ISAUnited
International Security Architects

Case Study:
Cyber Attacks on Critical Infrastructure

Contents

List of Figures

List of Tables

Cyber Attacks on Critical Infrastructure

Introduction

World is currently shifting towards digital era, as major part of our society, economy and critical infrastructures are handled by computer networks and information technology (IT). As, with the passage of time, dependence of society on information technology increases, the potential threats of security breaches in the form of cyber-attack are becoming more attractive and common. A report by Symantec Cybercrime claims that cost of cyber-attacks in 2014 was approximately USD 575 billion each year in the form of money steal, data theft, damage to intellectual property and one of the most increasing reasons is causing disruption and political instability in a country/region. During recent years, some of the major security breaches appeared on surface in the form of TalkTalk, Mossack Fonseca, the US Democratic National Committee and Yahoo [1, 2].

Currently, cyber-attacks are getting more and more common, as such type of security breaches are cheaper, safest, and convenient as compared to physical attacks. These breaches are resulting in the form of disruption in sensitive facilities of a city such as healthcare centers, electricity grids, water dams, chemical factories, and gas stations etc.

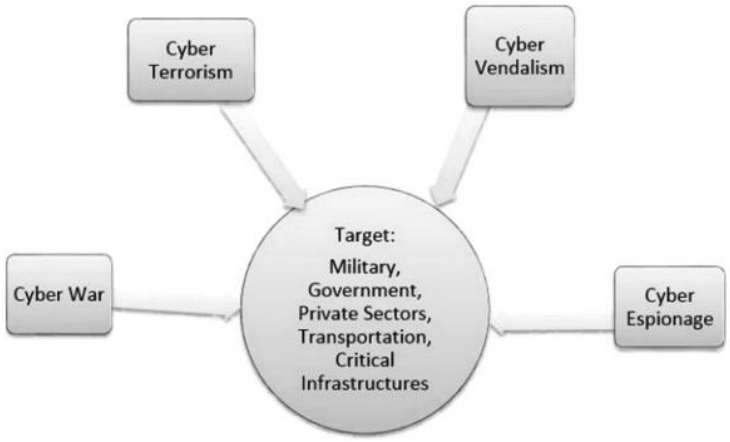

Figure 1. Cyber-attack Targets

Cyber-attacks – a threat to security

In current study, we are going to discuss the impacts of cyber-attacks on sensitive facilities and critical infrastructures and their potential impacts on environment, economy, sustainability, and land resources of a particular region.

1. Cyber-attacks on Healthcare Systems

Cyber-attacks on hospitals and healthcare systems are rising exponentially since 2010. Such kind of security breaches results in the form of disruption in providing health facilities, disclosure of patients'

personal data, loss of hospital records as well as tempering with medicinal and electronic medical records (EMR) [3]. One of the most critical incidents of this nature was cyber-attack on United Kingdom's National Health System Hospital. In May 2014, the healthcare facility faced a serious security breach of "WannaCry ransomware attack" on 25 trusts that caused delay in providing immediate treatment, rerouting of ambulance as hospital lost access to its information system and some serious financial consequences [4].

1.1. Cyber-crimes lead towards Economic Crisis

According to an estimate, cyber-crimes in US secondary and tertiary healthcare facilities costs approximately USD 6 billion annually [5]. Table 1 explains some of the major historical events and their potential financial cost.

Table 1. Hospitals effected by Cyber-attacks [5]

