IJIAET International Journal of Innovative Analyses and Emerging Technology

| e-ISSN: 2792-4025 | http://openaccessjournals.eu | Volume: 3 Issue: 6

Cybersecurity in Critical Infrastructures

Matthew N. O. Sadiku
Department of Electrical & Computer Engineering, Prairie View A&M University,
Prairie View, TX USA

Uwakwe C. Chukwu
Department of Engineering Technology, South Carolina State University, Orangeburg, SC, USA

Janet O. Sadiku
Juliana King University, Houston, TX, USA

Abstract: Critical infrastructures serve as the life support system of our daily existence. They are complex systems that form the lifeline of a modern society. They are becoming more complex and reliant on networks of connected devices, making them vulnerable to cyberattacks. The energy sector, transportation, public sector services, telecommunications, and other critical infrastructure systems are the main targets of cyber-attacks. Cyberattacks are growing at an alarming rate partly due to the widespread use of information technologies. This paper considers cybersecurity in critical infrastructures.

Keywords: critical infrastructures, cyber attacks, cyber threats, cybersecurity in critical infrastructures.

INTRODUCTION

Critical infrastructure (CI) systems are very essential to our society as they provide important services such as electric power distribution, telecommunications, transportation, water supply, etc. Any threat to these sectors could have potentially debilitating national security, economic, and public health. Cyberattacks have become some of the most common and dangerous types of threats against national security. Successful attacks can be devastating, disrupting financial services, power distribution systems, transportation systems, and other essential infrastructure.

US CRITICAL INFRASTRUCTURE

Critical Infrastructures (CI) are those assets, systems, and networks that provide functions necessary for our way of life. Americans depend on these infrastructures daily. There are 16 critical infrastructure sectors that are part of a complex, interconnected ecosystem in the US. These systems are interconnected to form the energy "grid." Critical infrastructures consist of the following [1]:

1. The Energy Services Sector: *This powers the US economy of the 21st century.*
2. The Dams Sector: *This supplies basic water maintenance and controls water services in the US.*
3. The Financial Services Sector*: This aims to protect our country's most vital source of economic vitality.*

4. The Nuclear Reactors, Materials, and Waste Sector: *This includes the nuclear infrastructure and power reactors that provide electricity.*
5. The Food and Agriculture Sector: *This is nearly completely privately owned and is comprised of an expected 2.1 million farms and 935,000 restaurants,*
6. The Water and Wastewater Systems Sector*: This ensures the supply of drinking water.*
7. The Healthcare and Public Health Sector: *This ensures health and safety for all US citizens.*
8. The Emergency Services Sector: *This is a community of millions of highly-skilled, trained emergency personnel.*
9. The Transportation Systems Sector: *This rapidly, securely, and safely moves individuals and products through the nation and abroad.*
10. The Chemical Sector: *This produces, stores, uses, and transports potentially hazardous chemicals.*
11. The Communications Sector: *This gives an "enabling function" overall basic infrastructure sectors.*
12. The Information Technology Sector: *Organizations, governments, the scholarly community, and private residents are progressively reliant upon Information Technology Sector capacities.*
13. The Defense Industrial Base Sector*: It empowers innovative work and the upkeep of military weapons to meet US military requirements.*
14. The Critical Manufacturing Sector*:This sector includes manufacturers of metals, machinery, automotive and transportation equipment, and electrical equipment producers. Figure 1 shows a manufacturing facility in North Charleston, South Carolina [2].*
15. The Government Facilities Sector:This *sector incorporates a wide array of buildings, situated in the US and abroad, that are owned or rented by US governments.*
16. The Commercial Facilities Sector: *This incorporates many different organizations that attract individuals for shopping, business, entertainment, or hospitality*.

These 16 critical infrastructure sectors, identified by the Department of Homeland Security, are illustrated in Figure 2 [3]. The reliability and secure operation of these systems is of paramount importance to national security and economic vitality. Disruption of electric power systems can be catastrophic on national security and the economy. The food and hospitality industries are the least likely to prioritize cybersecurity, because they are less likely to use security measures.

OVERFVIEW ON CYBERSECURITY

Cybersecurity refers to a set of technologies and practices designed to protect networks and information from damage or unauthorized access. It is vital because governments, companies, and military organizations collect, process, and store a lot of data. As shown in Figure 3, cybersecurity involves multiple issues related to people, process, and technology [4].

