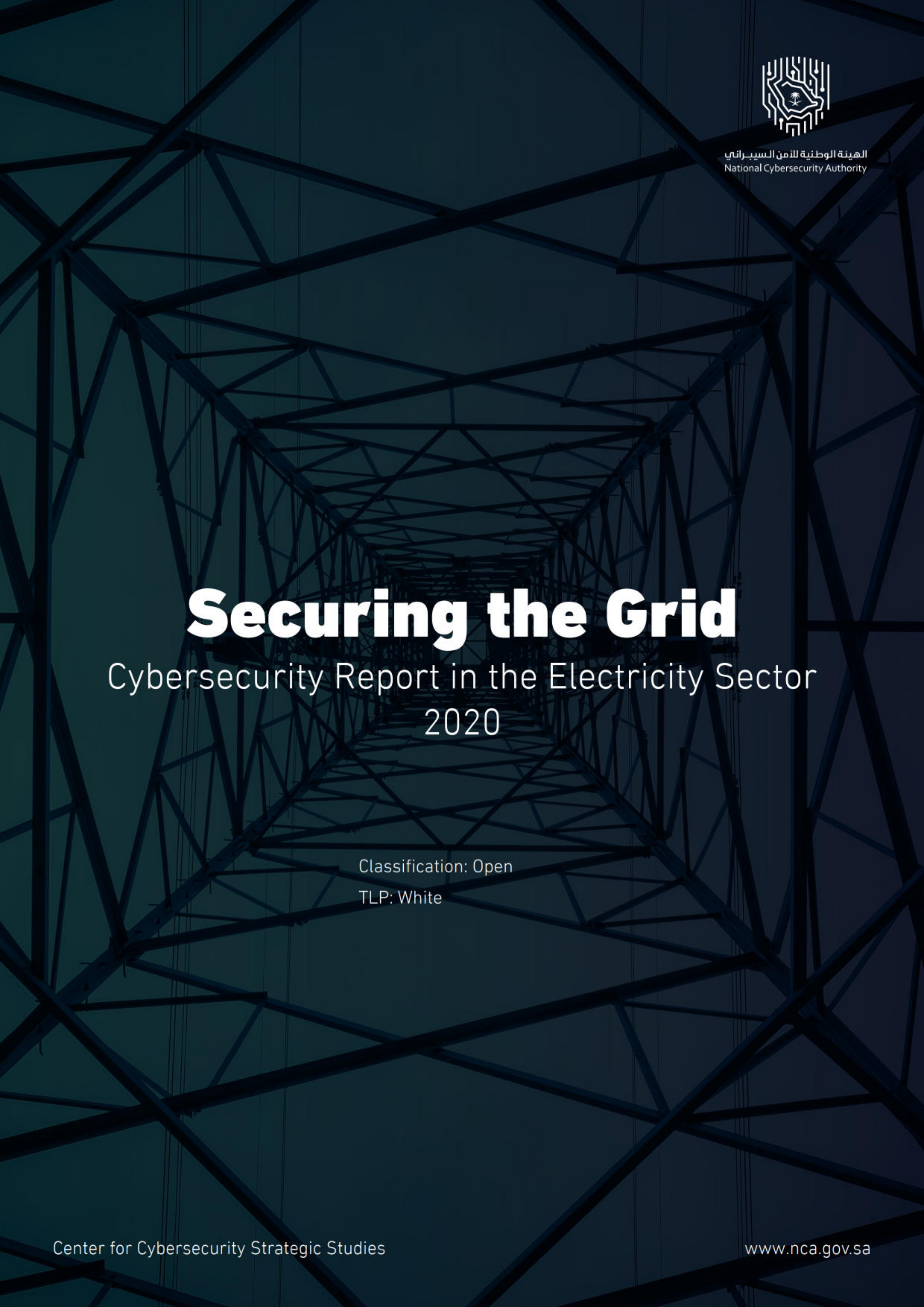


الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

Securing the Grid

Cybersecurity Report in the Electricity Sector 2020

Classification: Open

TLP: White

Center for Cybersecurity Strategic Studies

www.nca.gov.sa

ABOUT THE NCA

The National Cybersecurity Authority (NCA) was established in 2017. The NCA is the government entity in charge of cybersecurity in Saudi Arabia and it serves as the national authority on all related affairs. It has both regulatory and operational functions related to cybersecurity and works closely with public and private entities to improve the cybersecurity posture of the country in order to safeguard its vital interests, national security, critical infrastructures, high-priority sectors, and government services and activities.

This report contains the views of several parties and individuals, with the understanding that all information included in the report is indicative only. Also, the NCA does not bear any responsibility - under any circumstances - towards any party as a result of any decision or action taken or that will be taken by that party based on the content of this report. The NCA asserts that it is not completely or partially responsible for any direct or indirect prejudice that may occur.

CONTENTS

EXECUTIVE SUMMARY

EXECUTIVE SUMMARY

This report draws upon leading research, literature, and interviews with subject matter experts across academia, the electricity sector, and the cybersecurity industry to make recommendations for electricity professionals, the public sector, regulators, and supply chain vendors.

The electricity sector underpins all other sectors and therefore requires an acute level of attention with regards to cybersecurity. At the global level, cybersecurity regulations are enforced to a varying degree across geographies. There is a positive correlation between the cybersecurity maturity of the sector and the degree of enforcement.

Threat Landscape

The threat landscape is becoming more complex with an increase in sophisticated attacks against industrial control systems (ICS) and operational technology (OT) networks. Attacks have attempted, to disrupt electricity suppliers and phisically destroy equipment and have sometimes succeeded in doing so. Reconnaissance of ICS/OT networks remains a common theme of malware targeting the sector, whereby data about electricity networks and equipment is exfiltrated to remote computers under the control of attackers.

Challenges

Legacy infrastructure which lacks security capabilities is common in the electricity sector due to the long service lifespan and high cost of replacement of capital equipment. Therefore, generation and distribution sites were found to be an attractive target, while IT systems continue to provide attackers with a route into electricity organizations via phishing and watering hole attacks.

The supply chain is becoming ever more complex with the adoption of smart grid technologies, and it can be particularly difficult to assure the security of software, hardware, and business services vendors. Cybersecurity can therefore be difficult to implement as security leaders try to balance the contrasting security requirements of their IT and ICS/OT networks.

The cybersecurity, skills gap is compounded by the lack of experts who understand both ICS/OT and cybersecurity which is hindering the efforts of electricity sector leadership to promote their organizations' cyber maturity.

Recommendations

This report provides several recommendations on human skills, process, technology, governance, and collaboration to address the challenges identified.

Improving the cybersecurity culture in the sector is key to raising cybersecurity awareness, and by upskilling control engineers in cybersecurity, organizations can help close the skills gap. Senior management must support cybersecurity programs, while responsibility and ownership of ICS/OT assets should be assigned to designated personnel.

A variety of technology and technical practices are recommended to improve prevention, detection, and protection against cyber attacks and build resilience in the face of attempts and successful attacks.

The report recommends the harmonization of cybersecurity regulations to promote interoperability of cross-regional and international electricity projects, endorsement of internationally recognized standards, and the enforcement of regulations to improve cyber maturity. Finally, this report encourages collaboration across the electricity ecosystem to improve information sharing and help each other to respond to threats globally.

INTRODUCTION

> The growing connectivity of the electricity ecosystem is bridging industrial control systems with IT networks, presenting an attractive target to threat actors.

The modern world exists because of dependable access to electricity. While the first half of the 20th century saw industrialization and electrification spread through all sectors, the latter half built on this foundation, with interconnection and networking becoming the dominant commercial forces.
All of this was enabled by electricity.

At the global level, electricity underpins all other Critical National Infrastructure (CNI) sectors, such as communications, transportation, manufacturing, defense, and financial services. Each sector is entirely dependent on the electricity sector, and managing its associated risks should be of paramount importance to governments and national security officials.

From its foundations in the 19th century, the electrity sector has naturally focused on risks related to safety, but this is changing, and cybersecurity risks are becoming a key consideration. The high levels of interconnection in national and international electricity grids – and the cyber risks posed by this interconnection – are now a primary area of concern for policy makers, as well as key electricity sector stakeholders (across generation, transmission, distribution, and consumption).

It is clear that loss of power across a large region for an extended period would produce severe impacts across businesses, governments, and wider societies. It is also clear that cyber attacks against the electricity sector are growing in number and severity, and security experts note that the number of threat actors is increasing, along with their capabilities. In the US, for example, electricity is one of the top three sectors targeted for attack, with only two other sectors – critical manufacturing and communications – reporting more incidents.[1] A growing level of threat actor sophistication has also been seen in Europe, the Middle East, and Asia-Pacific, which indicates that this is a global challenge.

The cyber attacks against the Ukrainian electricity network in 2015 and 2016 signaled a paradigm shift in the ability of adversaries to affect critical national infrastructure.

This report aims to provide clarity and a balanced perspective on this pressing topic, for decision-makers in both the public and private sectors.

It begins by offering an overview of the Saudi electricity sector, the evolution of the modern electricity ecosystem, and the importance of regulation. The report then assesses growing sources of cyber risk in the electricity sector and identifies evolving threats, threat actors, and vulnerabilities. It examines the key challenges to improving cybersecurity in the electricity sector, including contrasting security requirements, the cyber skills shortage, and supply chain partners.

Finally, the report offers recommendations for improving cybersecurity and looks at future trends – including the rise of "smart" technologies – that could bolster cybersecurity or pose new challenges.

OVERVIEW ON THE SAUDI ELECTRICITY SECTOR

To understand cybersecurity risk in the electricity sector, it is useful to first provide some context for the sector in Saudi Arabia and explain the fundamental components and infrastructure of the electricity ecosystem.

Saudi Arabia is the 11th largest producer of electricity in the world, generating almost 384 terawatt-hours (TWh) in 2018. This accounted for approximately 31% of total Middle East electricity generation. For comparison, the two largest producers, China and the USA, generated 7,122 TWh and 4,461 TWh, respective-

Figure 1: 2018 Top 20 Countries by Electricity Generation Gross Output (TWh)