	Cases	Types	Year	Reported Effects	Financial Cost	Duration (Days)
Pre - 2020	WannaCry, half of Britains' NHS including 16 major healthcare centers	Ransomware	2017	200,000 PCs and 1200 equipment Cancellation of 20,000 appointments	USD 125 M	14
	Boston Children's Hospital	DDoS attack	2014	Websites, internal and external network	USD 300,000	14
	Montpellier University Hospital	Phishing	2017	649 – 6000 PC and equipment	Not reported	5 – 7
	Hollywood Presbyterian Medical Center	Ransomware	2016	Full shutdown in PC, Email, Equipment, Network	Demanded 9000 bitcoins	10
2020 and later	Champaign-Urbana Public Health District's	Ransomware	2020	Internal and external network access	Not reported	<14
	Vermont Hospital	Ransomware	2020	Hacking HER, delay in various departments	USD 1.5 M per day	<7
	UVM Health cyberattack	Ransomware	2020	5000 PC, Network, Shutdown IT and Med Centers Postponed services during incident	USD 63 M	40
	Maryland Hospital	Ransomware	2020	Network Shutdown, Continue Operations Postponed schedule appointments	Not reported	2
	Six US Hospitals	Ransomware	2020	Networks, using paper records Demanded USD 1 M Diverted ambulances during the downtime Postponed elective procedures and services	2000 new PC	7 – 14

1.2. Cyber-security in hospitals and Sustainability

United Nations with other organizations is working on 17 agendas to attain sustainability and a secure future for next generations. Cyber-attacks on hospitals are compromising these sustainable development goals (SDGs) (especially SDG 3, 8, 9 and 11) (Figure *1*Figure 2). Healthcare is increasingly becoming dependent on digitalization which are eventually effected by cyber-attacks resulting in the form of poor health facilities, economic threats (i.e. ransomware and appointment cancellation) and immense threats to sustainability of cities as well as infrastructures [6, 7]. Hence, such type of security breaches are responsible for direct hurdle in the smooth pathways of sustainable development of a country.

Figure 2. Cyber threats to hospitals and Sustainability

1.3. Rising Death Toll associated with Cyber-attacks.

A survey conducted on 600 healthcare centers by Ponemon Institute claimed that the cyber-attacks on hospitals are increasing many folds for since 2019. Results showed that approximately 70% of ransomware results in the form of disruption in providing medical facilities while 22% centers claimed that they had faced increase in death rate during time of security breach. The officials demand that cyber-threats must not be ignored as even if there is 1% or even 0.5% chance of causalities [8].

2. Cyber-attacks on Power Grids

Power grid stations are one of the critical infrastructures of a nation that are being secured by complex cyber-security programs to increase their performance, efficiency, reliability, and safety. These power stations (e.g., hydro-power plants, nuclear power plants etc.) are secured and run automatically or preferably through remote instructions to ensure their smooth functioning as well as security. In past few years, such facilities are also becoming a clear target of hackers [9].

One of the worst kinds of cyber-attack on power grid stations is on nuclear power plant. Such kind of attacks can lead to worst form of Cyber-terrorism resulting in the form of damage to human life, state's

security, properties, environmental health of region as well as long-term radiation exposure to whole world. Being highly sensitive and critical facilities, nuclear power plants are being secured by defense in-depth concept [10]. It is being claimed that it is quite impossible to compromise the security of any nuclear power plant. Yet, on October 30, 2019, the Nuclear Power Corporation of India Ltd. confirmed the news of occurrence of cyber-attack in early September on Thr Kudankulam Nuclear Power Plant in Tamil Nadu. The attack resulted in the form of separation of two power plants reactors (generating 1000 MW) electricity [11].

Studies claim that during current era, any mal-functioning events or nuclear blasts can be resulted in the form of disastrous environmental impacts and casualties as compared to Chernobyl Nuclear Power Plant Disaster or even nuclear war on Japan.

