United Nations Economic Commission for Europe
Group of Experts on Energy Efficiency

Task Force on Digitalization in Energy

Case study

Cyber Resilience of Critical Energy Infrastructure

ADVANCED COPY

Geneva, 2023

Contents

Acknowledgements

The case study was originally presented at the tenth session of the Group of Experts on Energy Efficiency (Geneva, 5-6 October 2023).

Andrei Covatariu (Co-Chair of the UNECE Task Force on Digitalization in Energy) is the lead author of the case study, supported by Dr Elizabeth Massey (Co-Chair of the UNECE Task Force on Digitalization in Energy), Sylvain Clermont (DigiTransfo Expertise), Dr Erlijn van Genuchten (Sustainable Decisions), Dr Romanas Savickas (UNEP-CCC), and Dr Fabian Heymann (Swiss Federal Office of Energy). Valuable inputs at various stages of research were provided by other members of the UNECE Task Force on Digitalization in Energy.

The findings, interpretations and conclusions expressed herein are those of the authors and do not necessarily reflect the views of the United Nations or its officials or Member States.

Mention of any firm, product, service or licensed process does not imply endorsement or criticism by the United Nations. The designations employed do not imply the expression of any opinion whatsoever on the part of the United Nations Secretariat concerning the legal status of any country, territory or area, or of its authorities.

Theoretical Introduction

Digitalization is gaining more and more attention as a way to support and complement the energy transition process. Digitalization entails the use of digital technologies for existing processes, as it helps address existing challenges in new ways.

While using an integrated energy system with intelligent connected devices has many advantages, it also causes challenges. One of these challenges is the increased surface of attack and thus the related cybersecurity risk.

In general, the aim of cyberattacks is to take control of the system, of the data and/or harm/damage/incapacitate the physical equipment. Thus, in the case of the smart integrated energy systems, the goal is to take control of the energy system so that energy cannot be produced, transmitted, distributed, and/or used as intended.

As energy systems are considered critical infrastructure, dealing with cyberattacks is critical for reliable sustainable development. This can be done by preventing, mitigating, and – eventually – recovering from cyberattacks:

- *Prevention* means that measures are put into practice that prevent cyberattacks on the energy system from taking place and being successful.
- *Mitigation* means that the consequences of cyberattacks on the energy system are limited as much as possible.
- *Recovery* means that the energy system is brought back to normal functioning as soon as possible after a successful attack.

To be able to prevent, mitigate, and recover from cyberattacks effectively, measures can be implemented both top-down and bottom-up:

- *Top-down* means that policies and regulations inform the workforce what to do to increase security.
- *Bottom-up* means that identified security issues on a technical level are reported to the management so that policies and regulations can be improved accordingly.

If these top-down and bottom-up strategies are implemented thoroughly and consistently, the number of different attack points for attackers reduces, leading to a higher overall security level of the energy system. As a consequence, this contributes to different sustainability aspects of the energy system. For example, on the economic level, a secure energy system reduces the loss of profits and reputational damage. On the social level, a secure energy system ensures many critical services including healthcare and communication. On the environmental level, a secure energy system prevents energy waste and environmental damage.

The UNECE Task Force on Digitalization in Energy has researched extensively the theoretical aspects related to cyber resiliency, while also generating practical considerations and policy recommendations, as well as suggestions to businesses and operators. These elements were compiled in the document “Key considerations and solutions to ensure cyber resiliency in the smart integrated energy systems” (ECE/ENERGY/GE.6/2023/3 − ECE/ENERGY/GE.5/2023/3) developed in 2023 by the Group of Experts on Energy Efficiency and the Group of Experts on Cleaner Electricity Systems on the platform of the Task Force on Digitalization in Energy.

In the following case study, an example of a successful cyberattack on the energy system and the consequences are explored in more detail.