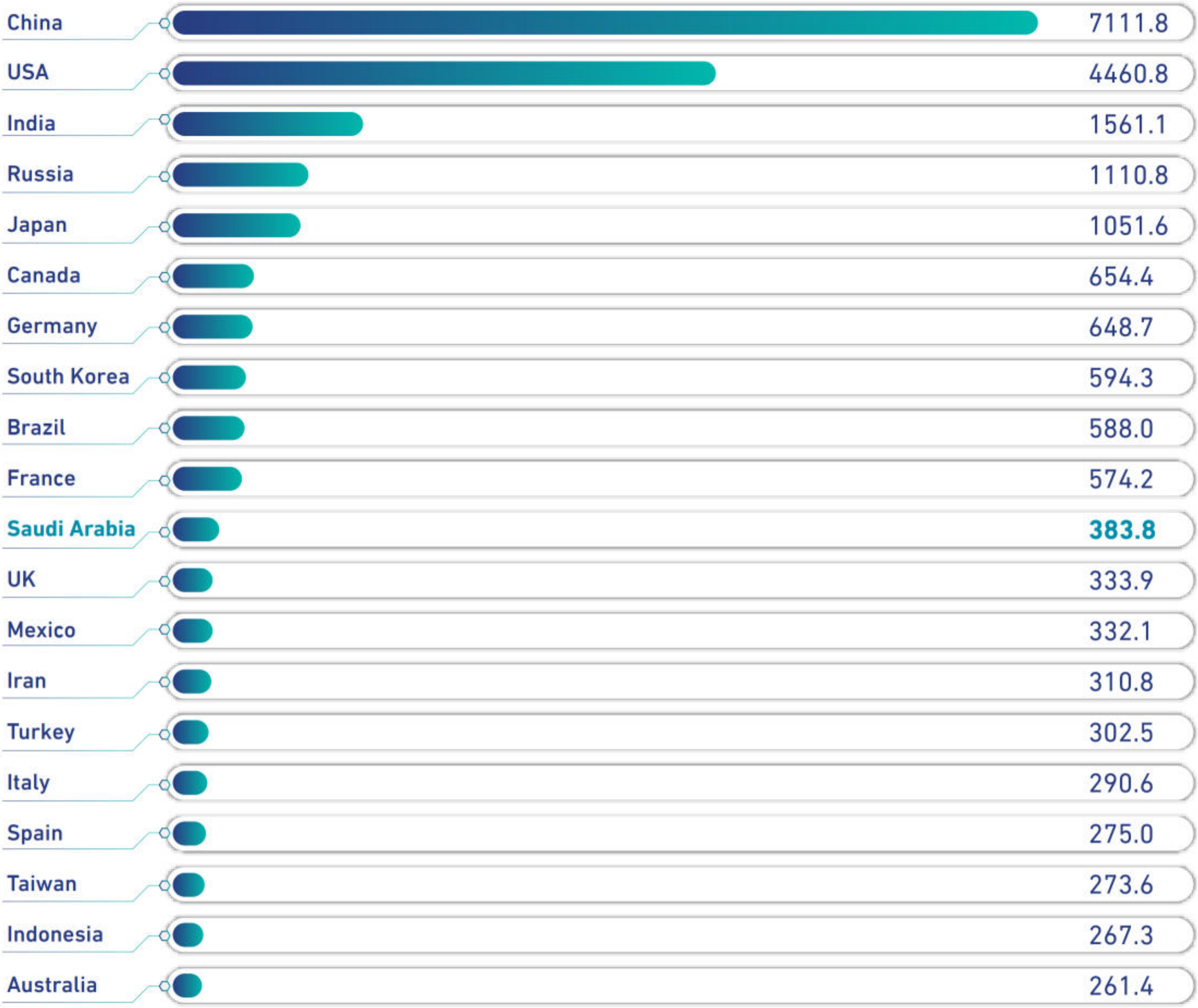
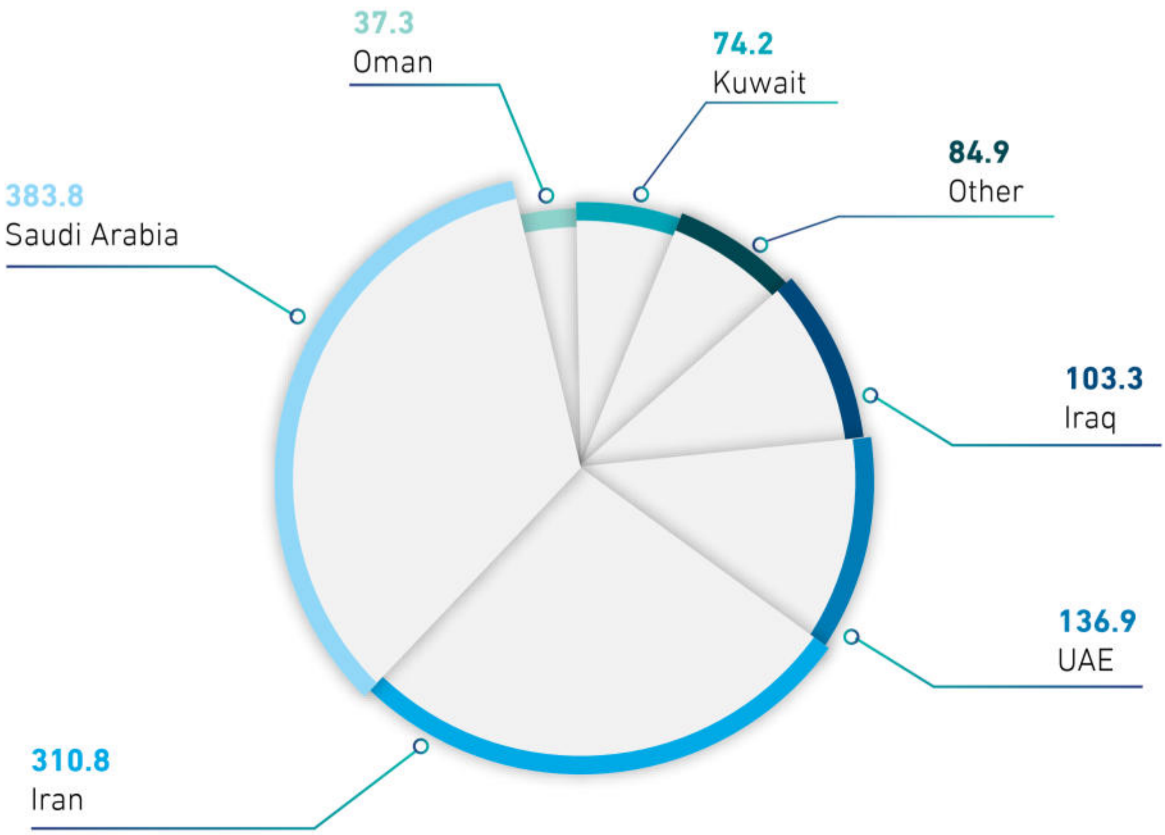


Figure 2: 2018 Middle East Electricity Generation Output by Country (TWh)



ly.[2]

To meet future demand, Saudi Arabia must increase its generation capacity to an equivalent maximum annual output of 1,420TWh by 2040. Consequently, the government is planning to invest $5bn in generation and $4bn in transmission and distribution (T&D) annually to achieve this.[3]

From a cybersecurity perspective, national electricity sectors across the globe face two key risks around data security and industrial control systems (ICS). Firstly, the various stakeholders across the electricity ecosystem hold commercially valuable information and customer data. A compromise of the confidentiality, integrity, or availability of this data could cause severe financial, operational, and reputational damage to the organization.

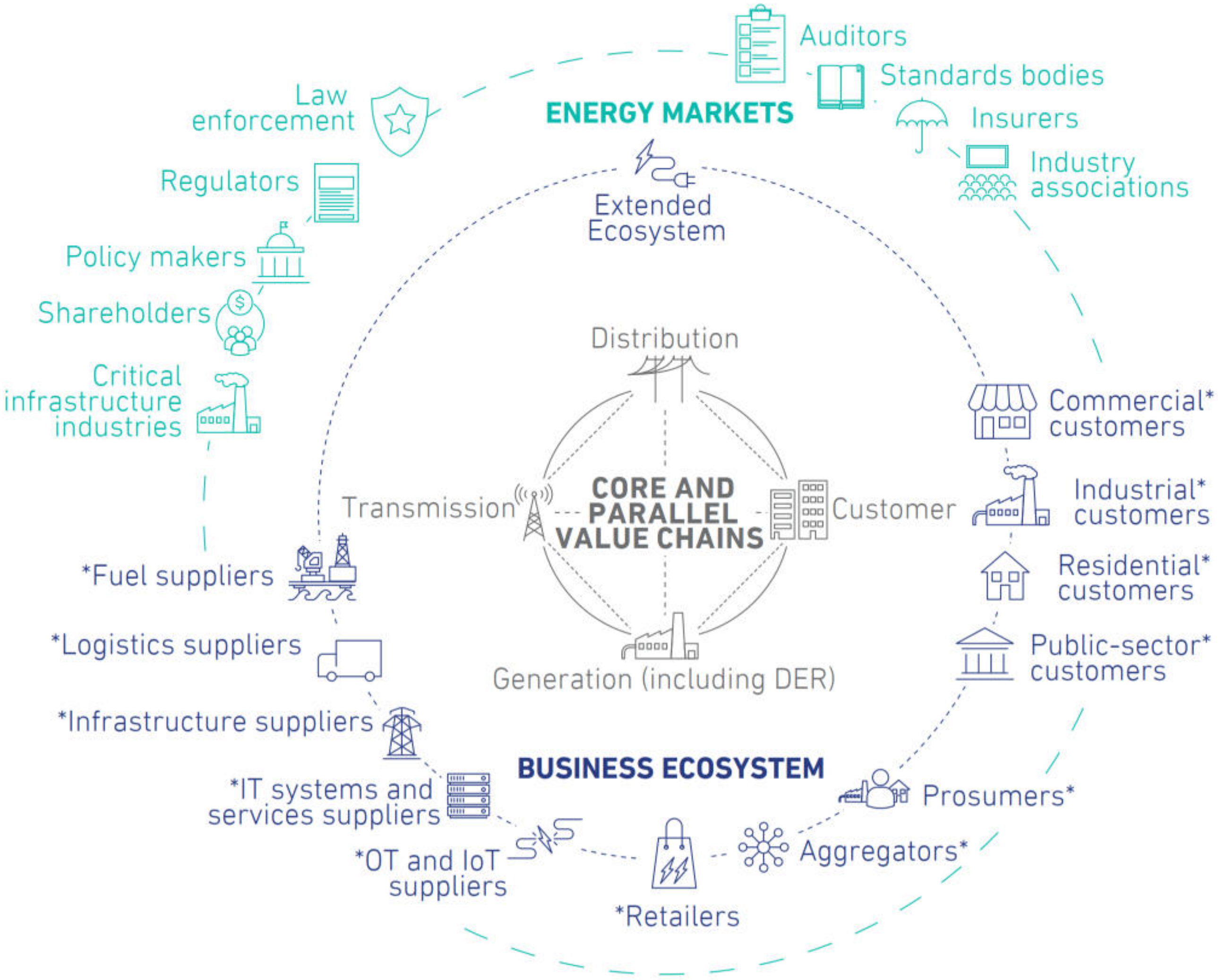
Secondly, electricity organizations around the world increasingly rely on control systems to interact and monitor production and distribution operations. The availability and integrity of network traffic in ICS is critical to the provision of a high quality, reliable electricity supply to the population and the safety of electricity sector workers.

An in-depth comparison of various security goals (including availability, integrity, and confidentiality) in IT systems and ICS/Operational Technology (OT) is detailed in the "Challenges to Improving Security" section, while the complex electricity ecosystem is examined in more detail in the next section.

ELECTRICITY INFRASTRUCTURE

The electricity ecosystem is vast, encompassing a wide range of stakeholders from generation through to customers and regulators to insurers, as shown in Figure 3. Suppliers are heavily depended upon to supply fuel and mission-critical spare parts, and they can contribute a significant portion of an organization's cyber risk.

Figure 3: The Modern Electricity Ecosystem[4]



*Entity has its own ecosystem

The ecosystem can be broken down into four distinct areas which form the core of the electricity infrastructure : generation, transmission, distribution, and consumption.

GENERATION – Power is commonly generated by thermal, hydroelectric, solar, and wind sources. Thermal plants use the heat of the fuel consumed to turn water into steam to drive a turbine, which in turn generates electricity. All major power plants in Saudi Arabia are thermal plants with a high dependency on fossil fuels. A disruption to the supply of these fuels would cause the plant to operate at a reduced capacity. Nuclear plants are in the thermal category and, while Saudi Arabia has no operating nuclear power plants at present, it seeks to have a functioning nuclear reactor in the coming years.[5]

The Kundankulam Nuclear Power Plant in India detected information stealing and reconnaissance malware, Dtrack, in its networks in September 2019. While the malware was not specifically designed to target industrial control systems, it provides an effective mechanism for monitoring and collecting information on software and network vulnerabilities which can be used for future attacks.[6] The clandestine nature of this malware enables it to remain undetected for long periods of time where strong cybersecurity measures are not in place.

