CYBER RISK ASSESSMENT IN THE PHARMACEUTICAL INDUSTRY: VULNERABILITIES, THREATS, AND GLOBAL RESPONSE STRATEGIES

PÎRCĂLĂBOIU ALEXANDRA
PHD. STUDENT, BUCHAREST UNIVERSITY OF ECONOMIC STUDIES
e-mail:pircalaboiualexandra18@stud.ase.ro

CAZONI CAMELIA
PHD. STUDENT, BUCHAREST UNIVERSITY OF ECONOMIC STUDIES
e-mail:cazonicamelia18@stud.ase.ro

CEAUȘESCU CASANDRA ELENA
PHD. STUDENT, BUCHAREST UNIVERSITY OF ECONOMIC STUDIES
e-mail: ceausescuelena23@stud.ase.ro

PETRE BOGDAN
PHD. STUDENT, BUCHAREST UNIVERSITY OF ECONOMIC STUDIES
e-mail:petremarius23@stud.ase.ro

DOBREA CĂTĂLIN RĂZVAN
PHD. PROFESSOR, BUCHAREST UNIVERSITY OF ECONOMIC STUDIES.
e-mail:razvan.dobrea@man.ase.ro

Abstract

This paper is a synthesis of cyberattacks and remediation measures at several major pharmaceutical companies, based on publicly available data. It examines notable incidents such as ransomware attacks on Merck, spear-phishing on Pfizer, and cyber espionage targeting Moderna, highlighting the operational disruptions, data breaches, and financial impacts these companies faced. The paper also evaluates the remediation strategies implemented, including enhanced cybersecurity infrastructure, data encryption, employee training, and operational continuity plans. The findings underscore the importance of a comprehensive and proactive approach to cybersecurity in mitigating the risks and minimizing the impact of future attacks on the pharmaceutical sector.

Keywords: *cyber attacks, risk management, pharmaceutical industry.*

1. Introduction and context of the study

Being in continuous development and one of the most important economic sectors globally, the pharmaceutical industry must keep up with digitalization and innovation, which have an impact on health and economic development [18]. As this industry continues to evolve, it becomes increasingly dependent on information systems and digital technologies, and the risks associated with cybersecurity are becoming more relevant [11]. Data protection and cybersecurity become important in the pharmaceutical industry to ensure the integration and confidentiality of sensitive information, such as patients' personal data or the intellectual property of pharmaceutical companies [3].

Over the years, the rapid digitalization of processes in the pharmaceutical industry, such as production, distribution, or research and development, has led to the accumulation of more sensitive

data. For large pharmaceutical companies that produce drugs, the most important and valuable asset is intellectual property, as innovations in the field of medicines are protected by patents, giving them a competitive advantage in the market [13].

Drug manufacturers invest large amounts of money and resources in the research and development of new treatments, and the protection of these investments is crucial for their long-term success and sustainability [3]. The theft of intellectual property can not only compromise the competitive advantage but also lead to significant economic losses and potentially affect investor confidence [4].

The pharmaceutical industry manages a large volume of personal data about patients, such as treatment information or medical history [4]. This data is extremely sensitive and is protected by strict international regulations, such as the General Data Protection Regulation (GDPR) in the European Union and the Health Insurance Portability and Accountability Act (HIPAA) in the United States [7]. In this context, a data breach or compromise of this data can lead not only to financial and reputational losses, but also to severe legal sanctions.[9]. The main cyber threats targeting the pharmaceutical sector are: intellectual property theft, phishing and malware attacks, ransomware attacks, as well as attempts to compromise patient data [8].

The main objective of this paper is to conduct a detailed assessment of cyber risks within the information systems of the pharmaceutical industry, identifying key vulnerabilities and cyber threats, and proposing effective measures for protection and prevention of attacks. Additionally, it provides a synthesis of the main cyberattacks and the security measures adopted by leading pharmaceutical companies worldwide**.**

To achieve the main objective of the paper, we have formulated the following research questions:

1. What are the main cyber risks in the pharmaceutical industry, given the sensitive nature of the data handled?

2. How do cyberattacks impact the operations of pharmaceutical companies?

3. What are the most effective measures to protect data and information systems in the pharmaceutical industry against cyber threats?

The paper is structured as follows: the theoretical part, which defines the key terms of the paper, the methodology used for data collection and analysis, the case studies analyzed, and the final part highlights the solutions proposed to address cyberattacks.

2. Literature review

Cybersecurity has become an increasingly important component in recent years for protecting personal data and critical infrastructures [10]. Cyberattacks have increased, leading to the development of advanced practices and technologies to prevent and combat these threats [5]. Cyberattacks vary based on the methods used and the attackers' objectives. The most common are phishing attacks, malware attacks, ransomware, Distributed Denial of Service (DDoS) attacks, man-in-the-middle attacks, software vulnerability exploitation, and social engineering attacks [1].

