International Multidisciplinary Research Journal Reviews (IMRJR)

International Multidisciplinary Research Journal Reviews (IMRJR)
A Peer-reviewed journal
Volume 1, Issue 1, September 2024
DOI 10.17148/IMRJR.2024.010101

Securing Healthcare IT Systems: Addressing Cybersecurity Threats in a Critical Industry

Shanavaz Mohammed[1], Muhammad Qadar Vali[2], Abdul Raheman Mohammed[3]

School of Computer and Information Sciences, University of the Cumberlands, Williamsburg, KY[1]

Jarvis College of Computing and Digital Media, DePaul University, Chicago, IL[2]

Lindsey Wilson College, Columbia, KY[3]

Abstract: The pharmaceutical industry has grown over the past decade especially with the embracing of technology in major parts of their operations. This dependence on the technology aspects has also resulted in increased vulnerability from attacks by hackers and other unauthorized persons on the internet. Various cybersecurity threats such as malware, ransomware, phishing, social engineering, insider threats, advanced persistent threats (APTs), and data breaches, have continuously caused loss of personal data as well as financial loss for companies. This research discusses these major cybersecurity threats that companies need to understand and put up measures to curb any unauthorized access to their systems. The key regulatory framework such as those outlined by HIPAA and FDA, are also explained and how companies can make sure they adhere to such guidelines. A detailed explanation of CISOs functions in pharmaceutical industry companies is also detailed herein.

Keywords: Malware, ransomware, phishing, social engineering, insider threats, advanced persistent threats (APTs), data breaches

I. INTRODUCTION

The pharmaceutical industry is responsible for the development of drugs as well as their processing and distribution to all parts of the supply chain. As the industry continues to grow in leaps and bounds, it has been forced to embrace better means of managing its resources and operations. For instance, they have been able to adapt some form of IT systems to automate and simplify their manual processes as well as ensure that there is real-time monitoring of transactions in the supply chain. They have been able to adopt technology in operations ranging from research and development (R&D) to manufacturing and distribution. These processes require huge data handling and processing which therefore means that the system needs high data integrity and protection of intellectual property to ensure data security [5]. IT systems enable pharmaceutical companies to store and analyze vast amounts of data, streamline clinical trials, manage supply chains, and comply with regulatory requirements. The industry is therefore prone to cybersecurity threats due to the high value data that is held. There have been several data breaches in the past that have led to loss of crucial data and financial losses. It therefore is crucial to understand the cybersecurity threats that are present and how to protect against these threats so as to ensure continued trust from stakeholders and regulatory bodies. By exploring the nature of these threats and the potential impacts of security breaches, the paper seeks to provide a comprehensive understanding of the current cybersecurity landscape within this sector.

II. OVERVIEW OF PHARMACEUTICAL IT SYSTEMS

There are several types of IT systems available for the pharmaceutical industry. Research and development (R&D) databases is the first type where they facilitate the collection, storage, analysis, and sharing of experimental data, enabling researchers to identify potential drug candidates, conduct preclinical studies, and manage the results of laboratory experiments [12]. This means that they store large data and they can be integrated with bioinformatics tools and models that can help hasten the process of drug discovery by ensuring accurate and efficient predictions. There are also manufacturing and supply chain management systems. These systems provide critical information on the movement and distribution of pharmaceutical products along the supply chain [9]. Information from the raw materials processing to finished goods dispatch is contained in thus system. They therefore help in tracking inventory levels, managing production schedules, and ensuring quality control. These systems are important in the pharmaceutical industry as they bring about transparency in logistical flow of drugs and other pharmaceutical products ensuring on time delivery complying with regulatory standards and reducing risks in the supply chain [6].

Another IT system in the pharmaceutical industry is the clinical Trial Management System. This system is involved in the entire testing and development phase of drugs. For instance, it is involved in the planning, tracking, and management of clinical trials.

International Multidisciplinary Research Journal Reviews (IMRJR)
A Peer-reviewed journal
Volume 1, Issue 1, September 2024
DOI 10.17148/IMRJR.2024.010101

These systems handle the complex logistics of trial design, patient recruitment, data collection, and regulatory compliance [11]. This system also facilitates communication with the stakeholders ensuring that the trial stages are conducted in accordance with the set procedures and regulations [2]. They can also handle huge amounts of data which ensures that the systems run efficiently and securely. Lastly there are patient records and healthcare IT systems. These systems help in managing the patient information and records by storing comprehensive patient data such as treatment plans, medical history, previous and current diagnostics [1].

