All stakeholders need to continuously monitor and assess cyber risks, and aim for maximum preparedness.

Preparedness and capabilities are uneven across industry stakeholders

Readiness for cyberattacks is uneven across industry stakeholders due to differences in technical capability to identify threats, understanding of risk-based best practice and compliance with regulations.

A 2019 survey of over 1 700 utility professionals worldwide found that only 42% of respondents rated their organisation's cyber readiness as "high", and only 31% were fully ready to respond to or contain a breach (Ponemon Institute & Siemens, 2019). The survey found that smaller utilities (i.e. fewer than 5 000 employees) reported consistently lower confidence in their ability to identify and contain threats compared to larger organisations.

Utilities face several key challenges in addressing cybersecurity risks (Ponemon Institute & Siemens, 2019; US Government Accountability Office, 2019), including:

- Increase in sophistication and frequency of attacks.
- Lack of strategic attention at the CEO and board levels until an attack occurs.
- Siloing of cybersecurity issues to the IT division.
- Limited resources to invest in cybersecurity protection, including training and personnel.
- Lack of availability of skilled personnel (human capital gap), including difficulties in hiring and keeping qualified cybersecurity employees.
- Uncertainties about how to implement cybersecurity standards and guidance, and challenges in complying with a patchwork of compliance regimes.
- Limited public–private information sharing of classified information.
- Lack of alignment between IT and OT security, including challenges in integrating new digital devices and equipment with legacy assets.

The next section provides guidance and examples on how electric utilities can enhance cyber resilience across the electricity value chain, and how policy makers and regulators can guide the industry.

Mechanisms to enhance resilience

Ensuring cyber resilience is the collective responsibility of all stakeholders across the electricity value chain, from generators to retailers and end users

Cyberthreats to the electricity system are constantly evolving. All system stakeholders need to continuously monitor and evaluate their main vulnerabilities and risk profile to work on readiness and resilience. They need to be aware of the risk posed by the system as well as the risk they pose on the system

To effectively plan and respond, utilities need to have a proper asset management approach to identify the capabilities and risks of their system from both IT and OT perspectives. At a higher level of abstraction, looking beyond technical specifics, it is also essential that policy makers, regulators and industry's senior decision makers understand the risk exposure and can communicate effectively on this matter.

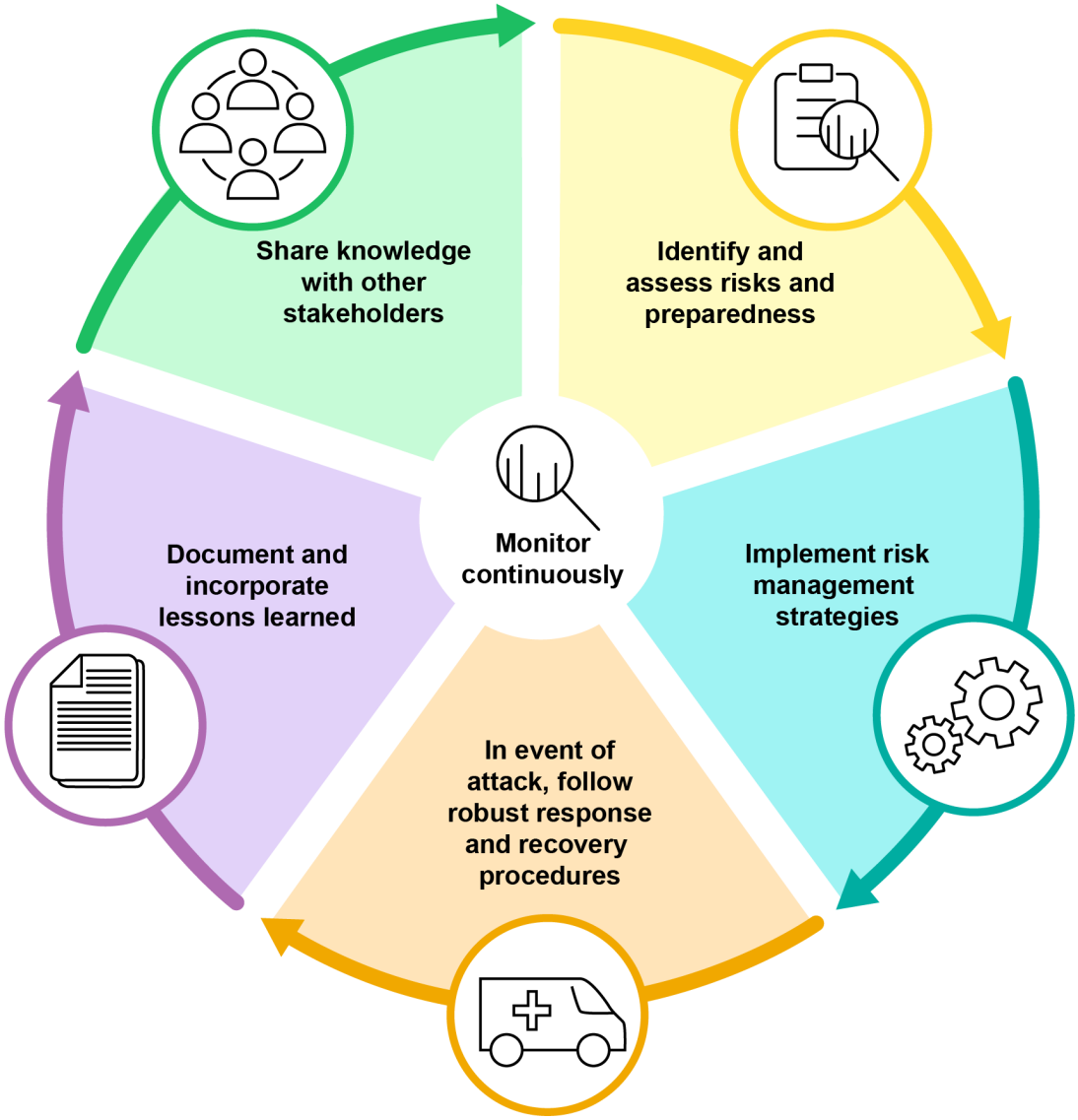
Actions by policy makers, regulatory authorities, regulated entities and other stakeholders can advance cybersecurity resilience across the electricity system and ensure appropriate measures are implemented. Several tools and frameworks can support these efforts.

This section outlines various instruments available to enhance resilience without aiming to expand on specific cybersecurity measures in technical detail.

Enhancing cyber resilience is a continuous process

Enhancing resilience is a continuous process that starts with decision makers assessing the current state on how prepared, or mature, their organisation is to face an attack and the risks to which they are exposed. Based on the identified risks and their criticality, they then start a prioritisation and implementation phase. In case of an attack, all relevant stakeholders need to follow the response and recovery mechanisms and guidelines. Finally, the same decision makers need to capture lessons learned and incorporate them through a feedback loop to enhance internal resilience, sharing them so they serve as additional knowledge sources.

Figure 5. Steps to enhance cyber resilience



Many tools and frameworks are available to provide guidance on each of these stages. Some address a broad spectrum of resilience, while others focus on particular steps or sectors. Cybersecurity guidance documents have a reputation for being lengthy, complex and with a great level of detail on correct process descriptions. Selected examples of widely used tools are described in the table below.

Table 4. Overview of regularly referred to instruments for cybersecurity in the electricity sector

	ES-C2M2	NIST CSF	NISTIR 7628 Guidelines for smart grid cybersecurity	ISO/IEC TR 27019	ISO 22301
Objective	The Electricity Subsector Cybersecurity Capability Maturity Model is an electricity sector-specific tool to evaluate the maturity of an organisation's cybersecurity capabilities, and help prioritise cybersecurity investment and actions to reach higher maturity levels.	NIST Cybersecurity Framework is a general resilience framework to understand, prioritise and manage cybersecurity risks. It simplifies and harmonises communication of cybersecurity needs within and outside the organisation.	NISTIR 7628 gives smart grid-specific guidelines to develop cybersecurity strategies. It includes a comprehensive risk assessment phase by complementary bottom-up threat analyses and top-down external and internal system interface assessment.	The ISO 27000 series sets information security standards for all sectors. The 27019 standard is an energy utility-specific international standard to guide organisations implementing information security controls.	ISO 22301 is for business continuity management and for all sectors. This standard emphasises the need for a well-defined incident response structure and is highly based on exercises to ensure measures will work as anticipated when required.
Used for	Self- evaluation usually facilitated by organisation internally. External facilitators may be used as well.	Self-assessment and implementation, usually facilitated by a qualified or certified individual.	Self- assessment and implementation.	Self-implementation accredited by external certification bodies.	Self-implementation accredited by external certification bodies.
Developed by	US Department of Energy in collaboration with energy industry cybersecurity practitioners.	US National Institute of Standards and Technology (NIST).	NIST	International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).	ISO.

	ES-C2M2	NIST CSF	NISTIR 7628 Guidelines for smart grid cybersecurity	ISO/IEC TR 27019	ISO 22301
Users	Originally developed for electricity sector. Has been adopted by US and international organisations across all critical infrastructure sectors	Governments (global level) and federal agencies, critical infrastructure sector.	Utilities, providers of energy management services (incl. aggregators, electric vehicle charging).	Generation, transmission and distribution utilities.	All organisations that provide essential services.
Key components	Cybersecurity practices evaluated across 10 domains (e.g. asset, change and configuration management, risk management) by maturity indicator level (MIL), ranging from 0 to 3.	NIST CSF contains five main functions (identify, protect, detect, respond, and recover) with further categories within each. Each category contains informative references, which are specific standards or guidelines to meet specific outcomes.	Divided into 7 smart grid domains (bulk generation, transmission, distribution, customer, markets, operations, and service provider).	It is intended to help apply ISO/IEC 27002 (114 security controls) and extend its content to the energy utility industry. The document provides 13 areas of control, with specific guiding practices in each.	Contains 10 main clauses (scope, normative references, definitions, context of the organisation, leadership, planning, support, operation, performance evaluation and improvement).
Complexity	Low Documentation and support available to ease implementation.	Medium Documentation available to ease implementation.	High Extensive documentation of technical and detailed nature.	High Extensive documentation plus certification required.	High Extensive documentation plus certification required.
Examples and additional information	The Michigan Public Service Commission in the United States conducted an assessment in 2019 to evaluate whether electric systems are adequate to	The use of CSF is mandatory for US federal agencies. Specific to the electricity subsector, NIST created the Cybersecurity	It is considered a flagship publication that guides cybersecurity requirement analysis and creation for smart grids.	While ISO standards are often applied voluntarily to ensure meeting industry standards, they can also be made mandatory by law. E.g. in Germany in	This standard encompasses resilience on a general level, not just from the cybersecurity angle.

	ES-C2M2	NIST CSF	NISTIR 7628 Guidelines for smart grid cybersecurity	ISO/IEC TR 27019	ISO 22301
	account for changing conditions. One of their recommendations to all electric utilities is to conduct annual self-assessments of cyber capabilities using the C2M2 self-evaluation tool (Michigan Public Service Commission, 2019).	Framework Smart Grid Profile to apply risk management strategies from the CSF to power systems. The profile includes considerations that power system owners/operators may have to address as they implement the CSF framework core (NIST, 2019).	However, there exists little guidance on implementation; therefore it is best for users with the right level of resources and experience. In response to implementation difficulties, NIST expects to publish in 2021 and 2022 a series of technical publications and set of companion guides that provide guidelines on cybersecurity best practices that are relevant to a highly distributed electric grid.	line with the IT Security Act and the German Federal Network Agency, network operators must prove information security compliance through certification. Estimates indicate that in Europe about 25% of transmission system operators are ISO 27001 certified.	A combination of ISO 22301 with NIST CSF is usually recommended as basic continuity management aligned with the standard reflects NIST CSF core practices (Graham, 2018; Tangen & Austin, 2012).

Notes: ES-C2M2, NIST CSF and NISTIR 7628 originated from the United States but are widely applied beyond. ISO 27019 and ISO 22301 are global standards.
Sources: NIST (2014, 2020a); US Department of Energy and US Department of Homeland Security (2014); ISO (2017).

There is no one-size-fits-all solution, as most tools are tailored to specific needs

These cyber resilience tools were created for users to meet specific needs or to comply with specific policies. There is no cyber resilience handbook that would be optimal for all types of utility in all possible systems today or in the future. Therefore, it is always advisable to complement or tailor a selected approach to ensure the appropriate level of coverage.

Several utilities, governments and even sectors have adopted their own version of a framework for enhancing resilience so that it is better adapted to their specific needs.

For example, the Australian Energy Market Operator developed the Australian Energy Sector Cyber Security Framework. It leverages existing tools and industry standards, including ES-C2M2 and NIST CSF, and aligns them with Australian policies such as the Australian Privacy Principles and the Australian Cyber Security Centre Essential Eight Strategies to Mitigate Cyber Security Incidents. The framework is adapted into two versions, each targeting different users and capabilities. The full self-assessment covers all practices within the framework and is aimed at utilities of high and medium criticality. A light version, intended only for low-criticality market entities, comprises easy-to-follow questions to respond to the needs of utilities with limited time and resources to address cybersecurity. Criticality is identified using the Criticality Assessment Tool, created specifically to place all participating entities on a single scale for reporting, benchmarking and support to set a target state of organisational maturity (AEMO, 2019b, 2019a).