Cybersecurity attacks on energy system components and their example consequences

As the energy system is identified as critical infrastructure and energy is the backbone of society, consequences of cyberattacks can be far-reaching, including economic, social, and environmental consequences. Recent examples of ransomware-based cyberattacks on critical infrastructure, resulting in temporary shutdowns and data loss, show a growing trend: ransomware attacks nearly doubled in 2022, and the last 6 months of 2023 witnessed a 35 per cent increase of ransomware attacks and a 53 per cent increase of malware and viperware that impacted industrial infrastructures. [1]

This trend is not surprising considering that preventing cyberattacks and mitigating the consequences is not a simple task; moreover, cybersecurity is often neglected for integral processes, from design to operations, despite the extensive attack surface of modern energy systems.

The integrated and intelligent devices, servers, computers, and systems by virtue of their connected-ness can all be potentially attacked in a myriad of ways as exemplified below:

1. Servers: by using services that should not be available to the outside world, by exploiting outdated software that has known vulnerabilities, by exploiting insecure configuration settings such as default passwords, and by gaining unauthorized access to sensitive data;
2. Networks: by bypassing authentication, by overloading the network so that normal functioning is impaired, by exploiting insecure configuration settings such as weak encryption, and by gaining unauthorized access to communication data of other users;
3. Websites: by using functionalities that should not be accessible, by exploiting known vulnerabilities, by exploiting insecure configuration settings such as default passwords, by gaining unauthorized access to sensitive data such as the underlying database or unencrypted communication, by gaining unauthorized access to the underlying server, by attacking other users, and by uploading malware;
4. Mobile applications: by using functionalities that should not be accessible, by exploiting known vulnerabilities, by exploiting insecure configuration settings such as default passwords, by gaining unauthorized access to sensitive data such as the underlying database or unencrypted communication, and by gaining unauthorized access to the underlying mobile devices;
5. Software and firmware: by bypassing authentication, by exploiting known vulnerabilities, by exploiting insecure configuration settings such incorrect/insufficient access rights management, and by gaining unauthorized access to sensitive data such as source code;
6. Webservices: by exploiting known vulnerabilities, by exploiting insecure configuration settings such as authentication without password, by gaining unauthorized access to sensitive data such as data from other users, and by gaining unauthorized access to the underlying server;

[1] Fortinet, *Global Threat Landscape Report. A Semiannual Report by FortiGuard Labs* (February 2023).

7. Cloud-based Platforms: by obtaining unauthorized access to data from other users such as files, by gaining unauthorized access to the underlying server, by exploiting insecure configuration settings such as authentication by guessing a weak password, by gaining unauthorized access to sensitive data such as passwords or access keys, and by exploiting known vulnerabilities;
8. Sensors, motors, relays, etc.: by exploiting known software vulnerabilities, by exploiting insecure configuration settings, by tampering with data sent by a sensor/motor/relay/etc, by manipulating a sensor's/motor's/relay's etc functionality, by making the sensor unavailable, and obtaining unauthorized access to data;
9. Hardware: by manipulating the hardware design, by adding malicious hardware in the network, by attacking interfaces that are made available for finding problems, and by manipulating transferred data;
10. Users: by malicious emails such as phishing emails that invite readers to provide sensitive data or attachments with malware, by inciting fear in people so that they are triggered to perform an action that harms them and may go unnoticed, by disinformation activities that provokes them into sharing sensitive information.

Many other types of attacks are potentially possible. These can be categorized into four types:

1. Physical attacks (on the physical components of the system), including:
   (a) Physical damage: attacking a component causing physical damage, or activating inappropriate or non-operational behaviors;
   (b) Social engineering: deceiving and manipulating individuals into sharing sensitive information that can be used for further attacks;
   (c) Node tampering or malicious node injection: a node in the smart integrated energy system is a part that connects a physical device to the Internet and is responsible for collecting, processing, and/or controlling data. Tampering sensitive data means not only reading but also changing it. This can be achieved by attacking an existing node, but also by adding a new node.
2. Software attacks (on computer programmes that are executed by physical devices in the energy system), including:
   (a) Malicious scripts: adding to existing software so that the latter contains additional, harmful functions, e.g., to steal login data;
   (b) Malware: installing software, which can support all kinds of harmful activities, e.g., spyware to steal data, viruses to damage or change files and/or data, viperware to wipe data and software, and ransomware to encrypt data;
   (c) Denial-of-service: a denial-of-service (DoS) attack makes the software or device unavailable, e.g., by overloading the software or shutting it down. If such an attack is performed from many computers at the same time, it is called a distributed denial-of-service (DDoS) attack.
3. Network attacks (gaining unauthorized access to, and perform unauthorized actions in the network), including:
   (a) Traffic analysis: gaining knowledge from characteristics of a data flow that can be observed, even when the content of the data flow remains hidden;