Phishing is one of the most common forms of cyberattack, aiming to obtain sensitive information such as login credentials or credit card data through deceptive messages. Generally, attackers pose as trusted entities like banks or companies and convince victims to provide personal data. According to a recent report, 86% of organizations encountered at least one phishing attempt in 2023 [3].

Malware is a general term referring to any harmful software designed to infect a system, corrupt or steal data, and cause significant damage. Common types of malware include viruses, trojans, and spyware [6].

Ransomware is also a form of malware that encrypts user data and demands a ransom for its decryption [17]. This type of attack has particularly targeted hospitals, government institutions, and financial organizations [23]. After infiltrating a system, attackers encrypt files and display a ransom note, usually demanding payment in a cryptocurrency like Bitcoin. According to a study by Check Point Research (2021), ransomware attacks increased by 57% in the first six months of 2021, and organizations pay an average of $150,000 to recover their data.

Distributed Denial of Service (DDoS) attacks aim to overload a server or network by sending massive amounts of traffic, rendering the targeted systems unable to serve users. [29]Typically, attackers use a network of infected computers, known as a "botnet," to launch these attacks. For example, in 2020, a massive DDoS attack on Amazon Web Services generated 2.3 Tbps of traffic, making it one of the largest attacks in history [1].

Man-in-the-middle (MITM) attacks involve intercepting and altering communication between two parties without their knowledge. They are used to intercept sensitive data transmitted between users and servers, such as passwords or banking details [17]. MITM attacks can occur on unsecured Wi-Fi networks when users connect to public hotspots without proper encryption. According to a study by Symantec (2024), such attacks are becoming increasingly frequent in corporate environments.

Exploiting software vulnerabilities is another type of cyberattack that involves leveraging "weak points" or errors in software to gain unauthorized access to a system or cause damage. For instance, attackers can exploit unpatched software vulnerabilities to gain privileged access to internal networks or install malware on a system [11].

Social engineering attacks involve manipulating users into revealing sensitive information or performing actions that could compromise system security. A common example is "vishing," a variant of phishing where attackers call victims pretending to be representatives of banks or other trusted institutions to obtain financial data [4].

This variety of cyberattacks reflects technological evolution and poses significant risks to organizations and individuals. In Figure 1, the weekly average of global cyberattacks per industry is represented, according to the study conducted by CheckPoint Blog in 2023. We can observe that the majority of cyberattacks target the education, government, and healthcare and pharmacy industries.