Cybersecurity certification and standards can play a crucial role in building confidence, but need to cope with the dynamics of cybersecurity

The main driver for the use of international standards is recognition among principal stakeholders of the need to establish common benchmarks for the steps needed to achieve specific goals. The cost-effectiveness of harmonisation is another advantage for industry.

Cybersecurity certification is a formalised evaluation of products, services and processes by an independent and accredited body. As such, it plays a critical role

in increasing trust and security in them (ENISA, 2020). Standardised processes allow this to happen on a cost-effective basis.

A potential unintended side effect of following or complying with specific certifications or standards is that risk management becomes an administrative box-ticking exercise without embedding a cyber resilience culture within every organisation that forms part of the system. Also, different jurisdictions can require compliance with different standards, creating the need for companies to achieve certification in each jurisdiction they operate in, often with differences depending on local practices.

The long and costly process of achieving certification of compliance with technical specifications can be a burden on smaller companies. It risks overwhelming them in its cost, complexity and timing, thus hindering competition. Moreover, a certificate for infrastructure is only relevant at the time of certification. Vulnerabilities might be introduced once it is commissioned or new vulnerabilities may be identified in other related parts of the system. The process of updating a standard typically moves slowly. Revision and update cycles typically take at least three to five years, whereas new cyberthreats emerge daily. Cybersecurity standards need to focus on risk management approaches and the processes by which security is maintained once equipment is commissioned (firmware updates, detection schemes, fallback solutions, etc).

Key elements of product certification

Four elements are critical in product certification: key decision makers within utilities who determine which products and systems need to be certified and why; a governing body to approve the certification criteria; testing labs to confirm that products adhere to the certification criteria; and an oversight body to ensure that utilities are only purchasing certified products or are granted waivers (World Economic Forum, 2020a).

Currently, there is no commonly accepted global framework or standard, although different programmes are being pursued worldwide. Differences in criticality between different stakeholders and the potential burden on small or emerging organisations were at the centre of EU policy design for cybersecurity measures in the electricity sector (European Court of Auditors, 2019). This is exemplified in the Cybersecurity Act (addressing various sectors), which sets a framework for establishing schemes that would allow product certificates issued under those schemes to be valid and recognised across all member states. Certification is

voluntary, but the European Commission assesses at least every two years whether a particular product certification should be made mandatory (Stassen, 2019).

Concerns have been raised over potential fragmentation that might result from having different regulators and supervisors, as the EU-wide certification schemes will still be supervised by national supervisory authorities designated by member states (Shooter & Shooter, 2019). In order to promote co-operation, in May 2020 the Connecting Europe Facility awarded funding for projects that promote co-operation among cybersecurity certification authorities on ICT products, services and processes (European Commission, 2019, 2020b).

In the United States, the North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) standard addresses supply chain risk in its recently adopted CIP-013-1, which came into force in October 2020 (Arampatzis, 2020; Fortress Information Security, 2020). Under this standard, electricity sector participants must develop and implement a comprehensive supply chain risk-management plan that requires review every 15 months. Mandatory elements focus on software and firmware integrity and authenticity, vendor remote access to bulk electric cyber systems, and vendor risk management and procurement controls (Accenture, 2018). However, as NERC CIP-013-1 comes into effect, all relevant stakeholders still need time to understand what repercussions they could face if they do not comply and adjust their operations accordingly. Implementation challenges have already been identified concerning scoping, vendor relationships and interpretation. To address such challenges, entities such as the North American Transmission Forum and some private companies have published implementation guidance (Furneaux, 2020). This is especially relevant as according to the State of the Electric Utility 2020 report, only 36% of the participating utilities have established procurement and supply chain cybersecurity protocols (Gahran, 2020).

Industry initiatives are emerging such as the Charter of Trust, which has been signed by 17 large companies who have committed to adhere to a minimum set of requirements that can be tracked in products and services across the value chain. Certification processes can be voluntary industry initiatives, can be done by means of self-attestation, can be incentivised by regulatory instruments, or can be made mandatory. This is a critical choice for any policy maker to make, especially for first movers, with potential impacts on a global industry.

Continuous assessment is required to enhance an organisation's resilience

The first step to enhance an organisation's cyber resilience is the assessment phase. In this phase, the organisation examines its cybersecurity risk practices to better understand any gaps between performance and objectives. It needs to perform assessments regularly, as the rapid evolution of technology and market structure modifies not only the risks that the organisation is exposed to, but also its liabilities.

Different tools are available for an organisation to initiate its assessment process, from simple checklists of points to consider, to more sophisticated models. Assessments are performed either by the organisation itself (self-assessment) or by an independent external entity, depending on the tool it uses as well as the organisation's capability and local or national requirements. Policy makers and regulators can take advantage of this wide variety of available tools to either select one or craft their own according to specific needs, mandating it or providing it as guidance when setting specific outcome targets.

Ofgem, the electricity and gas regulator in Great Britain, developed a set of cyber resilience guidelines for electricity and gas network companies as operational guidance to develop their cyber security and resilience. The guidance is directly linked to the price control mechanism (RIIO-2). Referring to over 40 elements, the guidelines describe the ideal outcome or best practice for each of them and indicate further guidance documents on how this outcome could be implemented, such as standards or well-known frameworks (Ofgem, 2020). By following these guidelines, organisations can determine whether they have considered each of the elements and to what extent and how they could be enhanced, thus giving the organisation a sense on their preparedness vis-à-vis cyber resilience. Moreover, as this guidance has been developed in the context of the regulator's price control process, it sends regulated entities a direct incentive signal.

Some of the most common self-assessment tools are maturity models. Maturity models guide organisations through three main questions: where are we, where are we going, and how do we get there? Mechanisms and processes are considered mature if they are expected to be effective in addressing the issues they are put in place for.

Maturity models help an organisation assess its cybersecurity capability and potential progression to a higher degree of preparedness

Maturity models allow an organisation to carry out assessments at regular points in time to understand and compare its preparedness in the context of a possible threat or attack scenario. Maturity models typically rely on industry best practices and may incorporate standards or other codes of practice.

A maturity model example that is not specific to the electricity sector is the IoT Security Maturity Model created in 2019 by the Industrial Internet Consortium. It uses a two-dimensional approach to measuring maturity, evaluating it by comprehensiveness and scope. Comprehensiveness evaluates how exhaustively and consistently the security practices are applied and work. Scope reflects the suitability of a measure to address an industry-specific or system need (Industrial Internet Consortium, 2018). This adds value by grading how suitable a practice is, depending on the system under consideration.

The ES-C2M2 is a maturity model widely used in the electricity sector. It was developed by the US Department of Energy through a public-private partnership of energy sector experts. As a voluntary self-evaluation programme, the model enables consistent evaluation and improvement of IT and OT cybersecurity capabilities. It uses a set of industry-vetted cybersecurity practices across 10 domains and indicates maturity levels for each domain at discrete levels from 0 to 3. It is an easy-to-implement tool, with extensive documentation on how to execute it and numerous organisations available to facilitate it. It is implemented across the electricity value chain by generators, system operators and service providers. It can help organisations benchmark their cybersecurity capabilities and document improvements over time and across business functions, and prioritise actions and investments for cybersecurity (US Department of Energy & US Department of Homeland Security, 2014).

By understanding an organisation's level of maturity in a market, operators and regulatory authorities can identify gaps and set further direction

Various maturity assessment tools are available for authorities. The National Association of Regulatory Utility Commissioners in the United States has developed a Cybersecurity Preparedness Evaluation Tool, which allows public utilities commissions to judge the maturity of a utility's cybersecurity

risk-management programme and to gauge capability improvements over time. Commissions can use the tool to identify gaps and accelerate the utility's adoption of additional mitigation strategies (NARUC, 2019).

Regulators must exercise caution when using self-assessments to compare different organisations. Organisations could have significant differences in resource capabilities, or play different roles and functions in the system (and thus show a different level of criticality). Comparisons of effectiveness are relevant only between equally capable and critical organisations. An external assessor could help evaluate a set of different organisations more objectively.

In Australia market participants across the National Electricity Market (NEM) and Western Australia Wholesale Electricity Market (WEM) were invited to self-assess their capabilities using the Australian Energy Sector Cyber Security Framework. The exercise conducted in 2018 resulted in market coverage of about 85% of each subsector in the NEM and 75% in the WEM. It provided market participants with clarity on the key areas they should further focus on and prioritise for cybersecurity investment. The Australian Energy Market Operator identified a number of next steps, including establishing a clearer cybersecurity vision with strategic goals and the suggestion for policy makers to strengthen the operator's authority to manage cybersecurity risk (AEMO, 2018).

In Canada the Ontario Energy Board made it mandatory for distribution and transmission system operators to report annually on the status of cybersecurity readiness, referencing their Ontario Cyber Security Framework (Ontario Energy Board, 2020). This tool is inspired by the NIST framework and contains an inherent risk profile tool, which allows each Ontario distribution company to be categorised objectively. Based on their size, maturity and capability, distribution companies will have different inherent risk profiles, which will require them to apply security controls to a varying degree to ensure an adequate level of confidence in their cybersecurity. The board will use this information to assess both the sector and an individual organisation's state of readiness, to determine if any further action is necessary (APPrO, 2018).

These surveys reveal crucial information to relevant authorities for them to understand general sector trends and barriers.

Risk management practices help utilities prioritise effort and investment to achieve a higher degree of cyber resilience

The next step to enhance cyber resilience is to assess and understand the risks to which an organisation is exposed. This enables the organisation to prioritise areas of work and investment decisions for maximum benefit in line with its economic capacity and risk appetite. To achieve this, it would balance the cost of the measures against the economic losses and other impacts that it could incur due to cyber incidents and their likelihood of occurring. As a note of caution, it is important to keep in mind that because the electricity sector has yet to suffer substantial losses compared to other sectors, it could run the risk of underestimating the impact.

Cyber resilience needs to be integrated into the culture of the organisation. It should therefore manage digital security risk by integrating its approach into its existing risk management framework. Otherwise, cyber resilience will remain a separate technical issue and the organisation cannot address the challenges that come with digital transformation holistically or consistently, putting its economic and social objectives at risk. Cyber resilience should be part of every department, from procurement to innovation.

A risk management strategy is a valuable tool that provides direction for analysing and prioritising cybersecurity measures based on identified risks and the organisation's tolerance for risk. The table below provides an overview of widely used risk management tools.

Table 5. Risk management instruments in the electricity sector

	ISO 27005	ISA/IEC 62443-3-2 and 3-3	Risk Management Process (RMP)	NCSC risk management guidance
General description	International standardised guidelines for information security risk management.	Industrial control system-specific standards for information security risk management.	Electricity sector-specific guideline to implement risk management process, establish risk tolerance levels and prioritise actions, developed by US Department of Energy.	High-level guidance to educate on risk management topics and provide an overview of approaches and tools, developed by the UK National Cyber Security Centre.

	ISO 27005	ISA/IEC 62443-3-2 and 3-3	Risk Management Process (RMP)	NCSC risk management guidance
Used by	All types of organisations (private, government agencies, non-profit).	All industry sectors and critical infrastructure that utilise control systems such as PLC and SCADA.	Electricity sector organisations regardless of size.	Applicable to large organisations and the public sector.
Key elements	Standard extends the ISO 27001 risk management process starting from context establishment to risk assessment and risk treatment. Includes continuous monitoring and reviewing and communication and consultation processes.	Guides the user through the process of risk assessment and helps them identify security countermeasures aligned with a targeted security level and required security level capability.	Top-down approach where organisations start by addressing risk from an organisational perspective in Tier 1 down to a technical IT and industrial control system perspective in Tier 3.	Collection of information on the fundamentals of risk management practices and approaches.

Sources: US Department of Energy (2012); International Society of Automation (2018); ISO/IEC (2018); National Cyber Security Centre (2018).

The risk assessment should be a basis for taking informed operational decisions based on a well-established methodology. It is absolutely essential to recognise that even with risk management practices in place and best-practice measures diligently applied, a successful attack could still occur. Risk management is intended to strengthen resilience as much as possible. Organisations need to understand the spectrum of risks they can and should mitigate, and the options for recovering from events when they happen. There is no single solution that will prevent attacks in a digitalised electricity system; thus, it is essential that policy makers provide relevant guidance and understand the cost-effectiveness of policy instruments.

It is important to keep in mind that regulation, by stepping in with mandatory or voluntary baseline requirements in an interconnected system, can avoid potentially extensive economic damage. This needs to be weighed against the burden that it might impose on certain stakeholders that have low criticality, or even the possibility that regulation does not keep up with market developments. These issues are discussed further in the next section.

Response and recovery procedures are crucial to cyber resilience

Risk management is key to reducing the risk of cyberattacks, but it cannot be eliminated completely. Robust response and recovery procedures can help maintain or restore operations in the event of a cyberattack, with responsibilities clearly allocated to all main stakeholders. This should minimise damage, prioritise actions, shorten recovery time and reduce breach-related expenses.

