IJIAET International Journal of Innovative Analyses and Emerging Technology

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

Cyber security in Manufacturing

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: The manufacturing industry is increasingly adopting smart manufacturing practices with unprecedented levels of automation using data and artificial intelligence. Smart manufacturing often requires greater network connectivity and industrial Internet of things (IIoT) sensing capabilities. With the increasing push toward smart manufacturing, cybersecurity has taken center stage in the operational risk profile of manufacturers. As the use of connected devices and digital processes increases in manufacturing, so do the cybersecurity risks. Manufacturers must modernize their cybersecurity practices because the cost of inaction is greater. This paper introduces the readers to cybersecurity in manufacturing.

Keywords: manufacturing, cyber attacks, cyber threats, cybersecurity in manufacturing.

INTRODUCTION

The manufacturing industry is one of the largest, most diverse, and rapidly changing segments of the global economy. Manufacturing is foundational to other areas of the economy. The manufacturing sector consists of many segments including aerospace and defense, automotive, chemicals, computer hardware, electronics, construction, consumer packaged goods, food and beverage, transportation, pharmaceuticals, and industrial manufacturing. It is a top target for cyber adversaries. Manufacturers are attractive targets for both criminal and nation-state attackers [1].

The massive digitalization of the manufacturing sector has yielded increased growth, efficiency, and profitability. However, this boost has also exposed the sector to malicious actors. The consequences of a breach for manufacturing companies include disruption of operations, loss of intellectual property, and loss of life. Most cybersecurity attacks in the manufacturing have focused on disrupting the operations of the plant by targeting the supervisory control and data acquisition (SCADA) systems. It is time to secure manufacturing from threats, hackers, and risks.

In addition, most manufacturers are small businesses that do not have established IT security practices to cope with a cyber incident. This lack of preparedness makes it easier for cybercriminals to attack and it increases the likelihood that impacted companies will experience longer periods of downtime [2].

IJIAET International Journal of Innovative Analyses and Emerging Technology

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

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 1, cybersecurity involves multiple issues related to people, process, and technology [3].

A typical cyber attack is an attempt by adversaries or cybercriminals to gain access to and modify their target's computer system or network. Cyber attacks 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) [4].

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 [5].

- *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 cyber attack. Cyber attacks vary from illegal crime of individual citizen (hacking) to actions of groups (terrorists). The following are typical examples of cyber attacks or threats [6]:

- *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 2 [7].

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 [8]. 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 MANUFACTURING

The most important technologies being deployed broadly by manufacturers are robotics, wearables, connected devices (IoT), additive manufacturing (3-D printing), virtual reality (VR) and augmented reality (AR), artificial intelligence (AI) and machine learning (ML), and big data analytics. Cyber security affects every company in all industries. Manufacturing is the second most commonly targeted industry by attackers. It accounted for 65% of all ransomware attacks in 2021. Manufacturing is acutely exposed to cyber crime. This may mean stopping or slowing production or making it harder to get back to the optimum levels of output that existed prior to the attack. Cyber threats for manufacturing companies are illustrated in Figure 3 [9]. There is a large and growing set of resources designed to improve cybersecurity in this sector. It is time to secure manufacturing from threats, hackers, and risks. Cybersecurity is applied in the following areas of manufacturing [1,10,11]:

- *Smart Factory:* There is no doubt that smart factories, driven by technology, are the future of manufacturing and can lead to improved productivity and performance. Digital transformation heralds a new era of connectivity which brings with it rising levels of cyber vulnerability. The rise of digital technologies brings a new level of cyber complexity to factories. Many manufacturers consider operational risk as an impediment to smart factory initiatives. As the number of smart factories and IoT devices increase, so does the risk of cyberattacks.
- *Industry 4.0:* What has become known as Industry 4.0 has been evolving and consolidating for almost a decade, with Germany driving innovation and investment. Industry 4.0 refers to a combination of hardware, software, and services that is modernizing manufacturing infrastructure to improve efficiencies in all aspects of manufacturing processes. Complete isolation has become impossible today. Industry 4.0 is a revolution in manufacturing by introducing disruptive technologies such as IoT and cloud-computing into the heart of the factory. No manufacturing organization can embrace an Industry 4.0 strategy without addressing the severe cybersecurity risks that attend it. As shown in Figure 4, Industry 4.0 enterprise faces intense risk [12].
- *Critical infrastructure:* The cybersecurity regulation regarding critical infrastructure providers has been evolving since shortly after the 911 attacks. Manufacturers in the U.S. should view recommendations for critical infrastructure providers as best practices.