A typical cyberattack is an attempt by adversaries or cybercriminals to gain access to and modify their target's computer system or network. Cyberattacks are becoming more frequent, sophisticated, dangerous, and destructive. They are threatening the operation of businesses, banks, companies, and government networks. They vary from illegal crime of individual citizen (hacking) to actions of groups (terrorists) [5].

The cybersecurity is a dynamic, interdisciplinary field involving information systems, computer science, and criminology. The security objectives have been availability, authentication, confidentiality, nonrepudiation, and integrity. A security incident is an act that threatens the confidentiality, integrity, or availability of information assets and systems [6].

- *Availability*: This refers to availability of information and ensuring that authorized parties can access the information when needed. Attacks targeting availability of service generally leads to denial of service.
- *Authenticity*: This ensures that the identity of an individual user or system is the identity claimed. This usually involves using username and password to validate the identity of the user. It may also take the form of what you have such as a driver's license, an RSA token, or a smart card.
- *Integrity*: Data integrity means information is authentic and complete. This assures that data, devices, and processes are free from tampering. Data should be free from injection, deletion, or corruption. When integrity is targeted, nonrepudiation is also affected.
- *Confidentiality*: Confidentiality ensures that measures are taken to prevent sensitive information from reaching the wrong persons. Data secrecy is important especially for privacy-sensitive data such as user personal information and meter readings.
- *Nonrepudiation*: This is an assurance of the responsibility to an action. The source should not be able to deny having sent a message, while the destination should not deny having received it. This security objective is essential for accountability and liability.

Everybody is at risk for a cyberattack. Cyberattacks vary from illegal crime of individual citizen (hacking) to actions of groups (terrorists). The following are typical examples of cyberattacks or threats [7]:

- *Malware*: This is a malicious software or code that includes traditional computer viruses, computer worms, and Trojan horse programs. Malware can infiltrate your network through the Internet, downloads, attachments, email, social media, and other platforms. Spyware is a type of malware that collects information without the victim's knowledge.
- *Phishing*: Criminals trick victims into handing over their personal information such as online passwords, social security number, and credit card numbers.
- *Denial-of-Service Attacks*: These are designed to make a network resource unavailable to its intended users. These can prevent the user from accessing email, websites, online accounts or other services.
- *Social Engineering Attacks*: A cyber criminal attempts to trick users to disclose sensitive information. A social engineer aims to convince a user through impersonation to disclose secrets such as passwords, card numbers, or social security number.
- *Man-In-the-Middle Attack*: This is a cyber attack where a malicious attacker secretly inserts him/herself into a conversation between two parties who believe they are directly communicating with each other. A common example of man-in-the-middle attacks is eavesdropping. The goal of such an attack is to steal personal information.

These and other cyber attacks are shown in Figure 4 [8].

Cybersecurity involves reducing the risk of cyber attacks. Cyber risks should be managed proactively by the management. Cybersecurity technologies such as firewalls are widely available [9]. Cybersecurity is the joint responsibility of all relevant stakeholders including government, business, infrastructure owners, and users. Cybersecurity experts have shown that passwords are highly vulnerable to cyber threats, compromising personal data, credit card records, and even social security numbers. Governments and international organizations play a key role in cybersecurity issues.

Securing the cyberspace is of high priority to the US Department of Homeland Security (DHS). Vendors that offer mobile security solutions include Zimperium, MobileIron Skycure, Lookout, and Wandera.

CYBERSECURITY FOR INFRASTRUCTURE

Today, we live in a digital landscape full of cyber threats and vulnerabilities. The vulnerability of critical infrastructure to cyberattacks has been a topic of research and discussion for decades. Cyberattacks on critical infrastructure have been witnessed from the timeline shown below [10]:

- 2008: An alleged cyberattack blew up an oil pipeline in Turkey shutting it down for three weeks.
- 2009: The Stuxnet computer worm destroyed hundreds of Iranian centrifuges, disrupting that country's nuclear fuel enrichment program.
- 2015: An attack brought down a section of the Ukrainian power grid for six hours, but substations on the grid had to be operated manually for months.
- 2018: The city of Atlanta, Georgia witnessed a massive cyberattack where multiple municipal services went down, including databases and years' worth of data destroyed. The city spent $2.7 million in recovering services.
- 2019: The city of Baltimore, all of its servers except for essential services, were taken offline. The city declined to pay the ransom demand, and eventually lost $18 million to direct costs and revenue shortfalls to recover from the attack
- 2021: The Colonial Pipeline was subject to the largest cyberattack on oil infrastructure in the history of the United States and paid out $4.4 million ransom in Bitcoin to resume its operations.
- 2021: JBS S.A., a Brazil-based meat processing company, suffered a cyberattack, disabling its beef, pork slaughterhouses and paid out $11 million ransom in Bitcoin to cybercriminals to resume its operations.

The Cybersecurity and Infrastructure Security Agency (CISA) works with the federal government to improve American cyber and infrastructure security. As the nation's risk advisor, CISA provides guidance to support state, local, and industry partners in identifying the critical infrastructure sectors. CISA shares information with sector stakeholders to enhance their cybersecurity and preparedness for responding to and managing incidents. All critical infrastructure organizations should maintain a relationship with CISA and integrate its products and outputs into their processes.

HOW TO PROTECT INFRASTRUCTURE

Since 1996, the United States has become increasingly focused on protecting our critical infrastructure and ensuring its resilience. The US government has mandated that critical infrastructure providers perform regular cybersecurity audits to remain in compliance.

To combat critical infrastructure cybersecurity threats, government agencies must understand the nature of threats as well as the performance of their security programs. Critical infrastructure can be protected by taking the following measures.

- *Active Defense:* There is an urgent need for a more proactive approach to defending cyberattacks. Owners of energy, water, transportation, and other critical infrastructure systems must be continuously ready to weather cyberattacks. When an infrastructure system is attacked by an adversary, system operators and IT staff must work together to ensure continued operation of critical system functions and simultaneously defend the system from the attack. Rather than being passive in the event of a cyberattack, engineers and operators become an active part of the response team [11].

- *Security Gateways:* In critical infrastructure, all connections to and from the ICS/SCADA network must be secured. If this data was tampered with, it could have catastrophic consequences. Using a security gateway is the failsafe way to protect your sensitive systems. The solution allows only designated data to pass in one direction, no malware or destructive data can infiltrate systems during data transfer, and no data leakage can occur [12].

- *NIST Cybersecurity Framework:* In 2014, the National Institute of Standards and Technology (NIST) developed the Cybersecurity Framework to provide voluntary guidance for critical infrastructure organizations. This excellent framework is highly recommend for your company to follow and protect your company's critical infrastructure. It is a proven framework to protect your business. As shown in Figure 5, NIST cybersecurity framework is made up of 5 core functions, which provide an overview of the cyclical process for managing cybersecurity risk. They are [13]:

  - ✓ *Identify*: First, identify what your business's core function is, what is the mission, and why it exists.

  - ✓ *Protect:* Second, protect the components identified to ensure the availability of infrastructure services.

  - ✓ *Detect:* Third, allow continuous monitoring of logs that can identify any anomalies occurring within the infrastructure that may point to a cybersecurity event.

  - ✓ *Respond:* Fourth, detail the actions to be taken in the event a cybersecurity incident occurs.

  - ✓ *Recover:* Finally, in the event of an incident implementing planning processes, restore assets to working order. This will allow quicker return to service and return to business operations.

- *Culture of Cybersecurity:* Cyber security awareness is primarily a mental condition. Training is essential to teach employees about avoiding increasingly common exploitative attacks. Any interested employee with the required resources can attend security training classes. Organizations also need to ensure data compliance regulations within their respective regions [14].

- *Insider Threats:* Workers are closest to the physical systems within a utility's network. They have the most opportunities to perpetrate a cyberattack or cause accidental exposure. It is incumbent on critical infrastructure operators to thoroughly assess their trustworthiness of employees. Employee cyber security education is to instill in them a sense of responsibility for their own safety in the face of cyber threats. Thoroughly vet staff with sensitive system access and limit that access based on the "least privilege" principle [15]. The incentives toward collaboration and social connection often work against the incentive toward short-sighted self-interest. Employees should be able to share sensitive information about potential vulnerabilities without fear of reprisal.