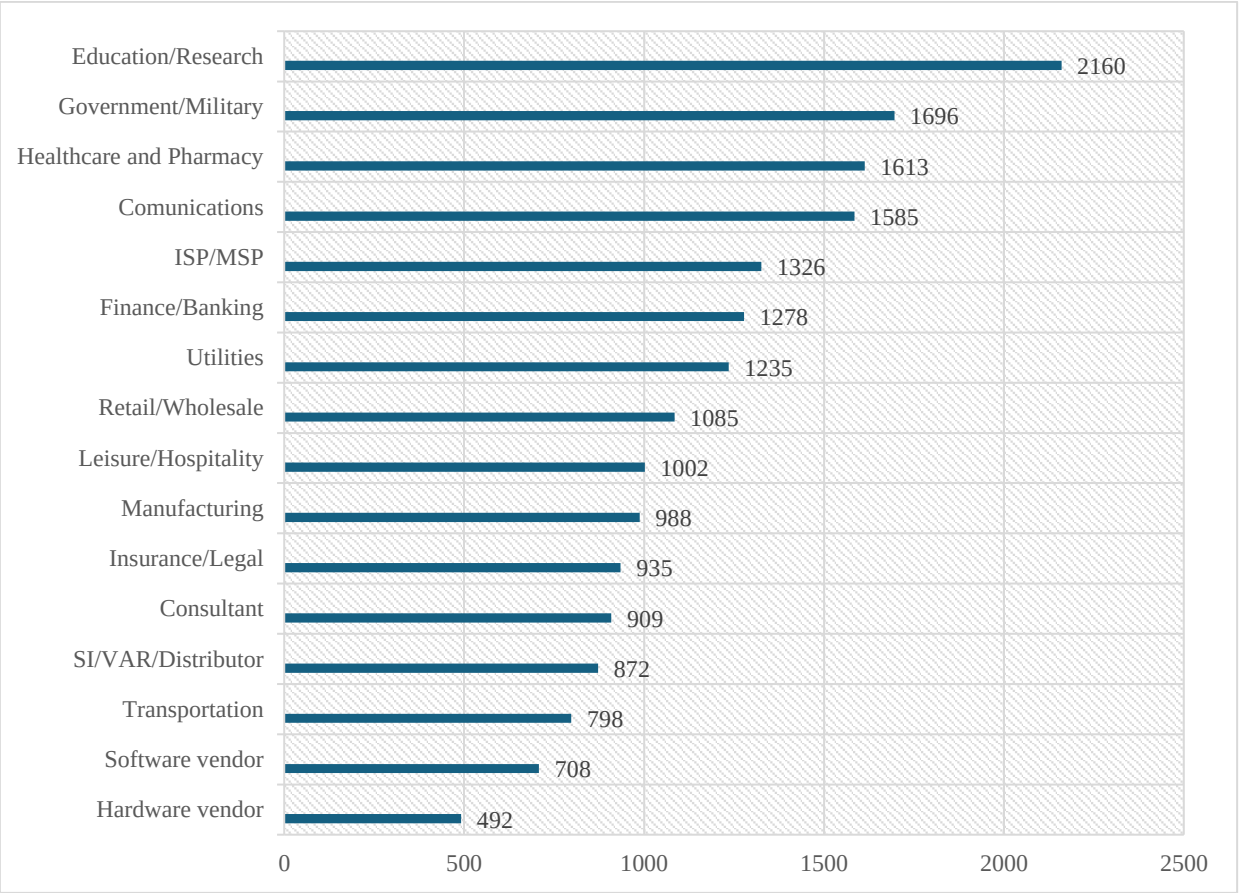

Figure No 1. Weekly average of global cyberattacks per industry,
Souce: authors based on information from [3]

In the era of digitalization, pharmaceutical companies have begun to use modern technologies to streamline their processes, including data management and clinical research. IBM Security produced a report in 2021 demonstrating that patient data, drug research and development data, or trade secrets are highly valuable on the digital black market. This makes the pharmaceutical industry an attractive target for hackers [16].

The storage and transmission of confidential data, which can be exposed to attacks, represent one of the greatest weaknesses in this industry. Research and development data, including clinical trial results and drug formulas, hold the highest value for competitors. Additionally, pharmaceutical companies frequently collaborate with external suppliers, including research contractors and distribution organizations, increasing the number of vulnerable access points to a cyberattack [15]

Beyond the enormous financial losses, cyberattacks can slow scientific research progress by disrupting access to essential data, which can negatively impact international collaborations and the production of new drugs and treatments [3].

Pharmaceutical companies invest billions of dollars in developing new drugs, and attackers attempt to steal this information to provide a competitive advantage to other companies [22]. Attacks are generally motivated by financial purposes but also by industrial espionage. In 2020, a study by Microsoft showed that during the COVID-19 pandemic, cyberattacks on pharmaceutical companies involved in vaccine and treatment development increased, highlighting attackers' interest in accessing critical data related to sensitive projects.

The biggest cybersecurity concerns in the pharmaceutical industry, represented in Figure 2, are social engineering and the human factor, ransomware, malware, state-sponsored hackers, distributed DDoS attacks, and outdated tools and unpatched systems.

The healthcare sector, including pharmacies, was among the most affected by ransomware, as they have extended recovery times and major financial losses in the event of a security breach [17].

Nation-states sponsor such attacks for various reasons, including industrial espionage or sabotaging the healthcare systems of other countries. Pharmacies, being connected to hospitals and larger health networks, become a vulnerable point in this ecosystem, allowing access to strategic information [14].

Unfortunately, many pharmacies do not implement effective employee awareness and training programs, which exposes them to major security risks, such as voice phishing/vishing attacks [2].