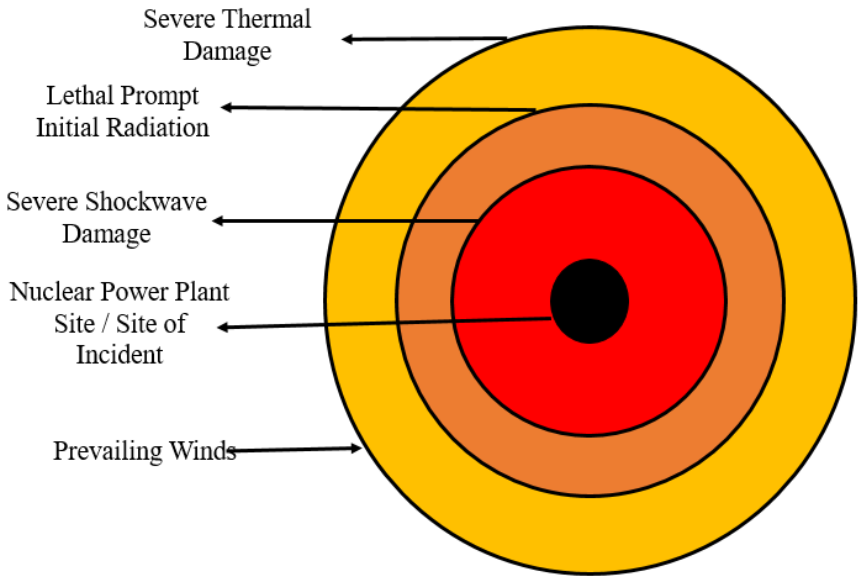

Figure 3. Illustration of estimated damage due to accident in Nuclear Power Plant

2.1. Case Study

One of the worst cyber-attacks on power grid was faced in 2015 in Ukraine's Power System in which power outage affected approximately 225,000 customers for 3 – 6 hours. During attack, human machine interface (HMI) was hacked, and power system was remote cut-down by opening circuit breakers. The situation became even more worsen as the communication system was compromised by installing denial of service (DoS) attack. The system software was also deleted to halt restoration of system [9].

2.2. Cyber-Threats to Power Grid and Sustainability

Cyber-threats on power grids are highly responsible for threatening a nation's security, life property as well as can cause some irreversible damage (i.e., in the case of nuclear power plant damage). Such breaches are resulting in the form of violation of SDG 7, 8, 9, 13, 14, 15, & 16 (Figure 4). These security breaches are expected to case direct impact to above-mentioned goals as well as an indirect effect to

the entire sustainability agenda proposed by United Nations. On one side, security threats halt process of supplying affordable and clean energy, while on the other hand it can also case a severe damage to life on land as well as in water and prolonged climate change impacts. One scenario of damage to nuclear power plant can be seen in Chernobyl that resulted in the form of 31 – 50 casualties and an effected area of approximately 150,000 square kilometres (including 2600 km^2 area of exclusive zone). Although the incident was not associated by cyber-attack but is one of the best examples to understand potential effects of damage to power station.

Figure 4. Cyber Threats to Power Grids can compromise some major SDGs

3. Cyber-attacks on Water-Treatment Facilities

World is currently facing the situation of water scarcity. According to a report published by United Nation World Water Development published in 2018, approximately half of world population, approximately 3.6 billion, is facing situation of water scarcity (at-least for one month during year) that is expected to increase till 2050 (becoming 6 billion) [12]. Globally, potable as well as wastewater treatment plants are controlled through Cyber-physical System (CPS) [12] Supervisory Control and Data Acquisition (SCADA) [13] that can be compromised or hijacked through cyber-attacks. Cyber-attacks on such facilities can cause cascading effects in the form of effect of public health due to consumption of polluted/chemically poisoned water, economic loss, and many other environmental catastrophes.

3.1. History of Cyber-attacks on Water Treatment Plants and their potential impacts

The cyber-attack on water facilities results when hackers take control of facilities and become able to alter chemical, pH and TDS level of water especially potable water. Such breach threatens lives of thousands of people that are consuming that water [13]. Some of the major events of cyber-attacks on water treatment plants are enlisted in Table 2.

Table 2. History of Cyber-attacks on Water Facilities [12]

Case	Year	Target	Attribution	Cause	Details	Impacts
Northern Colorado	2019	Operational Process (OP)	Cybercrime	Ransomware	Locked access to technical and engineering data	Disruption, Took about three weeks to unlock data
Kemuri Water	2016	OP	Hacktivist	Remote Access	Accessed PLC which is controlling chemicals responsible for water treatment	Identified and reverse changes
Bowman Avenue Dam	2016	OP	Hackers /Nation State	Remote Access	Hackers infiltrated ICS of facility and Accessed SCADA	Data exfiltration and approximately USD 30,000 on remediation cost
Florida Wastewater	2012	IT	Ex-Employ	Remote Access	Stolen login credentials were used to access district's computer system	Deleted and modified information
Maroochy Shire	2000	OP	Ex-Employee of contractor	Physical access	Masqueraded as a controller using stolen fake commands to the pumping station	Approximately 800,000 liters of sewage water was released into environment that harmed local parks, rivers.
						The spillage of contaminated water resulted killing marine life and impacted human life