Industry planning and collaboration are central to dealing with the aftermath of a cyberattack, especially in an interconnected system where the temporary loss of one or more element could destabilise the entire system. Similar to environmental or climate disaster-related recovery plans, there is value in considering different scenarios and planning across contingency types.

A response scheme is a useful tool to achieve this. Typically, these schemes rely on an up-to-date risk assessment identifying critical stakeholders and resources. They define and allocate responsibilities and resources depending on the type of incident, provide a plan for the hierarchy and channels of information flow, and finally establish an incident event log, which would include all steps taken during the attack. Utilities have long created black-start recovery plans and response plans to deal with weather incidents, physical attacks or frequency/voltage issues. These plans should also include a cyber-incident response procedure.

A good example of a publicly available tool for small to medium-sized utilities is the cyber incident response playbook developed by the American Public Power Association, which provides step-by-step guidance on preparing a cyber-incident response plan. It delivers a clear path of steps to follow, possible resources to use and a list of key contacts and response partners (American Public Power Association, 2019).

Another useful example is the North American Electric Reliability Corporation's GridEx exercise in the United States, which last took place in November 2019. This is a two-day event conducted every two years and involves utility companies, regional and federal government, critical infrastructure cross-sector utilities and supply chain stakeholders. It consists of a simulated cyberattack scenario to test the cyber and physical security resilience of the North American grid. Its intention is to improve incident response from both local and regional stakeholders, increase the participation of the supply chain and improve communication channels. As an illustration, during GridEx III in 2015 industry participants identified the need for a programme that would help electric companies restore

critical computer systems efficiently following a major cyber incident, which resulted in the electric power industry's Cyber Mutual Assistance programme (Edison Electric Institute, 2017).

Cyber resilience is a combination of preventive and corrective measures, building on lessons learned after a cyberattack. For companies, reflecting on past attacks is essential to implementing new measures, and reinforcing or redesigning existing measures if deemed necessary after an attack. Equally important is the feedback to stakeholders outside the organisation to reinforce existing threat awareness, and allow detection of blind spots and vulnerabilities. This is especially relevant as cyberattacks are often "the first of their kind" for a company, and thus learning from outside experience becomes especially important – finding a different way of thinking to anticipate what could happen.

To reflect this, policies need to include procedures for sector-wide response, as well as incentivising best practice and information-sharing across organisations.

Partnerships, information exchange programmes and research initiatives provide additional sources of knowledge to enhance cybersecurity preparedness

Examples of fruitful research partnerships can be found in the Cybersecurity for Energy Delivery Systems (CEDS) programme, where the US Department of Energy partners with industry, academia and national laboratories to foster R&D specifically designed to reduce cyber risks in energy delivery infrastructure. With approximately USD 300 million invested since 2010, CEDS has been able to deliver more than 80 products, tools and technologies, 51 of which have been commercialised or are already available for use. More than 1 500 utilities in all 50 states have purchased products developed under CEDS (CESER, 2018). Every two years the Office of Cybersecurity, Energy Security and Emergency Response conducts a peer review of the research partnerships to provide public accountability as well as recommendations for improvement. During the last peer review in 2018, over 30 active projects were assessed.

Policy makers from countries with more limited budget capabilities can also scale up activities and find synergies by means of international partnerships. Examples of international collaboration can be found in Europe's continuing research initiatives or the recently established ASEAN-Singapore Cybersecurity Centre of Excellence.

Knowledge of best practices and vulnerabilities can be shared through workshops, bulletins, training and online communities. One example of this is the cyber bulletins created by the Electricity Information Sharing and Analysis Center (E-ISAC), which include physical and cyber security information provided by member organisations, which can be electricity asset owners and operators in North America, as well as selected government and cross-sector partners (E-ISAC, 2019a).

E-ISAC also manages the Cybersecurity Risk Information Sharing Program (CRISP) on behalf of the US Department of Energy. CRISP is a voluntary subscription-based programme and participating electric utilities now account for about 75% of US electric customers. CRISP's main functions are network sensing, and data processing, analysis and sharing to discover adversary action against CRISP participants. In 2018 the key outcome of the programme was to identify 87 cases predicated on "indicators of compromise", resulting in reports to utility sites to support their security operations. It also provided 320 indicators from government-informed sources that were not available publicly and produced 85 reports to provide situational awareness of observed cyber activity targeting the US electricity industry (E-ISAC, 2019b).

ISACs are evolving in many regions. They are most often country-specific and can cover more sectors than just electricity. Governments often play a crucial role in setting up these ISACs by means of mandatory or voluntary requirements, guidance and direct funding. International ISACs can also become important as cybersecurity risks and solutions spread across borders. The European Energy ISAC (EE-ISAC) complements the range of energy ISACs in Europe and co-operates with energy-related ISACs around the globe.

The European Union has long advocated the establishment of such public-private partnerships, given that private organisations are particularly well placed to strengthen such international ISACs (ENISA, 2017). It is therefore important for policy makers to include knowledge sharing as a central element of policy recommendations, finding the right balance between the benefit of such information being shared, preserving the confidentiality of critical infrastructure data and overcoming well-known barriers to information sharing (Koepke, 2017).

An achievement to this end is the creation of MISP, an open-source platform that allows organisations to share indicators of compromise. Its aim is to help improve the response against targeted attacks and establish preventive actions and detection. The project is co-financed by the European Union through the Connecting Europe Facility (MISP, 2020). It is one of the tools most commonly

used by ISACs within the European Union as it allows the sharing of anonymised information, supports the creation of "circles of trust" where not every member has the same permissions when using the platform, and allows the automation of information sharing (ENISA, 2017).

Table 6. Overview of different principles to guide policy makers, regulatory authorities, suppliers and regulated entities to advance cybersecurity resilience across the electricity system

	Overview of cybersecurity actions
Utilities	• Cyber resilience needs to be integrated into the culture of the organisation; organisations should manage digital security risk and integrate their approach into their existing risk management framework. • Current state assessment allows organisations to examine their cybersecurity risk practices to better understand any gaps between performance and objective. • Assessing the risk an organisation is exposed to and establishing a clear risk management strategy are key to enabling the prioritising of areas of work and investment decisions to maximum benefit. • Utilities need to have a proper asset management approach to identify the capabilities and risks of their system from both an IT and OT perspective. • Robust response and recovery procedures can help maintain operations in the event of a cyberattack, with responsibilities clearly allocated to all main stakeholders. • Cyber resilience is a combination of preventive and corrective measures, building on lessons learned after a cyberattack. Reflecting on past attacks is essential for the implementation of new measures, or the reinforcement or redesign of existing measures, if deemed necessary after an attack. Equally important is the feedback to stakeholders outside the organisation to create awareness of existing threats and allow detection of blind spots and vulnerabilities.
Suppliers	• Cybersecurity certification plays a key role in increasing trust and security in crucial products, processes and services. • Cybersecurity standards need to focus on risk management approaches and the processes by which security is maintained once equipment is commissioned. • Four elements are essential in product certification: determining what products and systems need to be certified; a governing body to approve certification criteria; testing labs to confirm that products adhere to the criteria; and an oversight body to ensure only certified products are being purchased. • Promoting co-operation is critical to avoid the potential fragmentation that might be expected from having different regulators and supervisors.

	Overview of cybersecurity actions
Regulators	• It is essential that regulators understand the risk exposure and can communicate effectively on this matter. • Regulators can take advantage of the wide variety of tools available either to select one or craft their own according to specific needs, mandating it or providing it as guidance when setting specific outcome targets. • Regulators must exercise caution when using self-assessments to compare different organisations. Comparisons of effectiveness are relevant only between equally capable and critical organisations. • Regulators must be cautious because an unintended side effect of following or complying with a specific protocol is that risk management could become an administrative box-ticking exercise.
Policy makers	• It is essential that policy makers understand the risk exposure and can communicate effectively on this matter. • Policy makers can take advantage of the wide variety of tools available either to select one or craft their own according to specific needs, mandating it or providing it as guidance when setting specific outcome targets. • Industry planning and collaboration are key, especially in interconnected system where the temporary loss of one or more element could destabilise the entire system. • Policies need to include sector-wide response procedures as well as incentivise best practice and information sharing across organisations. • Setting up research partnerships with industry and academia can foster R&D specifically designed to reduce cyber risks in the energy sector. • Policy makers from countries with more limited budget capabilities can scale up activities and find synergies through international partnerships. • Knowledge sharing of best practices and vulnerabilities can be achieved through workshops, bulletins, training and online communities. • Governments have a crucial role to play in setting up ISACs by means of mandatory or voluntary requirements, guidance and direct funding. International ISACs can also become important as cybersecurity risks and solutions spread across borders.

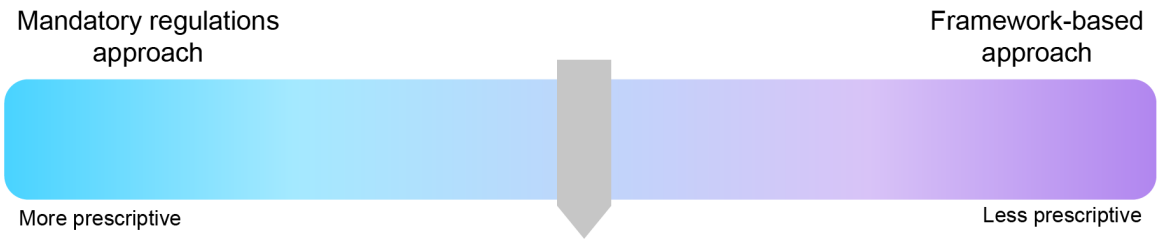
Policy and regulatory landscape

Setting effective cyber resilience regulation is a delicate balancing act between enforcement and innovation

Around the world a number of evolving policy approaches are used to ensure that the mechanisms and frameworks listed above are implemented. They can be broadly categorised on a scale ranging from highly prescriptive, where strict regulations set specific mandatory requirements, to less prescriptive framework-based approaches.

The more prescriptive approaches establish a detailed set of requirements for implementing, monitoring and reporting based on a number of predefined standards, fixed into regulatory, licensing or prequalification requirements. A prime example of this approach can be seen in cybersecurity regulations implemented in the United States through the North American Electric Reliability Corporation's Critical Infrastructure Protection standards (NERC CIP). Such approaches have the advantage of allowing for more streamlined compliance monitoring, but can face pushback from industry, which may see itself as too burdened by reporting requirements. Furthermore, there may be mismatches between the cycles of hardware, cybersecurity software and regulatory updates that recognise technology updates and keep pace with evolving cyber risks.

Figure 6. The regulatory spectrum for ensuring cybersecurity – the balance between prescription and outcome



Requirements to meet specific standards ensures:

+ minimum level across networks
+ streamlined monitoring for compliance
- but regulations can lag behind technology changes and focus more on compliance rather than risk

Establishing common criteria across networks allows:

+ customised approaches to achieve desired outcome
+ focus on outcomes to adapt to evolving risks
- but variable speed and level of cyber resilience risks weak link or contagion

Less prescriptive principle-based, performance-based or framework-based approaches are those that broadly indicate the structure of stakeholders and safeguards that need to be put in place to secure the electricity network.

Principle-based approaches aim to fulfil security principles while giving the operator some freedom when implementing the measures. Performance-based approaches, by contrast, are based on a number of metrics to assess the progress or the quality of implementation. Regulators can define specific target metrics, such as the achievement of specific standards or the time required to address a service disruption, leaving it to the operator to decide on the specific measures that will cost-effectively satisfy these metrics (Ragazzi et al., 2020).

An example of this is the approach taken recently by the European Commission through the directive on security of network and information systems (NIS Directive) and follow-up legislation. The NIS Directive requires each member state to establish a national framework for co-ordinating cybersecurity activities and designate essential service operators. Member states are then left with the responsibility of developing and implementing more specific sets of regulation, which can be more detailed and have broader scope. They have the discretion to allocate different roles across various stakeholders, including a single point of contact to monitor the implementation of the respective national strategy for cybersecurity; a national competent authority for digital service providers; and a national competent authority for operators of essential services.

Depending on the country, there might be a single or multiple authorities covering essential services such as electricity, gas, water, transport and banking. This allows for different implementation speeds and approaches, which has raised criticism of how to establish a coherent and robust cross-border approach to cybersecurity with tangible and effective impacts. Moreover, as the NIS Directive is a cross-sector framework, it requires further measures to be implemented in each sector. In the coming years, updates to grid codes are expected to bring more clarity as to concrete actions that can be implemented at the transmission and distribution level.

When the approach remains too conceptual and policy strategies have limited actual impact in mitigating risk exposure, the system is de facto depending on the voluntary initiatives of all electricity organisations active in the sector. Much can already be achieved this way, and many countries and individual organisations have made enormous progress over the past decade. But policy intervention will be essential to ensure that appropriate minimum security requirement levels are set for all stakeholders, to overcome conflicts between operators and

manufacturers, to nurture information sharing, and to achieve international collaboration. Policy should not necessarily aim to bring every organisation to the same level of security, nor to bring every organisation to the level of the most advanced. However, weak spots need to be avoided in a system that is interconnected digitally, electrically and via the supply chain.