BENEFITS

Critical infrastructure is now a prime target for hackers and hostile nation states. The key preventing cyberattacks is to understand the security issues, examine our own behaviors, identify deficiencies, and "eliminate ignorance." One solution is to hire more cybersecurity professionals, but that is not always easy in many industries. To establish a cybersecurity program, one must start with awareness and training. Maintaining good lines of communication is the key to improving your cybersecurity strategy.

CHALLENGES

Critical infrastructure, most of which is operated by private industry, faces the same risks and challenges that other sectors face. It has become easier and less risky to exploit vulnerabilities for profit. The cost of creating a successful attack is small for cyber criminals, which is why there are now so many attacks. Due to the complexity of the interdependences among computer, communication, and power infrastructures, the requirement to meet security on operations is a challenging issue.

CONCLUSION

Critical infrastructure in the United States supports the nation's economy, safety, and health. Public reporting on cyberattacks and cyber threats has been growing throughout the past decade [16]. Cyberattacks against critical infrastructure have increased. As cyberattacks become more sophisticated and dangerous, the threat to US critical infrastructure increases daily and puts national security, economy, business, and the public at risk. As a result of the growing threat, it is time for sector leaders to rethink cybersecurity strategies.

Cybersecurity entails the safeguarding of computer networks and the information they contain from penetration and from malicious disruption. When it comes to cybersecurity, securing our critical infrastructure is more consequential than ever.

More information about cybersecurity in manufacturing can be found in the books in [17-30] and the following related periodicals:

- *Journal of Cybersecurity*
- *Security Magazine*
- *International Journal of Critical Infrastructure Protection*

REFERENCES

1. “The 16 sectors of critical infrastructure cybersecurity” https://cipher.com/blog/the-16-sectors-of-critical-infrastructure-cybersecurity/
2. Kelly-Rozumalski, “The US cybersecurity imperative: Fortifying critical infrastructure,” January 2023, https://cyberscoop.com/critical-infrastructure-cybersecurity-imperative/
3. “Enhancing the protection and cyber-resilience of critical information,” infrastructure,” June 2021, https://digitalregulation.org/enhancing-the-protection-and-cyber-resilience-of-critical-information-infrastructure/
4. “Eliminating the complexity in cybersecurity with artificial intelligence,” https://www.wipro.com/cybersecurity/eliminating-the-complexity-in-cybersecurity-with-artificial-intelligence/
5. M. N. O. Sadiku, S. Alam, S. M. Musa, and C. M. Akujuobi, “A primer on cybersecurity,” *International Journal of Advances in Scientific Research and Engineering*, vol. 3, no. 8, Sept. 2017, pp. 71-74.
6. M. N. O. Sadiku, M. Tembely, and S. M. Musa, “Smart grid cybersecurity,” *Journal of Multidisciplinary Engineering Science and Technology*, vol. 3, no. 9, September 2016, pp.5574-5576.
7. “FCC Small Biz Cyber Planning Guide,” https://transition.fcc.gov/cyber/cyberplanner.pdf

8. “The 8 most common cybersecurity attacks to be aware of,” https://edafio.com/blog/the-8-most-common-cybersecurity-attacks-to-be-aware-of/

9. Y. Zhang, “Cybersecurity and reliability of electric power grids in an interdependent cyber-physical environment,” *Doctoral Dissertation*, University of Toledo, 2015.

10. G. Maini, “ Cybersecurity for critical infrastructure,” https://www.linkedin.com/pulse/cybersecurity-critical-infrastructure-gunangad-singh-maini

11. V. Wright, A. Ohrt, and A. Bochman, “Engineering cybersecurity into U.S. critical infrastructure,” April 2023, https://hbr.org/2023/04/engineering-cybersecurity-into-u-s-critical-infrastructure

12. “Cybersecurity in critical infrastructure,” Unknown Source.

13. A. Jacks, “What is the NIST cyber security frameworks (CFS) & how will it help my company?” October 2022, https://morefield.com/blog/nist-cyber-security-frameworks/

14. A. Rai, “5 Cybersecurity strategies to protect critical infrastructure,” https://caplocksecurity.com/5-cybersecurity-strategies-to-protect-critical-infrastructure/

15. S. Coleman, “ Five cybersecurity best practices for critical infrastructure,” March 2023, https://www.rmmagazine.com/articles/article/2023/03/02/five-cybersecurity-best-practices-for-critical-infrastructure

16. Z. Lanz, “Cybersecurity risk in U.S. critical infrastructure: An analysis of publicly available U. S. government alerts and advisories,” *International Journal of Cybersecurity Intelligence & Cybercrime*, vol. 5, no. 1, 2022, pp. 43-70.

