Commentary

Recent Developments and Trends in Cybersecurity in the Power Sector

Ahmed A. Albalawi¹, Frank A. Felder¹, Muhammad Khurram Khan²

¹ KAPSARC
² Center of Excellence in Information Assurance, King Saud University, Riyadh, Saudi Arabia

October 24, 2023 | KS–2023-CO28
About KAPSARC

KAPSARC is an advisory think tank within global energy economics and sustainability providing advisory services to entities and authorities in the Saudi energy sector to advance Saudi Arabia’s energy sector and inform global policies through evidence-based advice and applied research.

This publication is also available in Arabic.

Legal Notice

© Copyright 2023 King Abdullah Petroleum Studies and Research Center ("KAPSARC"). This Document (and any information, data or materials contained therein) (the "Document") shall not be used without the proper attribution to KAPSARC. The Document shall not be reproduced, in whole or in part, without the written permission of KAPSARC. KAPSARC makes no warranty, representation or undertaking whether expressed or implied, nor does it assume any legal liability, whether direct or indirect, or responsibility for the accuracy, completeness, or usefulness of any information that is contained in the Document. Nothing in the Document constitutes or shall be implied to constitute advice, recommendation or option. The views and opinions expressed in this publication are those of the authors and do not necessarily reflect the official views or position of KAPSARC.
Introduction

The power sector is a crucial component of critical national infrastructure, and its continuous and resilient operation underpins the socioeconomic prosperity of any nation. Energy security is a priority in many regions of the world, as it is essential for economic growth and prosperity. As the power sector undergoes a rapid digital transformation, the companies involved in electricity generation, transmission, distribution, and related services are becoming more susceptible to cyberattacks. The power sector is particularly vulnerable to disruptions in energy supply because electricity cannot be easily stored; thus, it must be generated and consumed in real time. Cyberattacks can have a significant impact on the availability of electricity, which can have a ripple effect on the economy and society as a whole and quickly lead to widespread blackouts. This commentary examines some recent developments of and trends in cybersecurity in the power sector. It also examines challenges and solutions that may help policymakers and organizations improve their cybersecurity posture against evolving cyber risks and threats.
Cybersecurity Drivers in the Power Sector

In the power system, cybersecurity is growing in importance with the ongoing transition to smart grids and the increase in electrification of other sectors. The power sector underpins all other sectors, and the consequences of cyberattacks on energy infrastructure extend to other key infrastructures. Therefore, it is essential to address all potential threats and risks that the power system could face. The electricity grid was built over the decades, with a focus on reliability and safety, but this assumption has now changed, and cybersecurity is becoming an integral component of the all-infrastructure ecosystem, not just energy.

Millions of daily cyberattacks on energy infrastructure occur with increasing sophistication and a rising magnitude and severity (James et al. 2019). Cyberattackers range from thrill-seekers to nation-states. Critical infrastructure organizations, such as the power industry, are particularly vulnerable to ransomware attacks because they are essential for the functioning of society. Ransomware attacks on the power industry could have a significant impact on the economy and public safety, and they are becoming a global cybersecurity challenge for individuals, organizations, and nations.

Moreover, decarbonizing the grid as part of the clean energy transition is resulting in increased distributed generation resources and connected devices such as rooftop photovoltaics (PVs) and smart appliances (Everhart et al. 2020). Each connected device is a potential access point for cyberattackers and, therefore, a point of vulnerability. These devices are connected to an already large and complex electricity grid (see Figure 1).

In Saudi Arabia, as of 2021, 671 generation units fed into 91,749 ckt. km of transmission lines connected to 741,713 ckt. km of the distribution network to serve over 10.5 million customers (Water & Electricity Regulatory Authority 2023). In addition, substations, smart meters, and different instruments are distributed across the system. To add to this complexity, the digital transformation is expected to shape the future operations of utilities, including an enhanced use of data, two-way communication, and automation.
Figure 1. Overview of the electric power system and control communications. The applications and typical communication interfaces illustrate the complexity of control and data exchanges across the network. The data include information such as voltage levels, frequencies, active and reactive power, the positions of switchgears at every busbar, signals and alarms, load frequency control and the automatic voltage regulation set point, remote commands, and power generation reduction commands (Torres 2013). Note: RCC is the regional control center, NCC is the national control center, and RTU is a remote terminal unit.
Cybersecurity Risks in the Power Sector

Cybersecurity for information technology (IT)\(^1\) systems has been addressed for many years. However, the cybersecurity of industrial control systems (ICSs)\(^2\) and operational technology (OT)\(^3\) networks is a relatively new challenge facing the energy and power sectors (Saunders, Bronk, and Bazilian 2022). Attacks on ICSs and OT networks can lead to physical damage that extends to large parts of infrastructure and the population. In 2015, a major cyberattack on the Ukrainian power grid by Russian operators led to the shutdown of 30 substations, which in turn caused power losses to 200,000 customers (Saunders, Bronk, and Bazilian 2022). The attackers were able to steal credentials for the ICS and infiltrate the system. The 2021 Colonial Pipeline Company ransomware incident, in which attackers managed to shut down a pipeline responsible for 45% of the gas and diesel delivery to the East Coast of the United States, is another example of an attack that can have severe physical implications. Although the attack did not target end customers, it led to fuel shortages and a state of emergency. Similar attacks could target the fuel supply of the power sector.