Prescriptive requirements evidently give the benefit of being very clear on who needs to do what. However, the scope of application set by an authority may simply follow from its own powers and not necessarily be optimal. The case of NERC CIP in the United States provides an interesting example. While being clear on what applies to all bulk electricity system utilities, it does not cover smaller entities as these simply do not fall under NERC's jurisdiction, as opposed to being a rational choice. When devising policy to ensure cyber resilience in the power system, policy makers should ensure they instigate ecosystem-wide resilience, covering all stakeholders interacting with the power system and their interlinkages, rather than only network or system operators.

Implementation strategies should be tailored to the national context while considering the global nature of risks

In addition to the choice of regulatory instrument for cyber resilience, there is the question of implementation. For more prescriptive approaches, a compliance-based strategy or checklist can be helpful in linking specific measures with known security risks. However, such approaches run the risk of becoming too focused on ticking boxes to meet the requirements, as well as facing the issue of a lag between technological change and the pace of regulatory change. Alternatively, prioritisation criteria can be applied as a sort of iterative risk assessment, identifying the logical next steps to make the system more secure. This approach to implementation may lend itself to more dynamic cyber resilience policies, but, as with performance-based regulations, may lack a clear direction or baseline for threat prevention, complicating evaluation of effectiveness or cost recognition by regulators.

There are inherent differences in the implementation of these general approaches, stemming partly from institutional contexts, for example differences in regulatory jurisdictions at federal and state levels versus at the union and member state levels, making direct comparisons difficult. While being the most often referred to examples, the United States and the European Union are not the only jurisdictions developing policy frameworks for cybersecurity. Countries around the world, such

as Australia, Brazil and Japan, show that it is possible to enact mixed approaches, borrowing on the strengths of both general approaches, but tailoring implementation closer to the realities of very diverse power systems.

Despite these differences in implementation, however, there is a degree of scope for establishing common approaches to cyber resilience. This is particularly important both because of the global nature of vulnerability to cyberattacks, and because many original equipment manufacturers supply globally, so once a vulnerability is identified in standard equipment it could be exploited in other power systems. For policy makers, this implies co-ordinating with and establishing guidelines for equipment manufacturers.

While policy can enforce a compliance check for the implementation of measures, a true outcome-based approach does not exist specifically for cybersecurity, in contrast to conventional electricity quality of service regulations (for grid development, regulated tariff setting and general SAIFI/SAIDI targets). It remains questionable whether an outcome-based approach can be fully relied upon as a reasonable strategy for the resilience of critical infrastructure. The situation differs from that in grid development, where an investment can be motivated by system modelling analysis showing reduced operational costs or higher reliability, and where the actual impact on grid losses or interruption durations can be measured. A cyber resilience investment can hardly ever be weighed against a monetisable benefit or proven effective in retrospect by demonstrating prevented attacks. It is exactly because simply setting targets is not realistic that cybersecurity policies for the electricity sector are a complex area for policy makers.

Information sharing has to be a priority

EU member states are obliged under the NIS Directive to create a national cyber alert centre, with a network of computer security-incident response teams (CSIRTs) intended to share information on incident alerts and best practices for cybersecurity standards.

Japan, Brazil and Chile also encourage co-operation through CSIRT networks. These focus primarily on training local experts for cybersecurity readiness and response. Japan has recently funded the establishment of a cybersecurity training centre in Bangkok as part of the Asia-Pacific Economic Cooperation's dedicated taskforce on cybersecurity.

Incident sharing is a complex subject, as utilities and vendors are often deterred from doing so because of the liabilities this might cause them, or due to the

possibility of exposing other possible vulnerabilities. This last point is regarded as a double-edged sword, as while it offers the possibility of addressing the exposed vulnerability, it may also make the exposed vulnerability more easily exploitable. It is essential for policies not to create disincentives for information sharing and even to consider positive regulatory incentives for doing so.

The body responsible for crafting cybersecurity policies can vary from one country to another

Looking back at the recent history of cybersecurity policymaking, a variety of stakeholders are given the principal responsibility for it, with their specific roles differing across countries. Policy makers can give government-level officials direct authority for setting out overarching strategies, although many activities are delegated to regulatory authorities, other government agencies and main system operators. In countries such as the United States, Brazil, and Australia, their respective national electricity system regulators have driven the introduction of security requirements in a way to ensure that any assets connected to their network are secure. Enacting new or updated cybersecurity standards often requires an intricate understanding of and active engagement with regulators.

International or regional co-ordination also creates several levels of delegation. Stakeholders engaged in cybersecurity policy design and implementation can range from the national security sphere – often close to the executive branch – to the private sector seeking to minimise bottom-line impacts. Given this wide range of participants, policy makers need to align priorities across all stakeholders to ensure consistent implementation throughout the power sector.

Table 7. Cybersecurity policy approaches for the electricity sector in selected countries and regions highlighting the differences in responsible authorities

	Overview of main cybersecurity policy approach
European Union	The NIS Directive establishes common criteria for operators of essential services, including the energy sector. Member states are required under NIS to identify operators qualifying as operators of essential services, which become subject to security and incident reporting requirements. NIS also requires the establishment of a national framework for cybersecurity co-ordination, consisting of a CSIRT, a single point of contact and a national NIS competent authority. The European Commission supplemented NIS in 2019 with recommendations on cybersecurity in the energy sector, providing guidance on how to address specific requirements of energy network operators when implementing internationally recognised cybersecurity standards.

	Overview of main cybersecurity policy approach
	Presently the European Union is looking into possible certification routes for critical products and services, as well as setting up more extensive regulation (network code) on cybersecurity (European Commission, 2020a).
United Kingdom	The first national cybersecurity strategy was introduced in 2011 and has been updated since; the current version covers 2016-21 and provides high-level guidance around three key objectives: defend, deter and develop. The government's Department for Business, Energy and Industrial Strategy and the energy regulator (Ofgem) are the joint competent authorities for the electricity sector. Other important regulations include the 2018 Network and Information Systems Regulations and the 2019 Network and Information Systems amendment under the European Union withdrawal act (UK Department for Business Energy & Industrial Strategy, 2018). Additionally, the UK National Cyber Security Centre provides a cyber assessment framework, including 14 high-level principles, to guide the compliance efforts of operators of essential services and to be used for auditing purposes (UK National Cyber Security Centre, 2020).
Germany	Cybersecurity policy is centralised in the Federal Office for Information Security. The 2015 national law for IT security lays down the reporting obligations for operators of critical infrastructure, including electricity. As the main authority for cybersecurity, the federal office has developed a set of detailed requirements built around 12 blocks: information security management, asset management, risk management, continuity of supply, technical security, personal security, physical security, event detection and response, readiness checks, external reporting, supply chain management and incident reporting protocols. It has been a frontrunner in making standards mandatory, including the ISO 27000 series for operators and specific security requirements for smart meters, which showed the pros and cons of very prescriptive approaches. Germany's smart meter gateway policies illustrated how high expectations from policy makers can be translated into very detailed certification requirements in a clear process that could be used for standardisation. Nevertheless, these strict requirements eventually resulted in smart meter gateways having to pass a market declaration by the Federal Office for Information Security, limiting new functionality and thus stifling innovative business models.
Australia	A tailored cybersecurity framework for the Australian energy sector – the Australian Energy Sector Cyber Security Framework – was developed in 2018 using international examples such as ES-C2M2 and NIST CSF. This enables sector participants to undertake assessments of their own cybersecurity capability and maturity and use the results to inform and prioritise investment to improve their cybersecurity position (AEMO, 2020).
Brazil	Since 2016 Brazil's grid code has stated the obligations on ONS (the country's transmission system operator) and utilities to commit resources to protect against cyberattacks. The first cybersecurity package proposal, submitted to the regulator in 2019, draws on elements from the NIST CSF, NERC-CIP, ES-C2M2 and ISA/IEC 62443. The main building blocks include system architecture, information security governance, hardware and software inventories, monitoring and incident response, access management and vulnerability management.

	Overview of main cybersecurity policy approach
India	India's Ministry of Power established four computer emergency response teams (CERTs) to monitor and take steps to improve cybersecurity in the power sector. The CERTs are responsible for formulating model cyber crisis management plans (CCMP) for the generation (hydro and thermal), transmission, and distribution portions of the power system (Ministry of Power, 2019). These CCMPs are based on the best practices and advice of CERT-In, India's national agency for cybersecurity, and the National Critical Information Infrastructure Protection Centre (India Smart Grid Forum, 2017). Under the CCMPs, the states, union territories and utilities are advised to appoint a chief information security officer and establish CSIRTs. The Central Electricity Authority maintains an information resource, pooling and sharing platform on cybersecurity in the power sector. Plans to implement mandatory cybersecurity measures for grid operators and regulatory agencies were published by the Central Electricity Regulatory Commission in January 2020 (Central Electricity Regulatory Commission Expert Group, 2020).
Japan	Japan released in 2017 (and has since revised) a cybersecurity policy for critical infrastructure protection, published by the National Center of Incident Readiness and Strategy for Cyber Security (NISC Japan, 2020). The policy also includes guidelines for establishing safety principles for ensuring information security of critical infrastructure and a risk assessment guide based on the concept of mission assurance in critical infrastructure.
United States	The Critical Infrastructure Protection Standards (NERC-CIP) entail a series of mandatory standards for all bulk electric utilities in the United States, which typically covers all assets at and above 100 kV (North American Electric Reliability Corporation, 2020). The NERC standards are developed with input from industry experts and submitted to the Federal Energy Regulatory Commission for approval; these are updated on a regular basis to keep up to date with evolutions in cybersecurity threats. Once approved by the commission, the standards become mandatory and are backed by possible fines of up to USD 1 million per day per violation.

The electricity sector is defined in many countries as critical national infrastructure. This means stakeholders from the national security arena play an increasingly important role in driving cybersecurity policy for the electricity system. National and strategic security strategy become closely intertwined with the electricity sector's cybersecurity policy, and they may result in special legislative powers for agencies outside the typical remit of energy policy. This can be seen in the close link that cybersecurity and critical infrastructure definitions have with the national security responsibilities of the defence ministries.

Contrary to system adequacy, operational security and climate resilience, which rely on system planning to cope with failures or external stimuli, cybersecurity is of a different nature. In cybersecurity the human factor, including the motivation and capability of hackers, drives the level of urgency. Further examples of cross-agency co-operation can be seen in Australia's recent national cybersecurity exercise for the electricity industry, bringing together participation of the Australian

Signals Directorate, the Australian Cyber Security Centre and the Australian Energy Market Operator. The topic of cybersecurity is also picked up at the international level under the umbrella of broader security activities, as illustrated in NATO's recent work assisting its members in education, exercises, information-sharing and response teams.

Policy makers are instrumental in building cybersecurity literacy across the electricity sector

Policies need to trigger appropriate action and eventually investment. However, the role of policy makers extends beyond setting target requirements. They have a critical role in fostering cybersecurity knowledge in the sector, overcoming barriers to cybersecurity literacy, preparing smaller regulators and utilities for this matter, and ensuring that a long-term sufficiently skilled workforce exists in the electricity sector.

Policy makers can help smaller utilities better address cybersecurity challenges by providing procurement guides and information to assist them in procuring the right types of products and services with appropriate specifications. They can also give guidance to regulatory authorities in case this responsibility is fragmented geographically. For example, the National Association of Regulatory Utility Commissioners in the United States produced a series of guidance materials including "procurement dictionaries" and "how-to" guides that help public utility commissions engage in meaningful dialogue when working with local municipal utilities. The NIST Cybersecurity Framework Smart Grid Profile is another example of providing guidance on cybersecurity, where power system owners and operators are offered a list of considerations relevant to new grid architectures (NIST, 2019).

The specific questions or requirements to be addressed will vary depending on the overarching cybersecurity approach. Nevertheless, building literacy across the sector is key to accelerating implementation in power systems. Cybersecurity literacy is naturally tied to the level and ability of the skilled professionals specialising in cybersecurity in the power sector. While measures such as those mentioned above are key to unlocking implementation in the short term, policy makers should also pay attention to strategies that foster the long-term development of a qualified workforce in this field.

Industry can have a proactive role in shaping cybersecurity policies

Public bodies are not the only ones driving the implementation of cybersecurity policies. Large manufacturers and electricity sector-service providers may wish to promote the introduction of industry standards to reduce their risk exposure and liabilities resulting from wider impacts to the system caused by cybersecurity vulnerabilities embedded in their products and services. By being proactive and remaining ahead of current thinking, they may also avoid very stringent policies being implemented.

Initiatives such as Siemens' partnerships with Alphabet's Chronicle and with TÜV SÜD, or Sunspec Alliance, which brings together over 100 solar and distributed storage participants, provide examples of how industry can drive new solutions and common practices. These allow its offering to be at the leading edge, create wider trust across customers and, of course, decrease its financial and reputational exposure in the event of a cybersecurity breach. Industry-driven standards are important in many markets. Regulators and policy makers need to be involved in this process in order to understand any potential vulnerabilities or deficiencies and enact complementary measures. Industry-driven initiatives need to be compatible with regulation and benefit from a robust ecosystem of testing and certification bodies.

