Analyzing the Sunpharma Ransomware Attack: Implications for Cybersecurity Laws, Regulations, and Guidelines in the Pharmaceutical Industry

Amolika Roy
Master Student, Cyberlaw and Information Security
National Law Institute University, Bhopal, India

Abstract

This research project delves into cyber security in the pharmaceutical industry, focusing on a significant incident involving Sun Pharmaceutical Industries. Extensive literature is analyzed to explore vulnerabilities, challenges, and the aftermath of information security breaches. It emphasizes the critical importance of cyber security governance, employee training, and proactive security measures. The study scrutinizes global regulations and guidelines that shape data protection in the industry. It also highlights the significance of domestically manufactured cyber security products in the Indian pharmaceutical sector. This research equips pharmaceutical companies with insights to enhance their information security measures.

Keywords: Cyber security, Pharmaceutical Industry, Data Breaches, Compliance, Incident Response, DPDP Act 2023, FDA Guidelines, HIPAA, FTC Regulations, Security Risk Management.

1. Introduction

In today's fast-paced world, where information and technology are paramount, the pharmaceutical and healthcare sectors are not immune to the ever-present threat of cyberattacks and data breaches. Recent incidents, such as the cyberattack on Sun Pharmaceutical Industries, highlight the vulnerabilities these industries face, which can have profound consequences on patient privacy, intellectual property, and business operations.

As the world becomes increasingly interconnected, safeguarding sensitive information, proprietary formulas, clinical research data, and personal health records is of utmost importance. The rise of cyber threats poses a grave risk to these sectors, as evidenced by attacks on pharmaceutical companies, clinical trial software providers, and medical device manufacturers. The potential consequences of such breaches, including unauthorized access to insulin pumps and vulnerabilities in medical devices, underscore the critical need for comprehensive cybersecurity measures.

In response to these challenges, governments and regulatory bodies around the world are enacting cybersecurity regulations and guidelines aimed at enhancing data protection and risk management in the pharmaceutical industry. From the DPDP Act 2023 in India to FDA recommendations for comprehensive cybersecurity risk management, these measures aim to ensure data integrity, patient safety, and industry-wide cybersecurity. This study delves into the evolving landscape of cybersecurity within the pharmaceutical and healthcare sectors, providing insights into recent threats, global regulations, and the steps required to protect valuable data, patient well-being, and the reputation of these vital industries. It examines how pharmaceutical companies, medical device manufacturers, and healthcare entities must adapt to this new era of cybersecurity to thrive in a digital world.

2. Literature Review

In Datta, ‘Ransomware Attack: Sun Pharma Says Business Operations Impacted’ [1]. The article discusses a recent cybersecurity breach at Sun Pharmaceutical Industries, attributing it to a ransomware group. This incident has impacted the company's operations and is expected to result in reduced revenue. While the group's identity remains undisclosed, it marks the third high-profile cyberattack on a major Indian drugmaker in three years. Asia witnessed a significant number of cyberattacks in 2022, with the manufacturing sector being a prominent target, according to IBM Security's X-Force Threat Intelligence Index for 2023.

Marino D, ‘Cybersecurity - Why Pharmaceutical Companies Are Vulnerable to Cyberattacks and What You Can Do to Protect Your Company’ [2]. The evolving cybersecurity landscape poses grave risks to private companies, with data breaches potentially compromising valuable digital assets, sensitive information, and critical systems. A Ponemon Institute study found that the global average cost of a data breach is $3.86 million. The pharmaceutical industry, handling sensitive drug data, faces unique challenges, including cyberattacks, employee training, and IoT-related privacy issues. To safeguard their assets, pharmaceutical firms must prioritize cybersecurity governance, employee training, and proactive

 | DOI: 10.20533/ijisr.2042.4639.2024.0123

measures such as tabletop scenarios and penetration tests. Recent incidents, like the NotPetya attack on Merck and WannaCry attacks, offer lessons for strengthening cybersecurity policies.

Alzoubi, Gill., and Anwar, 'Cybersecurity Enterprises Policies: A Comparative Study': [3]. The article discusses the increasing importance of cybersecurity (CS) in the context of growing digital transformation across various business domains. It highlights the need for organizations to safeguard their ICT infrastructure to protect customer information from cyber threats. The study explores different customer service policies aimed at effectively managing customer data and meeting their expectations. It covers industries like health, finance, education, aviation, and e-commerce, emphasizing common CS policies such as privacy, website security, data protection, and compliance with relevant laws like HIPAA and GDPR. The article underscores the critical role of CS in maintaining trust and security in today's digital landscape.