(b) Routing information: intercepting, changing, and/or redirecting data sent through the network to a different destination, e.g. to monitor or steal data, or disrupt the energy system service delivery;

(c) Sinkhole: a harmful node in the grid sends bogus messages to other nodes and tricks these nodes into sending information to the harmful node;

(d) Unauthorized access: getting access to the network without having permission.

4. Encryption attacks (circumventing the security by adding encryption, which requires a key to turn the code back into readable information or data), including:

(a) Cryptanalysis: aiming at finding out what information or data is encrypted, without knowing the key;

(b) Side-channel: using information that is unintentionally provided by a computer system when doing cryptographic operations to gain access to encrypted information;

(c) Man-in-the-middle: positioning between two communicating components, so that encrypted messages can be eavesdropped and even changed.

Oftentimes, different types of cyberattacks can be observed at once, therefore overlapping challenges and disruptions to potential victims. Additionally, cyberattacks can also complement other types of physical attacks.

Contextual introduction to the case study

The Colonial Pipeline is a North American oil pipeline system originating in Houston, Texas, and transports refined oil products (gasoline, diesel, jet fuel) to the Eastern areas of the United States. It carries more than half of all fuel consumed on the East Coast

The sequence of events has been established as follow:

May 6, 2021: Malicious actors launch an attack, stealing data, locking computers, and requesting a ransom.

May 7, 2021: Colonial Pipeline pays the ransom.

May 8, 2021: Colonial Pipeline publicly announces attack, then shuts off servers and some pipelines.

May 9, 2021: Colonial Pipeline makes a second public announcement, discussing its system restart plans.

May 10, 2021: The FBI confirms DarkSide ransomware caused the attack, and Colonial Pipeline releases two more statements around its restoration process.

May 11, 2021: Federal agencies release an advisory describing DarkSide ransomware and mitigation strategies while Colonial Pipelines releases a statement around fuel shipping.

May 12, 2021: Colonial Pipeline restores operations and announces fuel delivery timelines, amidst people "panic buying" gasoline.

The attack shut down Colonial Pipeline's operations for approximately five days, causing localized shortages of gasoline, diesel fuel, and jet fuel. Panic-buying by consumers depleted gasoline supplies at some service stations on the East Coast while also driving up retail gasoline prices.[2]

Alternatives to the pipeline, in the form of transporting fuel through trucks and tanker cars for trains, were slow to organize.[3]

Colonial Pipeline shut down its operational technology systems out of caution to halt further infection, but eventually paid the hackers over $4 million in cryptocurrency to restore its operating systems. Even after receiving the decryption key, it took days of work to restart the pipeline.

Cybersecurity experts also note that Colonial Pipeline would never have had to shut down its pipeline if it had more confidence in the separation between its business network and pipeline operations. Cybersecurity best practices indicate there should always be separation between data management and the actual operational technology. That a pipeline carrying almost 50 per cent of gas to the East Coast, had not implemented this as a basic practice raised questions for regulators and governments and its agencies.

The cybersecurity incident occurred at a time when there were increasing concern about the vulnerability of critical infrastructure to cyber threats. This heightened concern followed a series of prominent cyber incidents (e.g. SolarWinds breach), which targeted numerous federal government agencies, including the Departments of Defense, Treasury, State, and Homeland Security.

Cyberthreats are becoming increasingly prevalent across all economic sectors, and they pose cascading national security risks for the energy industry. The Colonial Pipeline attack could have gone further. For instance, the infamous Russian NotPetya (Ransomware) attack brought down most of Ukraine's operating systems by infiltrating computers via a common accounting software mechanism and wiping information.[4] The NotPetya attack caused approximately $10 billion in damages spread across multiple international industries[5] and crippled the country's infrastructure.