The policy path will depend substantially on the underlying institutional structure of utilities. This relates to differences in ownership (public versus private) and the degree to which they are regulated, which has an impact on risk appetite, the time horizon for investment and the role of shareholders.

In cybersecurity policymaking, co-ordination across different institutional levels is essential to avoid any conflicts of interest and to ensure that there are no blind spots. For example, most existing hard regulation of cybersecurity targets the bulk power system, without covering the distribution level. As power systems evolve to increasingly decentralised, interconnected systems, cybersecurity regulation and initiatives will have to extend to cover the demand side. This not only involves distribution network-connected assets, but also an increasing number of intelligent devices, both consumer-facing equipment and automated controls. Policy makers can keep control over this extended risk surface by monitoring the maturity of the overall system more closely and possibly enforcing more certification. Industry stakeholders can be proactive in this area as it is in their own commercial interest, to the benefit of the wider system, and can limit the need for more stringent regulation.

Defining criticality is a first step in setting priorities for risk management in a sector that covers very large to very local stakeholders

To ensure that cybersecurity measures extend to all levels of the electricity system, it is important first to define what is critical and assess which measures make sense according to the level of criticality and available resources. The review of criticality is addressed in various ways.

The question of criticality can be posed at a highly operational level for a specific utility. The extensive NERC CIP provisions, for example, rely on a clear classification of all assets in the bulk electricity system (CIP-002 on BES Cyber System Categorization). The NIST CSF smart grid profile also clearly calls for resources directly involved in the distribution of electricity to be prioritised over normal business processes when it comes to cybersecurity actions.

The more general question that policy makers need to address is which operators are critical and most urgently need to prepare for emerging threats. NERC CIP – while providing detailed provisions – only focuses on bulk electricity system operators (transmission and large generators). The EU NIS Directive requires each member state to identify operators of essential services, which in practice always includes the transmission system operators and largest distribution system operators, but does little more to guide policy makers on which parts of the electricity system are more critical.

Within the national realm, countries may have more specific definitions. The Netherlands, for example, has three groups of vital infrastructure, with category A – its highest priority – defined by economic impacts above 5% of real national income or physical, social or cascading impact.

This categorisation should not only be seen through a historical lens or from the vantage point of classical power system engineering. A proper identification of critical infrastructure needs to take into account relevant threat scenarios that could manifest themselves today. In conventional system analysis, the most critical system elements are most likely the main transmission grid assets, the control centre and large plants. Emerging cyberthreats could come from mass control of distributed assets by compromising software updates or communication channels to do this. This warrants a renewed consideration of which assets or services are considered critical.

Not all parts of the system are equally critical or vulnerable, but all need to be clearly considered and cybersecurity regulation made accordingly

While the above definitions of critical infrastructure typically focus on the supply side, it is important to consider the demand side and how cyberattacks can target the energy supply of specific customer groups or induce a loss of load that could potentially destabilise the power system as a whole. Japan, for example, has taken steps to recognise the importance of IoT devices as a potential threat to the power system. Consumer-facing devices could potentially be deployed to disrupt the power system through cascading effects, which could be facilitated by the presence of factory security settings vulnerable to attack. To this end, Japan has introduced cybersecurity guidelines for energy resource-aggregation businesses. They are aimed at businesses that wish to participate in ancillary service markets and cover aspects such as vulnerability assessments, service continuity and countermeasure requirements.

A further example of targeted policymaking defined around criticality can be seen in Australia. Following the introduction of the Australian Energy Sector Cyber Security Framework, which facilitates a utility's self-evaluation of its cybersecurity posture, the Australian Energy Market Operator has revised its screening conditions to apply a light-touch approach to smaller or new stakeholders in the power system. Targeting small independent service providers or small retail companies, this is a step to recognise that smaller companies may not have the institutional or personnel resources to implement cybersecurity safeguards at the same level as large market players.

In the Australian case, the criteria for setting proportional requirements are based on the share of load served by the entity or on specific customer thresholds. This aims to find a balance between ensuring that all stakeholders in the power system implement at least a basic level of safeguards, while avoiding unnecessary costs or stifling competition.

The Australian light-touch regulation works in a context where there are multiple players acting in a single market, levelling the playing field. Similarly, the introduction of clear regulations with proportionate minimum standards can help in power systems where larger international players interact with local companies serving smaller jurisdictions, to avoid distortive competitive effects. This was one of the motivations for the Brazilian national grid operator's introduction of minimum cybersecurity requirements in the Brazilian power system. While international utilities present in the country have substantial experience in cybersecurity and

can easily introduce such measures, it was a major concern to ensure that local companies were also prepared, with a common set of tools to guarantee overall security of supply.

A recent expert group gave suggestions to the European Union on cybersecurity rules for the electricity sector that could be taken up in a network code (as an EU regulation). The recommendations of this group also highlighted the need for a proportional approach. The application of ISO/IEC 27001 was recommended for all grid operators. In addition, clear consideration needs to be given to which baseline requirements should apply to all operators, according to international standards. The suggestions include many examples of possible minimum security requirements and call attention to the belief that critical stakeholders are not only grid operators, but also system integrators and product vendors. Additional security requirements would apply to operators of essential services, as identified via the NIS Directive implementation.

This exercise shows how complex the question of defining criticality is. It is not just a question of who is too big to fail. It requires clear understanding of which threats manifest themselves and which baseline requirements can actually be applied to all stakeholders, including grid operators, generators, service providers, system integrators and product vendors. There is no case where this question has already been successfully addressed in full.

Policies must aim to ensure resilience at the grid edge and across the entire electricity system value chain

As electric vehicles, other behind-the-meter distributed energy resources and connected devices become more prevalent, the potential for cyberattacks to cause significant disruption to electricity systems could grow.

Protection systems in end-consumer devices are often beyond the typical scope of energy ministries or energy regulators. Their regulation may lie with other government bodies such as consumer protection authorities, public safety and civil protection bodies, energy efficiency departments and even special agencies for IT security, as is the case in Germany and France. In this sense, it is important for energy policy makers to engage across various government levels as well as with manufacturer associations and standards bodies to understand the potential risks to the system and how best to address these efficiently and effectively.

As companies become increasingly interdependent for industrial and service processes, it is important to build supply chain resilience. Policy makers should

ensure that there are platforms for industries and businesses to validate, communicate and improve on any potential cyber-related vulnerabilities in the supply chain. A further important consideration for policy makers is whether this is steered via transparency and trust, or if this is enforced by certification, incentives and penalties.

Clear institutional responsibilities are essential

Establishing a robust cybersecurity strategy for electricity systems requires a broader scope beyond the typical sphere of the electricity industry, to include manufacturing, telecommunications and standardisation stakeholders.

The first step to establishing a comprehensive strategy is identifying the whole spectrum of stakeholders that need to be involved. This includes the typical stakeholders such as the energy regulator, bulk power system-service providers, manufacturers and certifying bodies.

The next step is to establish a clear framework of obligations and responsibilities through a collaborative process. For example, is the transmission system operator responsible for cybersecurity as part of its continuity of supply mandate? Is the energy regulator responsible for oversight and incentive setting? Who is in charge of developing and adopting standards, as well certifying compliance? What are the liabilities for manufacturers or service providers at all levels? How does all this play out in context of an internationally interconnected system?

How these obligations are enforced (e.g. instrument type, voluntary or mandatory) will depend mostly on whether a policy maker has greater confidence in processes that can be audited, or in industry properly following objectives and guidance.

Clear monitoring, measurement and enforcement mechanisms are particularly important to ensure cybersecurity along the whole value chain. Regardless of the chosen approach (e.g. self-regulation with standardisation bodies vs monitoring and compliance), cyber resilience should not be seen in isolation and care is needed on how it affects digitalisation of the sector and its associated benefits. Furthermore, cyber resilience policies need to focus not only on past incidents and present systems, but keep a clear eye on unfolding trends and emerging risks, most notably related to a more decentralised electricity system.

Building on this, establishing frameworks for information sharing and improving security is the cornerstone of robust cybersecurity. For such systems to be efficient, it is important that regulators set the right reporting obligations, while

assuaging concerns over competition and business privacy. Moreover, it is essential that any experience and feedback regarding vulnerabilities or new threats be reflected in updated regulations and standards.

The success of effective policies depends on various criteria – there is no simple or single best solution

Many jurisdictions have taken positive steps in developing effective policies and approaches. The effectiveness of policies will depend on context-specific criteria and considerations. Policy makers will need to consider a range of criteria when developing policy approaches for cyber resilience, such as coherence, scope, resources and ease of implementation, among others.

Table 8. Key criteria for developing cyber resilience policy approaches in the electricity sector

Criterion	Description
Coherence	Ensure cybersecurity policies are consistent with the overall regulatory framework and policy approach for the energy sector.
Scope	Develop cybersecurity policies that go beyond high-level strategies and give a clear energy sector-specific plan. This plan needs to articulate the particularities of the electricity system and fully address purpose, scope and methodology for application. Sector interdependencies (with gas, telecoms, etc.) need to be taken into account where relevant.
Proportionality	Adopt policies that identify high-risk areas and are proportional depending on size, capability and criticality of an organisation. A key example is how grid-edge aspects need to be and can be covered.
Assessment	Make sure an assessment framework is in place to identify particular national and regional risks to critical assets and operations in the electricity sector, based on emerging threat scenarios.
Measurable targets	Outline goals and activities for addressing cybersecurity risks facing the electricity system. Ensure progress can be monitored going beyond pure output performance, but also looking at process implementation. This is relevant for both regulated and non-regulated entities and needs to be prioritised based on criticality of the activity. Measuring progress is not a goal in itself, but can support prioritisation to meet specific goals.
Resources	Assess and address what a cybersecurity strategy will cost and what types of resources and investments will be needed. Take into account how regulated and non-regulated stakeholders are incentivised to make appropriate investments. Set appropriate incentives in price control reviews and where possible set transparent benchmark costs or cost criteria.

Criterion	Description
Roles and responsibilities	Identify all key stakeholders throughout the power system; identify the mechanisms for ensuring co-ordination and the organisations/bodies responsible for achieving goals, objectives and activities of cybersecurity policy. This also implies looking beyond the electricity sector and possibly aligning with responsibilities in national security
Ease of implementation	Evaluate challenges to implementation across stakeholders of various sizes and criticality.
Adaptability	Maintain a process, including input from all stakeholders, for assessing and revising regulations and standards to ensure these adapt to the evolving understanding of cyberthreats.
Information sharing	Establish and maintain information-sharing relationships and communications paths for collecting and disseminating intelligence on cybersecurity-related risks and vulnerabilities, response activities and lessons learned. Incentivise information sharing as much as possible and avoid conflicts with data confidentiality or perceptions of liability risks.

Sources: IEA analysis based on US General Accounting Office (2004) and US Government Accountability Office (2019).

Annex

Annex A: Types of cybersecurity measures

Table 9. National Institute of Standards and Technology categorisation of cybersecurity measures applied by utilities, including data confidentiality

Measure	Description
Access control	Ensure systems are only accessed by appropriate personnel. Monitor for inappropriate access attempts. This is done by implementing access control policies and procedures, account management and having control over information flow.
Awareness and training	Design training programmes based on roles and responsibilities to change the way personnel access programs and applications with the aim of increasing incident prevention.
Audit and accountability	Conduct periodic audits to examine records and activities to determine the adequacy of the information system security requirements, ensure compliance with policies and detect breaches in security services.
Security assessment and authorisation	Monitor and review performance of information systems via compliance audits and incident investigations to determine the effectiveness of the security programme.
Configuration management	Implement a change management process to ensure only approved and tested changes are made to the information system configuration, including vendor updates and patches.
Continuity of operations	Provide policies, roles and responsibilities, training, testing and recovery responses to have the capability to continue or resume operations in the event of disruption.
Identification and authentication	Have in place authentication policies and procedures for users and devices with a defined management authority.
Information and document management	Put record retention and document management systems in place to ensure all sensitive information is protected, with appropriate versions retained.
Incident response	Put policies and procedures in place for incident response monitoring, handling, reporting, testing, training and recovery of the information systems.
Information system development and maintenance	Design the security measures specifically tailored for the information system in place and sustain it through effective routine and preventive maintenance guided by policies and procedures.
Media protection	Limit access to media, such as memory sticks and printed reports, to authorised users. Also, establish protection measures for distribution, handling, storage, transport and sanitisation.