4. Cyber-attacks on Chemical Factories

Chemical factories such as refineries, chemical production units and pharmaceutical industries uses Distributed Control System (DCS) and Programmable Logic Control (PLG) that can be vulnerable to cyber-attacks. Control of DCSs and PLCs by an outsider can lead to severe consequences including fire, explosion, or environmental release. Hence, care must be taken to prevent access to both the industrial equipment computer systems as well as to ensure the physical security of the devices and assets being controlled or monitored to avoid catastrophes [14]. Cyber-attacks on chemical factors can cause following types of impacts.

1. Release of toxic chemicals into the environment.

2. Compromising highly sensitive data.
3. Stealing chemicals to use them in making chemical weapons (which is highly prohibited according to the Organization of Prohibition of Chemical weapons, 2008).
4. Causing cyber-terrorism in the form of blasts and fires
5. Causing gaseous spillage
6. Financial damage
7. Computer system damage (as in the case of cyber-attack on Saudi Aramco Oil Refinery)
8. Ransomware

4.1. Bhopal Tragedy and Death Rate

One of the drastic impacts of compromising a chemical industry (pesticide) was scene in 1984 in Bhopal, India. Although, the event was not associated with cyber-attack, but is a valid example to understand impact of mal functioning of chemical industry. In 1984, one of the pesticide industries in Bhopal faced some reactor mal-functioning and resulted in the form of release of tons of methyl isocyanate gas. The immense release of toxic gas resulted in the form of killing approximately 16,000 people while 500,000 people were severely injured. Incident is considered to be one of the worst kind to chemical spillage tragedy of history [14].

5. Major Environmental Impacts of Cyber-crimes

Cyber-crimes on critical infrastructures i.e., water utilities (on, either potable water or wastewater treatment plants), power plants, and factories or even on smart cities are majorly responsible for series of environmental crisis. Some of the major crisis are listed below.

1. Addition of chemicals such as Sodium hydroxide, change in pH and TDS level of water that can endanger life of millions of people as well as animals.
2. Impact of cyber-attacks on environmental factors can be analyzed through attack on water treatment plant in Florida. In February 2021, the attackers managed to change the level of sodium hydroxide in potable water from 100 parts per million (ppm) to 11,100. Although the change was detected earlier and was diverted but if operators could not detect it at earliest, it can poison and cause serious threats to the health of thousands of people in Florida and its surroundings.
3. Addition of chemicals into land due to sewage release and causing soil pollution.
4. Contamination of sewage into surface water bodies causes water pollution.
5. Threatening and damaging sensitive plants species due to chemical poisoning.
6. Increasing risks of many epidemic deceases due to unhealthy conditions.
7. Damaging plants that are highly sensitive towards excess of water/salts.

8. Addition of harmful chemical gases that can cause suffocation.
9. Digesters of wastewater treatment plants produce excessive amounts of methane due to anaerobic respiration of sewage. Compromising such a facility can lead towards sudden release of excessive amount of methane into environment and can suffocate nearby population. Another threat of release of methane is that it is highly inflammable and can result in a catastrophic situation.
10. Release of nuclear radiation due to cyber-attack is even worse as uranium possesses half-life of 4.5 billion years. Such accidents cause irreversible and prolonged impacts on the environment and its biotic as well abiotic factors.
11. Chemical addition and release due cyber-breach into water bodies can even lead towards killing marine life and destroying complete aquatic ecosystem.
12. Cyber-attacks are also responsible for social restlessness in people as these types of practices create an environment of risks, no-safety as well as disruption in daily activities such as in the case of traffic jams due to cyber-attacks on signaling system.