TRANSMISSION – This stage transports electricity from the generation site to distribution substations at very high voltages. Transmission networks also provide communications across the grid, making it susceptible to cyber attack. Transmission infrastructure includes pylons, power lines, cables, transformers, and circuit breakers. In 2016, a Ukrainian transmission substation was targeted in an extremely sophisticated attack using Industroyer/Crashoverride malware, the first of its kind specifically designed for the electricity sector.[7]

Figure 4: A Conventional Electricity Grid Model

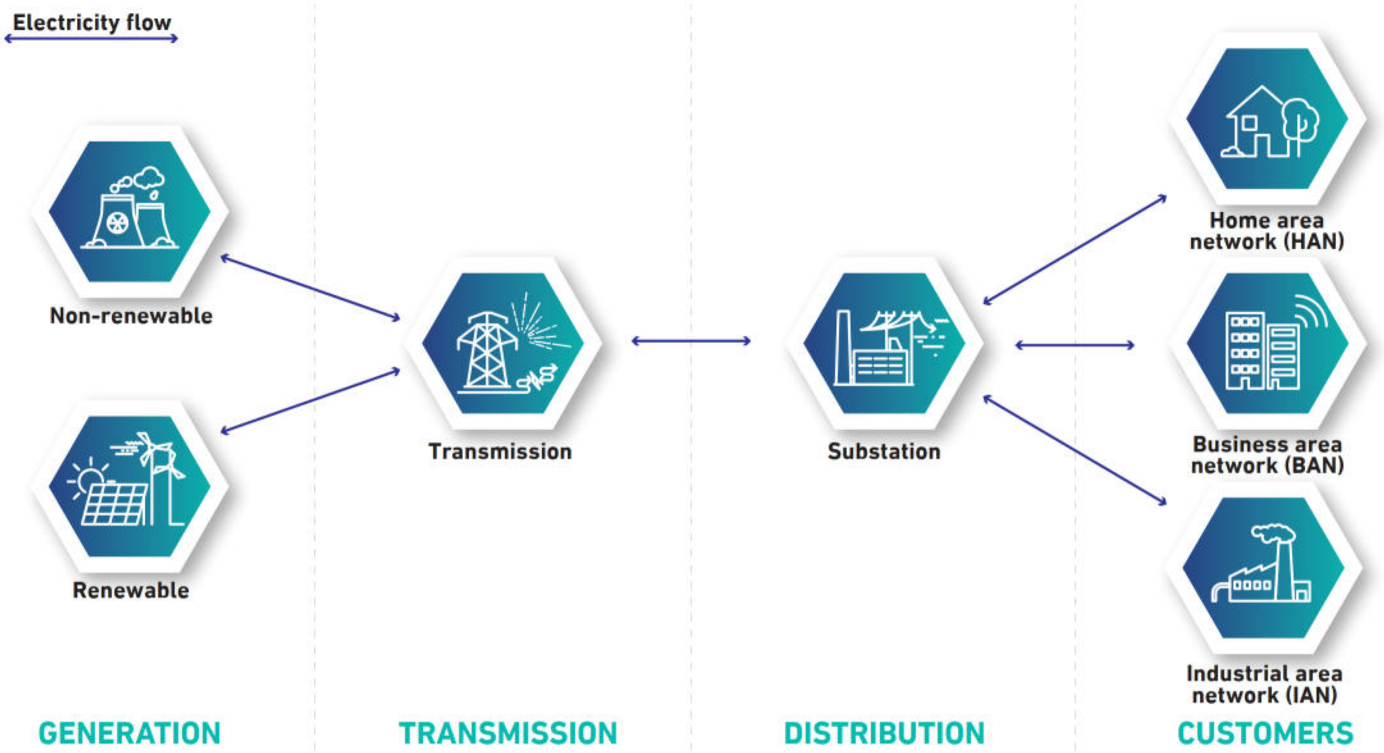


Figure 4 illustrates the interactions between these four areas.

This model of a conventional electricity grid is evolving from a hierarchical top-down system towards a smart grid – a more dynamic ecosystem characterized by a proliferation of data exchange and the emergence of the 'prosumer' (someone who both produces and consumes energy).[9]

DISTRIBUTION – Substations receive high-voltage electricity from the transmission network and step the voltage down gradually in accordance with the requirements of the various customer networks they serve. Electricity can then be distributed to customers via underground cables or overhead lines, dependent on proximity and customer density. Three distribution sites in Ukraine were targeted in 2015 with BlackEnergy3 malware, which caused outages to approximately 225,000 customers for at least six hours.[8]

CUSTOMERS – These can be categorized – per the National Institute of Standards and Technology (NIST) – as home, business, and industrial area networks. Each category has its own requirements in terms of priority and supply capacity.

TOWARDS THE SMART GRID

Efficiency is the main driving force behind the move to smart grids. Conventional grids have been built with excess capacity to withstand peak loads, yet this results in an inefficient system in off-peak periods. Smart grids offer several benefits over conventional grids, including:

- reliability through improved automated real-time monitoring and control;
- optimal power generation, transmission, and distribution, leading to minimized operational and maintenance expenditure;
- improved security in terms of access control, authentication, authorization, privacy, and intrusion detection;
- accommodation of a range of generation options: central, distributed, intermittent, and mobile; and
- predictive and self-healing networks that automate corrective action.[10,11]

Advanced Metering Infrastructure (AMI) is a key technology required in any smart grid. It is used to monitor energy consumption through smart meters in real time to ensure a reliable and secure electricity supply.[10] In an ideal smart grid, smart devices and distributed generation equipment (such as solar panels) would communicate their consumption and output, respectively, with their electricity supply's smart meter. In real time, smart meters then feed this data back to the energy provider, who performs data analysis to accurately predict demand across the entire network.

Two-way communication with smart meters enables energy suppliers and utilities companies to modify customers' service-level parameters. In effect, it facilitates the ability to limit or cut off supply to customers who fail to pay their bills. Utilities companies have traditionally struggled with load balancing and revenue protection, and AMI provides a solution to both issues. Furthermore, in-person meter readings are no longer required as smart meters transmit accurate consumption data and diagnostic logs back to the energy provider, contributing to cost savings and ending the practice of estimated bills.[12]

However, if a malicious actor had access to this infrastructure and issued an 'open' command to several thousand smart meters, it could have the same unbalancing effect as shutting down a power generation plant.

The introduction of advanced metering infrastructure and new supply chain parties associated with the smart grid increases cyber risk, as both of these elements are attractive targets for attackers. The challenges to managing this risk – along with pragmatic recommendations for doing so – are a primary focus of this report.

The rise of the smart grid and the introduction of new market players will undoubtedly complicate an already complex regulatory landscape. The following section provides a high-level comparative view of regulation in the UK and USA, two relatively cyber-mature nations.

THE DIVERSE REGULATORY LANDSCAPE

Regulation is widely recognized across many sectors as an effective tool for aligning and improving business practices. To date, regulation in the electricity sector has predominantly focused on safety. Recent technological innovations – including the move towards the smart grid – and the evolving cyber risk landscape necessitate a comparable focus on cybersecurity regulation to protect against large-scale disruption.[13]

Regulations and internal compliance have improved cyber hygiene across the electricity sector, but regulation alone does not guarantee strong security.[12] Countries take varying approaches to cybersecurity regulations - from prescriptive to risk-based - and their effectiveness depends upon the degree to which they are enforced. Furthermore, risk management frameworks and standards may be interpreted by organizations differently depending on the maturity of regulation within the country.

In the UK, regulations take a risk-based approach that considers the threat landscape facing the organization. Assets are scored in terms of criticality as defined by the Centre for Protection of National Infrastructure and a mix of controls are recommended, including physical and personnel security, based on the Cyber Assessment Framework.

The US approach is more prescriptive - specifying procedures and controls - and has improved greatly in recent years. For example, early regulations specified firewalls to be installed at various network interfaces with no further guidance, whereas today's regulations now provide specific firewall configuration settings.

Regulations are strictly enforced in the US, and organizations must remain compliant to obtain and retain a license to operate. However, in the UK, regulations are not enforced so rigidly, and there is less incentive for organizations to invest in (potentially costly) security controls. Furthermore, many organizations will struggle to understand how to implement and comply with standards and guidance, as they lack the skills in house or the resources to access external expertise.[14,15]

Further complexity arises for multinationals that operate in different countries, facing the challenge of having to adhere to a patchwork of regulatory frameworks. An organization-wide risk-based approach that aligns security controls with business priorities is a prudent first step to addressing this challenge.[15]

A VOLATILE SECURITY ENVIRONMENT

> The electricity sector is facing a growing number of sophisticated cyber attacks.

It's clear from cybersecurity threat reports that the electricity sector is facing a growing number of sophisticated cyber attacks. Recent studies found energy and resources to be the most targeted sector globally. The Middle East and Africa ranked as the fifth most targeted region in the sector.[16] The growing connectivity of the electricity ecosystem is bridging ICS/OT with IT networks, presenting an attractive target to threat actors.

EVOLVING CYBER THREAT

There are an increasing number of threat actors capable of attacking the electricity sector, ranging from highly skilled advanced persistent threat (APT) groups to criminals, terrorists, and insiders. This is now a top concern among utilities security professionals, with 64% of survey respondents raising concerns about the possibility of sophisticated attacks and 54% expecting an attack on CNI throughout 2020. These concerns appear valid, given that 25% of respondents also claimed to have experienced large-scale attacks, which were linked back to nation-state actors.[15]

APTs have the most resources to develop and carry out attacks, but insiders remain a top concern for security teams, given their access and understanding of highly specialized and proprietary electricity systems. Research has shown how incidents are increasingly being attributed to organized crime gangs and states – sometimes in collaboration.[1,15]

The introduction of commercial off-the-shelf (COTS) equipment and open protocols into the electricity sector, along with the convergence of IT and operational technology (OT) networks, has also allowed less skilled attackers to participate, and many are now equipped with powerful and readily available tools developed by APTs.

The electricity sector is facing cyber-attackers with at least three distinct motivations. Electricity IT networks have been targeted (via ransomware attacks) by organized crime gangs seeking financial gain, while other actors have conducted cyber espionage and disinformation operations. APTs are known to target ICS/OT networks seeking to perform pre-attack reconnaissance or cause outright damage and disruption.[17]

Furthermore, all modern infrastructure, for instance telecommunication and financial services, as well as other critical national infrastructures, strongly depends on electricity. Power outages can therefore have a wide range of cascading effects, from reputational damage through to putting human safety at risk. Critical businesses will often have back-up power solutions in place to mitigate outages, but they are not designed to operate over extended periods of time.

While the threat landscape is becoming even murkier, there are intelligence tactics, techniques, and procedures that can isolate some of the signal from the noise and more clearly link threat actors to exploitation and attacks. Figure 5 offers an overview of the top threats facing the sector.

Sophisticated threats are here to stay. As ICS malware development continues apace, it is increasingly being reused, making attribution more difficult. It is therefore important to identify vulnerabilities in the ecosystem so that security controls can be put in place. In this respect, there are two main areas of concern: first, insecure legacy infrastructure, which offers both entry points and vulnerable targets where IT and OT technologies converge; and second, the supply chain, which could be vulnerable to malicious interference (e.g. hardware or software) and the exploitation of third party service providers.

Figure 5 offers an overview of the top threats facing the sector.

Figure 5: Top Threats

MALWARE: TRISIS

The TRISIS/TRITON malware targets Safety Instrumented Systems (SIS), specifically Schneider Electric's Triconex 3008 process control modules. Successful exploitation of the vulnerability allowed the threat actor(s) to gain elevated privileges, which could then be used to manipulate emergency shutdown systems.[16]

MALWARE: CRASHOVERRIDE/INDUSTROYER

This malware, which affected an electrical grid in 2017, targets ICS systems used in the electricity grid. The malware can automate mass power outages and includes plug-in components that allow it to be adapted to different electric utilities, easily reused, and launched simultaneously across multiple targets. And it can also control switches and circuit breakers. This malware is the first and only of its kind that is specifically developed for the electrical grid.