Measure	Description
Physical and environmental security	Set in place security practices that encompass protection of physical assets from damage, misuse, theft or environmental threats, by addressing access control, physical boundaries and surveillance.
Planning	Ensure planning policies and procedures consider security to prevent interruptions, plan for continuity of operations to maintain information systems during and after an interruption and plan to identify mitigation strategies. Also clarify the rules of behaviour that describe the responsibility and expected behaviour with regard to information system usage.
Security programme management	Implement security procedures that define how to implement and manage a security programme, taking establishment of responsibilities and accountability into consideration.
Personnel security	Consider within the security programme the roles and responsibilities during all phases of staff employment, including termination where a confidentiality or non-disclosure agreement could be put in place.
Risk management and assessment	Continuously identify and classify risks by developing risk assessment policies and procedures with clear objectives, roles and responsibilities, risk management plan and clear risk assessment update scheduling.
Information system and services acquisition	Have a policy in place for reviewing the contracting and acquisition of system components, software, firmware, and services from employees and contractors with the aim of reducing the introduction of vulnerabilities.
Information system and communication protection	Protect the communication links between information system components from cyber intrusions by implementing techniques such as security function isolation, partitioning between data acquisition and management functionality, cryptographic key establishment and message authentication.
Information system and information integrity	Establish policy and procedure for identifying, reporting and correcting information system flaws or detecting malicious code that could compromise information integrity, including sensitive data that could be modified or deleted in an unauthorised or undetected manner.

Source: NIST (2014).

Annex B: Electricity-related cyber incidents since 2015

Table 10. Selection of electricity-related cyber incidents since 2015, based on public information

Incident	Description (target, mechanism of attack, attacker and impacts)	Sources
Supply chain cyberattack on IT service provider December 2020	Attackers compromised business software updates to distribute malware, infecting up to 18 000 organisations. The compromised software was reportedly widely used by US government agencies and electric utilities. Impacts stemming from the attacks are still being determined.	FireEye, 2020b; Sobczak, 2020
Ransomware attack on market operator in Great Britain May 2020	Attackers compromised the internal IT system of the organisation responsible for Great Britain's power market balancing and settlement mechanisms. Though the system has close ties with that of the transmission system operator, no further systems were reportedly infected.	Ambrose, 2020
Ransomware attack on Canadian utility April 2020	Attackers compromised the website and business systems of a Canadian utility. The utility's email system was shut down, but electricity systems were not impacted.	Strong, 2020
Ransomware attack on Portuguese utility April 2020	Attackers used the Ragnar Locker ransomware to breach the corporate network of a major Portuguese utility and steal over 10 terabytes of company data. The utility reported no impacts on power supply or other critical infrastructure.	Lempriere, 2020
Intrusion on SharePoint environment of European association of transmission system operators March 2020	The platform used by European transmission system operators to exchange information was infiltrated by attackers. This platform is commonly used business software and is not directly linked to system operation tools of individual system operators. No further impact was reported.	ENTSO-E, 2020
Ransomware attack on US equipment vendor March 2020	Attackers used ransomware to steal information from an electric equipment vendor in the United States. The stolen data included schematics and drawings from one of the vendor's customers, a large electric utility. The utility stated that the data was "not confidential information related to our critical or customer operations".	Vasquez, 2020; Walton, 2020a

Incident	Description (target, mechanism of attack, attacker and impacts)	Sources
Spearphishing campaign on smaller US utilities April to August 2019	Seventeen smaller US utilities, many located near other critical infrastructure, were targeted by a spearphishing campaign over several months. The phishing emails targeted employees with malicious attachments attempting to spread the LookBack malware, which has a wide range of capabilities including stealing data files. None of the attacks were successful, but some utilities were unaware of the attempt.	Doffman, 2019; Proofpoint, 2019; Smith and Barry, 2019; Walton, 2019
Denial-of-service attack on western US utility March 2019	A denial-of-service attack disabled security devices in a Utah-based utility, resulting in a temporary loss of visibility to certain parts of the utility's SCADA system. The attacker exploited a known firewall vulnerability at one of the utility's vendors, allowing an unauthenticated attacker to cause unexpected reboots of devices. These unexpected reboots caused brief communications outages between field devices and the control centre, but did not result in blackouts or other effects on power generation.	Kaspersky ICS CERT, 2019; Mai, 2019; Sobczak, 2019a, 2019b; US Department of Energy, 2019
Global WannaCry ransomware attack May 2017	The WannaCry ransomware attack affected over 100 000 organisations in 150 countries, taking advantage of an access point in Microsoft operating systems for which some users had failed to install the secure update. Several electric utilities were attacked, including Iberdrola and the West Bengal State Electricity Distribution Co. Ltd.	Norton Rose Fulbright, 2017; Sengupta, 2017
Attack on the Irish transmission system operator April 2017	Hackers gained access to an internet router used by the Irish transmission system operator, giving them access to all internal communications passing through the site for almost seven hours. The attackers copied all the firmware and files on the compromised routers, which included information on commercial customers, but there was no interruption of operations.	Coffman Smith, 2017; McMahon, 2017
Spearphishing attack on US electricity companies September 2017	Attackers conducted a spearphishing campaign targeting US electricity companies. The attack appeared to be early-stage reconnaissance. The attack was detected and stopped, and no operational impact on facilities or systems was reported.	FireEye, 2017; Mitchel & Dilanian, 2017
Malware attack on Ukrainian electric utility December 2016	Attackers used the Industroyer malware (also known as Crash Override) to view, block, control and destroy grid control equipment such as circuit breakers. Its design suggests expert knowledge of several standardised industrial communication protocols widely used to control infrastructure – not only electricity grids – throughout Europe, Asia and the	Cherepanov & Lipovsky, 2017; Greenberg, 2017; Lee, 2017

Incident	Description (target, mechanism of attack, attacker and impacts)	Sources
	Middle East. This was an example of a cyber intrusion into the OT domain of critical infrastructure. The attack resulted in a power outage in a section of Kiev (roughly one-fifth of capacity, or 200 MW) for about one hour.	
Viruses and malware in German nuclear power plant April 2016	Computer systems in a German nuclear power plant were infected with computer viruses designed to steal files and spread through electricity networks by copying itself onto removable data drives. Malware was also found on removable data drives in computers maintained separately from the plant's operating systems. Because the computers were isolated from the internet, they posed no threat to the operations of the facility.	Steitz & Auchard, 2016
Ransomware attack on a municipal utility in the United States April 2016	A ransomware attack shut down the accounting and email systems of a municipal utility in Michigan after an employee unknowingly opened an email with an infected attachment. The attack did not affect electric and water distribution, but forced the shutdown of telephone lines, including a customer service line.	Palmer, 2016
Attack on the western Ukraine power grid 2015	This 2015 attack was the first confirmed cyberattack specifically against an electricity network with impact on system availability. Attackers accessed and manually switched off substations (via SCADA and firmware) with a combination of malware, personnel credentials obtained by means of email phishing, and denial-of-service attacks. Investigators concluded that a large well co-ordinated team had prepared the attack over several months. 30 substations were taken offline, resulting in 225 000 people losing power as a result of the attack.	E-ISAC, 2016; Zetter, 2016

Annex C: Potential cyberattack scenarios

Table 11. Potential cyberattack scenarios in the electricity system

Scenario	Description	Impacts
Virus infiltrates industrial control system through USB flash drives	The attacker infiltrates the industrial control system with a virus, and threatens to disrupt the process and take control of the infected equipment.	Low impact with loss of productivity and repair of devices and systems.
Phishing attack to gain remote access to a human-machine interface	The attacker first infiltrates the general office IT system of the network operator, then obtains access to control systems of the attacked organisation. This attack does not address individual power system equipment, but allows access to all control systems of the organisation.	Direct impact of successful phishing is low, but can be widespread and has a fair chance of success. Depending on intrusion point and resulting access rights, next stage attacks may be possible.
Compromised control room SCADA	The attacker exploits a SCADA app on the smartphone of a control room engineer or uses any other entry point that is successfully attacked to gain privileged access to a system operator or generator SCADA. By establishing remote access to the control room, the attacker could manipulate the system and launch secondary attacks against generation units or substations.	Potentially drastic consequences depending on the degree of secondary attacks, ranging from disruption of service to damage to facilities.
Compromised OT asset firmware update or remote maintenance communication link	The communication channel between vendor and an asset in the field used for firmware updates is compromised. Altering firmware updates can be used to eventually disrupt the local network or manipulate operations.	Low to moderate impact as a single asset is attacked. It could be an entry point for further attack on higher-level control systems. See Angle et al. (2019) for a detailed case study on variable frequency drives.
Compromised equipment through supply chain vulnerabilities	Equipment and components could be compromised during development, production, shipping and maintenance prior to final installation. For example, malicious firmware could be introduced during production that introduces a backdoor to change relay settings and set points.	Compromised equipment could cause operational errors that could eventually result in catastrophic impacts, given the low likelihood of detection until the disruption event.

Scenario	Description	Impacts
Forced entry via intrusion detection or prevention systems	The system designed to detect and prevent intrusion is an interesting point of attack. It often has access rights to many assets and operates at a high privilege level. Many legacy systems depend on a physical security perimeter protected by such a system, which is essentially a digital tool with potential vulnerabilities.	Potential for high impact as it becomes an entry point to many OT assets within the utility.
Malicious firmware update of smart meters triggering mass disconnection	The attacker installs compromised firmware on a target smart meter in each neighbourhood. Many smart meters in an area operate in a hierarchical master/slave set-up. The compromised smart meters then become masters for a smart meter-based botnet, and transmit the malicious firmware to other smart meters. The malicious firmware propagates throughout the neighbourhood and uses them to achieve a mass remote disconnection scheduled at the same time.	Utility loses sensor and billing functionality, compromising market participation but also potentially impacting at transmission level if this triggers a massive simultaneous disconnection of load.
Manipulation of a large number of grid edge devices that may lack robust cybersecurity protections	There is a growing number of distributed energy resources (e.g. distributed generation, behind-the-meter storage, electric vehicles and chargers), as well as high-wattage connected devices (e.g. air conditioners, heat pumps). These devices are expected to have external interfaces for firmware updates, remote accessibility by the user, and possible accessibility by aggregators or other third parties. Scenarios described above based on phishing, firmware update channels, supply chain issues or SCADA attacks at operators can potentially be used to attack these assets and trigger mass tripping.	Potential for high impact on system stability in case of successful mass attack and disconnection. Detailed examples are discussed in Acharya et al., 2020; Angle et al., 2019; Soltan et al., 2018; World Economic Forum, 2019.

Source: IEA analysis based on Fischer et al. (2018).

References

Accenture (2018). Forging Stronger Links: NERC CIP Supply Chain Cybersecurity. https://www.accenture.com/_acnmedia/pdf-88/accenture-nerccip-suppychain.pdf.

Acharya, S., Dvorkin, Y., & Karri, R. (2020). Public Plug-in Electric Vehicles + Grid Data: Is a New Cyberattack Vector Viable? IEEE Transactions on Smart Grid, 1–1. https://doi.org/10.1109/tsg.2020.2994177.

AEMO (2018). 2018 Summary Report into the cyber security preparedness of the National and WA Wholesale Electricity Markets. https://www.aemo.com.au/-/media/Files/Cyber-Security/2018/AEMO-2018-AESCSF-Report.pdf.

AEMO (2019a). 2019 AESCSF Lite Assessment. https://aemo.com.au/-/media/files/cyber-security/2019/aescsf-lite-self-assessment-overview-2019-v1.pdf?la=en&hash=3496EFFBEFC112195DCDAA2D62A3E9F4.

AEMO (2019b). AESCSF framework and resources. https://aemo.com.au/initiatives/major-programs/cyber-security/aescsf-framework-and-resources.

AEMO (2020). Cyber Security. https://aemo.com.au/en/initiatives/major-programs/cyber-security.

Ambrose, J. (2020). Lights stay on despite cyber-attack on UK's electricity system . The Guardian. https://www.theguardian.com/business/2020/may/14/lights-stay-on-despite-cyber-attack-on-uks-electricity-system.

American Public Power Association (2019). Cyber Incident Response Playbook. https://www.publicpower.org/system/files/documents/Public-Power-Cyber-Incident-Response-Playbook.pdf.

Angle, M. G., Madnick, S., Kirtley, J. L., & Khan, S. (2019). Identifying and Anticipating Cyberattacks That Could Cause Physical Damage to Industrial Control Systems. IEEE Power and Energy Technology Systems Journal, 6(4), 172–182. https://doi.org/10.1109/jpets.2019.2923970.

APPrO (2018). Ontario's Cyber Security Framework is now in force. https://magazine.appro.org/news/ontario-news/5545-1529540280-ontario's-cyber-security-framework-is-now-in-force.html.

Arampatzis, A. (2020). So You Want to Achieve NERC CIP-013-1 Compliance... Tripwire. https://www.tripwire.com/state-of-security/ics-security/achieve-nerc-cip-013-1-compliance/.

Bailey, T., Kolo, B., Rajagopalan, K., & Ware, D. (2018). Insider threat: The human element of cyberrisk. McKinsey. https://www.mckinsey.com/business-functions/risk/our-insights/insider-threat-the-human-element-of-cyberrisk.

Bain & Company (2018). Cybersecurity Is the Key to Unlocking Demand in the Internet of Things. https://www.bain.com/insights/cybersecurity-is-the-key-to-unlocking-demand-in-the-internet-of-things/.

BloombergNEF (2018). Smart Meter Market Size. https://www.bnef.com/core/interactive-datasets/2d5d59acd900001c.

