Lessons Learned from Previous Cyberattacks on Energy Systems – Global and Australian Context

Kapila Susantha
School of Electrical and Data Engineering
University of Technology Sydney
Sydney, Australia
0009-0008-9732-0006

Dylan Lu
School of Electrical and Data Engineering
University of Technology Sydney
Sydney, Australia
0000-0003-2145-0580

Xu Wang
School of Electrical and Data Engineering
University of Technology Sydney
Sydney, Australia
0000-0001-9439-6437

***Abstract*—The threat landscape for cyberattacks has grown dramatically as the energy sector's reliance on digital technology and networked systems has grown. Previous attacks on energy infrastructure have highlighted the significance of comprehensive cybersecurity methods and learning from past mistakes. This conference paper examines the lessons learnt from prior cyberattacks on energy systems, with an emphasis on noteworthy case studies such as the Ukraine power grid attack, the TRITON/TRISYS malware attack on Saudi industrial systems, and several other breaches around the world, and in Australia. The study examines these occurrences to illustrate the techniques used by threat actors, the vulnerabilities exploited, and the repercussions felt in the energy industry. These case studies give helpful guidance for improving cybersecurity measures in the energy business. Common themes, challenges, and recommendations derived from these incidents are discussed, including the role of insider threats, the significance of information sharing and collaboration, the need for continuous monitoring and incident response capabilities, and the integration of secure coding practices in energy system development. The findings presented in this paper serve as a valuable resource for policymakers, energy sector professionals, and cybersecurity experts seeking to safeguard critical energy infrastructure. By leveraging the lessons learned from previous cyberattacks, stakeholders can proactively strengthen resilience, mitigate risks, and ensure the reliable operation of energy systems in an increasingly interconnected world.**

Keywords— cyberattacks, energy systems, lessons learned, black energy, malware

I. Introduction

The increasing digitization and interconnectedness of energy systems have brought significant benefits to the energy sector, enabling improved efficiency, enhanced grid management, and the integration of renewable energy resources. However, these developments are accompanied by an increasing threat of cyberattacks on key energy infrastructure. Numerous cyber events in the energy sector have shown weaknesses and underlined the necessity for effective cybersecurity measures.

Previous cyberattacks on energy systems, both nationally and globally, have served as useful lessons, providing insights into malicious actors' tactics, techniques, and consequences. These occurrences have shown the possible implications of a successful cyberattack, such as power outages, financial losses, and public safety risks. This conference paper aims to delve into these lessons, offering insight on the tactics employed by malicious actors, the vulnerabilities exploited, and the impacts experienced in the energy sector.

To achieve this objective, this conference paper will draw upon notable cyber incidents that have impacted the energy sector. Case studies of incidents such as the Ukraine power grid attack and the TRITON/TRISYS malware attack on industrial systems in Saudi Arabia will be examined. Further to this several cyber threats on Australian energy companies will also be examined. These case studies offer valuable insights into the attack vectors, techniques, and impacts that can inform effective cybersecurity strategies.

The Ukraine power grid attack, which occurred in 2015, was a landmark event in the energy sector. Malicious actors targeted the operational technology (OT) systems, leading to widespread power outages and disruptions. This case study presents lessons on the importance of securing OT systems, enhancing incident response capabilities, and establishing robust recovery plans [1].

The TRITON/TRISYS malware attack, discovered in 2017, specifically targeted safety instrumented systems (SIS) used in industrial control systems (ICS) [2]. This incident demonstrated the evolving tactics of threat actors and their willingness to exploit vulnerabilities in critical infrastructure as depicted in [3, Fig. 1]. Lessons from this case study revolve around the need for heightened supply chain security, improved detection and response capabilities, and the adoption of a proactive security posture.

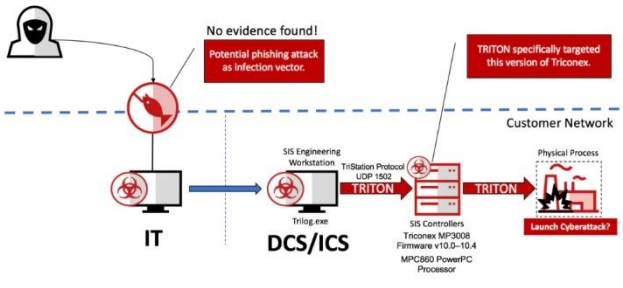

Fig. 1. Possible attack framework for TRITON/TRISYS malware [3]

Building on these case studies, this conference paper will identify common themes, challenges, and recommendations derived from previous cyberattacks on energy systems. The structure of this paper will have two main sections to explore the Global context and the National (Australian) context of these threats and their lessons.