MALWARE: JOANAP / BRAMBUL

Joanap, a RAT, and Brambul, a server message block (SMB) worm, have been observed targeting critical infrastructure. These two malware strains allow the attacker to perform reconnaissance, execute commands, and move laterally across the network.[18]

MALWARE: STONEDRILL

Stonedrill contains a wiper module that erases data outside the Windows directory and a remote access tool (RAT). It has similarities with the Shamoon 2.0 malware, which previously targeted organizations in Saudi Arabia and other nations in the Middle East.[19]

MALWARE: HAVEX

Havex has been distributed through spam email, exploit kits, and compromised vendor websites. The malware scans the network for Open Platform Communications (OPC) servers, used to control hardware, and relays information on connected resources to remote servers.[20,21]

MALWARE: AGENT TESLA

AgentTesla is a RAT designed for information stealing, including authentication data, screenshots, web camera, and keyboard strokes. The malware is commonly distributed by phishing emails containing a malicious MS Word attachment. It poses a serious threat to ICS/OT because the information collected can be used to plan and execute targeted attacks.[22]

MALWARE: GREYENERGY

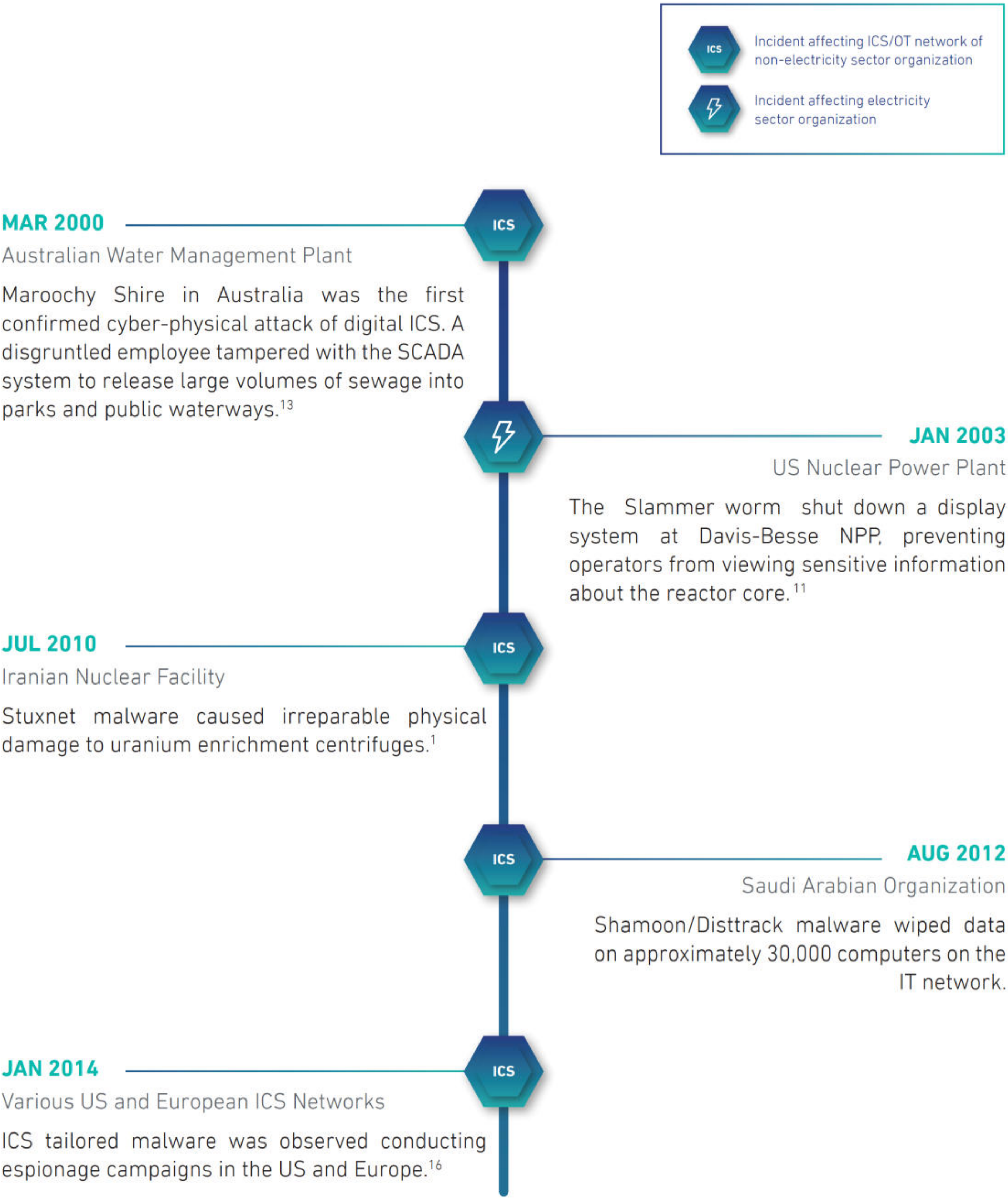
This malware is suspected to be the successor variant of BlackEnergy. In 2018, researchers uncovered an operation against energy organizations in Poland and Ukraine. The malware is capable of exfiltrating sensitive data while removing traces of its actions.[16]

MALWARE: IMECAB/SORGU

Imecab and Sorgu were observed in Middle East power sector networks in mid-2018, as well as the financial, government, and transportation sectors. The malware is often installed via watering-hole attacks and provides attackers with remote access to infiltrate target networks and exfiltrate sensitive data.[16]

Vulnerabilities in far more critical systems, including nuclear power plants (NPP), have been targeted by attackers, as shown below, and demonstrate how increasing interconnectedness can reach even the most (allegedly) secure facilities.

Figure 6: Notable Cyber Incidents in the Electricity and Related Sectors Timeline



ICS Incident affecting ICS/OT network of non-electricity sector organization

ϟ Incident affecting electricity sector organization

MAR 2000 ICS

Australian Water Management Plant

Maroochy Shire in Australia was the first confirmed cyber-physical attack of digital ICS. A disgruntled employee tampered with the SCADA system to release large volumes of sewage into parks and public waterways.[13]

JAN 2003 ϟ

US Nuclear Power Plant

The Slammer worm shut down a display system at Davis-Besse NPP, preventing operators from viewing sensitive information about the reactor core.[11]

JUL 2010 ICS

Iranian Nuclear Facility

Stuxnet malware caused irreparable physical damage to uranium enrichment centrifuges.[1]

AUG 2012 ICS

Saudi Arabian Organization

Shamoon/Disttrack malware wiped data on approximately 30,000 computers on the IT network.

JAN 2014 ICS

Various US and European ICS Networks

ICS tailored malware was observed conducting espionage campaigns in the US and Europe.[16]

⚡

JAN 2014

Japanese Nuclear Power Plant

Monju NPP in Japan and the Gori NPP in South Korea suffered information theft due to malware attacks.[13]

ICS

DEC 2014

German Steel Mill

A German steel mill attack disabled the shutdown systems of the plant, causing massive physical damage.[13]

⚡

DEC 2015

Ukraine Power Grid 1 (Black Energy)

The sophisticated attack framework known as BlackEnergy3 was used to distribute KillDisk malware causing the Ukrainian grid to go offline for six hours.[1]

ICS

MAR 2016

Undisclosed Water Treatment Plant

Attackers altered treatment chemicals added to the water supply. The attackers were able to exploit unpatched web vulnerabilities in the internet-facing customer payment portal.[23]

ICS

MAR 2016

US Water Dam

A water dam in the US was targeted and its control system was accessed.[16]

ICS

NOV 2016

Saudi Arabian Organization

A re-emergence of the Shamoon/Disstrack malware from 2012 once again targeted 21 organizations in Saudi Arabia, including two petrochemical organizations. This attack, however, only affected the IT systems.

⚡

DEC 2016

Ukraine Power Grid 2 (Industroyer)

A cyber attack cut off power for over one hour. The malware (Industroyer/Crashoverride) was expressly developed to attack electrical grids.[1]

ICS

AUG 2017

Saudi Arabian organization

TRITON/TRISIS malware remotely targeted safety instrumented system controllers. A bug in the application code conveniently caused the failure of a validation check, which initiated a safe shutdown.

ICS

MAR 2019

Norwegian Aluminum Manufacturer

LockerGoga ransomware infected the networks of Norsk Hydro and resulted in the widespread encryption of computer hard drives.[24]

ICS

APR 2019

Vietnamese Oil and Gas Company

A data exfiltration malware, dubbed SILKBUILDER, was discovered on networks. The suspected purpose was intellectual property theft.[16]

ICS

MAY 2019

Middle Eastern ICS Networks

FlushTunnel malware, designed to gain initial access and persistence, was observed in ICS networks in the Middle East.[16]

⚡

SEP 2019

Indian Nuclear Power Plant

Computer networks at the Kudankulam NPP were infected with data extraction malware linked to North Korea. There are suggestions that both IT and OT networks were affected.[25]

⚡

MAY 2020

UK Electricity Market Operator

A suspected ransomware attack on the IT systems of a large UK electricity market operator resulted in the release of confidential documents on the dark web, including passport copies and financial records. An out-of-date VPN service was believed to be the route of entry into the organization.[26,27]

INSECURE LEGACY INFRASTRUCTURE

Industrial control systems were not designed with cybersecurity in mind. In fact, the term "cybersecurity" only gained momentum in the mid-1990s, some 30 years after the birth of the modern ICS.[28] Availability and safety were the key drivers for ICS development, leading to the development of an inherently insecure environment. This legacy infrastructure remains dominant in the electricity sector across the globe, due to the financial costs and disruption associated with implementing upgrades. Over the years, IT systems have been introduced for business and operational purposes, adding a further layer of complexity and risk.

As ICSs evolve to provide operational efficiency and two-way communications with equipment, they become more vulnerable to cyber attack. The move from proprietary to COTS devices – and from closed to open protocols – is increasing the attack surface across the sector.[14] This is often exacerbated by lack of encryption, authentication, or logging as well as the use of default manufacturer passwords on equipment throughout OT networks.[29]

Where legacy infrastructure persists, isolated and fragmented systems are one of the top concerns for plant operators. While isolation may create a level of separation from the internet, the resulting lack of visibility into these systems removes the opportunity to monitor control process status and detect anomalous or malicious activity. Furthermore, many endpoints in the network remain unsecured due to financial constraints or a lack of appropriate controls.[14,15] There is a growing trend of directly exposing devices in ICS/OT networks to the internet, either intentionally or otherwise, which presents an open invitation to threat actors seeking a route into the network.

Generation and distribution sites are home to both IT systems and critical safety equipment, such as protective relays. Providing both routes into the grid and targets for maximum effect, the convergence of technologies at these sites presents a particularly attractive target to threat actors.

ATTRACTIVE TARGETS: GENERATION & DISTRIBUTION SITES

Thermal power generation sites traditionally benefit from robust physical security to ensure human safety and protect public services from serious risk. Remote power generation sites, such as widely distributed wind turbines, however, often suffer from a lower level of physical security. They also require remote connectivity, which presents additional routes of entry to attackers.

Cyber attacks on generators have been shown to cause physical destruction (e.g. during controlled experiments), while the loss of a generation facility could put enough stress on the grid to cause localized blackouts. In such an event, a control engineer's first response might be to shed load, further reducing output. Therefore, attackers do not necessarily have to directly override control systems to successfully create disruption, but can indirectly achieve their goals by creating conditions that force control engineers to reduce output.[29]

Duqu

Duqu is a sophisticated and well-designed piece of malware, and is based on the infamous Stuxnet malware that was used to disrupt Iranian nuclear enrichment at Natanz. Duqu has the ability to monitor and learn device behavior in order to identify vulnerabilities. It has been found in power generation and T&D networks and can build a tailored attack by issuing commands and observing their effects.[27]

Distribution organizations have the difficult task of securing endpoints and networks, both physically and logically, as their assets tend to be spread over a wide geographical area. Distribution, in conjunction with transmission, provides electricity to large sectors of the population, and the impact of a cyber-attack could be widely felt. The move towards digitalization in recent years, particularly in distribution, without due consideration for cybersecurity, is a cause for concern.

Control engineers at remote generation and distribution sites may be less familiar with cybersecurity practices than those in larger generation sites, where cybersecurity practices are more widely practiced and enforced. Engineers' laptops are inherently insecure and may introduce vulnerabilities when connected to the network, either through engineers browsing malicious websites or unpatched software.

Some systems may rely on physical access to install software updates or security patches and could therefore remain vulnerable for months or years depending on maintenance schedule priorities. IT systems, at both generation and distribution sites, provide an important link to OT networks, the wider organization, and the internet. While this link is necessary for efficient business operations in today's world, it presents threat actors with an opportunity – a route in.

A ROUTE IN: IT SYSTEMS

IT systems are a relatively soft target as they contain COTS operating systems and hardware and are generally connected to the internet. While IT systems are usually kept more up to date than their OT counterparts, they are layered on top of legacy equipment and can only provide so much security.

There is a major trend in the electricity sector to increase the connectivity between IT and ICS/OT networks for administration over wide areas. However, despite the security controls in place, threat actors can leverage physical or logical connections to move between IT and ICS/OT networks.

Unpatched operating systems are a particular risk and a symptom of poor cybersecurity management. A cyber attack - such as a ransomware infection - can create significant business disruption, and operators may, again, feel forced to terminate or degrade service to prevent propagation of the threat, even if there is minimal risk of malware crossing over to OT networks and creating safety risks.[29] Recovering from a ransomware attack is most effective when systems can be restored from unaffected backups. However, in the event that backups are not properly maintained and tested, the recovery process can be long, expensive, and painful.