These systems support care giving especially for the chronically ill patients. Therefore, healthcare IT systems also support pharmacovigilance activities by monitoring and reporting adverse drug reactions [18].

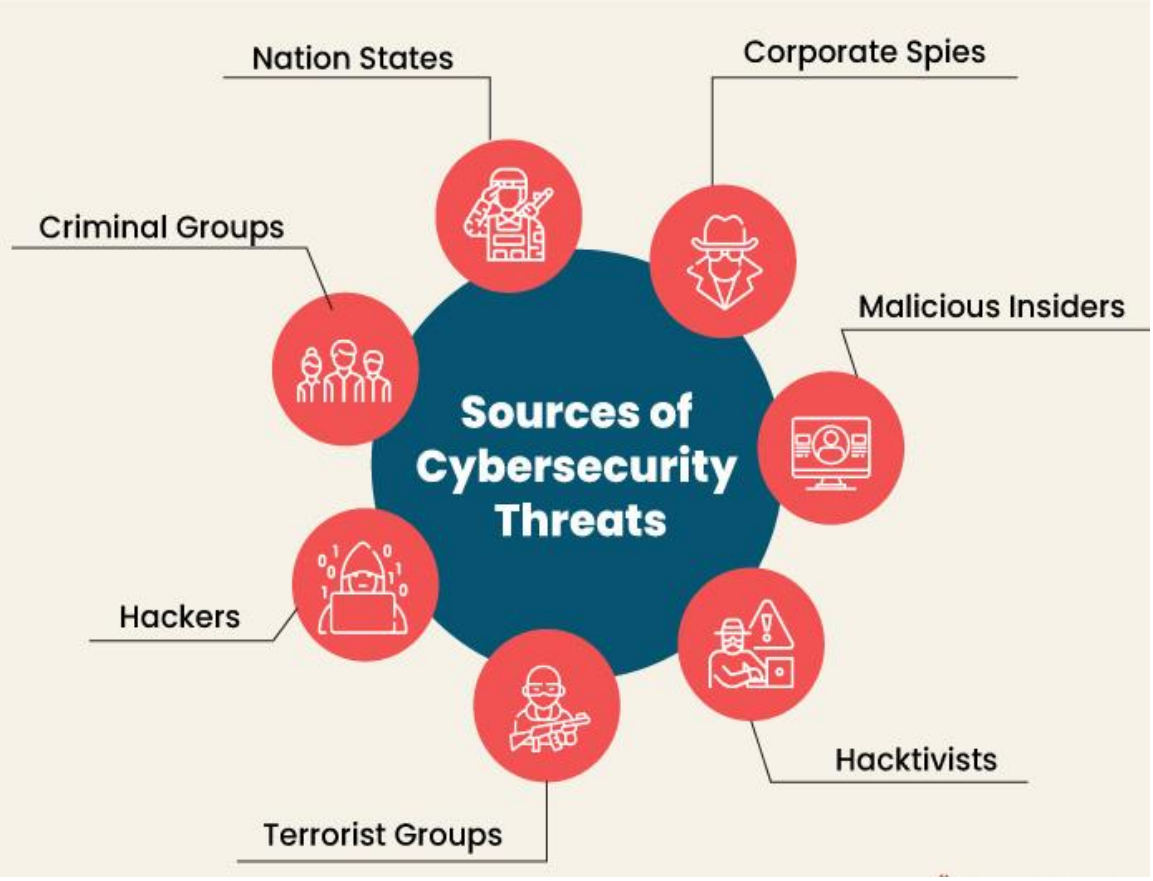

Figure 1: Common sources of cybersecurity threats

Regulatory framework of the Pharmaceutical Industry

Pharmaceutical industry as well as healthcare industry in general is regulated with very strict policies that are aimed at achieving patient data security. The most common and strict agency responsible for regulations is the Health Insurance Portability and Accountability Act (HIPAA). HIPAA provides some of the most comprehensive and up to date cybersecurity measures that organizations must adhere to. It regulates the data usage for critical entities such as the healthcare providers, health care plans and clearing houses ensuring that organizations safeguard the sensitive data while still allowing smooth operations at all times [5].