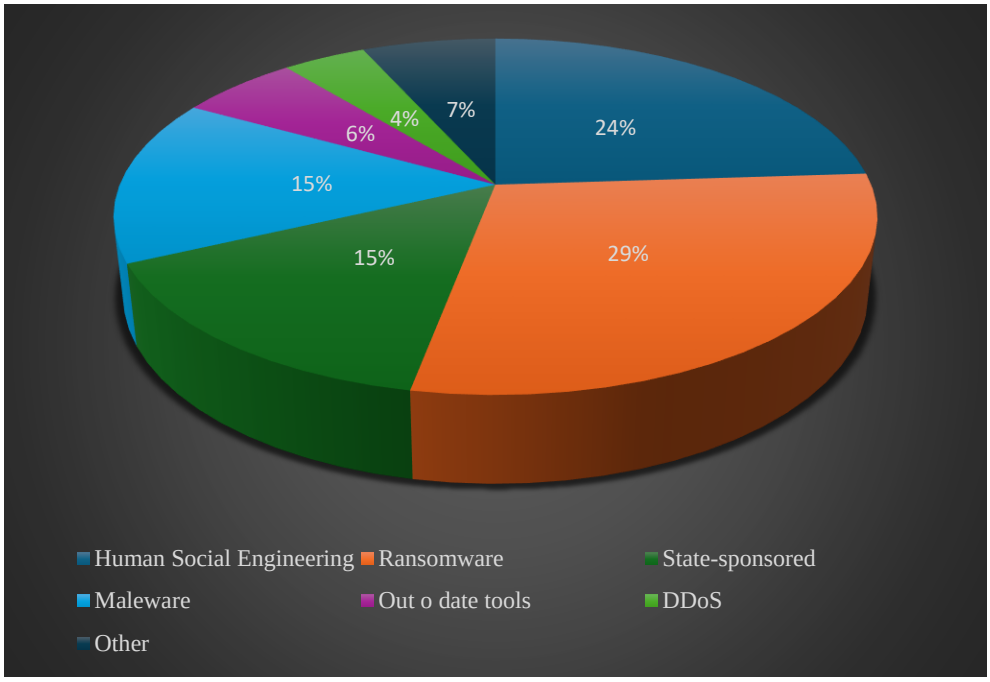

Figure No 2. The biggest cybersecurity concerns
Source: authors based on informations from [20]

3. Methodology

In recent years, many companies have become vulnerable and targeted by cyberattacks due to the immense volume of sensitive data they handle. Additionally, the COVID-19 pandemic amplified this vulnerability, as pharmaceutical companies became attractive targets for hackers, including state-sponsored attacks eager to gain access to important discoveries, such as vaccines. Once cyberattacks were amplified by COVID-19, a multiple case study analysis was chosen to understand the risks faced by the analyzed companies, as well as to assess the impact and potential mitigations.

This research method is particularly effective for understanding complex phenomena within their real-world context, especially when there are multiple variables at play and the boundaries between the phenomenon and the context are not clearly evident [31].

The multiple case study approach allows for a more comprehensive analysis by examining several companies in the pharmaceutical sector [30]. This method enables the researcher to identify common patterns and divergences across different cases, offering a richer understanding of how various organizations respond to cyber threats [14]. Additionally, the use of multiple cases enhances the generalizability of the findings, as they are not based on a single instance, but on a broader range of experiences.

Table no 2. Advantages and disadvantages of multiple case study methodology

Advantage	Disavantages
Examining multiple cases can increase the reliability of the study.	A risk of overgeneralizing findings if significant contextual differences between cases are not adequately considered.
A holistic view of the phenomenon under investigation.	Given the complexity of the data generated by multiple cases, it can be challenging to synthesize and integrate findings across cases.
In multiple case studiesprovides rich, in-depth data.	One of the major drawbacks of multiple case studies is that they are time-consuming and require significant resources to conduct
Multiple case studies facilitate cross-case analysis**,** enabling researchers to compare and contrast different companies' responses to similar situations.	Obtaining access to confidential data.
Allows for broader generalizability of findings.	

Source: authors

The case studies presented below illustrate the diversity and magnitude of cyber risks faced by the pharmaceutical industry, including ransomware attacks, cyber espionage, and insider threats. Moreover, these examples highlight the recovery strategies used by companies to minimize losses and restore critical operations. Table no. 3 presents the pharmaceutical companies that have been subject to the largest cyberattacks.

Table no. 3. Key information on major pharmaceutical companies

Company	Founded	Revenue (2023/2024)	Brief Description
Merck & Co.	2000	$62.48 milions (june 2024)	Merck & Co., known as MSD outside North America, is a global leader in pharmaceuticals, focusing on oncology, vaccines, and cardiometabolic treatments [26].
Pfizer	1849	$55,16 millions (june 2024)	Pfizer is a leading American pharmaceutical company, famous for developing vaccines, including the COVID-19 vaccine [28].
Moderna	2010	$5, 05 millions (june 2024)	Moderna is a biotechnology company based in the U.S., specializing in messenger RNA (mRNA) therapies, known for its COVID-19 vaccine [27].
AstraZeneca	1999 (via merger)	$49.13 millions (june 2024)	AstraZeneca is a British-Swedish biopharmaceutical company, focused on developing treatments for oncology, cardiovascular, and respiratory diseases [24].
Bayer	1863	€ 47,11 millions (june 2024)	Bayer is a German multinational, known for innovations in health care and agriculture, with products like aspirin and cancer treatments [25].

Source: authors based on informations from [25], [26],[27],[28], [29]

4. Major cyberattacks in pharmaceutical companies

In 2017, Merck & Co., one of the largest pharmaceutical companies in the world, was severely impacted by a global ransomware attack known as NotPetya. This attack caused significant disruptions to the company's operations and led to losses of nearly $1.4 billion. Merck managed to recover some of the losses through a legal action against its insurer, who initially refused payment, citing a war exclusion clause [12].

Pfizer fell victim to a spear-phishing attack targeting its clinical research. Hackers accessed sensitive information about drug development, jeopardizing the confidentiality of the research and causing major reputational risks for the company [21].