Cryptojacking

Cryptojacking is one particularly prominent attack type that poses a risk to critical infrastructure networks. Cryptojacking malware uses a computer's processing power to mine (or earn) cryptocurrencies, creating financial gain for the attacker. Cryptomining is a very energy-intensive process, therefore attackers naturally seek to avoid this cost by hijacking computers belonging to other people or organizations.

Cryptocurrency values were particularly high in the first half of 2019, which was reflected in the growth of cryptojacking malware infections. In 2019 Q1 cryptojacking malware grew by 629%, while ransomware activity was observed to have decreased by 32%.[16]

Cryptojacking malware is prevalent around the globe. It has been found in OT networks throughout Asia, seeking to leverage the combined computing power of ICS components.[16] In Russia, threat actors were responsible for installing 6,000 cryptomining devices in an abandoned power facility.[30] Electricity infrastructure owners are advised to be on their guard for cryptojacking malware, as it can provide an entry point for far more dangerous attacks.

A TARGET FOR MAXIMUM EFFECT: PROTECTIVE RELAYS

Protective relays are valuable components of safety systems in ICS environments which are designed to alert control engineers to dangerous frequencies and currents in electrical equipment. Yet, they rarely have any cybersecurity controls in place.[29] Protective relays are difficult to attack directly, as this requires in-depth knowledge of system design, relay specifications, electronics designs, and firmware.

However, today's control engineers – who understand these systems – are more likely to have some software development experience and, through coercion or influence, are well-placed to develop targeted malware or share their knowledge with other threat actors. This highlights the need for appropriate vetting of personnel and developing a positive culture of cybersecurity in the organization.

Cyber attacks against the Ukrainian electricity grid demonstrated the reality of cyber threats to the sector, and their potential to undermine standard power restoration procedures.

Ukraine 2016 Attack

A 2016 cyber attack against the Ukrainian electricity grid caused a blackout lasting for one hour. One part of the attack targeted a vulnerability in four unpatched digital protective relays. Analysis suggests that the blackout would have led engineers to re-energize equipment with the aim of bringing the grid back online. With the protective relays out of action, this could have caused catastrophic physical damage to power lines and transformers. Fortunately, for Ukraine, this part of the plan did not succeed due to a networking misconfiguration.[31]

SUPPLY CHAIN INTERFERENCE

While generation and distribution sites can offer direct routes into the electricity grid, the supply chain and third parties offer a growing range of routes into CNI organizations and are commonly found to be the root cause of cyber-attacks.

Physical hardware can be compromised during manufacture to insert backdoors which can be exploited by attackers to access OT networks after the equipment has been installed. Third party providers – ranging from suppliers of accountancy services to heating, ventilation, and air conditioning vendors – provide touchpoints with organizations that can be exploited through cyber attacks or social engineering. For example, the technique of island hopping is a common supply chain attack whereby attackers abuse the trust and transactions that an organization has with its suppliers – through various means – to gain access to that organization.[32]

In modern electricity grids, data is shared extensively and it can be a challenge for organizations to monitor data creation, collection, analysis, distribution, and disposal – not least when numerous third parties are involved in this process. Given a sharp rise in the amount of data being collected and processed, the associated risk of data breaches increases exponentially, resulting in a significant impact.

The gradual introduction of smart meters, electric vehicles, and distributed renewable feed-in energy production demonstrates the new ways in which consumers are interacting with the grid. These developing technologies require advanced controls, digital sensors, and new network architectures, increasing the degree of cyber risk. A vulnerability in a commonly installed solar panel control system, for example, could be exploited to cause service disruption across the grid by creating load balancing issues due to the collective reduction in supply. Smart meters - and the associated use of wireless AMI - are unique in that they offer easy physical access to a key component of the future electricity grid. One study showed how a microwave oven could be used to jam the signals in the wireless sensor network of an AMI, causing a denial of service.[33]

As the electricity sector evolves, cyber risks are emerging from a number of newer, smaller, and less cyber-mature players in the market. On the supply side, renewable energy providers are supplying the grid, but, where this is done without appropriate security controls, there is a risk they will provide insecure access points into the grid.

The increasing number of cyber attacks on ICS and electricity networks over recent years suggests that cybersecurity in the electricity sector is far from where it should be. While electricity sector leadership has begun to understand the importance of cybersecurity, there are a number of challenges preventing the implementation of cybersecurity strategies and controls.

CHALLENGES TO IMPROVING SECURITY

> “The complexity inherent in the electricity sector means a challenge of maintaining and updating technical cybersecurity controls.”

The electricity sector faces the same challenges around the cybersecurity skills shortage and supply chain interference as many others. However, the nature and criticality of the electricity sector engenders a unique perspective on these challenges.

Firstly, cybersecurity personnel who also possess an understanding of control systems are scarce. Secondly, a combination of the complex electricity ecosystem and its critical national importance results in a wider range of opportunities and motives for supply chain interference than in other sectors.

IT systems and networks have enjoyed cybersecurity solutions such as anti-virus and firewalls for decades. However, it is only in recent years that OT security has been considered. Due to the fast pace of digital transformation, cybersecurity strategies and controls can become outdated within a few years, while OT infrastructure is typically designed to have a 20+ year service lifespan.[34]

Therefore, it is important to understand the role that service lifespan plays – among other factors – in terms of the security requirements of both technologies.

CONTRASTING CYBERSECURITY REQUIREMENTS

IT and OT both require a very different set of cybersecurity requirements and priorities due to their function, criticality, and potential impact on human safety. Many organizations have reported difficulties aligning their IT and OT cybersecurity strategies and controls, which are often based on the misconception that IT cybersecurity controls are effective for OT.[15] Cybersecurity standards can also be interpreted differently by IT and OT experts. Therefore, senior leadership should prioritize IT and OT cybersecurity requirements and ensure a non-biased interpretation of relevant standards.

The data security objectives in IT and OT environments differ notably. Confidentiality is often the main focus in IT security, while, in the OT environment, integrity and availability are usually prioritized because the tolerance for timing delays on the network is very low. For example, delayed or malformed control messages could cause outages or damage to equipment. However, the main emphasis in OT environments is on human safety, system reliability, and the protection of equipment and T&D, above and beyond data security. This focus on functionality and safety has resulted in the development of OT network protocols and architectures that are inherently insecure. Security managers must carefully consider the conflicting security requirements when connecting IT and OT infrastructure, as outlined in Figure 7 below.

Figure 7: Key Requirements for IT and OT Environments[4,12]

Operational Technology	Cybersecurity Requirement	Information Technology
1. Availability 2. Integrity 3. Confidentiality	Data security	1. Confidentiality 2. Integrity 3. Availability
Very high, rebooting not acceptable	Availability	Medium, rebooting permitted
Critical	Timeliness	Delays tolerated
20+ years	Lifespan	3-5 years
Infrequent	Patch management	Regular
Occasional	Cybersecurity testing	Scheduled, possibly mandatory
Stable tree hierarchy	Architecture	Flexible, dynamic, software-defined networks
Proprietary operating systems, private networks, IEC61850, and DNP protocols	Technology	Diverse operating systems, public networks, and TCP/IP based protocols
Low but increasing	Cybersecurity awareness	Mature

The inherent complexity of electricity sector infrastructure has resulted in many organizations facing the challenge of maintaining and updating technical cybersecurity controls, with some Chief Information Security Officers reporting over 300 different solutions in place. The consequences of these can be witnessed in the smart grid and on the general service lifespan.

SMART GRID

The effects of contrasting cybersecurity requirements can have a significant impact in the deployment and effective use of the smart grid. Moving towards a secure smart grid will have considerable implications, calling for additional cybersecurity requirements, including authentication, integrity, auditability, and non-repudiation – particularly in OT networks – to reduce the risks connectivity poses to the wider internet. Furthermore, the introduction of wireless sensors in infrastructure presents new attack vectors. While technology plays an important role in cybersecurity, the US-based Electric Power Research Institute has recommended that all aspects of the smart grid incorporate cybersecurity policies, assessments, and training, in addition to technical solutions. Fulfilling these additional security requirements will ensure that only legitimate control messages are transmitted on the network and enable a complete forensic analysis in the discovery, response, and remediation stages.

An additional implication will be on smart meters, as they are a key component of the smart grid and require robust authentication mechanisms to reduce the risk of billing fraud. These mechanisms must provide a scalable, efficient, and secure key management solution that can deliver authentication yet also provide ease of key redistribution when a consumer moves between energy suppliers. Security managers and equipment manufacturers should consider how authentication will be implemented in small devices with low computational power, such as the wireless sensors previously mentioned.

It is inevitable that data generated through the smart grid will be shared with third parties for purposes of billing, data mining, vendor diagnostics, usage analysis, and home automation, thus introducing an additional level of complexity concerning privacy and data protection. Therefore, privacy requirements should be considered in line with customer expectations and any applicable legislation.[33]

SERVICE LIFESPAN

Contrasting cybersecurity requirements will also have an impact in the context of CNI service lifespans. Specifically, while cybersecurity in the electricity sector has improved in recent years, and boards are beginning to take it seriously, the sector still lags behind others – such as financial services – by approximately five to seven years.

This lag is partly due to the rigorous testing that new controls and policies undergo to avoid service disruption to critical processes. The disparity in lifespan have an implication on the architecture, as IT professionals today are used to the flexibility of virtualized cloud computing, which can be modified relatively quickly and inexpensively. Conversely, the design of OT architecture patterns requires a longer-term view to provide security-by-design from the outset.

Furthermore, cybersecurity managers express a lack of incentive in their organizations to prioritize cybersecurity requirements over efficiency, as cybersecurity is often viewed as a cost with an immeasurable return on investment.

Therefore, remediating cybersecurity issues inherited from legacy infrastructure often involves huge capital expenditure, and the logistics of maintaining the grid at full capacity, while undertaking such an overhaul, is no easy feat.

As the sector is focused on making profits, reducing costs, and meeting carbon emission targets, the motivation to invest in cybersecurity will remain a low priority until regulation mandates major cybersecurity initiatives.

SHORTAGE OF CYBERSECURITY PROFESSIONALS

One of the key challenges facing all sectors around the globe is the critical shortfall of skilled cybersecurity personnel, as demand consistently outstrips supply.[14] This shortage is frequently exacerbated by a lack of investment in training and the siloed nature of the electricity sector across generation, T&D, and consumer equipment.[15] A 2019 study of cybersecurity employment across multiple sectors showed that organizations with fewer than 500 employees were understaffed in ICS/OT cybersecurity roles.[35]

Organizations with fewer than 5,000 employees report concerns with regard to achieving critical cybersecurity tasks. The key difficulties include: understanding the operational impacts of attacks; low proficiency in discovering, monitoring, and prioritizing assets; and low confidence in the ability to detect, manage, and respond to threats. The electricity sector requires cybersecurity personnel who understand control systems, and these individuals are both scarce and in high demand.

COMPLEX SUPPLY CHAINS

Modernization, privatization, and globalization are continually increasing the attack surface. From connected equipment to new market entrants and multinationals operating across borders, there are more connections into the electricity ecosystem than ever before. Third parties and components present risks through the supply chain, and the onus is on organizations to take responsibility for assuring the security of the components and services that the grid is built upon.[36]

Complex and diverse supply chain ownership across the organization can lead to inefficient pooling of resources, such as supply chain risk intelligence and the ability to thoroughly audit suppliers. Organizations should consider improving governance of supply chain assessments and procurement processes, through standards such as IEC 62443-2-4, to standardize procurement across the organization.[1,37]

Boards are increasingly putting pressure on management to move to the cloud for cost cutting, interoperability, and scalability. Third party software-as-a-service solutions are commonly hosted on the cloud, yet there have been many examples of data breaches due to inadequate security configurations. Therefore, software vendors' and cloud providers' security and privacy policies should be reviewed with care and assessed in accordance with business risk appetite.[1] Cloud providers operate shared responsibility models, which can vary slightly between providers and levels of service. Therefore, organizations should be aware that migration into the cloud does not necessarily remove cyber risk or their cybersecurity responsibilities.

New products and solutions are being developed and marketed to the electricity sector at a rapid pace; therefore, cybersecurity assurance is key when building and expanding CNI. Products that pass software and hardware cybersecurity assurance testing provide a level of confidence that they function as intended and have been tested against a list of known vulnerabilities. In the UK, the Commercial Product Assurance certification scheme developed by the UK National Cyber Security Centre provides security assurance for SMETS2 smart meters.[38] Government-led schemes can be an effective, thorough, and credible mechanism to test and assure the security of components that make up the most critical elements of a nation's infrastructure.