[2] https://www.washingtonpost.com/business/2021/05/12/faq-gas-shortages/

[3] https://www.nytimes.com/2021/05/14/us/politics/pipeline-hack.html

[4] https://www.washingtonpost.com/world/national-security/russian-military-was-behind-notpetya-cyberattack-in-ukraine-cia-concludes/2018/01/12/048d8506-f7ca-11e7-b34a-b85626af34ef_story.html

[5] https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

The intervention and the changing factor

From an AAG-IT 2023 report, *Ransomware* is a malware designed to deny a user or organization access to files on their operational systems (computers). By encrypting these files and demanding a ransom payment for the decryption key, cyberattackers place organizations in a position where paying the ransom is the easiest and cheapest way to regain access to their files. Some variants have added functionality – such as data theft – to provide further incentives for ransomware victims to pay the ransom.[6]Over 93 percent of ransomware attacks are on Windows-based executables and organizations in the US account for 47 per cent of attacks. It is not all bad news however, approximately 90 per cent of ransomware attacks fail or have the result in zero-losses for the organization attacked.

On May 6, 2021, the Colonial Pipeline suffered a ransomware attack. It started when a hacker group identified as DarkSide accessed the Colonial Pipeline network, culminating in a multiple staged and multilayered attack. Attackers stole 100 gigabytes of data within the first few hours of the attack. The second wave of the attack was the infection of the IT network with ransomware that infected many computer systems (billing and accounting included).

The most common entry point for ransomware is phishing. Attackers were able to penetrate the Colonial Pipeline network through an exposed VPN password account. From that moment onward, the DarkSide group used its ransomware-as-a-service (RaaS) model to hold the pipeline network hostage until the ransom was paid.

The initial response of the Colonial Pipeline was to shut down its systems to prevent the ransomware attack from spreading, pay the ransom, decrypt the locked systems and begin the damage control needed to quell the growing panic of Americans for whom petroleum-based gasoline is a daily necessity. Subsequently, authorities were notified to begin an official investigation. The Biden Administration issued an executive order for U.S. Government agencies, directing them to take a series of proactive cybersecurity steps. As this attack crossed state boundaries, and affected major geographical and economic regions, federal authorities such as the Federal Bureau of Investigation (FBI), U.S. Department of Energy (DoE), Department of Homeland Security (DHS), and Cybersecurity and Infrastructure Security Agency (CISA) were now involved. The effects of the Colonial Pipeline attack were both immediate and lasting. In the immediate term, once news reached the public channels about the attack, panic-buying due to fears of an impending gas shortage led to long lines at gas stations across Florida, Georgia, Alabama, Virginia and the Carolinas. Seizing the competitive opportunity, station owners raised prices to USD $3/gallon (expensive at the time). Longer lasting effects included a product safety alert being issued to those who were filling plastic bags with gasoline, while the Product Safety Commission considered issuing new regulations to enforce proper dispensing of flammable liquids.

The Biden administration issued an order that advocates a Software Bill of Materials (SBOM). This has the effect to allow developers of software components to ensure those components are up

[6] https://aag-it.com/the-latest-ransomware-statistics.

to date and to respond quickly to new vulnerabilities. Buyers are protected as well by the SBOM by using it to perform vulnerability or license analyses, both of which can be used to evaluate risk in a product.[7]

By 7 June 2021, and with the collaborative efforts of multiple agencies, 63.7 bitcoin (approximately USD $2.3 million at the time) were recovered from the attackers.[8] The Biden administration is seeking USD $26 billion is cyber funding for the 2024 fiscal year.

[7] https://www.cisa.gov/sbom

[8] https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know

The effects and lessons learned

Numerous major effects have derived from the cyberattack and the forces shutdown.

The perspective of gas shortage led to individual customers filling their personal stocks, leading to long lines at gas stations. This caused a spike in the prices of gas and, in some cases, real shortages.