17. F . Liu et al., *Science of Cyber Security*. Springer, 2018.

18. T. A. Johnson (ed.), *Cybersecurity: Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare*. Boca Raton, FL: CRC Press, 2015.

19. S. Rass et al. *Cyber-Security in Critical Infrastructures*: *A Game-Theoretic Approach*. Springer International Publishing, 2020.

20. N. Nedjah et al. (eds.), *Robotics and AI for Cybersecurity and Critical Infrastructure in Smart Cities*. Springer, 2022.

21. P. Ackerman, *Industrial Cybersecurity: Efficiently Secure Critical Infrastructure Systems*. Packt Publishing, 2017.

22. US Department of State, *Critical Infrastructure Protection: Department of Homeland Security Faces Challenges in Fulfilling Cybersecurity Responsibilities - Scholar's Choice Edition*. Scholar's Choice, 2015.

23. M. Martellini, *Cyber Security: Deterrence and IT Protection for Critical Infrastructures*. Springer, 2013.

24. I. Kantzavelou, L. Maglaras, and M. A. Ferrag (eds.), *Cyber Security of Critical Infrastructures*. MDPI AG, 2021.

25. L. Sukhostat and O.B. Popov (eds.), *Cybersecurity for Critical Infrastructure Protection Via Reflection of Industrial Control Systems*. IOS Press, 2022.

26. H. Janicke, L. Maglaras, and M. A. Ferrag, *Cyber Security and Critical Infrastructures Volume II*. MDPI AG, 2022.

Published under an exclusive license by open access journals under Volume: 3 Issue: 6 in Jun-2023

27. K. S. Manoj, *Cyber Security for Critical Infrastructure: Redefining National Security Concepts*. Notion Press, 2022.
28. J. Lopez, R. Setola, and S. Wolthusen (eds.), *Advances in Critical Infrastructure Protection: Information Infrastructure Models, Analysis, and Defense.* Springer, 2012.
29. D. Gritzalis, G. Stergiopoulos, and M. Theocharidou (eds.), *Critical Infrastructure Security and Resilience: Theories, Methods, Tools and Technologies.* Springer, 2019.
30. R. Tehan, *Cybersecurity: Critical Infrastructure: Authoritative Reports and Resources*. CreateSpace Independent Publishing Platform, 2017.

ABOUT THE AUTHORS

Matthew N. O. Sadiku is a professor emeritus in the Department of Electrical and Computer Engineering at Prairie View A&M University, Prairie View, Texas. He is the author of several books and papers. His areas of research interest include computational electromagnetics and computer networks. He is a life fellow of IEEE.

Uwakwe C. Chukwu is an associate professor in the Department of Industrial & Electrical Engineering Technology of South Carolina State University. He has published several books and papers. His research interests are power systems, smart grid, V2G, energy scavenging, renewable energies, and microgrids.

Janet O. Sadiku holds bachelor degree in Nursing Science in 1980 at the University of Ife, now known as Obafemi Awolowo University, Nigeria and Master’s degree from Juliana King University, Houston, TX in December 2022. She has worked as a nurse, educator, and church minister in Nigeria, United Kingdom, Canada, and United States. She is a co-author of some papers and books.

Figure 1 A manufacturing facility in North Charleston, South Carolina [2].