- *Robotics:* While the use of robots in manufacturing has continued to expand over the decades, the majority are still used in automotive plants. As factories implement digitalization with robotics, automation, machinery, IIoT, and smart devices, it is important to secure all Internet connected devices from the full spectrum of on-line risks including malware and ransomware threats. Figure 5 shows how robots are used in manufacturing [13].
- *Digital Manufacturing:* Digitalization of manufacturing is revolutionizing the traditional manufacturing industry by rethinking manufacturing as a service. It consists of embedded electronics, sensors, actuators, and control software to enable the machines and the components within them to exchange data. It exploits the information from the various sensors and devices to streamline the process and material flow. The distributed and collaborative nature of digital manufacturing exposes it to risks.
- *Industrial Internet of Things:* These refer to a broad set of physical devices that combine embedded sensors, processing power, software, and often analytic capabilities to communicate real-time information.
- *3-D Printing:* This enables the creation of three-dimensional objects by building up an object one layer of material at a time. Still, the size, speed, and quality of 3-D printing have improved to the degree that the technique is used in space, aerospace, etc.

BENEFITS

A lot is at stake in the manufacturing industry. Competition is stiff. As the industry becomes more digitized, the cybersecurity risks increase.

Manufacturing companies are a lucrative and accessible target for ransomware due to their low tolerance for downtime and the relatively low level of cyber maturity concerning other sectors. Attackers are motivated by money most of the time [14]. A complete migration to smart manufacturing environment cannot be successful without cybersecurity itself becoming a foundational pillar of this new era. The manufacturing sector must prepare itself against the growing threat landscape by becoming cyber-resilient to reap the benefits of digitalization. By better understanding operational weaknesses, manufacturers can guard against future attacks and threats. Some cybersecurity standards already exist for heavy industries, such as the Cybersecurity Maturity Model Certification (CMMC). Although CMMC is designed for Department of Defense (DoD) contractors, it can be a helpful guide for all industrial and manufacturing companies [15].

CHALLENGES

Modern manufacturers are dealing with complex challenges and face a battery of cyber security risks. To be cyber secure implies constantly trying to hit a moving target. Cybersecurity is becoming more challenging as connectivity increases and malicious actors become more sophisticated. Integrity is essential to the degree it ensures safety and availability. Cost remains the main barrier to companies installing cyber protection. Another challenge in operational technology (OT) security is the capital-intensive nature of manufacturing where the manufacturing equipment is expected to last for decades, often with limited software and firmware updates. The lack of investment coupled with an inherently big data problem has created the dearth of manufacturing-oriented cybersecurity tools we face today [16]. Another difficulty is that basic threat intelligence information is often lacking on attacks targeting OT and IIoT infrastructure.

CONCLUSION

Manufacturers are increasingly under threat from cyber attacks. The scale and variety of cyber-threats to manufacturers have grown considerably in recent years. The most successful manufacturers in the

world recognize the increasing importance of cyber security. Manufacturers should be aware of the different cybersecurity threats the industry faces today. Manufacturers must think of cybersecurity holistically. To protect from intellectual property theft, manufacturers should recognize their weakest point, and that is human error. There is no silver bullet solution to cyber security issues due to its "moving target" nature. More information about cybersecurity in manufacturing can be found in the books in [17-20] and the following related periodicals:

- *Journal of Cybersecurity Education Research and Practice*
- *Journal of Cybersecurity*
- *Security Magazine*
- *Journal of Manufacturing Systems*
- *Manufacturing Letters*

REFERENCES

1. "A comprehensive guide to manufacturing cyber security,"

   https://www.missionsecure.com/manufacturing-cyber-security

2. E. Forsyth, " The 5 most common cybersecurity threats to manufacturers," October 2019,

   https://www.nist.gov/blogs/manufacturing-innovation-blog/5-most-common-cybersecurity-threats-manufacturers

3. "Eliminating the complexity in cybersecurity with artificial intelligence,"

   https://www.wipro.com/cybersecurity/eliminating-the-complexity-in-cybersecurity-with-artificial-intelligence/

4. 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.

5. 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.

6. "FCC Small Biz Cyber Planning Guide,"

   https://transition.fcc.gov/cyber/cyberplanner.pdf

7. "The 8 most common cybersecurity attacks to be aware of,"

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

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

9. J. Miller, "Top 7 cyber attacks threatening manufacturing companies," July 2021,

   https://www.bitlyft.com/resources/cyber-attacks-threatening-manufacturing-companies

10. J. Bush, "Manufacturing under attack: Cyber security on the agenda," March 2023,

    https://www.themanufacturer.com/articles/manufacturing-under-attack-cyber-security-on-the-agenda/#:~:text=Manufacturing%20had%20a%20reported%2023.2,exploitations%20from%202020%20to%202021.