Business Wire (2020). Navigant Research Report Finds Global Annual Market for Energy IT and Cybersecurity for Software and Services Is Expected to Reach $32 Billion by 2028. https://www.businesswire.com/news/home/20200211005108/en/Navigant-Research-Report-Finds-Global-Annual-Market.

Buurma, C., & Sebenius, A. (2020). Ransomware Shuts Gas Compressor for Days in Latest Attack - Bloomberg. Bloomberg. https://www.bloomberg.com/news/articles/2020-02-18/ransomware-shuts-u-s-gas-compressor-for-2-days-in-latest-attack.

Canadian Centre for Cyber Security (2020). Cyber Threat Bulletin: The Cyber Threat to Canada's Electricity Sector - Canadian Centre for Cyber Security. https://cyber.gc.ca/en/guidance/cyber-threat-bulletin-cyber-threat-canadas-electricity-sector.

Central Electricity Regulatory Commission Expert Group (2020). Report of the Expert Group: Review of Indian Electricity Grid Code. http://www.cercind.gov.in/2020/reports/Final Report dated 14.1.2020.pdf.

CESER (2018). From Innovation To Practice□: Systems To Survive. July. https://www.energy.gov/sites/prod/files/2018/09/f55/CEDS From Innovation to Practice FINAL_0.pdf.

Cherepanov, A., & Lipovsky, R. (2017). Industroyer: Biggest threat to industrial control systems since Stuxnet. WeLiveSecurity. https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/.

CIPedia (2020). National Cyber Security Strategy. https://websites.fraunhofer.de/CIPedia/index.php/National_Cyber_Security_Strategy.

Cisco (2020). Cyber Attack - What Are Common Cyberthreats? https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html.

Coffman Smith, A. (2017). "State-sponsored" hackers breach Irish power grid, fears linger over hidden code. S&P Global Market Intelligence. https://www.spglobal.com/marketintelligence/en/news-insights/trending/ipmw9xubup18kznj0nyroa2.

Costantini, L., & Acho, M. (2019). NARUC Cybersecurity Manual. https://pubs.naruc.org/pub/7932B897-CF16-0368-BF79-EDC5C5A375EE.

CSIS (2020). Significant Cyber Incidents. https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents.

DiChristopher, T. (2020, February 19). Cyberattack uncovers shortfalls in natural gas pipeline security. S&P Global Market Intelligence. https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/cyberattack-uncovers-shortfalls-in-natural-gas-pipeline-security-57179953.

Doffman, Z. (2019). Chinese State Hackers Suspected Of Malicious Cyber Attack On U.S. Utilities. Forbes. https://www.forbes.com/sites/zakdoffman/2019/08/03/chinese-state-hackers-suspected-of-malicious-cyber-attack-on-u-s-utilities/#d8873c6758cc.

Dragos (2019). Bridging the IT and OT Cybersecurity Divide. https://www.dragos.com/resource/bridging-the-it-and-ot-cybersecurity-divide/.

E-ISAC (2016). Analysis of the Cyber Attack on the Ukrainian Power Grid Defense Use Case. https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf.

E-ISAC (2019a). E-ISAC Brochure 2019. https://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC Brochure_March 2019.pdf.

E-ISAC (2019b). E-ISAC End of Year Report. https://www.wecc.org/Administrative/TLP Green E-ISAC End of Year Report.pdf.

Edison Electric Institute (2017). More Than 6,000 Electric Company and Government Officials Tested Energy Grid Security During GridEx IV Exercise. https://www.eei.org/Pages/pr.aspx?p=86-More-Than--Electric-Company-and-Government-Officials-Tested-Energy-Grid-Security-During-GridEx-IV-Exercise---.

ENISA (2017). Information Sharing and Analysis Centres (ISACs) Cooperative models. https://doi.org/10.2824/549292.

ENISA (2020). EU cybersecurity certification framework. https://www.enisa.europa.eu/topics/standards/certification.

ENTSO-E (2020). ENTSO-E has recently found evidence of a successful cyber intrusion into its office network. https://www.entsoe.eu/news/2020/03/09/entso-e-has-recently-found-evidence-of-a-successful-cyber-intrusion-into-its-office-network/.

EPRI (2015). Analysis of Selected Electric Sector High Risk Failure Scenarios (Version 2.0). https://smartgrid.epri.com/doc/NESCOR Detailed Failure Scenarios v2.pdf.

European Commission (2019). €10 million EU funding available for projects stepping up EU's cybersecurity capabilities and cross border cooperation. https://ec.europa.eu/digital-single-market/en/news/eu10-million-eu-funding-available-projects-stepping-eus-cybersecurity-capabilities-and-cross.

European Commission (2020a). Critical infrastructure and cybersecurity. https://ec.europa.eu/energy/topics/energy-security/critical-infrastructure-and-cybersecurity_en?redir=1.

European Commission (2020b). 21 new EU funded projects to assist EU Member States in building up their cybersecurity capabilities and cooperating. Shaping Europe's Digital Future. https://ec.europa.eu/digital-single-market/en/news/21-new-eu-funded-projects-assist-eu-member-states-building-their-cybersecurity-capabilities-and.

European Court of Auditors (2019). Challenges to effective EU cybersecurity policy. https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EN.pdf.

EY (2018). Is cybersecurity about more than protection? EY Global Information Security Survey 2018–19. https://www.ey.com/Publication/vwLUAssets/ey-global-information-security-survey-2018-19/$FILE/ey-global-information-security-survey-2018-19.pdf.

FireEye (2017). North Korean Actors Spear Phish U.S. Electric Companies. https://www.fireeye.com/blog/threat-research/2017/10/north-korean-actors-spear-phish-us-electric-companies.html.

FireEye (2020a). Navigating the MAZE: Tactics, Techniques and Procedures Associated With MAZE Ransomware Incidents. https://www.fireeye.com/blog/threat-research/2020/05/tactics-techniques-procedures-associated-with-maze-ransomware-incidents.html.

FireEye (2020b). Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor. https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html.

Fischer, L., Uslar, M., Morrill, D., Döring, M., & Haesen, E. (2018). Study on the Evaluation of Risks of Cyber-Incidents and on Costs of Preventing Cyber-Incidents in the Energy Sector. https://ec.europa.eu/energy/sites/ener/files/evaluation_of_risks_of_cyber-incidents_and_on_costs_of_preventing_cyber-incidents_in_the_energy_sector.pdf.

Fortress Information Security (2020). NERC CIP-013 Deadline Delay: 5 Facts You Need To Know. https://fortressinfosec.com/nerc-cip-013-delay/.

Furneaux, A. (2020). CIP-013 Implementation: Know Supplier Posture & Accelerate Compliance. CyberSaint Security. https://www.cybersaint.io/blog/cip-013-implementation-guidance-know-supplier-posture-accelerate-compliance.

Gahran, A. (2020). State of the Electric Utility 2020. https://www.utilitydive.com/news/state-of-the-electric-utility-2020/572374/.

Gartner (2017). Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016. https://www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016.

Gartner (2018). Gartner Forecasts Worldwide Information Security Spending to Exceed $124 Billion in 2019. https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019.

Gartner (2020a). Gartner Says 5.8 Billion Enterprise and Automotive IoT Endpoints Will Be in Use in 2020. https://www.gartner.com/en/newsroom/press-releases/2019-08-29-gartner-says-5-8-billion-enterprise-and-automotive-io.

Gartner (2020b). Information Technology Glossary. https://www.gartner.com/en/information-technology/glossary.

Graham, A. (2018). Become cyber secure with NIST, ISO 27001, and ISO 22301. IT Governance Publishing Blog. https://www.itgovernancepublishing.co.uk/blog/become-cyber-secure-with-nist-iso-27001-and-iso-22301.

Greenberg, A. (2017). Crash Override Malware Took Down Ukraine's Power Grid Last December. Wired. https://www.wired.com/story/crash-override-malware/.

GSMA (2020). The Mobile Economy 2020. https://www.gsma.com/mobileeconomy/.

Guri, M. (2018). Air-Gap Research Page. https://cyber.bgu.ac.il/air-gap/.

IDC (2019a). The Growth in Connected IoT Devices Is Expected to Generate 79.4ZB of Data in 2025, According to a New IDC Forecast. https://www.idc.com/getdoc.jsp?containerId=prUS45213219.

IDC (2019b). Worldwide Security Spending Guide. https://www.idc.com/getdoc.jsp?containerId=IDC_P33461.

IEA (2017). Digitalization & Energy. https://www.iea.org/reports/digitalisation-and-energy.

IEA (2020). World Energy Investment 2020. https://www.iea.org/reports/world-energy-investment-2020.

India Smart Grid Forum (2017). Smart Grid Handbook for Regulators and Policy Makers. https://indiasmartgrid.org/reports/Smart Grid Handbook for Regulators and Policy Makers_20Dec.pdf.

Industrial Internet Consortium (2018). IoT Security Maturity Model: Description and Intended Use. https://www.iiconsortium.org/pdf/SMM_Description_and_Intended_Use_2018-04-09.pdf.

International Society of Automation (2018). Standards: New ISA/IEC 62443 standard specifies security capabilities for control system components. https://www.isa.org/intech/201810standards/.

IRENA (2019). Artificial Intelligence and Big Data. https://www.irena.org/-/media/Files/IRENA/Agency/Publication/2019/Sep/IRENA_AI_Big_Data_2019.pdf?la=en&hash=9A003F48B639B810237FEEAF61D47C74F8D8F07F.

ISO/IEC (2018). ISO/IEC 27005:2018 Information technology — Security techniques — Information security risk management. 2018. https://www.iso.org/standard/75281.html.

ISO (2017). Information technology — Security techniques — Information security controls for the energy utility industry. ISO/IEC 27019:2017. https://www.iso.org/obp/ui/#iso:std:iso-iec:27019:ed-1:v2:en.

ITU (2019). Global Cybersecurity Index 2018. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf.

Kaspersky (2019). Quiet please: two-thirds of industrial organizations don't report cybersecurity incidents to regulators. https://www.kaspersky.com/about/press-releases/2019_two-thirds-of-industrial-organizations-dont-report-cybersecurity-incidents-to-regulators.

Kaspersky ICS CERT. (2019). Threat landscape for industrial automation systems, 2019 H1. https://ics-cert.kaspersky.com/media/H1_2019_kaspersky_ICS_REPORT_EN.pdf.

Koepke, P. (2017). Cybersecurity Information Sharing Incentives and Barriers-Massachusetts Institute of Technology. http://web.mit.edu/smadnick/www/wp/2017-13.pdf.

Krauss, C. (2018). Cyberattack Shows Vulnerability of Gas Pipeline Network. The New York Times. https://www.nytimes.com/2018/04/04/business/energy-environment/pipeline-cyberattack.html.

Lee, R. M. (2017). CRASHOVERRIDE: Analyzing the Malware that Attacks Power Grids. Dragos. https://dragos.com/resource/crashoverride-analyzing-the-malware-that-attacks-power-grids/.

Lempriere, M. (2020). Wind giant EDP hit by Ragnar Locker ransomware attack. Current. https://www.current-news.co.uk/news/edp-hit-by-ragnar-locker-ransomware-attack.

Lloyd's & University of Cambridge Centre for Risk Studies (2015). Business Blackout: The insurance implications of a cyber attack on the US power grid. https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/crs-lloyds-business-blackout-scenario.pdf.

Madnick, S. (2020). How to Safeguard Against Cyberattacks on Utilities. Harvard Business Review. https://hbr.org/2020/01/how-to-safeguard-against-cyberattacks-on-utilities.

Mai, H. (2019). NERC finds first remote hacker interference on US grid from cyberattack. Utility Dive. https://www.utilitydive.com/news/nerc-finds-first-remote-hacker-interference-on-us-grid-from-cyberattack/562478/.

Malik, N. S. (2018). Energy Companies Aren't Doing Much to Defend Against Soaring Cyber Attacks. Bloomberg. https://www.bloomberg.com/news/articles/2018-04-27/-cyber-blindspot-threatens-energy-companies-spending-too-little.

McCallum, J. C. (2020). Disk Drive Prices 1955+. https://jcmit.net/diskprice.htm.

McKinsey & Company (2019). Critical infrastructure companies and the global cybersecurity threat. https://www.mckinsey.com/business-functions/risk/our-insights/critical-infrastructure-companies-and-the-global-cybersecurity-threat.

McMahon, C. (2017). "State-sponsored" hackers targeted EirGrid electricity network in "devious attack." Independent. https://www.independent.ie/irish-news/state-sponsored-hackers-targeted-eirgrid-electricity-network-in-devious-attack-36005921.html.

Michigan Public Service Commission (2019). Statewide Energy Assessment-Initial Report Michigan Statewide Energy Assessment Initial Report. https://www.michigan.gov/documents/mpsc/Sea_Initial_Report_with_Appendices_070119_659452_7.pdf.

Microsoft (2018). 2019 Manufacturing Trends Report. https://info.microsoft.com/rs/157-GQE-382/images/EN-US-CNTNT-Report-2019-Manufacturing-Trends.pdf.