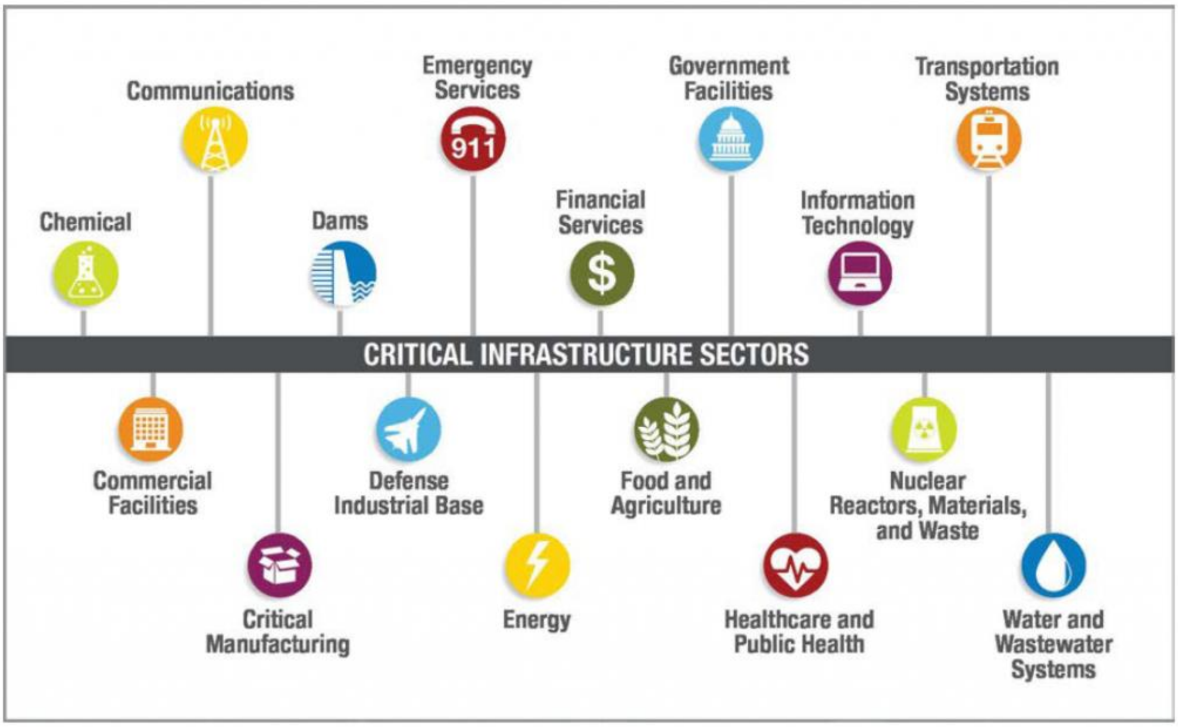

Figure 2 16 US critical infrastructures [3].

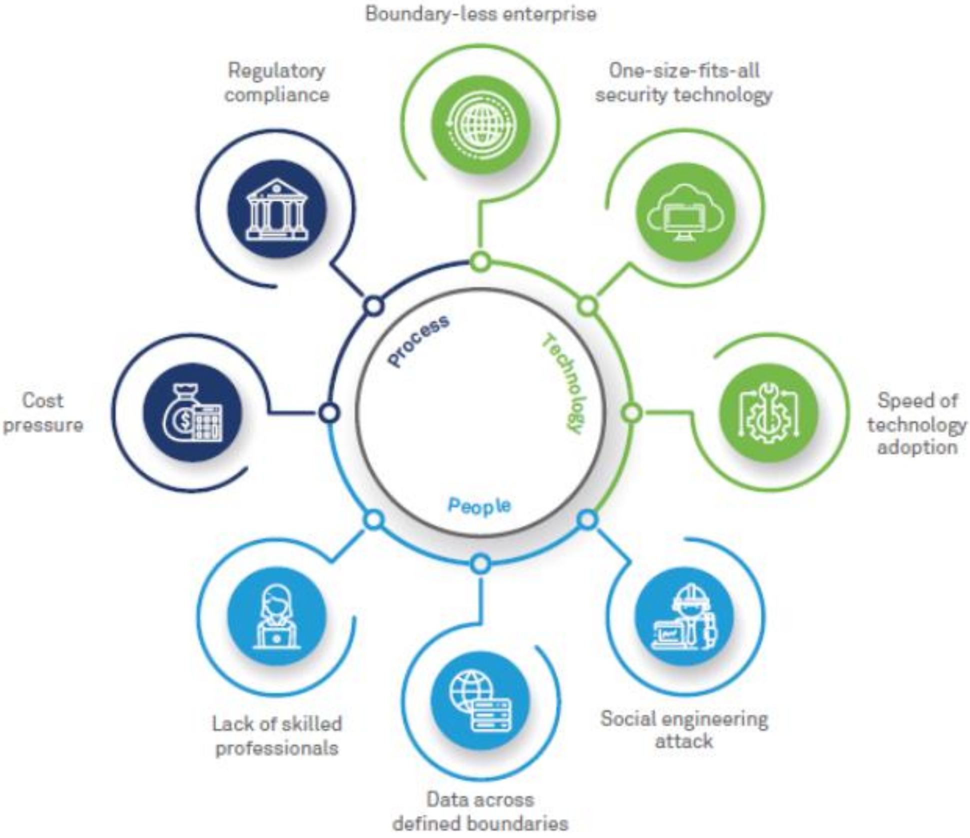
Boundary-less enterprise
Regulatory compliance
One-size-fits-all security technology
Cost pressure
Process
Technology
People
Speed of technology adoption
Lack of skilled professionals
Social engineering attack
Data across defined boundaries