Implementing security updates can be difficult because each Original Equipment Manufacturer must validate patches for each component in the system before they will distribute these to the customer. Furthermore, terms of contract with equipment vendors are typically unique to each plant, making a fleet patch management program very difficult to execute.

While the challenges faced by the electricity sector have limited its progress in terms of cyber maturity, they are not insurmountable. The following section makes recommendations in three key areas – people, process, and technology – and demonstrates the value that collaboration can provide to the entire electricity ecosystem.

RECOMMENDATIONS

> Security, collaboration, regulation, and standards provide opportunities to drive the electricity sector to higher cybersecurity maturity

The following recommendations will support more effective management of the cyber risks facing the electricity sector. The tried and tested structure used below – of people, process, and technology – provides an internal focus on security, while collaboration, regulation, and standards provide opportunities to drive sector-wide cybersecurity maturity.

THE HUMAN FACTOR – IMPROVE SECURITY CULTURE

The cyber-threat against electricity sector organizations from employees - largely unintentional – is greater than that from external actors. Phishing emails are designed to deliver malware into the IT infrastructure and can be extremely effective. The success rate is increasing, primarily because "lots of people become blind to cunning attacks" as attackers continue to create more sophisticated phishing emails and social engineering techniques. A 2020 study found that the number of users who clicked on malicious links in emails rose by 80% from January to April, partly due to the rise of COVID-19 related phishing emails.[39]

Secondly, the majority of employees in electricity organizations do not prioritize cybersecurity. It is important to vet candidates before employment to ensure they have a credible background, and where necessary, it may be prudent to require candidates to undergo a more thorough government vetting process owing to the sector's critical national importance. For this reason, governments may consider forming national teams of OT cybersecurity experts to perform the most sensitive tasks. Ensuring fair working conditions, good employee relations, and a positive culture goes a long way in increasing employee loyalty in the business. Furthermore, organizations can employ user behavior analytics software to detect suspicious user activity on the network.

Cybersecurity and phishing awareness programs are important methods of informing all electricity sector employees of the risks involved. These programs must be delivered to all levels of the organization and promoted by senior leadership to create a security culture. It is imperative that employees feel confident coming forward to report phishing attempts if they believe they may have unwittingly opened a malicious attachment or link.

The cybersecurity culture can be deepened further by providing more in-depth cybersecurity training to relevant personnel who possess unique skills, knowledge, and experience critical to the business. It is much easier to teach cybersecurity to a control engineer than it is to teach a cybersecurity graduate about ICS.[40] Therefore, electricity sector organizations need to develop their existing talent to bridge the skills gap. Training all personnel to even a basic level of cybersecurity can benefit the ecosystem in terms of phishing awareness and data protection.

Providing employees with a new set of skills will not only improve the cybersecurity maturity of the organization but can also lower workforce attrition and improve employee satisfaction. Internal employee development offers an effective and affordable alternative to external recruitment in the midst of the global cybersecurity skills gap.

PROCESS – STRENGTHEN CYBERSECURITY GOVERNANCE

Strong cybersecurity governance provides strategic direction and oversight for all cybersecurity activities within electricity sector organizations and the wider grid. It plays an instrumental role in aligning IT, OT, data security, and physical security programs in order to implement a robust and comprehensive cybersecurity strategy across the ecosystem.[4]

A comprehensive cybersecurity program with well-defined security policies must be supported by senior management from the top down, with a chain of command back to the C-suite to be most effective.[15] Employee acceptance of and compliance with the security policies must be enforced across the organization.

Management should be held accountable for understanding and managing the risks arising from the wider electricity ecosystem and supply chain and take responsibility for the resilience of the organization.[41] Furthermore, consideration should be given to the risks the organization, its culture and its practices present towards the ecosystem, highlighting the critical nature that the infrastructure plays on a national level.

Responsibilities and ownership for OT assets should be delegated and assigned to employees so they can perform a full asset inventory, an assessment of controls, and audits in the future.[15] An adequately funded program can then be designed to protect the most critical assets incorporating people, process, and technology.[1] Going beyond mere compliance is pivotal to developing a robust security program that addresses risks specific to the electricity sector more broadly.[4]

From a regulatory perspective, the Critical Systems Cybersecurity Controls (CSCC) in Saudi Arabia provide a number of measures for identified sensitive systems to guarantee a continuous commitment to enhancinng their security. This complements the Essential Cybersecurity Controls (ECC) by extending the scope of the basic controls to provide additional protection capability when facing heightened levels of cyber risk.[56]

TECHNOLOGY – ENHANCE TECHNICAL PROFICIENCY

There are a range of technical – and technology-focused – solutions being deployed in the electricity sector. Some of these are fundamental security controls designed to isolate or segment legacy infrastructure from the internet, while others offer more advanced threat detection or threat-hunting solutions.

For mature organizations, it is becoming essential to examine attack patterns using a methodolgy to categorize the steps or activities that a threat actor might take while attempting an intrusion. The Mitre ATT&CK Framework[42] and Lockheed Martin Cyber Kill Chain[43] are globally recognized, and, among security professionals, they serve as a starting point for organizations looking to improve their defenses.

Cybersecurity management can introduce various technical measures – as described below – to bolster their cyber defense and resilience.

SECURITY AND RESILIENCE BY DESIGN

Building security and resilience into equipment and infrastructure is crucial because of multi-decade service lifespans

- Install redundant equipment to cope with component failure and enable patching
- Ensure diversity of equipment to avoid a single point of failure
- Maintain an inventory of regularly tested spare equipment
- Design fault-tolerant control systems to prevent dangerous states or total outage
- Build in fail-safe control systems to prevent physical damage or harm
- Use secure software development processes to reduce the risk of inadvertent vulnerabilities
- Choose vendor-supported operating systems which can receive regular security updates
- Secure a source of fuel supply for backup generators in the event of a cyber-related outage

NETWORK SECURITY

Securing and segregating networks will help protect inherently insecure OT infrastructure from cyber-attacks

- Use private networks where feasible to reduce the attack surface
- Use VLANs and encryption
- Use updated and secure versions of network protocols
- Implement strong network access controls
- Ensure secure time synchronization within the network
- Configure firewalls, IDPS, subnets, and access control lists to provide segregation and defense-in-depth
- Physically secure hardware in locked cabinets with adequate access controls to sensitive areas and data centers
- Use data diodes to enforce one-way data transfer when required
- Separate SCADA and Energy Management Systems from the corporate network

CENTRALLY MANAGED CYBERSECURITY POLICIES

Central management provides visibility and control of infrastructure security across the organization

- Apply security patches across IT and OT endpoints on a regular basis
- Deploy endpoint protection solutions and cybersecurity policies to endpoints
- Configure device security settings to remove insecure default configurations
- Perform regular centralized backups of all relevant endpoints
- Prevent the use of mass media storage devices
- Perform audits of access control for OT endpoints
- Use IAM systems to enforce authentication of users and roles
- Ensure all device and user account passwords comply with policy

CYBERSECURITY REGULATION AND STANDARDS

The convergence of IT and OT is blurring the boundaries of safety and cybersecurity in industrial sectors, where security breaches can have both direct and indirect effects on human safety. The development of cybersecurity regulations should be coordinated with safety regulatory bodies to ensure the most effective and comprehensive risk-reducing outcomes.

In addition, projects such as the GCC Interconnector,the proposed Saudi-Egypt electricity link, and future international electricity trading agreements would benefit from a harmonization of regulations and standards between participating states.[44] Removing overlap or contradiction is a key step towards successful regulatory integration.

Internationally recognized standards should be adopted to ensure rigor and promote interoperability between electricity operators. Regulators should periodically review and incorporate the best practices and approved standards. Regulators should also provide organizations with a reasonable timeframe in which to implement these standards.

Ultimately, regulations are only as effective as they are enforceable, but they must also maintain flexibility to adapt to evolving cyber challenges.[14] For example, post-quantum safe encryption standards may need to be adopted to safeguard existing data and protect future communications from quantum computer-based attacks.

Regulators will need to communicate and collaborate closely, both to improve regulatory consistency at the national, regional, and international levels and to increase their adaptability to new risks, technologies, and market opportunities.

COLLABORATE ON CYBERSECURITY

The growth of cyber attacks against the electricity sector has increased the need for national, regional, and global collaboration and threat intelligence sharing. This is made more urgent by the steady convergence of IT and OT, which has created new cybersecurity and safety requirements that are now a high priority for the electricity sector.

The process of countering evolving and sophisticated threats cannot be done in isolation. A robust and mature cybersecurity strategy is increasingly reliant upon close collaboration between major stakeholders, including:[45]

- electricity producers and distributors,
- hardware and software manufacturers,
- cybersecurity researchers and academics,
- governments, and
- regulators.

Collaboration can enable faster and more effective responses to emerging cyber-threats and be conducted in a way that benefits everyone. This can involve sharing information such as vulnerabilities and threat data, as well as internal lessons learned and near misses.[46]

COLLABORATION CHALLENGES

There are several barriers to effective collaboration between the stakeholders above, which organizations in the electricity sector are advised to examine in detail as they explore possibilities for partnership. These include:

GROWING NUMBER OF SECTOR PLAYERS

The electricity sector in many countries has yet to establish a trusted information and threat intelligence sharing platform that encompasses all relevant stakeholders in today's market.

Whereas collaboration has traditionally taken place between a limited number of key established players, the number of stakeholders has now grown. Many of them play important roles in electricity production, distribution, and consumption and would advocate for inclusion in any cybersecurity collaboration. The risk of critical information and threat intelligence being shared outside a trusted group is non-trivial and, if not guarded against rigorously, could compromise sensitive intelligence.

SAFEGUARDING COMMERCIAL SECRETS

Effective collaboration at the national, regional, and international levels is highly dependent on interaction between the public and private sectors.[47] The relationship between public and private sectors varies widely between countries, as do the expectations of (or safeguards against) companies and government officials sharing commercially sensitive information (e.g. as part of an industrial strategy). If threat intelligence and security collaboration are to thrive, strict controls are needed to safeguard commercially sensitive information.[48]