The airline industry was also significantly disrupted, as jet fuel shortages were recorded by many carriers, including American Airlines, leading to limited disturbance to major airports.[9]

After the attack, the DarkSide group asked for a ransom of 75 bitcoins (approximately $4.4 million on the day of the attack).

As the Colonial Pipeline CEO later testified during Congressional hearings, at the time of the ransom demand it was unclear how large the intrusion was or how long would the restoration of exposed systems would take, therefore how long the disruption would last.

Consequentially, the Colonial Pipeline paid the hacking group the amount claimed, for the decryption key needed to restore the management of the systems. The Colonial Pipeline restarted pipeline operations on May 12, 2021.

Since that attack two years ago this past May, which is known as 'a watershed moment in the short but eventful history of cybersecurity'[10], the CISA has focused on implementing and deploying systems and protocols to improve the resilience of critical infrastructure across the US. One of the areas of greatest need for companies and industries vulnerable to cyberattacks is access to actionable and timely information on best practices for system cyber- and cyberphysical security. To address this need CISA established the **Stop Ransomware[11]** government sponsored website as a central repository of information for businesses to learn about and report ransomware related attacks.

To ensure that efforts can scale to meet both today's and tomorrow's cyberthreats, the Joint Ransomware Task Force (JRTF)[12] has been established as a collaboration with FBI partners and a Joint Cyber Defense Collaborative (JCDC)[13] a cross-sectoral initiative which brings together experts in cybersecurity from public and private sectors and industries to share insights and information in real-time and as a feedback/feed-forward loop into the central information repository for, among other things, publicly accessible services.

Although a variety of efforts have brought successful outcomes (e.g., avoided potential future threats, heretofore unseen collaborations amongst government entities, open communication across sectors and amongst competitive agencies) much is still to be done. In light of complex threats and increasing geopolitical tensions, diligence across major economic systems (e.g.

[9] https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know

[10] https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years

[11] https://www.cisa.gov/stopransomware

[12] https://www.cisa.gov/news-events/news/readout-second-joint-ransomware-task-force-meeting

[13] https://www.cisa.gov/topics/partnerships-and-collaboration/joint-cyber-defense-collaborative

transportation, communications, food supply, etc.) and attack surfaces is evermore necessary. Policy support is strongly needed to upgrade technologies that underpin critical infrastructures with a focus on security rather than commercialization, with cybersecurity being part of the earliest requirements and design processes.

Further, cybersecurity needs to be prioritized at the highest levels of industry with proactive collaboration amongst government and industry, regardless of commercial or competitive interests and with a core focus on the effect to society at large and those who are most vulnerable to attack.

Conclusion, policy recommendations, and considerations for other geographies

Considering the above-described events – and given the literature research performed by the Task Force on Digitalization in Energy – a few considerations ought to be formulated both for developed energy systems and economies, as well as for developing energy networks and emerging economies. Moreover, a series of recommendations for both operators (be they private or state-operated) and public authorities are proposed.

Setting up cross-national and national cybersecurity strategies that extensively describe how to prevent and manage cyberattacks of critical infrastructure and smart integrated energy systems.

In doing so, collaborating with peer countries on potential threat actors and how to effectively overcome potential cybersecurity risks is paramount.

To this end, the strategy development processes must identify roles and responsibilities of different stakeholders, including government agencies, central and local authorities, businesses and their employees, and individuals.

Implementing business continuity management plans describing how to manage cybersecurity events is very important, especially where the threat of energy system outages is higher.

From a regulatory point of view, an important element is to enforce (and reinforce) the implementation of applicable standards and guidelines which address matters of improving cybersecurity for operational technology in automation, control systems, and cybersecurity for critical infrastructure;

In this context, developing regulations to make reporting of data protection and cybersecurity standards to official bodies to stimulate bottom-up strategies is essential

Financially, tax incentives for the adoption/implementation of relevant cybersecurity standards ought to become a common practice across all geographies.

Equally important, awareness-raising actions – both among employees involved in the energy sector, as well as among customers – is highly recommended, as the pace of digitalization adoption intensifies.