Malware can infiltrate the system through any connected device, and its impact can vary depending on both its intended and unintended objectives. Some malware threats include manipulating the emergency system to prevent alarms, controlling circuit breakers, stealing information, controlling hardware, exfiltrating sensitive data, and giving remote access to outside parties. Malware can affect the system through any connected device, including emerging technologies not traditionally part of the grid, such as electric vehicles, smart meters, and roof top solar units. It is essential to secure any vulnerabilities in the system with adequate control and measures. Legacy infrastructure and supply chains are two critical areas of concern that are more susceptible to cyberattacks.

Legacy infrastructure can be found everywhere in the network. It involves equipment that was designed with legacy ICSs and focuses on their availability and safety. Legacy infrastructure includes some equipment that is more than 40 years old and still operational and functioning. However, having advanced two-way communication systems and interoperability means that these systems may become a point of vulnerability to

---

\(^1\) Information technology (IT) refers to systems and technologies that are used to store, manage, and exchange information.

\(^2\) Industrial control systems (ICSs) are a subset of OT systems that are used to control critical infrastructure, such as power grids.

\(^3\) Operational technology (OT) refers to systems and technologies that are used to control and monitor physical processes.
cyberattacks. This is especially a concern for remote assets such as distribution network endpoints where IT software updates must be physically performed on-site. Financial and logistical challenges can make it difficult to ensure that software updates are timely, especially for remote villages and large territories. In the 2016 cyberattack against Ukraine’s power system, the vulnerability was in four unpatched digital protective relays (Slowik 2019). A patch is a piece of software that is designed to fix a security vulnerability. If software is unpatched, then it has not been updated with the latest patches, and therefore, its vulnerabilities can be exploited by attackers.

Not all cyberattacks are launched on operational infrastructure. The supply chain for the modern grid includes multiple players, from equipment manufacturers to software and service suppliers. Each of these players has a role in securing the grid, but they also represent potential points of vulnerability. Compromising physical hardware in the supply chain is one way of obtaining stealth access to the OT system once that hardware is installed. In many instances, these hardware devices are well-known off-the-shelf products, such as solar PV inverters, and attackers may easily have access to them to test their malware. Furthermore, many devices are provided by third-party small and medium-size enterprises that can be exploited through cyberattacks or social engineering⁴, thus giving the attacker backdoor access to a large utility. Indeed, supply chain integrity is a challenge for the modern grid.

⁴ Social engineering in this context is a type of cyberattack that relies on human interaction to trick victims into revealing sensitive information or taking actions that harm their security, for example, phishing emails.
Costs of Cyberattacks on the Power Sector

The costs of cyberattacks on the power sector can be significant in terms of both direct and indirect costs. It is important for power companies to take steps to protect themselves from these attacks, as the costs of a successful attack can be devastating in terms of both service to consumers and revenue. Estimating the cost of cyberattacks on the power sector is very complicated. Cyberattacks vary by nature and differ in their intentions, and the costs will ultimately depend on the damage incurred due to the cyberattack. Cyberattacks can be stealthy and difficult to detect until after they have already breached data or caused damage. Additionally, infiltrated companies or systems may not disclose the facts and details of cyber incidents. Some studies have attempted to estimate the cost of cyberattacks from different perspectives.

Researchers conducted a comprehensive study of the financial impact of data breaches on over 500 organizations worldwide (IBM Security and Ponemon Institute 2022). The report, which was published by IBM Security and the Ponemon Institute, found that the average cost of a data breach in the energy sector was $4.72 million. This cost is an increase of 1.5% from the previous year. Another study estimated that the average annualized cost of cybercrime against utilities was $17 million (Ponemon Institute 2017). In terms of utility investment to safeguard against cyberattacks, utilities in the U.S. are increasingly investing in technology and infrastructure cybersecurity. In 2019, Duke Energy estimated that it would invest $137 million in capital over three and a half years as part of its cybersecurity IT-OT across the corporation’s six utility operating companies (FERC 2019). In the same year, Ameren Corp. in Missouri proposed an investment of $448 million in technology and cybersecurity as part of its five-year capital investment program (James et al. 2019).