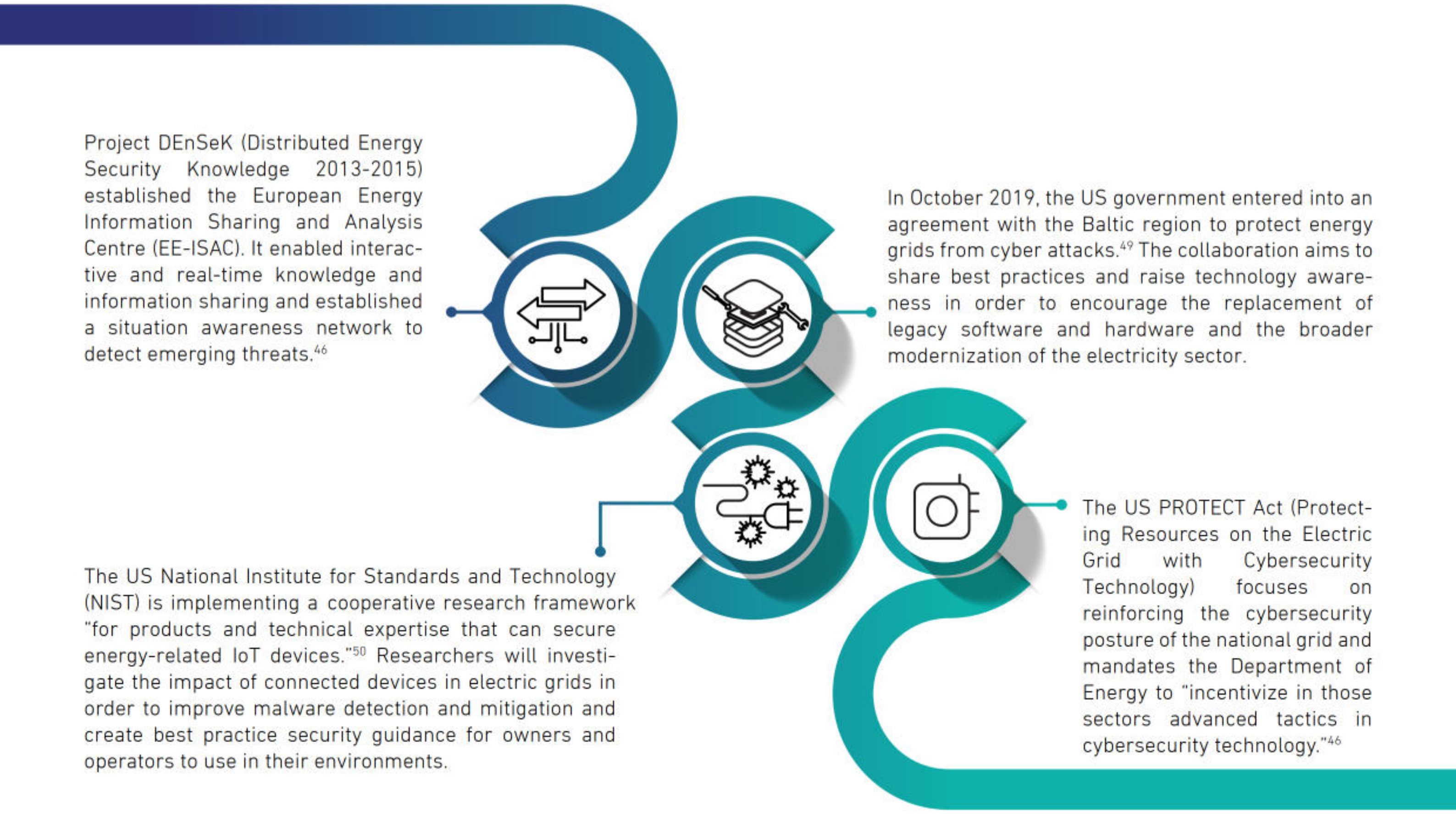
AGREEING ON A COMMON FRAMEWORK

In order to achieve effective collaboration, stakeholders need to have a common framework to structure – and govern – data sharing and analysis. This can include methods, models, languages, representations, and tools, which can be tailored to the specifics of the stakeholders.[47]

Stakeholders need to agree on a common data model design, which can be particularly difficult when each stakeholder advocates for the model that best suits them. This can be a challenging barrier to overcome (not least in the early stages of collaboration), but without a common framework, collaboration is difficult to initiate and even more difficult to sustain.

CYBERSECURITY COLLABORATION EXAMPLES

Despite the challenges and limitations noted above, a number of successful examples have emerged in the electricity sector which pave the way for deeper collaboration. These include:



Project DEnSeK (Distributed Energy Security Knowledge 2013-2015) established the European Energy Information Sharing and Analysis Centre (EE-ISAC). It enabled interactive and real-time knowledge and information sharing and established a situation awareness network to detect emerging threats.[46]

In October 2019, the US government entered into an agreement with the Baltic region to protect energy grids from cyber attacks.[49] The collaboration aims to share best practices and raise technology awareness in order to encourage the replacement of legacy software and hardware and the broader modernization of the electricity sector.

The US National Institute for Standards and Technology (NIST) is implementing a cooperative research framework "for products and technical expertise that can secure energy-related IoT devices."[50] Researchers will investigate the impact of connected devices in electric grids in order to improve malware detection and mitigation and create best practice security guidance for owners and operators to use in their environments.

The US PROTECT Act (Protecting Resources on the Electric Grid with Cybersecurity Technology) focuses on reinforcing the cybersecurity posture of the national grid and mandates the Department of Energy to "incentivize in those sectors advanced tactics in cybersecurity technology."[46]

Cybersecurity collaboration and information sharing in the electricity sector is no longer a luxury; it is an essential component of a mature cybersecurity strategy. Despite the complexity and challenges that an effective collaboration framework faces, the benefits it provides will offer a competitive advantage to those organizations who participate and contribute.

FUTURE TRENDS

> The medium and long-term future of the electricity industry will be characterized by technological innovation and disruption for market participants of all sizes, and it will be essential to consider cybersecurity when developing, procuring, and deploying these new technologies.

The electricity sector is currently undergoing a period of significant evolution, and there are at least two main factors that characterize this change.

NEW PLAYERS, NEW PRIORITIES: A CUSTOMER-FOCUSED APPROACH

At a national level, the electricity industry has traditionally been characterized by a handful of key players who manage the production and distribution of electricity as an output to customers who would sit, largely passively, at the end of the value chain.

Increasingly, we are witnessing a shift from this previously linear process to more complex and dynamic interaction-led relationships, whereby a wider number of agents of different sizes play intrinsic roles. There are two main changes that are influencing these developing relationships.

RISE OF THE PROSUMER

The convergence between IT and OT has played a major role. As this convergence takes place in smart grids, the function of the network has been enhanced insofar as it represents the necessary platform upon which these two can interact. This is being enabled by upgrades to communications infrastructure (especially 5G), which offer the possibility of commercial and technological advances.

These advances will enable customers to play a new role in continuously informing electricity production by permitting real-time information sharing of consumption and, increasingly, electricity generation data. This constant and iterative process aims to improve generation and consumption forecasting and grid efficiency.[51]

As stated above, there are challenges around securely processing this data at source, in transit, and after it arrives at its various destinations. An electricity network that increasingly relies on a telecommunications network introduces a new dependency. Recent concerns over the security of 5G equipment providers have raised questions regarding its suitability for supporting critical national infrastructure.

Ideally, data should be encrypted and digitally signed at source to ensure end-to-end confidentiality and integrity. However, low-powered devices such as sensors and smart meters may not have the computational power or battery reserves to facilitate this. Electricity operators should consider how these distributed assets can be supported to provide the necessary security capabilities.

DISTRIBUTED RENEWABLE INFRASTRUCTURE

The growing societal focus on sustainability – and more broadly, the transition into a low-carbon future – requires cultural change and the commodification of novel power-generating sources. This is driving innovation and investment in the sector in wind and solar generation, smart home technology, and electric vehicles.[51]

Customers are also installing renewable generators and negotiating electricity transmission and bill prices directly. These prosumers are becoming integral parts of the electricity cycle – at the same time both suppliers and consumers. This will ultimately change energy demands by placing a higher focus on customer choices and giving them the ability to become inherent parts of the grid.

These developments notwithstanding, the ability of the prosumer to feed data back into the network presents a new attack surface to be exploited. The variety of communication devices that transmit data between prosumer generation equipment and electricity network operators could contain vulnerabilities. These could then be exploited to damage or misconfigure generation equipment or allow attackers to access prosumers' personal devices on their home networks.

Similarly, attackers could use communication devices to send malicious commands back to the electricity network. Regulators should seek to enforce a level of software and hardware assurance over devices which facilitate two-way communications with the electricity network, as already exists with the CPA of SMETS2 smart meters.

These two changes will play a crucial role in the evolution of the electricity industry, as they create "the opportunity to access consumer intelligence at the edge of the electric power network, enabling distributed, individual agents to transact and coordinate their plans and actions."[52]

Utility companies and national entities will inevitably have to update their business models and resilience strategies to incorporate distributed energy generation, develop network resilience against power outages, and protect the data being created and shared by new players.

TECHNOLOGY INNOVATION

New technologies promise to enhance the electricity generation and consumption cycle and the marketplace. Digital transformation across the sector will continue to connect systems and organizations, leading to new and more complex cybersecurity challenges. These innovations include:

IOT STANDARDIZATION

The standardization of infrastructure, data formats, and advanced programming interfaces (APIs) used by Internet of Things (IoT) devices aims to overcome interoperability issues that limit the potential for automation and efficiency in the sector. Remote sensing and monitoring, fault detection in wires, automated fault repair, and smart home equipment could benefit from a new degree of interoperability.[53] Smart devices in the home and in industry will be able to respond autonomously to market price fluctuations, thus enabling previously impossible levels of market efficiency.

OPEN SOURCE CODE VULNERABILITIES

Standardization can increase security as software developers can use open source code libraries instead of attempting to implement custom interfaces. Conversely, vulnerabilities in widely used shared code libraries can expose a large number of systems to cyber-attacks. Developers should adopt a secure software development lifecycle and conduct static and dynamic analysis on codebases to identify and remove potential vulnerabilities.

ARTIFICIAL INTELLIGENCE ATTACKS

Machine learning and artificial intelligence will be used in localized micro-grids to improve operational efficiency, ensure resilient connection to larger traditional grids, and maximise currently limited autonomous capabilities.[54] This includes micro-grids in rural and remote areas, or in sensitive places like hospitals and prisons. However, it is possible that an advanced adversary could use machine learning modeling data to conduct a slow, sophisticated attack in which the grid would enter a critical state. Such an attack would be very difficult to detect. Standardization can increase security as software developers can use shared code libraries instead of attempting to implement custom interfaces. Conversely, vulnerabilities in widely used open source code libraries can expose a large number of systems to attack. Developers should adopt a secure software development lifecycle and conduct static and dynamic analysis on codebases to identify and remove potential vulnerabilities.

BLOCKCHAIN RESILIENCE

Blockchain technology is being trialed in the electricity sector to enable different actors to trade with each other to support peer-to-peer trading platforms so that customers and suppliers can transact confidently in wholesale markets. There is the potential for this trading to improve market efficiency, given that local prices by commercial utility companies can be higher than alternatives offered by renewable sources.[55]

Future developments in quantum computing may provide attackers with the means to forge digital signatures of other users. This could allow attackers to violate the integrity of the blockchain by modifying transaction history and taking ownership of digital assets belonging to others. As a result, it would not be possible to gain a true view of the market. Blockchain developers should consider implementing quantum-resistant cryptographic algorithms to futureproof markets against this type of cyber-attack.

The medium- long-term future of the electricity industry will be characterized by technological innovation and disruption for market participants of all sizes, and it will be essential to consider cybersecurity when developing, procuring, and deploying these new technologies.

CONCLUSION

> “This report aims to help the electricity sector strengthen cyber defenses and manage cyber risks more effectively – both today and in the future.”

The English author L.P. Hartley once observed that ‘the past is another country, they do things differently there.’ This holds true for the electricity sector, where recent decades have seen immense change and growth.

Many readers of this report will be able to easily identify the differences between the past and today – for example, electrification stretching to the remotest corners of the globe, the growth of alternative energy sources, and the modern world’s complete reliance on electricity – including the electricity that powers the laptop or smartphone you are using to read this report.

Along with these changes come new risks – in particular, cyber risks affecting the electricity sector. Some of these risks relate to threat actors and malicious software, while others relate to legacy infrastructure, complex supply chains, contradictory regulations, or inadequate governance. While the implications of these risks are clear, others – such as the likelihood of catastrophic cyber-attacks – are harder to identify.

Many tools are available to manage these risks, and much can be accomplished by consistently applying the fundamentals of cyber security to the electricity sector, along with crafting clear and consistent regulation that can provide a foundation for future growth.

In many ways, this future is also another country – full of opportunity and promise, but also opaque, shifting, and yet to be clearly defined. It is our hope that the perspectives and recommendations outlined in this report will help the electricity sector to strengthen its cyber defenses and manage cyber risks more effectively – both today and in the future.

REFERENCES

Contributors

LEAD AUTHOR

National Cybersecurity Authority	Kingdom of Saudi Arabia

The National Cybersecurity Authority thanks the following individuals for participating in discussions, interviews, and questionnaires that contributed to the development of this report.

INDIVIDUAL CONTRIBUTORS

Ivan Dragnev	Cyber Security Principal Technical Lead Europe, EPRI, Spain
Laurent Hausermann	Co-founder, Sentryo, France
Sandeep Pathania	OT Cybersecurity Expert, France
Ian Speller	Director of Security, SmartDCC, UK
Jonathan Tubb	Lead Cyber Business Developer, Siemens, USA

INDUSTRY CONTRIBUTORS

Electricity & Cogeneration Regulatory Authority (ECRA)	Kingdom of Saudi Arabia
Marafiq	Kingdom of Saudi Arabia
Saudi Electricity Company	Kingdom of Saudi Arabia
Saudi Information Technology Company (SITE)	Kingdom of Saudi Arabia
Deloitte	Deloitte supported the production of this report by contributing primary and secondary research.