Violation of any HIPAA laws can lead to criminal or civil liabilities as outlined in their guidelines. It requires that organizations must encrypt patient data in storage or transmission at all times. It also requires that risk analysis should be conducted on a regular basis to identify any potential threats on time [20]. It also provides that access controls should be enforced in electronic systems to prevent any unauthorized entries. Lastly, it requires that employees training on current threats should be undertaken regularly.

International Multidisciplinary Research Journal Reviews (IMRJR)
A Peer-reviewed journal
Volume 1, Issue 1, September 2024
DOI 10.17148/IMRJR.2024.010101

Figure 2: Diagram illustrating 5 key purposes of HIPAA (Anwita, 2024)

Another body that is responsible for providing a framework for pharmaceutical industry players is the Food and Drug Administration (FDA). FDA has been instrumental in regulating how information is shared among the key users especially with regards to medical devices. For instance, pharmaceutical manufacturing processes must comply with Good Manufacturing Practices (GMP), which are designed to ensure products are consistently produced and controlled according to quality standards [4]. It also outlines that the supply chain operations must follow the Good Distribution Practices (GDP) to maintain product integrity during transportation and storage. One critical regulatory standard that pharmaceutical companies must adhere to is the FDA's 21 CFR Part 11, which governs the use of electronic records and electronic signatures in place of traditional paper records and handwritten signatures in FDA-regulated activities. The main aim of this section 11 is to bring about reliability and integrity around electronic records which would in turn ensure safety of medical devices. One of the provisions of Part 11 is that medical devices and electronic devices must be updated and validated regularly to ensure accurate performance. It also provides for usage of secure electronic signatures with unique IDs and authentication codes [20]. Organizations must also restrict access to electronic records as well as ensure data integrity at all times. Failure to comply with these regulations can lead to severe consequences, including regulatory actions by the FDA, which may involve penalties, product recalls, or even suspension of operations.

Cybersecurity Threats

Cybersecurity issues can be from anyone who desires to access an organizational database without proper authorization. For instance, the common sources include insiders, hackers, terrorist groups, criminal groups and nations [4]. They utilize several avenues to access these restricted areas. One of the most common cybersecurity avenue is malware and ransomware. These are malicious software that are meant to access computer systems without permission. They disrupt and damage computer programs and include viruses, Trojans and spyware. Ransomware software is used to encrypt the data in a victim's computer which results to inability to access the computer. Cyber criminals use ransomware to demand for ransom so as to restore access to the computer. Some common ransomware includes NotPetya and WannaCry software [13]. Malware and ransomware have had some significant impact on the pharmaceutical industry in the past. For instance, this software negatively affects the integrity of the data in the clinical trial stages where it disrupts the research and development process.

International Multidisciplinary Research Journal Reviews (IMRJR)
A Peer-reviewed journal
Volume 1, Issue 1, September 2024
DOI 10.17148/IMRJR.2024.010101

The loss of access to critical data and systems can delay drug development, disrupt supply chains, and result in significant financial losses [8]. Access of private information by unauthorized persons can lead to regulatory fines and which can cause loss of credibility for companies.

Another threat involves phishing and social engineering to deceive the victims into disclosing sensitive or personal details. For instance, email phishing is a common method where attackers send emails that deceive the receivers with a hope that they will reveal their passwords through clicking of links in the emails [17].

Spear phishing and pretexting are also used to deceive their receivers. In 2020, University of San Diego Health, a large pharmaceutical company in the US was a victim of email phishing where the company exposed the employees details as well as disclosing other sensitive data [15]. Another major case of phishing occurred in 2014 where Anthem Inc. was attacked and more than 78 million patient information was exposed [3]. Anthem Inc. was fined $16 million for failure to protect sensitive information.

Insider threats also present another cybersecurity threat which can either be intentional or unintentional. Insiders are employees who expose the company's information to outsiders through knowingly or unknowingly. In pharmaceutical companies, it has been recorded that almost 70% of all the cybersecurity threats are attributed to insider threats [10]. 80% of these threats are unintentional or as a result of human error. Instances of unintentional actions include sending private information to the wrong client or even leaving a computer open which allows unauthorized access to private information [18]. Stealing trade secrets in order to sell to competitors is also a form of intentional exposure threats.