Dealing with the consequences of detected cyberattacks is part of the indirect costs of cyberattacks. The cost of remediation includes the cost of restoring data, repairing systems, and hiring experts to help with the remediation process. Security upgrades are another aspect of the aftermath costs. For example, in 2011, a Stuxnet attack successfully damaged Iran’s nuclear facilities (Kushner 2013). This incident demonstrated that a cyberattack can lead to major infrastructure damage. Many organizations have implemented security upgrades to improve their resilience to cyberattacks in response to the Stuxnet attack. These upgrades have included implementing new security software, strengthening network security, and improving employee training with regard to cybersecurity (Burton 2022).
Response to Cybersecurity

Although the digital transformation of the power sector presents some challenges, it offers a wide range of solutions from emerging technologies that enable utilities to collect, process, analyze, and share data with high precision and accuracy. Artificial intelligence (AI) technologies, for example, can allow cyberdefenders to detect changes in configuration, anomalies, and tampering (Hollern 2022). Cybersecurity defense products, solutions and service capabilities can be costly but are essential due to the criticality and dependence of other critical infrastructure on power and electrical grids.

Responding to a high-impact cyberattack requires a coordinated technical, tactical, operational, and logistical effort between all stakeholders within the power system, including policymakers, regulators, and utilities. This effort is part of grid resilience, which addresses the impacts of low-probability, high-consequence events and how best to respond to them. Resilience has been defined by the Federal Energy Regulatory Commission (FERC) as “the ability to withstand and reduce the magnitude and/or duration of disruptive events, which includes the capability to anticipate, absorb, adapt to, and/or rapidly recover from such an event”. Additionally, the European Union (EU) defines resilience as “a critical entity’s ability to prevent, protect against, respond to, resist, mitigate, absorb, accommodate and recover from an incident”. All definitions reflect a holistic approach to addressing dynamic and impactful risks by anticipating, withstanding, recovering from, and adapting to various threats. Traditionally, these definitions were linked to power system physical assets (generation, transmission, and distribution). However, the digitalization of the power sector means that cyber resilience is integral to understanding what the power system should be resilient to. In its Enhancing Cyber Resilience in Electricity Systems report, the International Energy Agency (IEA) recommends a cyber resilience approach to develop policies that articulate the particularities of the electricity system and fully address the purpose, scope and methodology for application. The approach consists of institutionalizing responsibilities and incentives, identifying risks, managing and mitigating risks, monitoring progress, and responding to and recovering from disruptions (Haesen et al. 2021).

The cybersecurity aspect of grid resilience is addressed in different ways. Some countries take a risk-based approach in which assets are evaluated against potential threats and appropriate controls are recommended to protect them. Others take a perspective approach, where procedures and controls are recommended as a means of early intervention to protect the system (National Cybersecurity Authority 2020). In both approaches, the key to successfully implementing cybersecurity measures is enforcing regulations and ensuring compliance. Doing so may require regulators to implement an incentive scheme to encourage utilities to invest in state-of-the-art cyber measures.

Beyond technology, the human factor plays an important role. The skill gap in this specialty is a critical challenge. Having people who understand OT and are also cyber experts requires targeted training programs. The OT systems in the power sector are critical and must react immediately to any changes in the system. Additionally, personnel such as technicians, field engineers, procurement specialists, and managers need to understand the cybersecurity issues that could arise and what measures are put in place to address them. The challenge also extends to senior...
management and decision-makers, education about the value of cybersecurity can significantly accelerate its implementation. The rapid development of emerging digital technologies such as the Internet of Things, AI, and machine learning further exacerbates the skill gap. Sophisticated products are programmed and engineered to work with live data and running systems, and if these solutions are developed in isolation from the field workers who are going to use them, then this development will create an additional concern for their use and security. Indeed, there has been a response to this demand by schools and organizations, which started offering specialized training. For example, at the senior level, a program for a chief digital officer (CDO) would prepare executives to lead the digital transformation of an organization. Cybersecurity is embedded in the digital transformation of the organization by ensuring that security is a top priority for everyone. Training at all levels for nonspecialists is necessary to increase awareness of the risks and to promote good security habits and practices.
Regulatory Aspects of Cybersecurity

For a utility, cybersecurity defense must start with an asset inventory with detailed physical and digital asset identification. An assessment of the security monitoring and controls of these assets can help inform the current vulnerabilities in the system and the necessary actions. Such an assessment includes reviewing and managing vendor and third-party access. The implementation of system-wide security also needs to incorporate workforce awareness, training and upskilling. Furthermore, documentation and reporting of cyber events must be conducted as part of the response and recovery plan.