Moderna, the developer of one of the first COVID-19 vaccines, was targeted by a cyberattack from state actors attempting to steal vaccine data. The company detected and countered the attack, protecting its intellectual property [19].

AstraZeneca uncovered an insider threat in 2019, when an employee attempted to steal sensitive commercial data. The incident was prevented in time, but it underscored the need for rigorous data access management [8]

Bayer was affected by a cyberattack on IoT devices in its production systems. Hackers compromised automated processes, causing delays and impacting production quality [17].

For each case, the type of cyberattack, the specific risk, and its impact have been identified and is presented in table no. 4.

Table No 4. Specific risks for each company after cyberattacks

Company	Type of Cyber Attack	Specific Risks
Merck	Ransomware (NotPetya)	Complete network shutdown
Merck	Ransomware (NotPetya)	Loss of financial data
Merck	Ransomware (NotPetya)	Disruption of drug manufacturing
Merck	Ransomware (NotPetya)	Inability to access research files
Merck	Ransomware (NotPetya)	Significant operational delays
Pfizer	Spear-Phishing	Compromise of employee credentials
Pfizer	Spear-Phishing	Unauthorized access to sensitive research
Pfizer	Spear-Phishing	Loss of intellectual property
Pfizer	Spear-Phishing	Reputation damage from data leaks
Pfizer	Spear-Phishing	Phishing spread across departments
Moderna	Cyber Espionage	Theft of vaccine development data
Moderna	Cyber Espionage	Competitors gaining access to proprietary information
Moderna	Cyber Espionage	State-sponsored hacking attempts
Moderna	Cyber Espionage	Intellectual property theft
Moderna	Cyber Espionage	Exposure of confidential communications
AstraZeneca	Insider Threat	Insider theft of intellectual property
AstraZeneca	Insider Threat	Exposure of confidential R&D data
AstraZeneca	Insider Threat	Insider sabotage of systems
AstraZeneca	Insider Threat	Reputational damage
AstraZeneca	Insider Threat	Legal consequences from data leaks
Bayer	IoT Attack	Compromise of IoT devices in production
Bayer	IoT Attack	Remote access to industrial systems
Bayer	IoT Attack	Tampering with automated processes

Bayer	IoT Attack	Delays in drug manufacturing
Bayer	IoT Attack	Financial losses from production downtime

Source: authors

The case studies analyzed highlight different types of cyberattacks: ransomware (Merck), spear-phishing (Pfizer), cyber espionage (Moderna), and attacks on IoT devices (Bayer). The risk matrix, Figure no 3, allowed for a systematic assessment of the specific risks associated with each attack, providing a clear perspective on the impact and mitigation measures necessary to minimize damages. For example, in the case of the NotPetya attack on Merck, loss of financial data was assessed as "very high", and mitigation measures include regular security updates and robust recovery plans Similarly, in the case of Pfizer, spear-phishing attacks highlighted the risk of compromising sensitive research data, necessitating encryption solutions and employee awareness programs [12].
The use of the risk matrix (Figure no. 3) helped prioritize the cybersecurity issues faced by pharmaceutical companies, emphasizing the need for comprehensive cybersecurity strategies that include preventive measures, early threat detection, and business continuity plans.

	Negligible	**Minor**	**Moderate**	**Significant**	**Severe**
Very Likely			Complete network shutdown (**Merck)** Reputation damage from data leaks (**Pfizer)** State-sponsored hacking attempts (**Moderna)** Exposure of confidential R&D data **(AstraZeneca)**	Compromise of employee credentials (**Pfizer)** Phishing spread across departments **(Pfizer)** Tampering with automated processes	Theft of vaccine development data **(Moderna)** Loss of financial data (**Merck)** Exposure of confidential communications **(Moderna)**
Likely			Disruption of drug manufacturing (**Merck**) Compromise of IoT devices in production (**Bayer)**	Significant operational delays(**Pfizer)** Insider sabotage of systems **(AstraZeneca)** Delays in drug manufacturing (**Bayer)**	Competitors gaining access to proprietary information **(Moderna)** Legal consequences from data leaks **(AstraZeneca)** Remote access to industrial systems (**Bayer)**
Possible			Inability to access research files (**Merck**) Reputational damage **(AstraZeneca)**	Unauthorized access to sensitive research (**Merck)** Compromise of employee credentials (**Pfizer)**	Insider theft of intellectual property **(AstraZeneca)** Intellectual property theft **(Moderna)** Financial losses from production downtime (**Bayer)**
Unlikely					
Very Unlikely					

Figure No 3. Risk matrix
Source: authors

5. Remediation solutions for cyberattack

Remediation solutions for cyberattacks in the pharmaceutical industry require an integrated, multidimensional approach that addresses technological, procedural, and human aspects. First, improving cybersecurity infrastructure is essential to prevent ransomware attacks and reduce vulnerabilities in critical systems. After the NotPetya attack, Merck realized the importance of developing backup and recovery solutions not only at the local level but also globally, to ensure redundancy and prevent the complete shutdown of operations. The company invested significantly in IT infrastructure, ensuring that all essential systems are consistently updated with the latest security patches and implementing active network monitoring to detect abnormal activity in real-time.This approach not only reduces the risk of future attacks but also enhances the organization's ability to respond quickly to incidents, minimizing recovery time and financial impact.