Figure 3 Cybersecurity involves multiple issues related to people, process, and technology [4].

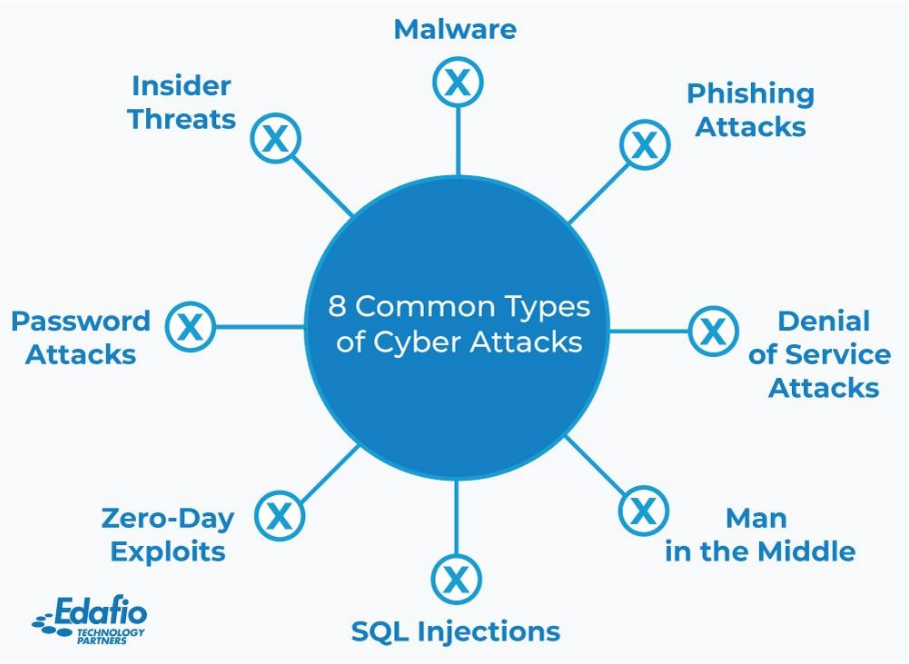

Figure 4 Common types of cyber attacks [8].

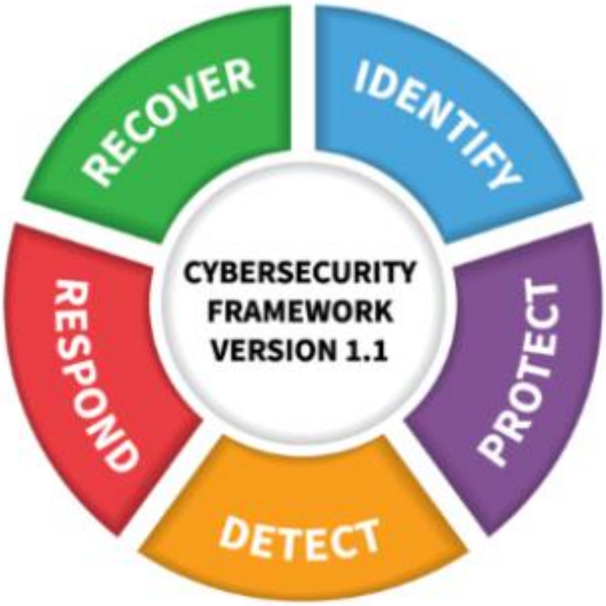

Figure 5 NIST cybersecurity framework is made up of 5 core functions [13].