II. Global Context Key Learniing Points

A. *Increased Connectivity Increases Vulnerability*

One of the most significant lessons learned from previous cyberattacks on energy systems is that increased connectivity increases vulnerability. The more devices that are connected to a network, the more opportunities there are for a cyberattack to occur. This is particularly true for energy systems, which are becoming increasingly connected through the use of smart grid technologies.

For example, the Stuxnet worm, which was discovered in 2010, targeted SCADA systems used in the Iranian nuclear program. The worm was able to spread through USB drives and infect computers that were not connected to the internet. Once the worm was inside the network, it was able to take control of the SCADA systems and cause physical damage to centrifuges used in the uranium enrichment [4].

Similarly, in 2015, the Ukrainian power grid was targeted by a cyber-attack that caused a blackout affecting over 200,000 people. The importance of Cybersecurity in energy systems grew exponentially with this incident given its scale and impact on the country's economy. Three utilities companies in Ukraine were hit by 'Black Energy' malware. The attack was carried out by hackers who gained access to the power grid through a spear-phishing campaign. Once inside the network, the hackers were able to take control of the SCADA systems and shut down the power grid [1], [5].

In 2017, TRITON/TRISYS malware attack on industrial systems in Saudi Arabia, highlighting the need to address traditional attack vectors and adapt cyber defense strategies to encompass new grid technologies and distributed energy resources (DER) [2]. This attack also signifies how important to segment the critical network in a DER.

B. *Attackers are Becoming More Sophisticated*

Another lesson learned from previous cyberattacks on energy systems is that attackers are becoming more sophisticated. In the past, many attacks were carried out by amateur hackers using off-the-shelf tools. However, recent attacks have been carried out by more sophisticated attackers who have the resources and expertise to carry out complex attacks.

For example, in 2017, the NotPetya ransomware attack targeted companies in Ukraine, but quickly spread to other countries, including the UK and the US. The attack was carried out by a nation-state actor and used advanced techniques to spread through networks and evade detection [6].

C. *The Human Factor is Critical*

Another lesson learned from previous cyberattacks on energy systems is that the human factor is critical. Many cyberattacks are successful because of human error, such as employees clicking on phishing links or using weak passwords.

For example, in 2014, the German steel mill, ThyssenKrupp, was targeted by a cyberattack that caused significant damage to the plant's blast furnace. The attack was carried out by hackers who gained access to the plant's network through a spear-phishing campaign. Once inside the network, the attackers were able to gain control of the plant's control systems and cause physical damage to the blast furnace [7].

Similarly, in 2018, the US Department of Energy reported that a spear-phishing campaign had successfully targeted several employees at a nuclear power plant. The attackers were able to gain access to the plant's network and exfiltrate sensitive data [8].

These examples highlight the importance of educating employees about cybersecurity best practices and implementing strong security policies and procedures. In most modern organisations cybersecurity policies are embedded into various mandatory training programs with staff induction and on the go training programs to keep them educated and updated.

D. *Collaboration and Sharing Information*

The Another lesson learned from previous cyberattacks on energy systems is that collaboration and information sharing are key to preventing and responding to attacks. Energy systems are complex, interconnected, and often involve multiple stakeholders, including government agencies, private companies, and academic institutions. For example, there are studies that suspect of possible code similarities among past cyberattacks as illustrated in [9, Fig 2].

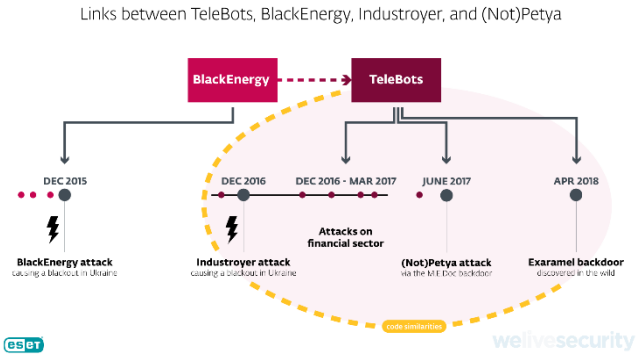

Fig. 2. Code Similarities among past cyberattacks [9]

In response to the Ukrainian power grid attack, the US Department of Energy established a public-private partnership called the Cybersecurity Risk Information Sharing Program (CRISP) to facilitate information sharing between government agencies and the private sector [10]. The program provides a platform for stakeholders to share information about cyber threats and vulnerabilities and coordinate incident response efforts.