11. V. Mullet, P. Sondi, and E. Ramat, "A review of cybersecurity guidelines for manufacturing factories in Industry 4.0," *IEEE Access*, vol. 9, February 2021, pp. 23235-23263.
12. "Manufacturing cybersecurity,"
    https://www.towardzero.com/technology/manufacturing-cybersecurity
13. "Manufacturing is the most targeted sector by cyberattacks. Here's why increased security matters," May 2023,
    https://www.weforum.org/agenda/2023/03/why-cybersecurity-in-manufacturing-matters-to-us-all/
14. J. Isaacson, "What the manufacturing sector should know about cybersecurity," March 2022,
    https://www.netify.com/learning/what-you-need-to-know-cybersecurity-manufacturing
15. D. Partida, " Who's responsible for cybersecurity in industrial and manufacturing settings?" August 2021,
    https://ohsonline.com/articles/2021/08/23/cybersecurity-industrial-and-manufacturing.aspx#:~:text=The%20CIO%20or%20CSO%20can,infrastructure%20and%20train%20other%20employees
16. L. Lim and B. Amavasai, "Cybersecurity in manufacturing," https://www.databricks.com/blog/2023/03/01/cybersecurity-manufacturing.html
17. F . Liu et al., *Science of Cyber Security*. Springer, 2018.
18. K. Stouffer et al. *Cybersecurity Framework Manufacturing Profile*. US Department of Commerce, National Institute of Standards and Technology, 2017.
19. L. Thames and D. Schaefer. *Cybersecurity for Industry 4.0*. Heidelberg: Springer, 2017.
20. National Instituteof Standards, *Cybersecurity Framework Manufacturing Profile: Whitepaper (Final Draft) (NIST) (Volume 10).* 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.

IJIAET International Journal of Innovative Analyses and Emerging Technology
| e-ISSN: 2792-4025 | http://openaccessjournals.eu | Volume: 3 Issue: 6

Figure 1 Cybersecurity involves multiple issues related to people, process, and technology [3].

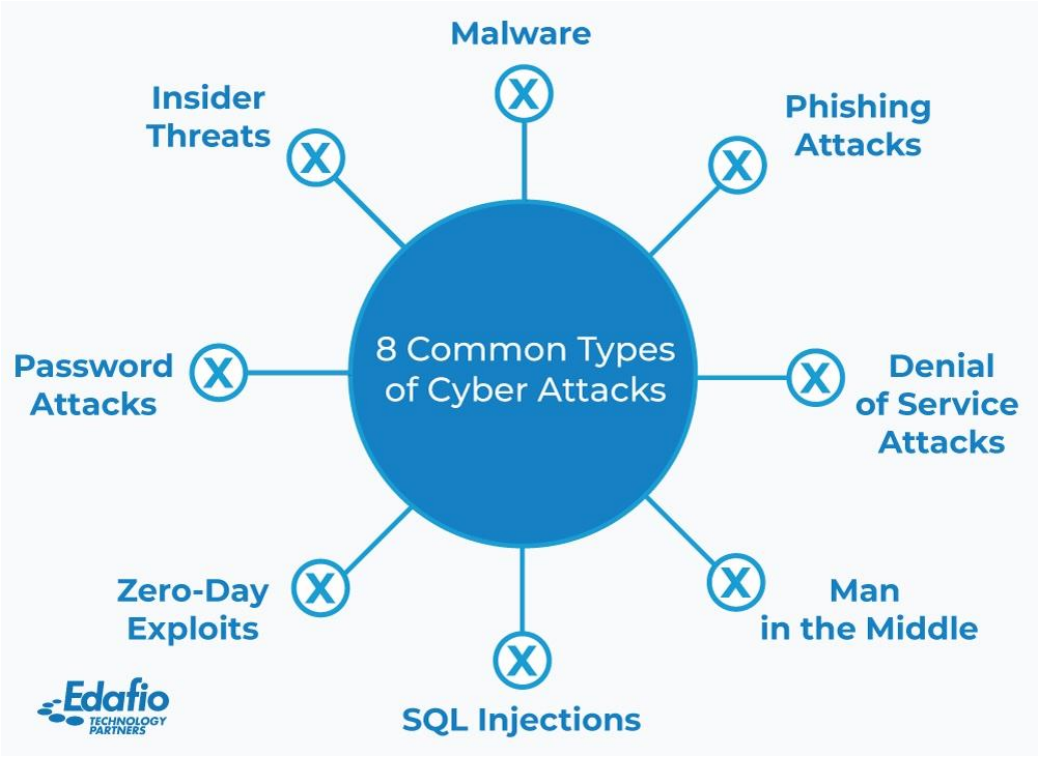

Figure 2 Common types of cyber attacks [7].

IJIAET International Journal of Innovative Analyses and Emerging Technology
| e-ISSN: 2792-4025 | http://openaccessjournals.eu | Volume: 3 Issue: 6

Figure 3 Cyber threats for manufacturing companies [9].

Figure 4 Industry 4.0 enterprise faces intense risk [12].

IJIAET International Journal of Innovative Analyses and Emerging Technology
| e-ISSN: 2792-4025 | http://openaccessjournals.eu | Volume: 3 Issue: 6

Figure 5 Robots are used in manufacturing [13].