Data Integrity and Compliance with CGMP Guidance for Industry, U.S. Department of Health and Human Services Food and Drug Administration Center for Drug Evaluation and Research (CDER) Center for Biologics Evaluation and Research (CBER) Center for Veterinary Medicine (CVM), [4] "The purpose of this guidance is to clarify the role of data integrity in current good manufacturing practice (CGMP) for drugs, as required in CFR parts 210, 211, and 212. It outlines the FDA's expectations for reliable and accurate data in compliance with CGMP regulations. While FDA guidance documents typically offer recommendations and reflect the Agency's current thinking, they are not legally binding unless specific regulatory or statutory requirements are mentioned. The use of "should" in FDA guidance signifies suggestions or recommendations rather than obligations".

Venkateswaran, 'Cybersecurity Is a Top Priority for Pharmaceutical Organizations' [5]. The pharmaceutical industry has witnessed a surge in cybersecurity measures due to increasing cyber threats. Ransomware attacks, especially during the COVID-19 pandemic, have targeted research and development infrastructure for intellectual property theft. A study revealed that pharmaceutical organizations have been exposed to data breaches, with the average cost of such breaches being $5.3 million, significantly higher than other industries. Factors driving this trend include digital transformation, mergers and acquisitions, and ecosystem collaboration. Consequently, pharmaceutical organizations are adopting comprehensive cybersecurity strategies, including zero trust, third-party risk assessment, and security awareness programs, to safeguard their operations and intellectual property.

Perlroth N, 'Clinical Trials Hit by Ransomware Attack on Health Tech Firm' [6]. A Philadelphia-based clinical trial software provider, eResearchTechnology (ERT), was targeted by a ransomware attack that disrupted clinical trials, including COVID-19 vaccine research. The attack, reported two weeks after it occurred, impacted pharmaceutical companies like IQVIA and Bristol Myers Squibb. ERT's software is widely used in clinical trials globally. While the attack did not jeopardize patients, it forced researchers to resort to manual tracking. The incident underscores the growing threat of ransomware to the healthcare and pharmaceutical sectors, which were crucial during the pandemic.

Amlegals, 'Data Privacy in Pharmaceutical Industry in India'[7]. The article highlights the significance of data privacy in the healthcare sector, particularly in the context of patient information protection. It discusses the need for healthcare practitioners to ensure patient data security and privacy, especially when dealing with sensitive medical information. The article also mentions the absence of comprehensive data protection legislation in India and the impending Personal Data Protection Bill. It emphasizes compliance with the General Data Protection Regulation (GDPR) and the potential impact on businesses operating in India. Additionally, the article touches on the use of blockchain technology for patient data confidentiality in the healthcare industry.

Commissioner O of the 'Part 11 Electronic Records Electronic Signatures Scope and Application' [8]. 21 CFR Part 11 is a U.S. FDA regulation from 1997 that sets guidelines for electronic Records and Signatures in pharmaceuticals and medical devices. It ensures secure electronic records with features like data protection, time stamps, and audit trails. Electronic signatures, though convenient, lack standardization. The regulation aims to permit widespread electronic technology use while maintaining data integrity.

Networks N, 'Ensuring Cybersecurity of Medical Devices: What Changed in the FD and C Act?'[9]. "The 2023 Omnibus Appropriations Act introduced significant changes to medical device cyber security regulations. It empowers the FDA to mandate security measures in medical devices, emphasizing security by design. Manufacturers must submit plans for vulnerability monitoring, secure design, updates, and software components.

The legislation also addresses broader healthcare sector cyber security issues and highlights the vulnerability of legacy technologies. Additionally, the HHS released a guide on implementing the NIST Cyber security Framework, emphasizing enterprise-wide risk management and access to cyber security expertise [14]. Monitoring and visibility are crucial for reducing dwell time and addressing cyber threats

 | DOI: 10.20533/ijisr.2042.4639.2024.0123

in healthcare settings".

3. Statement of Problem

In this case study, the problem under scrutiny is the Sun Pharma information security incident and subsequent ransom ware attack. The primary objective is to assess the effectiveness of the company's response strategy, the extent of financial impact, and the potential legal consequences. Furthermore, this research aims to identify any unforeseen adverse repercussions arising from the breach, contributing valuable insights to the evolving landscape of cyber security in the pharmaceutical industry.