Similarly, in 2019, the European Union established the European Network for Cyber Security (ENCS), a non-profit organization that works with energy companies to improve cybersecurity in the energy sector. The organization provides training, testing, and certification services to help energy companies identify and mitigate cyber risks [11].

E. *Protecting the Supply Chain is critical*

The SolarWinds attack, discovered in December 2020, was a significant cybersecurity incident that had widespread

implications for organizations and critical infrastructure. This attack highlighted several crucial lessons that can guide future cybersecurity practices and defenses. The attack demonstrated the vulnerability of software supply chains. Attackers targeted the software update mechanism of SolarWinds' Orion platform, compromising the supply chain and distributing a malicious software update to thousands of organizations [12]. This incident underscores the importance of implementing robust software development and distribution practices, including rigorous security testing and verification procedures.

The incident also emphasized the importance of adopting a zero-trust architecture. In the SolarWinds attack, once the initial compromise occurred, attackers could move laterally within the network, gaining access to sensitive systems and data. Implementing a zero-trust model, where access is continuously verified and authenticated, can mitigate the risk of lateral movement and unauthorized access [13].

The below is a tabular representation of the incidents and lessons learned from each of the cases provided in the above section.

TABLE I. SUMMARY OF CYBER ATTACKS ON ENERGY SYSTEMS AND LESSONS LEARNED – GLOBAL CONTEXT

Incident	*Year*	*Location*	*Impact*	*Lessons Learned*
Stuxnet	2010	Iran	Physical damage to centrifuges	Increased connectivity increases vulnerability Importance of supply chain security
Ukrainian Power Grid Cyberattack	2015	Ukraine	Blackout affecting over 200,000 people	Increased connectivity increases vulnerability: Segmentation and redundancy for resilience.
TRITON/ TRISYS Malware Attack	2017	Saudi Arabia	Shutdown of industrial safety system	Increased connectivity increases vulnerability: Importance of segmenting critical networks in distributed energy resources.
NotPetya Ransomware Attack	2017	Multiple	Rapid spread with advanced techniques	Attackers are becoming more sophisticated: The NotPetya attack used advanced techniques, showing the evolution of cyber attackers.
Thyssen Krupp Cyberattack	2014	Germany	Physical damage to a blast furnace	The Human Factor is Critical Importance of cybersecurity education and strong security policies.
US Nuclear Power Plant Spear-Phishing	2018	USA	Sensitive data exfiltration	The Human Factor is Critical: Spear-phishing campaign targeted employees. Emphasis on employee education and cybersecurity policies.
SolarWinds Supply Chain Attack	2020	Multiple	Widespread supply chain compromise	The vulnerability of software supply chains. Emphasis on robust software development, security testing, and zero-trust architecture.

III. AUSTRALIAN CONTEXT KEY LEARNIING POINTS

The Australian energy sector has witnessed a rise in cyber threats that pose significant risks to the reliability, integrity, and availability of its energy systems. The Australian Cyber Security Centre (ACSC) has been at the forefront of identifying and analyzing these threats to provide valuable insights into their nature and impact. This paper aims to shed light on the cyber threats faced by Australian energy systems, drawing upon the expertise and findings of the ACSC.

The Director General of Australian Signals Directorate's (ASD) (2021), speech at National Press Club revealed that "twenty-five per cent of cyber security incidents responded to by ASD in 2020 were against our critical infrastructure – energy, water, telcos and health to name a few." The recent cyberattacks on Medibank, Optus in 2022 were an eye opener for the energy sector in Australia. On 27 January 2022, a collaboration paper was released by the six electricity distributors across NSW, ACT, Tasmania, and NT to start a discussion about what distributors need to do to make electricity networks resilient to disruptive events including the effects of climate change and cyberattacks [14]

According to a case study on the ACSC's Annual Cyber Threat Report, July 2021 to June 2022, in April 2022, the ACSC's CHIPs program reached out to various Australian organizations operating in the government, critical infrastructure, transportation, and services sectors after a vulnerability was publicly disclosed [15]. The program notified them about the possibility of having vulnerable software installed on their internet-facing servers and offered assistance. Among the organizations contacted was an energy provider in Australia. The energy provider, upon receiving the notification from the ACSC's CHIPs program, promptly acted, and discovered that two of their servers had been compromised. Fortunately, the network segmentation, which involved keeping a separate network called a demilitarized zone (DMZ) to safeguard information from untrusted networks, such as the internet, was effective. Consequently, the energy operations were not disrupted. The provider acted swiftly and resolved the issue by restoring the affected servers from backups. Based on the available evidence, it appears that the exploitation was carried out by various actors, including both state-sponsored and criminal entities, and much of it was likely automated. Advanced actors attempted to obtain user login information, with the probable aim of acquiring more lasting access after the initial compromise had been resolved.