Data breaches and intellectual property theft is another cybersecurity threat that has been prone to the pharmaceutical industry. Data breaches occur when the security systems are not strong enough to keep off attackers. Lack of a robust control system, or lack of appropriate measures to prevent any vulnerabilities, or even poor storage of credentials can lead to data breaches [4].

Attackers usually exploit software vulnerabilities, use stolen credentials, or employ brute-force attacks to gain unauthorized access to sensitive data. Insufficient network segmentation and inadequate encryption practices can further expose valuable information to attackers [14]. Intellectual properties have also been stolen as a result of data breaches leading to loss of market share and financial loss as well. These breaches have also led to loss of pharmaceutical research data which delays the drug development and discovery processes.

Lastly, Advanced Persistent Threats (APTs) are threats that go on for a very long time and the victims do not realize of the breach for a long time [7]. Attackers gain initial entry to computer or security system and stay in the systems without detection. They rarely do exploits in the initial days but they observe for future attacks.

APTs are characterized by their sophisticated techniques, including social engineering, zero-day exploits, and custom malware [16]. Attackers often aim to steal sensitive information, such as intellectual property, trade secrets, and strategic plans. One of the most notable incidents that occurred in the pharmaceutical industry is the 2020 cyberattack on Pfizer during the COVID-19 pandemic [3]. The attackers' intentions were to steal the COVID vaccine research data.

What can be done to counter the cyber threats?

The main person in charge of ensuring that pharmaceutical companies are safeguarded against the cyber-attacks is the Chief Information Security Officers (CISOs). He must ensure that regulatory compliance is adhered to among other safety measures. For instance, he must ensure that there is a comprehensive cybersecurity strategy in place that is tailor made for the specific company's industrial and regulatory landscape.

This plan should be determined keeping in mind the company goals and objectives as well as the mission statement. The most important objectives for any pharmaceutical company in line with cybersecurity is to safeguard the clinical trial data, patient information as well as the company's intellectual property. It should also plan to engage current as well as future emerging threats.

International Multidisciplinary Research Journal Reviews (IMRJR)
A Peer-reviewed journal
Volume 1, Issue 1, September 2024
DOI 10.17148/IMRJR.2024.010101

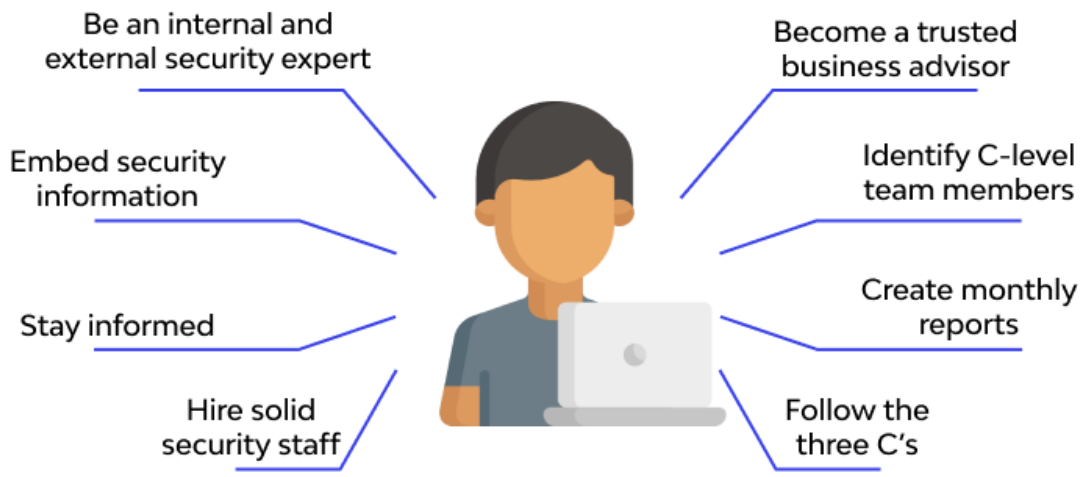

Figure 3: Diagram showing the role of CISOs (Ivan, 2024)

Another key undertaking that CISOs should complete is a thorough risk assessment for the company's assets. This exercise is meant to identify any threats before they cause much damage to the systems. They must undertake a risk assessment of the IT infrastructure to identify ant potential weaknesses or vulnerabilities that might expose the firm to cyberattacks. For instance, they must address any software weaknesses or human factor that might bring about vulnerability. This proactive approach helps in minimizing the damage from potential breaches and ensuring that the company's defenses are robust and up-to-date.