Ministry of Power, India (2019). Annual Report 2018-19. https://powermin.nic.in/sites/default/files/uploads/MOP_Annual_Report_Eng_2018-19.pdf.

MISP (2020). MISP Threat Sharing. https://www.misp-project.org/index.html.

Mitchel, A., & Dilanian, K. (2017). Experts: North Korea Targeted U.S. Electric Power Companies. NBC News. https://www.nbcnews.com/news/north-korea/experts-north-korea-targeted-u-s-electric-power-companies-n808996.

NARUC (2019). Cybersecurity Preparedness Evaluation Tool. https://pubs.naruc.org/pub/3B93F1D2-BF62-E6BB-5107-E1A030CF09A0.

National Cyber Security Centre (2018). Risk management guidance. https://www.ncsc.gov.uk/collection/risk-management-collection.

Navigant Research (2019). Energy IT and Cybersecurity Overview. https://www.navigantresearch.com/reports/energy-it-and-cybersecurity-overview.

Nielsen Norman Group (2019). Nielsen's Law of Internet Bandwidth. https://www.nngroup.com/articles/law-of-bandwidth/.

Nikolewski, R. (2019). California operator of electricity grid fends off millions of cyberattacks each month. The San Diego Union-Tribune. https://www.sandiegouniontribune.com/business/energy-green/story/2019-06-12/california-grid-operator-a-target-for-millions-of.

NISC Japan (2020). National center of Incident readiness and Strategy for Cybersecurity. https://www.nisc.go.jp/eng/.

NIST (2014). Guidelines for Smart Grid Cybersecurity NISTIR 7628. https://doi.org/10.6028/NIST.IR.7628r1.

NIST (2015). Utility Sector Best Practices for Cyber Security Supply Chain Risk Management. https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/case_studies/USRP_NIST_Utility_093015.pdf.

NIST (2019). Cybersecurity Framework Smart Grid Profile - NIST Technical Notes 2051. https://doi.org/10.6028/NIST.TN.2051.

NIST (2020a). Framework for Improving Critical Infrastructure Cybersecurity. https://www.nist.gov/cyberframework.

NIST (2020b). Glossary. Computer Security Resource Center. https://csrc.nist.gov/glossary/.

North American Electric Reliability Corporation (2020). CIP Standards. https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx.

Norton Rose Fulbright (2017). WannaCry Ransomware Attack Summary. Data Protection Report. https://www.dataprotectionreport.com/2017/05/wannacry-ransomware-attack-summary/.

O'Flaherty, K. (2020). U.S. Government Issues Powerful Cyberattack Warning As Gas Pipeline Forced Into Two Day Shut Down. Forbes. https://www.forbes.com/sites/kateoflahertyuk/2020/02/19/us-government-issues-powerful-cyberattack-warning-as-gas-pipeline-forced-into-two-day-shut-down/#7bbb21815a95.

Ofgem (2020). RIIO-2 Cyber Resilience Guidelines. https://www.ofgem.gov.uk/publications-and-updates/riio-2-cyber-resilience-guidelines.

Ontario Energy Board (2020). Electricity Reporting & Record Keeping Requirements. https://www.oeb.ca/sites/default/files/RRR-Electricity-20200127.pdf.

Oughton, E. J., Ralph, D., Pant, R., Leverett, E., Copic, J., Thacker, S., Dada, R., Ruffle, S., Tuveson, M., & Hall, J. W. (2019). Stochastic Counterfactual Risk Analysis for the Vulnerability Assessment of Cyber-Physical Attacks on Electricity Distribution Infrastructure Networks. Risk Analysis, 39(9), 2012–2031. https://doi.org/10.1111/risa.13291.

Palmer, K. (2016). Lansing utility paid $25,000 ransom after cyberattack. Detroit Free Press. https://eu.freep.com/story/news/local/michigan/2016/11/09/bwl-paid-ransom-cyberattack/93576218/.

Ponemon Institute & Accenture (2019). The Cost of Cybercrime. https://www.accenture.com/_acnmedia/pdf-96/accenture-2019-cost-of-cybercrime-study-final.pdf.

Ponemon Institute & Siemens (2019). Caught in the Crosshairs: Are utilities keeping up with the industrial cyber threat? https://assets.new.siemens.com/siemens/assets/api/uuid:35089d45-e1c2-4b8b-b4e9-7ce8cae81eaa/version:1572434569/siemens-cybersecurity.pdf.

Proofpoint (2019). LookBack Forges Ahead: Continued Targeting of the United States' Utilities Sector Reveals Additional Adversary TTPs. https://www.proofpoint.com/us/threat-insight/post/lookback-forges-ahead-continued-targeting-united-states-utilities-sector-reveals.

Ragazzi, E., Stefanini, A., Benintendi, D., Finardi, U., & Holstein, D. K. (2020). Evaluating the Prudency of Cybersecurity Investments: Guidelines for Energy Regulators. https://pubs.naruc.org/pub.cfm?id=9865ECB8-155D-0A36-311A-9FEFE6DBD077.

Raman, G., AlShebli, B., Waniek, M., Rahwan, T., & Peng, J. C.-H. (2020). How weaponizing disinformation can bring down a city's power grid. PLOS ONE, 15(8), e0236517. https://doi.org/10.1371/journal.pone.0236517.

Reichl, J., Schmidthaler, M., & Schmidinger, S. (2020). Blackout Simulator. http://www.blackout-simulator.com/.

Robb, J. B. (2019). Testimony of James B. Robb, President and Chief Executive Officer North American Electric Reliability Corporation Before the House Committee on Energy and Commerce Subcommittee on Energy "Keeping the Lights On: Addressing Cyber Threats to the Grid." https://www.nerc.com/news/testimony/Testimony and Speeches/House Energy and Commerce Cyber Hearing Testimony 7-12-19.pdf.

RTE (2019). 2018 Reliability Report. https://www.services-rte.com/files/live/sites/services-rte/files/pdf/bilan-surete/Bilan_Surete_2018_UK.pdf.

Sengupta, D. (2017). Ransomware WannaCry hits Bengal power utility. The Economic Times. https://economictimes.indiatimes.com/tech/internet/ransomware-wannacry-hits-bengal-power-utility/articleshow/58682739.cms?from=mdr.

Shooter, S., & Shooter, S. (2019). European Union's new Cybersecurity act: what do you need to know? Bird & Bird. https://www.twobirds.com/en/news/articles/2019/global/european-unions-new-cybersecurity-act.

Smith, R., & Barry, R. (2019). Utilities Targeted in Cyberattacks Identified. The Wall Street Journal. https://www.wsj.com/articles/utilities-targeted-in-cyberattacks-identified-11574611200.

Sobczak, B. (2018). FERC orders utilities to report hacking incidents. EnergyWire. https://www.eenews.net/energywire/stories/1060089829?t=https%3A%2F%2Fwww.eenews.net%2Fstories%2F1060089829.

Sobczak, B. (2019a). Experts assess damage after first cyberattack on U.S. grid. EnergyWire. https://www.eenews.net/stories/1060281821/.

Sobczak, B. (2019b). First-of-a-kind U.S. grid cyberattack hit wind, solar. EnergyWire. https://www.eenews.net/energywire/stories/1061421301/.

Sobczak, B. (2020). Major hack hits energy companies, U.S. agencies. E&E News. https://www.eenews.net/stories/1063720705.

Soltan, S., Mittal, P., & Poor, H. V. (2018). BlackIoT: IoT botnet of high wattage devices can disrupt the power grid. Proceedings of the 27th USENIX Security Symposium, 15–32. https://www.usenix.org/conference/usenixsecurity18/presentation/soltan.

St. John, J. (2020). Smart Meters Set for $30B Gusher of Investment Over Next 5 Years | Greentech Media. Greentechmedia. https://www.greentechmedia.com/articles/read/wood-mackenzie-world-will-invest-30b-in-smart-meters-through-2025.

Stassen, M. (2019). The EU Cybersecurity Act: Addressing the Risks of a Connected Europe | Retail & Consumer Products Law Observer. Crowell Moring. https://www.retailconsumerproductslaw.com/2019/08/the-eu-cybersecurity-act-addressing-the-risks-of-a-connected-europe/.

Steitz, C., & Auchard, E. (2016). German nuclear plant infected with computer viruses, operator says - Reuters. Reuters. https://uk.reuters.com/article/us-nuclearpower-cyber-germany-idUKKCN0XN2OS.

Strong, W. (2020). NTPC confirms "cyber attack" from unknown source on Thursday, RCMP investigating. CBC. https://www.cbc.ca/news/canada/north/ntpc-apparent-ransomware-attack-1.5551603.

Tangen, S., & Austin, D. (2012). Business continuity - ISO 22301 when things go seriously wrong. ISO. https://www.iso.org/news/2012/06/Ref1602.html.

The Economist (2019). Ubiquitous computing - Drastic falls in cost are powering another computer revolution. Technology Quarterly. https://www.economist.com/technology-quarterly/2019/09/12/drastic-falls-in-cost-are-powering-another-computer-revolution.

Tripwire (2016). Tripwire Study: Energy Sector Sees Dramatic Rise in Successful Cyber Attacks. https://www.tripwire.com/company/press-releases/2016/04/tripwire-study-energy-sector-sees-dramatic-rise-in-successful-cyber-attacks/.

UK Department for Business Energy & Industrial Strategy (2018). Security of Network and Information Systems Regulation 2018. http://www.legislation.gov.uk/uksi/2018/506/contents/made.

UK National Cyber Security Centre (2020). NCSC CAF guidance - NCSC.GOV.UK. https://www.ncsc.gov.uk/collection/caf.

US Department of Energy (2012). Electricity Subsector Cybersecurity: Risk Management Process (Issue May). https://www.federalregister.gov/articles/2012/05/23/2012-12484/electricity-subsector-cybersecurity-risk-management-process.

US Department of Energy (2019). OE-417 Electric Emergency and Disturbance Report - Calendar Year 2019. https://www.oe.netl.doe.gov/OE417_annual_summary.aspx.

US Department of Energy & US Department of Homeland Security (2014). Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2). https://www.energy.gov/sites/prod/files/2014/02/f7/ES-C2M2-v1-1-Feb2014.pdf.

US Department of Homeland Security (2020). Ransomware Impacting Pipeline Operations. https://www.us-cert.gov/ncas/alerts/aa20-049a.

US General Accounting Office (2004). Evaluation of Selected Characteristics in National Strategies Related to Terrorism. www.gao.gov/cgi-bin/getrpt?GAO-04-408T.

US Government Accountability Office (2019). Actions Needed to Address Significant Cybersecurity Risks Facing the Electric Grid. https://www.gao.gov/assets/710/701079.pdf.

Vasquez, C. (2020). “Ransomware” hackers hit supplier to power. EnergyWire. https://www.eenews.net/energywire/stories/1062684959.

Walton, R. (2019). Phishing campaign continues to target utilities, evolves attack techniques. Utility Dive. https://www.utilitydive.com/news/state-sponsored-phishing-campaign-continues-to-target-utilities-evolves-at/563575/.

Walton, R. (2020a). Utilities say they are prepared to meet cyber threats. Are they? Utility Dive. https://www.utilitydive.com/news/utilities-say-they-are-prepared-to-meet-cyber-threats-are-they/572080/.

Walton, R. (2020b). Ameren Missouri supplier hit by ransomware attack amid growing concern for critical infrastructure. Utility Dive. https://www.utilitydive.com/news/ameren-missouri-supplier-hit-by-ransomware-attack-amid-growing-concern-for/574823/.

Wood Mackenzie (2020). AMI global forecast 2020-2025: H1 2020. https://www.woodmac.com/our-expertise/focus/Power--Renewables/ami-forecast-h1-2020/.

World Economic Forum (2019). Cyber Resilience in the Electricity Ecosystem: Principles and Guidance for Boards. http://www3.weforum.org/docs/WEF_Cyber_Resilience_in_the_Electricity_Ecosystem.pdf.

World Economic Forum (2020a). Cyber Resilience in the Electricity Industry: Analysis and Recommendations on Regulatory Practices for the Public and Private Sectors. http://www3.weforum.org/docs/WEF_Cyber_Resilience_in_the_Electricity_Ecosystem_Policy_makers_2020.pdf.

World Economic Forum (2020b). The Global Risks Report 2020 Insight Report 15th Edition. http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf.

Zetter, K. (2016). Inside the Cunning, Unprecedented Hack of Ukraine’s Power Grid. Wired. https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

"*This publication has been produced with the financial assistance of the European Union as part of the Clean Energy Transitions in Emerging Economies programme. This publication reflects the views of the International Energy Agency (IEA) Secretariat but does not necessarily reflect those of individual IEA member countries or the European Union (EU). Neither the IEA nor the EU make any representation or warranty, express or implied, in respect to the publication's contents (including its completeness or accuracy) and shall not be responsible for any use of, or reliance on, the publication.*"

The Clean Energy Transitions in Emerging Economies programme has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 952363

IEA Publications

International Energy Agency

Website: www.iea.org

Contact information: www.iea.org/about/contact

Typeset in France by IEA – April 2021

Cover design: IEA

Photo credits: © Shutterstock