Another case study on the same Annual Cyber Threat Report, July 2021 to June 2022, in 2021, CS Energy, an electricity generator owned by the Queensland Government and responsible for producing 10% of the electricity for the national electricity market, became the target of the Conti ransomware group, which affected the company's corporate ICT network [13]. On November 27, 2021, CS Energy was made aware of the ransomware attack on its corporate network and acted swiftly by disconnecting the external internet connection to the network and implementing business continuity measures. CS Energy made sure to physically isolate its OT systems from the corporate network in order to safeguard them from the incident, thus preventing any impact on the generation of electricity and ensuring a continuous energy supply. This occurrence emphasizes the significance of network segmentation and stresses the need to have well-defined.

According to the most recent literature, Energy Australia was affected by a cyber issue mere days after the Medibank intrusion. "The incident resulted in the exposure of data for 323 residential and small business customers," according to the corporation [16]. This event emphasises the importance of password complexity, which now includes the use of 12-character passwords for Energy Australia customers.

TABLE II. SUMMARY OF CYBER ATTACKS ON ENERGY SYSTEMS AND LESSONS LEARNED – AUSTRALIAN CONTEXT

Incident	*Year*	*Lessons Learned*
Cyberattacks on Medibank and Optus	2022	Australian energy sector vulnerable to cyber threats; Medibank and Optus incidents as wake-up call.
Ukrainian Power Grid Cyberattack	2015	Increased connectivity increases vulnerability: Attackers targeted the power grid through a spear-phishing campaign Segmentation and redundancy for resilience.
TRITON/TRISYS Malware Attack	2017	Increased connectivity increases vulnerability: Importance of segmenting critical networks in distributed energy resources.
NotPetya Ransomware Attack	2017	Attackers are becoming more sophisticated: The NotPetya attack used advanced techniques, showing the evolution of cyber attackers.
ThyssenKrupp Cyberattack	2014	The Human Factor is Critical Importance of cybersecurity education and strong security policies.
US Nuclear Power Plant Spear-Phishing	2018	The Human Factor is Critical: Spear-phishing campaign targeted employees. Emphasis on employee education and cybersecurity policies.
SolarWinds Supply Chain Attack	2020	The vulnerability of software supply chains. Emphasis on robust software development, security testing, and zero-trust architecture.

IV. CONCLUSION AND FUTURE PLAN

As the energy sector continues to embrace digital transformation and interconnected technologies, the lessons learned from previous cyberattacks serve as a valuable resource for policymakers, energy sector professionals, and cybersecurity experts. By applying these lessons, stakeholders can proactively strengthen resilience, mitigate risks, and ensure the reliable operation of energy systems in an increasingly interconnected world.

We have discussed the need for a comprehensive cybersecurity framework that encompasses risk assessment, threat intelligence, incident response, and information sharing. The implementation of security standards such as ISO 27001, NIST Cybersecurity Framework, and the Australian Energy Sector Cyber Security Framework (AESCSF) can provide a solid foundation for organizations to manage cybersecurity risks effectively.

Furthermore, the adoption of advanced technologies like intrusion detection and prevention systems, security analytics, and threat intelligence platforms can bolster the defense against emerging cyber threats. Collaborative efforts between government agencies, energy sector organizations, and cybersecurity experts are vital to promote information sharing, incident response coordination, and the development of best practices. Additionally, a skilled cybersecurity workforce and ongoing training programs are crucial to ensure that organizations have the expertise needed to address evolving threats. Public-private partnerships and collaboration with academic institutions can contribute to the development of a strong cybersecurity talent pool and foster innovation in the energy sector.

However, it is important to recognize that cybersecurity is an ongoing process, and vigilance is required to adapt to the changing threat landscape. Regular assessments, audits, and exercises are necessary to identify vulnerabilities and strengthen resilience. Continuous improvement in cybersecurity practices, information sharing, and threat intelligence will enable the Global and Australian energy sector to mitigate risks and respond effectively to cyber incidents.