[1] Livingston, S., Sanborn S., Slaughter, A., Zonneveld P. (2019) "Managing Cyber Risk in the Electric Power Sector", Deloitte Insights. https://www2.deloitte.com/insights/us/en/industry/power-and-utilities/cyber-risk-electric-powersector.html

[2] BP (2019), 'Statistical Review of World Energy 2019 | 68th Edition'. https://www.bp.com/content/dam/bp/business-sites/en/global/corporate/pdfs/energy-economics/statistical-review/bp-stats-review-2019-full-report.pdf

[3] Export.gov (2018), "Saudi Arabia Country Commercial Guide – Power". https://www.export.gov/article?id=Saudi-Arabia-Power

[4] World Economic Forum (2019) "Cyber Resilience in the Electricity Ecosystem: Principles and Guidance for Boards", Centre for Cybersecurity and Electricity Industry Community. http://www3.weforum.org/docs/WEF_Cyber_Resilience_in_the_Electricity_Ecosystem.pdf

[5] King Abdullah City for Atomic and Renewable Energy (2020) "The National Atomic Energy Project". https://www.energy.gov.sa/ar/snaep/Pages/ov.aspx

[6] Thomas, B. (2019) "Cyber-Attack on Indian Nuclear Power Plant Exposes Threat of 'Snooping' Malware", BitSight. https://www.bitsight.com/blog/cyber-attack-on-indian-nuclear-power-plant-exposes-threat-of-snooping-malware

[7] Dragos (2017) "Crashoverride: Analyzing the Threat of Electric Grid Operations". https://www.dragos.com/wp-content/uploads/CrashOverride-01.pdf

[8] US-CERT (2016) "Cyber-Attack Against Ukrainian Critical Infrastructure". https://www.us-cert.gov/ics/alerts/IR-ALERT-H-16-056-01

[9] European Parliament Think Tank (2016) "Electricity Prosumers", European Parliament Think Tank. http://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI(2016)593518

[10] Almakrami, H. (2016) "Intrusion Detection System for Smart Meters", Saudi Arabia Smart Grid. https://ieeexplore.ieee.org/document/7849674

[11] Sardana V., Shehhi H. I. A. (2017) "Securing Abu Dhabi's electricity grid from cyber attacks: Cost effective approach to hardening of substation control and monitoring systems", International Conference on Electrical and Computing Technologies and Applications. https://ieeexplore.ieee.org/document/8251926

[12] Liu, J., Xiao, Y., Liang, W., Chen, C. L. P. (2012) "Cyber Security and Privacy Issues in Smart Grids", Institute of Electrical and Electronics Engineers, 14:4. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.462.4054&rep=rep1&type=pdf

[13] Poresky C., Andreades C., Kendrick J. C., Peterson P. F. (2017) "Cyber Security in Nuclear Power Plants: Insights for Advanced Nuclear Technologies", Center for Long-Term Cybersecurity UC Berkeley. http://fhr.nuc.berkeley.edu/wp-content/uploads/2017/09/TH-Report-UCBTH-17-004.pdf

[14] US Government Accountability Office (2019) "Critical Infrastructure Protection: Actions needed to address significant cybersecurity risk facing the electric grid", GAO Highlights. https://www.gao.gov/assets/710/701079.pdf

[15] Siemens, Ponemon Institute (2019) "Caught in the Crosshairs: Are Utilities Keeping Up with the Industrial Cyber Threat?", Siemens. https://assets.new.siemens.com/siemens/assets/api/uuid:35089d45-e1c2-4b8b-b4e9-7ce8cae81eaa/version:1572434569/siemens-cybersecurity.pdf

[16] Deloitte (2018) "Analysis of internal data".

[17] Deloitte (2019) "Managing Cyber Risk in the Electric Power Sector", Deloitte. https://www2.deloitte.com/us/en/insights/industry/power-and-utilities/cyber-risk-electric-power-sector.html

[18] US-CERT (2018) "Alert (TA18-149A)", US CERT. https://www.us-cert.gov/ncas/alerts/TA18-149A

[19] KasperskyLab (2018) "From Shamoon to Stonedrill", Kaspersky. https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07180722/Report_Shamoon_StoneDrill_final.pdf

[20] F-Secure (2020) “Backdoor:W32/Havex”, F-Secure. https://www.f-secure.com/v-descs/backdoor_w32_havex.shtml

[21] Trendmicro (2014) “HAVEX Targets Industrial Control Systems”, Trendmicro. https://www.trendmicro.com/vinfo/us/threat-encyclopedia/web-attack/139/havex-targets-industrial-control-systems

[22] Kaspersky (2019) “Threat Landscape for Industrial Automation Systems H1 2019”, Kaspersky. https://ics-cert.kaspersky.com/media/H1_2019_kaspersky_ICS_REPORT_EN.pdf

[23] Leyden, J. (2016) “Water treatment plant hacked, chemical mix changed for tap supplies”, The Register. https://www.theregister.co.uk/2016/03/24/water_utility_hacked/

[24] O’Donnell, L. (2019) “Ransomware Behind Norsk Hydro Attack Takes On Wiper-Like Capabilities“, ThreatPost. https://threatpost.com/lockergoga-ransomware-norsk-hydro-wiper/143181/

[25] Findlay, S., White, E. (2019) “India confirms cyber attack on nuclear power plant “, Financial Times. https://www.ft.com/content/e43a5084-fbbb-11e9-a354-36acbbb0d9b6

[26] 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

[27] Clowes, Ed (2020), “Hackers who hit grid taunt Elexon with dark web files”, The Telegraph. https://www.telegraph.co.uk/business/2020/06/07/hackers-hit-grid-taunt-elexon-dark-web-files/

[28] Hayden, E. (2019) “An Abbreviated History of Automation & Industrial Controls System and Cybersecurity”, SANS Institute. https://www.sans.org/reading-room/whitepapers/physical/abbreviated-history-automation-industrial-controls-system-cybersecurity-35697

[29] Rafat R., McLorn W. G., Tural T., Hassan A., Sheikh A. (2016) “Addressing cyber security for the oil, gas and energy sector”, 2016 Saudi Arabia Smart Grid (SASG) Conference. https://ieeexplore.ieee.org/document/7849685

[30] Partz, H. (2018) “Crypto Farm With 6000 Miners Shut Down in Russia For Overdue Electricity Bill”, Cointelegraph. https://cointelegraph.com/news/crypto-farm-with-6000-miners-shut-down-in-russia-for-overdue-electricity-bill.

[31] Slowik, Joe (2019), “CRASHOVERRIDE: Reassessing the 2016 Ukraine Electric Power Event as a Protection-Focused Attack”, Dragos. https://dragos.com/wp-content/uploads/CRASHOVERRIDE.pdf

[32] Carbon Black (2019) “How to Combat Island Hopping”, Carbon Black. https://www.carbonblack.com/resource/how-to-combat-island-hopping-ebook/

[33] Yan Y., Qian Y., Sharif H., Tipper D. (2013) “A survey on smart grid communication infrastructures: Motivations, requirements and challenges”, Institute of Electrical and Electronics Engineers, 15(1):5-20. https://ieeexplore.ieee.org/document/6157575

[34] Council of European Energy Regulators (2018) “CEER Cybersecurity Report on Europe’s Electricity and Gas Sectors”, Council of European Energy Regulators. https://www.ceer.eu/documents/104400/-/-/684d4504-b53e-aa46-c7ca-949a3d296124

[35] (ISC)2 (2019), “(ISC)2 Cybersecurity Workforce Study – Strategies for Building and Growing Strong Cybersecurity Teams”. https://www.isc2.org/-/media/ISC2/Research/2019-Cybersecurity-Workforce-Study/ISC2-Cybersecurity-Workforce-Study-2019.ashx?la=en&hash=1827084508A24DD75C60655E243EAC59ECDD4482

[36] Nodar, T. (2019) “Michael Chertoff on OT cybersecurity in the utilities industry”, The Cyberwire. https://thecyberwire.com/events/Michael-Chertoff-on-OT-cybersecurity-in-the-utilities-industry.html

[37] Sardana V., Al Shehhi H. A. (2017) “Securing Abu Dhabi’s electricity grid from cyber attacks: Cost effective approach to hardening of substation control and monitoring systems”, International Conference on Electrical and Computing Technologies and Applications, 1-5. https://ieeexplore.ieee.org/document/8251926

[38] National Cyber Security Centre UK (2019) “Commercial Product Assurance (CPA)”, National Cyber Security Centre. https://www.ncsc.gov.uk/information/commercial-product-assurance-cpa

[39] Mimecast (2020) “Threat Intelligence: Awareness Training Reduces Unsafe Clicks Amid Coronavirus Cyber Threats”. https://www.mimecast.com/blog/2020/04/threat-intelligence-briefing-security-awareness-training-reduces-unsafe-clicks-amid-surging-coronavirus-cyber-threats/

[40] The CyberWire (2019) “Interview with Robert M. Lee, CEO at Dragos”.

[41] Community El. (2019) “Cyber Resilience in the Electricity Ecosystem: Principles and Guidance for Boards In collaboration with Boston Consulting Group”, World Economic Forum. http://www3.weforum.org/docs/WEF_Cyber_Resilience_in_the_Electricity_Ecosystem.pdf

[42] MITRE (2019), “ATT&CK for Enterprise”, MITRE. https://attack.mitre.org/resources/enterprise-introduction/

[43] Hutchins, M. E., Cloppert J. M., Amin N. R. (2011) “Intelligence – Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains”, Lockheed Martin Corporation. https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf

[44] Wogan, D., Pradhan S., Albardi, S. (2017) “GCC Energy System Overview”, King Abdullah Petroleum Studies and Research Center. https://www.kapsarc.org/research/publications/gcc-energy-system-overview-2017/

[45] Leszczyna, R., Wrobel, R. M. (2014) “Security Information Sharing for Smart Grids”, 9th International Conference for Internet Technology and Secured Transactions. https://www.researchgate.net/publication/282255776_Security_information_sharing_for_smart_grids_Developing_the_right_data_model

[46] McGuire Woods LLP (2019) “PROTECT Act seeks to bolster domestic electric grid cybersecurity”, Lexology. https://www.lexology.com/library/detail.aspx?g=1a655017-2599-436e-80a2-29aabc9bee5d

[47] Baker, S., Schneck P. (2011) “In the Dark: Critical Industries Confront Cyberattacks”, CSIS. https://csrc.nist.gov/CSRC/media/Events/ISPAB-JULY-2011-MEETING/documents/Jul14_CIP-CSIS-2011-ISPAB.pdf

[48] Lam, J. (2016) “IIET – Cyber security in modern power systems – Protecting large and complex networks”, Institution of Engineering and Technology. https://ieeexplore.ieee.org/document/7835821

[49] Euractiv with AFP, (2019) “US to help secure Baltic energy grid against cyber-attacks”, Euractiv. https://www.euractiv.com/section/energy/news/us-to-help-secure-baltic-energy-grid-against-cyber-attacks/

[50] Johnson, B. D. (2019) “NIST looking for partners to secure energy IoT”, FWC – Federal Computer Week. https://fcw.com/articles/2019/10/07/nist-energy-cyber-johnson.aspx

[51] Energy Networks Association (2018), “Electricity Network Innovation Strategy”, Energy Networks Association. http://www.energynetworks.org/assets/files/electricity/futures/network_innovation/electricity_network_innovation_strategy/Energy%20Networks%20Association%20-%20Electricity%20Network%20Innovation%20Strategy-March%202018.pdf

[52] Kiesling, L. (2010) “Promoting innovation in the electricity industry” in Economic Affairs, 30(2):6-12. https://www.researchgate.net/publication/227670308_Promoting_innovation_in_the_electricity_industry

[53] ENISA (2016) “NCSS Good Practice Guide: Designing and implementing national cybersecurity strategies”, European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications/ncss-good-practice-guide

[54] Ellsmoor, J. (2018) “6 Renewable Energy Trends To Watch in 2019”, Forbes. http://www.forbes.com/sites/jamesellsmoor/2018/12/30/6-renewable-energy-trends-to-watch-in-2019/#7e04f5454a1f

[55] Organization for Economic Co-operation and Development (2018) “A Chain Reaction: Disruptive Innovation in the Electricity Sector”, Organization for Economic Co-operation and Development. https://www.oecd.org/competition/A-chain-reaction-disruptive-innovation-in-the-electricity-sector.pdf

[56] National Cybersecurity Authority. www.nca.gov.sa