For regulators and policymakers, a clear framework for cybersecurity with defined responsibilities should be developed with the objective of increasing the flow of information while preserving the privacy of customers. Information sharing between different stakeholders enhances situational awareness and helps standardize defense mechanisms, which in turn helps reduce costs and improve performance. In January 2023, the FERC directed the North American Electric Reliability Corporation (NERC) to develop internal network security monitoring standards, which are a set of cybersecurity requirements for critical infrastructure organizations to help detect and respond to malicious activity within their internal networks (Federal Energy Regulatory Commission 2023). The forthcoming standards will address concerns of supply chain vulnerability by enabling visibility of network traffic between connected devices. A month earlier, in December 2022, the EU issued a directive on the cybersecurity of network and information systems (NIS2), which updates and replaces the NIS Directive. This directive requires EU member states to strengthen their cybersecurity capabilities, and it introduces cybersecurity risk management measures and reporting in critical sectors, along with rules on cooperation, information sharing, supervision and enforcement (European Union (EU) 2022).

Additionally, incentivizing cybersecurity investments might be necessary. The collection and analysis of cyber events can generate insights for all stakeholders. Regulators should also audit the performance of utilities against developed cybersecurity performance criteria. The cost of cybersecurity measures, as well as their value, needs to be assessed to set a cost recovery mechanism for utilities. Finally, it is essential to have uniform expectations and standards for cybersecurity architecture requirements and language across the sector to avoid any ambiguity in planning and documentation.

The government of Saudi Arabia has established the National Cybersecurity Authority (NCA) to be the government entity in charge of cybersecurity for IT and OT. As part of its role in regulating and protecting the Kingdom’s cyberspace, it has issued multiple cybersecurity controls and guidelines, including controls for OT and critical national infrastructure. Power sector regulators must have continuous communication between utilities and relevant stakeholders to ensure alignment with regard to all challenges and solutions.
Recommendations

The power sector requires multilateral efforts for the prevention of, mitigation of, preparedness for, response to, and recovery from cyber risks, which can jeopardize the socioeconomic prosperity of a country. The following high-level recommendations may help policymakers improve the cybersecurity posture of the power sector:

- Establish a Public–Private Advisory Council on Power Sector Cybersecurity: Creating a high-level advisory council composed of diversified stakeholders would allow the power sector to oversee and promote strategic oversight and cooperation among all stakeholders for a cyber-resilient ecosystem.

- Develop and Update Regulations, Frameworks, and Guidelines for Power Sector Cybersecurity: For a secure, reliable, and resilient power sector, it is recommended to build regulatory frameworks and cybersecurity guidelines for public and private sector organizations engaged in the generation, transmission, and distribution of electricity. Additionally, the regulations should include a wider range of organizations, such as cloud service providers and operators of critical information infrastructures.

- Human Capital and Skills Development: The unprecedented demand for cybersecurity skills has created a global shortage of cybersecurity human capital. To balance the supply and demand for the right skillset, cybersecurity workforce development is a major challenge for countries worldwide. Through local educational and training institutions, critical infrastructure sectors such as the power sector must build the capacity and capability necessary for addressing cybersecurity challenges.

- Cooperation for Information Sharing, Benchmarking, and Best Practices: Due to technological interdependence, it is imperative to build protocols and processes for benchmarking, information sharing, and lessons learned with national, regional, and international partners to limit and contain the impact of cyberattacks on the national power sector.
Concluding Remarks

Cybersecurity poses a constant and substantial challenge to the power sector. Cyberattacks regularly threaten critical infrastructure, which can seriously undermine national security and the economy. Companies are increasingly vulnerable to cyberattacks due to the rapid digital transformation of the industry, legacy infrastructure, and supply chain vulnerabilities. Cyberattacks, such as ransomware and distributed denial of service attacks, may provide hackers access to crucial operational components in the power sector, causing disruptions in business operations and jeopardizing the lives of people through physical harm. Therefore, the power sector must take adequate technical, operational, and organizational measures to manage risks to the security of the networks, information, and operational systems that they use for business operations or service delivery and to prevent or lessen the impact of cascading effects due to cyber incidents. Regulatory bodies are taking steps to improve the cybersecurity of critical infrastructure by updating directives and guidelines. Implementing additional measures such as incentive programs, specialized training, and a public–private advisory council can help make the power sector more secure.
References


Recent Developments of and Trends in Cybersecurity in the Power Sector


About the Project

This paper is part of the project “Innovations in electricity markets, network regulations, low-carbon investments and technologies” under KAPSARC’s Energy Transitions and Electric Power program. This project aims to provide insights on the transformation of the Saudi electricity sector. This transformation is characterized by a willingness to increase the share of renewables and replace liquid fuels with natural gas. It must also ensure fiscal balance, expand electricity exports, produce green hydrogen and diversify the Saudi economy through localization. This project provides insights into this transition by discussing and learning from electricity markets worldwide.