In addition to technological improvements, special attention must be given to managing and protecting sensitive data. Given that pharmaceutical companies hold valuable information related to clinical research and intellectual property, spear-phishing attacks and cyber espionage have become major concerns. Pfizer, after experiencing a spear-phishing attack, implemented a set of preventive measures, including advanced encryption of sensitive data and adopting two-factor authentication solutions for all critical data access. These encryption measures protect the information even if intercepted by attackers, while multifactor authentication reduces the risk of an attacker gaining access to internal systems through stolen credentials. Moreover, Pfizer and other companies have recognized the importance of employee training to identify and appropriately respond to phishing attacks or other social engineering methods. Employee awareness of the tactics used by hackers is crucial, as one careless click can pave the way for a devastating cyberattack.

Table No 5. Impact and mitigation for each specific risks

Company	Type of Cyber Attack	Specific Risks	Impact	Mitigation
Merck	Ransomware (NotPetya)	Complete network shutdown	Severe disruption to global operations	Improve global network security, frequent system updates
Merck	Ransomware (NotPetya)	Loss of financial data	Loss of critical financial data, risking compliance issues	Encryption and secure backups of financial data
Merck	Ransomware (NotPetya)	Disruption of drug manufacturing	Delayed drug production, affecting supply chain	Implement redundant manufacturing systems
Merck	Ransomware (NotPetya)	Inability to access research files	Research and development delays	Enhanced disaster recovery plans
Merck	Ransomware (NotPetya)	Significant operational delays	Long-term operational delays	Long-term system monitoring and upgrades
Pfizer	Spear-Phishing	Compromise of employee credentials	Loss of sensitive data affecting competitive advantage	Advanced email filtering and employee training
Pfizer	Spear-Phishing	Unauthorized access to sensitive research	Major breach in intellectual property protection	Encryption of research and development files
Pfizer	Spear-Phishing	Loss of intellectual property	Confidential research exposed to competitors	Restrict access to sensitive IP via multi-factor authentication
Pfizer	Spear-Phishing	Reputation damage from data leaks	Reputation loss among stakeholders	Crisis management and PR strategies for reputation

Pfizer	Spear-Phishing	Phishing spread across departments	Widespread phishing attacks increasing vulnerability	Company-wide phishing awareness programs
Moderna	Cyber Espionage	Theft of vaccine development data	Critical loss of vaccine development data	Advanced threat detection and monitoring
Moderna	Cyber Espionage	Competitors gaining access to proprietary information	Proprietary data in competitors' hands	Isolate critical systems and IP
Moderna	Cyber Espionage	State-sponsored hacking attempts	Long-term IP theft affects future projects	Collaboration with government agencies for protection
Moderna	Cyber Espionage	Intellectual property theft	Loss of international trust in proprietary technology	Cybersecurity drills for handling IP breaches
Moderna	Cyber Espionage	Exposure of confidential communications	Diplomatic tensions due to state-sponsored hacks	Strengthen encryption on all communications
AstraZeneca	Insider Threat	Insider theft of intellectual property	Loss of valuable IP affecting long-term competitiveness	Monitor employee access to sensitive data
AstraZeneca	Insider Threat	Exposure of confidential R&D data	Legal actions from exposed confidential data	Restrict insider access to valuable IP
AstraZeneca	Insider Threat	Insider sabotage of systems	Sabotage of R&D projects leads to severe financial impacts	Implement behavioral analysis for insider risk
AstraZeneca	Insider Threat	Reputational damage	Long-lasting reputational damage	Enforce strict legal consequences for insider threats
AstraZeneca	Insider Threat	Legal consequences from data leaks	Potential government penalties for insider vulnerabilities	Create awareness campaigns about insider risks
Bayer	IoT Attack	Compromise of IoT devices in production	Full compromise of production IoT systems	Isolate IoT networks from production systems
Bayer	IoT Attack	Remote access to industrial systems	Unauthorized remote access to industrial systems	Regular audits of IoT system vulnerabilities
Bayer	IoT Attack	Tampering with automated processes	Alteration of automated production processes	Frequent security patching for IoT devices
Bayer	IoT Attack	Delays in drug manufacturing	Delayed production timelines causing financial losses	Monitor and restrict external access to IoT systems
Bayer	IoT Attack	Financial losses from production downtime	Loss of customer trust due to compromised drug quality	Develop IoT-specific disaster recovery plans