Looking ahead, it is imperative to maintain an ongoing dialogue and collaboration among academia, industry, and government agencies to address emerging cyber threats and evolving attack vectors. This collaboration can foster the development of innovative solutions, the sharing of best practices, and the continuous improvement of cybersecurity measures in the energy sector.

In conclusion, the analysis of previous cyberattacks on energy systems has provided valuable insights and lessons learned that can inform the development and implementation of robust cybersecurity strategies. By leveraging these lessons, stakeholders can enhance the resilience of energy systems, protect critical infrastructure, and safeguard the reliable delivery of energy services.

REFERENCES

[1] Ukrainian Government. (2016). "Lessons learned from the cyber attack on the Ukrainian power grid." Government of Ukraine, Kyiv.

[2] FireEye. (2017). "Attackers deploy new ICS attack framework 'TRITON' and cause operational disruptions." Retrieved from https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html

[3] "Triton Malware Spearheads Latest Attacks on Industrial Systems | McAfee Blogs," www.trellix.com. https://www.trellix.com/en-hk/about/newsroom/stories/research/triton-malware-spearheads-latest-generation-of-attacks-on-industrial-systems1.html (accessed Jun. 07, 2023).

[4] R. Langner, "Stuxnet: Dissecting a Cyberwarfare Weapon," IEEE Security & Privacy Magazine, vol. 9, no. 3, pp. 49–51, May 2011, doi: https://doi.org/10.1109/msp.2011.67.

[5] "Packets Don't Lie: LogRythm NetMon Freemium Review | SANS Institute," www.sans.org. https://www.sans.org/white-papers/37517/

[6] J. Wolff, Cyberinsurance Policy. MIT Press, 2022.

[7] "Exclusive: Hackers accessed Telegram messaging accounts in Iran - researchers," Reuters, Aug. 02, 2016. Available: https://www.reuters.com/article/ctech-us-iran-cyber-telegram-exclusive-idCAKCN10D1AM

[8] "U.S. officials say Russian government hackers have penetrated energy and nuclear company business networks," Washington Post. Available: https://www.washingtonpost.com/world/national-security/us-officials-say-russian-government-hackers-have-penetrated-energy-and-nuclear-company-business-networks/2017/07/08/bbfde9a2-638b-11e7-8adc-fea80e32bf47_story.html

[9] "New TeleBots backdoor: First evidence linking Industroyer to NotPetya," WeLiveSecurity, Oct. 11, 2018. https://www.welivesecurity.com/2018/10/11/new-telebots-backdoor-linking-industroyer-notpetya/

[10] "Cybersecurity Risk Information Sharing Program (CRISP)." Available: https://www.energy.gov/sites/default/files/2021-12/CRISP%20Fact%20Sheet_508.pdf

[11] "ENCS ensures cyber security in the EU | about ENCS," ENCS. https://encs.eu/about-us/

[12] L. Sterle and S. Bhunia, "On SolarWinds Orion Platform Security Breach," 2021 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/IOP/SCI), Atlanta, GA, USA, 2021, pp. 636-641, doi: 10.1109/SWC50871.2021.00094.

[13] R. Zeng, N. Li, X. Zhou and Y. Ma, "Building A Zero-trust Security Protection System in The Environment of The Power Internet of Things," 2021 2nd International Seminar on Artificial Intelligence, Networking and Information Technology (AINIT), Shanghai, China, 2021, pp. 557-560, doi: 10.1109/AINIT54228.2021.00114.

[14] "Submission to the 2022 Collaboration Paper on Network Resilience," Australian Energy Regulator, Mar. 10, 2022. https://www.aer.gov.au/publications/submissions/previous-submissions/submission-to-the-2022-collaboration-paper-on-network-resilience

[15] Australian Cyber Security Centre, "ACSC Annual Cyber Threat Report, July 2021 to June 2022 | Cyber.gov.au," Cyber.gov.au, 2021. https://www.cyber.gov.au/about-us/reports-and-statistics/acsc-annual-cyber-threat-report-july-2021-june-2022

[16] "Change your password now: Another Australian company hit by cyber attack," 7NEWS, Oct. 21, 2022. https://7news.com.au/news/cyber-security/passwords-compromised-as-another-major-aussie-company-hit-by-cyber-attack-c-8619385