CISOs must also ensure that governance and cybersecurity policies are well outlined. These policies must outline the roles and responsibilities of all the cybersecurity personnel's in the organization. Policies must be crafted in line with industry standards and compliance requirements, such as HIPAA, GDPR, and FDA cybersecurity guidance [19]. The security agents must understand their value in maintaining the security of the organization's digital assets and should always be updated on legal repercussions for failure to maintain compliance. In the same manner, the organization must ensure that they invest properly in Cybersecurity Technologies for proper security in case of attacks. Tools like CybelAngel, which offer data breach prevention, domain protection, dark web monitoring, asset discovery, and account takeover prevention, can be particularly useful in maintaining a secure IT environment [9]. Investment should be made in firewalls, intrusion detection systems, encryption, antivirus software, and multi-factor authentication. By securing adequate budget allocations for these technologies, CISOs can ensure robust defenses against both current and emerging threats.

Another critical area that would help protect the company from cyber-attacks is employee training and awareness. CISOs must prioritize training and awareness programs to educate employees, vendors, and partners about the importance of cybersecurity and best practices. For instance, the employee trainings must address issues such as phishing recognition, data handling procedure, and how to go about reporting data breaches. Cybersecurity must be a collective responsibility of the whole company and all the employees. They must all be aware of incident response plan that aims to stop further attack access in case of a breach. CISOs should develop and regularly update a plan that includes preparation, detection, analysis, containment, eradication, and recovery steps [11]. They must also ensure carrying out of regular drills and simulations that will test the effectiveness of the incident response plan.

The CISOs must also be vigilant with monitoring cybersecurity situation at a regular basis. This will ensure that they identify any loopholes or potential threats before they can even happen. This will also allow proper reaction before any attack fully matures. Companies can set up threat intelligence feeds that will inform them of any breaches. Collaboration with other key pharmaceutical industry key players will also help companies take action ahead of potential threats [12]. By constantly monitoring the situation, CISOs can adapt their defenses to counter new vulnerabilities as they arise, maintaining a proactive stance in cybersecurity management. CISOs should actively network with cross-functional teams within their organizations, engage with executive leadership to secure buy-in for cybersecurity initiatives, and connect with industry peers and government agencies [5]. Participation in cybersecurity communities allows for the sharing of best practices, threat intelligence, and lessons learned from previous incidents.

International Multidisciplinary Research Journal Reviews (IMRJR)
A Peer-reviewed journal
Volume 1, Issue 1, September 2024
DOI 10.17148/IMRJR.2024.010101

III. CONCLUSION

The 21st century has been keen on technology advancement in all sectors of the economy which has also results in creating new avenues for cybersecurity issues. It is therefore important for companies to recognize the threat and put in place mechanisms and measures to deal with any vulnerability created. The pharmaceutical industry's reliance on IT systems for managing critical functions—from R&D and clinical trials to manufacturing and patient records—has made it a prime target for cybercriminals. The companies need to learn from the devastating effects of the previous cyberattacks attacks and ensure that they put up measures to prevent financial and reputation loss. By adopting comprehensive cybersecurity strategies, pharmaceutical companies can safeguard their sensitive data, protect their intellectual property, and ensure the continuity of their vital operations.

REFERENCES

[1] Anwita, (2024). What is the Purpose of HIPAA (A Detailed Overview). Retrieved from https://sprinto.com/blog/what-is-the-purpose-of hipaa/#:~:text=The%20purpose%20of%20HIPAA%20is%20to%20provide%20organizations%20with%20essential,and%20responsibly%20by%20covered%20entities.

[2] Bernard, R., Bowsher, G., & Sullivan, R. (2020). Cyber security and the unexplored threat to global health: a call for global norms. *Global Security: Health, Science and Policy*, *5*(1), 134-141.