Source: authors

6. Conclusions

The main risks in the cyber industry are the compromise of patient data and the loss of intellectual property. In the analysis conducted in this paper, it was emphasized that the pharmaceutical industry is exposed to major cyber risks due to the sensitive nature of the data it handles, such as clinical research and intellectual property. This sensitivity makes the pharmaceutical sector an attractive target for attackers, given the strategic and financial value of the stored information. In particular, the major cyber risks identified in this industry include ransomware attacks, phishing, insider threat and IoT Attack. These attacks not only target data theft but also disrupt critical operations, which can have long-term consequences for the companies involved.

They affect the daily operations of these companies, often causing delays in the production of medicines, which can lead to shortages in the market and, consequently, considerable financial losses.

For example, the attack on Merck resulted in massive production disruptions and the loss of essential data for the development and production of new medicines. Similarly, Pfizer was affected by data compromise, which impacted the company's ability to remain competitive and undermined public trust in these large corporations.

To counter these threats, pharmaceutical companies have begun to implement stricter cybersecurity measures. Enhancing security infrastructure is one of the most effective solutions, including the use of advanced data encryption to protect sensitive information.

In conclusion, a proactive and integrated approach is important to effectively protect pharmaceutical companies against evolving cyber threats. This requires continued investment in security technologies and close collaboration between IT, operations, and human resources teams to minimize risks and ensure the protection of valuable digital assets.

Further research can continue with the collection of more examples of cyberattacks and a deeper cause-effect analysis of these incidents, as well as the extraction of best practices for other companies in the field.

7. References

[1] **Aamir M, Zaidi SMA** 2020 DDoS attack detection with feature engineering and machine learning: The framework and performance evaluation. International Journal of Information Security ;18(6):761–785. doi: 10.1007/s10207-019-00434-1

[2] **Aassal A, El S, Baki A. Das, Verma RM.** 2020 An in-depth benchmarking and evaluation of phishing detection research for security needs. IEEE Access. 2020;8:22170–22192. doi: 10.1109/ACCESS.2020.2969780.

[3] **Check Point Research** 2021, A Continuing Cyber-Storm with Increasing Ransomware Threats and a Surge in Healthcare and APAC region. Retrieved from :https://blog.checkpoint.com/security/a-continuing-cyber-storm-with-increasing-ransomware-threats-and-a-surge-in-healthcare-and-apac-region/, Accessed on: 30 august 2024

[4] **Check Point Research** 2024, Cyber attacks trends: 2021 mid-year report. Retrieved from: https://research.checkpoint.com, Accessed on: 30 august 2024

[5] **CISCO** 2024, What is cybersecurity? Retrieved from :https://www.cisco.com/site/us/en/learn/topics/security/what-is-cybersecurity.html , Accessed on: 30 august 2024

[6] **Coveware** 2020 Ransomware payments continue to climb as organizations struggle to recover. Retrieved from : https://www.coveware.com/reports, Accessed on: 27 august 2024

[7] **Cremer F, Sheehan B, Fortmann M, Kia AN, Mullins M, Murphy F, Materne S.** 2022, Cyber risk and cybersecurity: a systematic review of data availability. Geneva Pap Risk Insur Issues Pract. 2022;47(3):698-736. doi: 10.1057/s41288-022-00266-6. Epub 2022 Feb 17. PMID: 35194352; PMCID: PMC8853293.

[8] **CSO Online** 2023, How much cybersecurity expertise does a board need?, Retrieved from : https://www.csoonline.com/article/656596/how-much-cybersecurity-expertise-does-a-board-need.html , Accessed on: 5 septembrie 2024

[9] **DEDZINS, R., & JAMES, M.** 2015 BIOPHARMACEUTICAL TECHNICAL RESOURCE GUIDE. In EMERSON. Retrieved from : https://www.lakesidecontrols.com/getattachment/7846bd01-541d-4b2d-a700-17a37c651f76/article-continuous-shm-assures-pfizer-s-automation-system-performance-pharmaceutical-manufacturing-nov-2015.pdf Accessed on: 1 septembrie 2024

[10] **Deloitte** 2024, Why Cyber? Retrieved from : https://www2.deloitte.com/ro/en/pages/risk/cybersecurity/cyber-homepage.html Accessed on: 9 septembrie 2024.