Conclusion

During current era of digitalization, where computers and algorithms are majorly responsible for the security of major sensitive facilities and data, the ratio of threats is also increasing exponentially. Such risks are resulting in the form of high environmental as well as social and economic losses to companies. Hence, there is need to develop a highly sophisticated and complex system that protect such facilities and lower the chances of cyber-attacks and its drastic impacts.

Reference

[1] G. Martin, P. Martin, C. Hankin, A. Darzi, and J. Kinross, "Cybersecurity and healthcare: How safe are we?," *BMJ*, vol. 358, 2017, doi: 10.1136/BMJ.J3179.

[2] J. Jang-Jaccard and S. Nepal, "A survey of emerging threats in cybersecurity," *J. Comput. Syst. Sci.*, vol. 80, no. 5, pp. 973–993, 2014, doi: 10.1016/J.JCSS.2014.02.005.

[3] S. T. Argaw, N. E. Bempong, B. Eshaya-Chauvin, and A. Flahault, "The state of research on cyberattacks against hospitals and available best practice recommendations: A scoping review," *BMC Med. Inform. Decis. Mak.*, vol. 19, no. 1, pp. 1–11, Jan. 2019, doi: 10.1186/S12911-018-0724-5/TABLES/1.

[4] S. T. Argaw *et al.*, "Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks," *BMC Med. Inform. Decis. Mak.*, vol. 20, no. 146, 2020, doi: 10.1186/s12911-020-01161-7.

[5] H. Ghayoomi, K. Laskey, E. Miller-Hooks, C. Hooks, and M. Tariverdi, "Assessing resilience of hospitals to cyberattack," *Digit. Heal.*, vol. 7, pp. 1–15, 2021, doi: 10.1177/20552076211059366.

[6] S. Bhuvaneswari, "BPF-Cyber Security How does good cybersecurity contribute to the growth of and trust in ICTs and Internet Technologies, and their ability to support the Sustainable Development Goals (SDGs)?" https://www.intgovforum.org/multilingual/index.php?q=filedepot_download/5065/721 (accessed Oct. 24, 2022).

[7] N. America, "Securing Digital Dividends: Appendix: The SDGs and Cybersecurity," *New America*. https://www.newamerica.org/cybersecurity-initiative/reports/securing-digital-dividends/appendix-the-sdgs-and-cybersecurity/ (accessed Oct. 24, 2022).

[8] N. Wetsman, "Hospitals say cyberattacks increase death rates and delay patient care - The Verge," *The Yerge*, Sep. 28, 2021. https://www.theverge.com/2021/9/27/22696097/hospital-ransomware-cyberattack-death-rates-patients (accessed Oct. 24, 2022).

[9] C. C. Sun, A. Hahn, and C. C. Liu, "Cyber security of a power grid: State-of-the-art," *Int. J. Electr. Power Energy Syst.*, vol. 99, pp. 45–56, Jul. 2018, doi: 10.1016/J.IJEPES.2017.12.020.

[10] "Cybersecurity in the Nuclear Sector."

[11] M. Robbins, "Cyberattack Hits Indian Nuclear Plant | Arms Control Association," *Arms Control Association*, Dec. 2019. https://www.armscontrol.org/act/2019-12/news/cyberattack-hits-indian-nuclear-plant (accessed Oct. 24, 2022).

[12] N. Tuptuk, P. Hazell, J. Watson, and S. Hailes, "A Systematic Review of the State of Cyber-Security in Water Systems," *Water*, vol. 13, p. 81, 2021, doi: 10.3390/w13010081.

[13] R. Setola, V. Rosato, E. Kyriakides, and E. Rome, *Managing the complexity of critical infrastructures: A modelling and simulation approach*, 90th ed. Springer Open, 2016. doi: 10.1007/978-3-319-51043-9.

[14] "Environmental risks: cyber security and critical industries," *Environmental Risk Consultation Team*. https://axaxl.com/-/media/axaxl/files/pdfs/insurance/cyberenvironmentalrisks_whitepaper_us_ca_axa-xl.pdf (accessed Oct. 25, 2022).