[3] Devliyal, S., Goyal, H. R., & Sharma, S. (2023, May). Cyber Attack Detection Techniques in Cyber Physical System for Pharmaceutical Care Services. In *2023 Third International Conference on Secure Cyber Computing and Communication (ICSCCC)* (pp. 281-286). IEEE.

[4] George, A. S., Baskar, T., & Srikaanth, P. B. (2024). Cyber threats to critical infrastructure: assessing vulnerabilities across key sectors. *Partners Universal International Innovation Journal*, *2*(1), 51-75.

[5] He, Y., Aliyu, A., Evans, M., & Luo, C. (2021). Health care cybersecurity challenges and solutions under the climate of COVID-19: Scoping review. *Journal of medical Internet research*, *23*(4), e21747.

[6] Huff, A. J., Burrell, D. N., Nobles, C., Richardson, K., Wright, J. B., Burton, S. L., ... & Brown-Jackson, K. L. (2023). Management Practices for Mitigating Cybersecurity Threats to Biotechnology Companies, Laboratories, and Healthcare Research Organizations. In *Applied Research Approaches to Technology, Healthcare, and Business* (pp. 1-12). IGI Global.

[7] Ivan lee, (2024). CISO: Job Roles & Responsibilities. Retrieved from https://www.wallarm.com/what/what-is-chief-information-security-officer-ciso

[8] Lehto, M., Neittaanmäki, P., Pöyhönen, J., & Hummelholm, A. (2022). Cyber security in healthcare systems. In *Cyber Security: Critical Infrastructure Protection* (pp. 183-215). Cham: Springer International Publishing.

[9] Lopez, J. J. (2024). Maximising pharma's data security with a layered defence system. *Manufacturing Chemist*, *95*(1), 26-29.

[10] Mohammed, Z. A., Mohammed, M., Mohammed, S., & Syed, M. (2024). Artificial Intelligence: Cybersecurity threats in pharmaceutical IT systems.

[11] Nadikattu, R. R. (2020). New Ways of Implementing Cyber Security to Help in Protecting America. *Journal of Xidian University*, *14*(5), 6004-6015.

[12] Ntantogian, C., Laoudias, C., Honrubia, A. J. D., Veroni, E., & Xenakis, C. (2021). Cybersecurity threats in the healthcare domain and technical solutions. In *Handbook of Computational Neurodegeneration* (pp. 1-29). Cham: Springer International Publishing.

[13] Priyadarshini, I., Kumar, R., Tuan, L. M., Son, L. H., Long, H. V., Sharma, R., & Rai, S. (2021). A new enhanced cybersecurity framework for medical cyber physical systems. *SICS Software-Intensive Cyber-Physical Systems*,1-25.

[14] Radhakrishnan, V. (2023). Review Analysis of CyberSecurity in Healthcare System: A Systematic Approach of Modern Development.*International Journal of Innovative Research in Computer Science &Technology*,*11*(3),38-42.

[15] Salama, R., Altrjman, C., & Al-Turjman, F. (2024). Healthcare cybersecurity challenges: a look at current and future trends. *Computational Intelligence and Blockchain in Complex Systems*, 97-111.

[16] Sandhane, R., Patil, K., & Sharma, A. R. (2024, February). Cyber Security Risk Assessment for Electronic Medical Records (EMRs). In *2024 4th International Conference on Innovative Practices in Technology and Management (ICIPTM)* (pp. 1-6). IEEE.

[17] Shekokar, N. M., Vasudevan, H., Durbha, S. S., Michalas, A., Nagarhalli, T. P., Mangrulkar, R. S., & Mangla, M. (Eds.). (2022). *Cyber Security Threats and Challenges Facing Human Life*. CRC Press.

[18] Solfa, F. D. G. (2022). Impacts of cyber security and supply chain risk on digital operations: evidence from the pharmaceutical industry. *International Journal of Technology, Innovation and Management (IJTIM)*, *2*(2), 18-32.

[19] Yoo, C. S., & Lee, B. C. (2022). Optimizing Cybersecurity Risk in Medical Cyber-Physical Devices. *Wm. & Mary L. Rev.*, *64*, 1513.

[20] Zaldivar, D., Lo'Ai, A. T., & Muheidat, F. (2020, January). Investigating the security threats on networked medical devices. In *2020 10th annual computing and communication workshop and conference (CCWC)* (pp. 0488-0493). IEEE.