[11] **Deloitte** 2024, Deloitte Cyber Industry Insights: Read the lates? Retrieved from : https://www.deloitte.com/mt/en/services/risk-advisory/services/deloitte-cyber-industry-insights-read-the-latest.html, Accessed on: 5 septembrie 2024.
[12] **Demberger, A.** 2022, Merck awarded $1.4 billion for NotPetya after 5 years of legal battle. Risk & Insurance,
[13] **Eisenhardt, K. M., & Graebner, M. E**. 2007, Theory building from cases: Opportunities and challenges. Academy of Management Journal, 50(1), 25-32, Retrieved from : https://josephmahoney.web.illinois.edu/BADM504_Fall%202019/Eisenhardt%20and%20Graebner%20(2007).pdf, Accessed on: 28 august 2024.
[14] **Field, M.** 2018, WannaCry cyber attack cost the NHS £92m as 19,000 appointments cancelled. 2018, Retrieved from : https://www.telegraph.co.uk/technology/2018/10/11/wannacry-cyber-attack-cost-nhs-92m-19000-appointments-cancelled/ Accessed on: 28 august 2024.
[15] **Fierce Pharma** 2017, A new strain of ransomware targets healthcare; cyberattack causes disruptions at NHS hospital. Fierce Pharma, Retrieved from: https://www.fiercehealthcare.com/privacy-security/a-new-strain-ransomware-targets-healthcare-another-cyberattack-causes-disruptions Accessed on: 25 august 2024.
[16] **GAO** 2021, CYBER INSURANCE—Insurers and policyholders face challenges in an evolving market. Retrieved from : https://www.gao.gov/assets/gao-21-477.pdf., Accessed on: 23 august 2024.
[17] **Greenberg, A.** 2018, The untold story of NotPetya, the most devastating cyberattack in history. Wired. Retrieved from : https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ Accessed on: 28 august 2024.
[18] **Giansanti D.** 2021, Cybersecurity and the Digital-Health: The Challenge of This Millennium. Healthcare (Basel). Jan 11;9(1):62. doi: 10.3390/healthcare9010062. PMID: 33440612; PMCID: PMC7827661.
[19] **IBM Security.** 2021, Cost of a Data Breach Report 2021. IBM. Retrieved from : https://www.ibm.com/security/data-breach 2021 Accessed on: 2 septembrie 2024.
[20] **McCaskill S.** 2017, Ransomware & Humans Are Silicon Readers' Biggest Cybersecurity Concerns. m Retrieved from : https://www.silicon.co.uk/security/biggest-security-concern-220287, Accessed on: 3 septembrie 2024.
[21] **Pharmaceutical Technology** 2021, five pharma cybersecurity breaches to know and learn from the transition to digital, expedited by the Covid-19 pandemic, has opened up new cybersecurity concerns, Retrieved from : https://www.pharmaceutical-technology.com/features/pharma-cyber-attacks/?cf-view Accessed on: 5 septembrie 2024.
[22] **Reuters** China-backed hackers 'targeted COVID-19 vaccine firm Moderna' 2020. Retrieved from : https://www.reuters.com/article/technology/exclusive-china-backed-hackers-targeted-covid-19-vaccine-firm-moderna-idUSKCN24V38H/ Accessed on: 9 septembrie 2024.
[23] **Symantec** 2024, WannaCry: The ransomware that shook the world. Retrieved from : https://www.symantec.com/research 2024. Accessed on: 9 septembrie 2024.
[24] **Stock Analysis** 2024, AstraZeneca PLC (AZN), Retrieved from : https://stockanalysis.com/stocks/azn/financials/ Accessed on: 9 septembrie 2024.
[25] **Stock Analysis** 2024, Bayer Aktiengesellschaft (BAYRY), Retrieved from : https://stockanalysis.com/stocks/bayry/financials/ Accessed on: 9 septembrie 2024.
[26] **Stock Analysis** 2024, Merck & Co., Inc. (MRK), Retrieved from : https://stockanalysis.com/stocks/mrk/financials/ , Accessed on: 9 septembrie 2024.
[27] **Stock Analysis** 2024, Moderna, Inc. (MRNA), Retrieved from : https://stockanalysis.com/stocks/mrna/financials/, Accessed on: 9 septembrie 2024.
[28] **Stock Analysis** 2024, Pfizer Inc. (PFE), Retrieved from : https://stockanalysis.com/stocks/pfe/financials/ , Accessed on: 9 septembrie 2024.

[29] **Verizon Business** 2023, Data Breach Investigation Report, Retrieved from : https://www.verizon.com/business/resources/Tbc9/reports/2023-data-breach-investigations-report-dbir.pdf . Accessed on: 10 septembrie 2024.
[30] **Yin, R. K**.. 2018, Case study research and applications: Design and methods (6th ed.). Sage.
[31] **Zhou YY, Cheng G, Jiang SQ, Dai M**. 2020, Building an efficient intrusion detection system based on feature selection and ensemble classifier. Computer Networks;174:17. doi: 10.1016/j.comnet.2020.107247