Hypothesis

The hypothesis suggests that there may be a connection between how well Sun Pharma responds to the information security incident and the severity of financial losses and legal issues they face. It also anticipates that unexpected consequences will arise from the incident, potentially influencing how cybersecurity is approached in the pharmaceutical industry. The research aims to explore and confirm these potential relationships.

Research Question

- How did Sun Pharma's response strategy mitigate the security incident's impact, and what factors led to its success?
- What is the financial impact of the breach and its effect on Sun Pharma's overall financial health?
- What legal challenges does Sun Pharma face, and how will they address them?
- Have unexpected consequences emerged from the breach, and how might they affect Sun Pharma and the pharmaceutical cybersecurity landscape?
- How can insights from this study enhance pharmaceutical cybersecurity practices?

Research objectives

- Evaluate the effectiveness of Sun Pharma's response strategy to the security incident and ransom ware attack.
- Quantify the financial impact of the breach on Sun Pharma and its financial health.
- Identify and assess potential legal consequences faced by Sun Pharma due to the security incident.
- Investigate any unexpected repercussions resulting from the breach and their potential impacts on Sun Pharma and the broader pharmaceutical cyber security landscape.
- Formulate recommendations for enhancing cyber security practices in the pharmaceutical industry based on lessons learned from this case study.

Scope limitation

This research will examine pharmaceutical information security with a focus on laws and regulations set by organizations such as the FDA, WHO, HIPAA, and DPDP Act. It aims to provide a comprehensive understanding of their impact on the pharmaceutical industry's cyber security landscape

Research methodology

This research employs a doctrinal approach, involving the systematic review and analysis of existing legal documents, regulations, and guidelines related to pharmaceutical industry cybersecurity.

4. Analysis

Sun Pharma, recognized for popular products like Revital vitamins and Volini pain relief medicine, saw a nearly 14% increase in its total revenue, reaching ₹11,241 crore ($1.37 billion) in the last quarter. The company initially stated that the information security incident reported on March 2 had no impact on its operations. However, Sun Pharma now acknowledges that its containment efforts have indeed affected its operations. The containment measures implemented by Sun Pharma negatively impacted its business operations as the company is expected to see a decline in its revenues.

The Sun Pharmaceutical Industries Ltd., a prominent Indian pharmaceutical company, experienced a significant data breach. The cyber attack, attributed to the ALPHV ransom ware group, impacted the company's IT systems [10]. The attackers claim to have obtained more than 17TB of data, which includes sensitive customer and vendor information and comprehensive records of over 1,500 US employees. The ransom ware group alleges that Sun Pharma attempted to downplay the incident and set up honeypots to trap them within their network.

The Sun Pharmaceutical acknowledged the cyber-attack and is taking swift action to mitigate the incident's impact. They are implementing containment and eradication protocols while involving cyber security experts to ensure system integrity. The breach involved certain file systems and data theft, which has led to business disruption and an expected reduction in revenues. The company anticipates incurring expenses for remediation.

 | DOI: 10.20533/ijisr.2042.4639.2024.0123

However, it's uncertain whether there will be further repercussions, such as additional security incidents, increased insurance costs, diverted management attention, or potential legal action.

A recent case study was done by S. Subramanian Associate Professor, Strategic Management, Indian Institute of Management, Kozhikode on the "Corporate Governance issues Sun Pharmaceutical Industries Ltd" [11], which talks about the Sun Pharmaceutical Industries Ltd.'s board convened in November 2019 to deliberate on unaudited financial results. However, the company had been under scrutiny due to corporate governance issues stemming from whistleblower complaints since October 2018. The Securities and Exchange Board of India (SEBI) had even ordered a forensic audit of the company's accounts in September 2019. With the company's stock falling over 40% since the initial whistleblower complaint, the board faced the imperative task of restoring investor confidence by enhancing corporate governance and transparency, particularly in related party transactions.

4.1. Assessing Cybersecurity in Healthcare and Pharmaceutical Sectors: A Global and Indian Outlook

Cyber security is vital for safeguarding sensitive information and trade secrets in the pharmaceutical and healthcare industries. In India, the Ministry of Electronics and Information Technology promotes domestically manufactured cyber security products and encourages "Make in India" to bolster the ecosystem. Developing incident response platforms and automation aims to enhance security monitoring and response times. Given the intellectual property and sensitive data handled, information security governance is paramount, extending beyond entities' perimeters. US and European regulatory authorities have also strengthened healthcare data protection measures.

Verizon's Data Breach Investigation Report revealed that 58% of security incidents in healthcare were due to insiders, while 42% resulted from external threats. Ransomware attacks have targeted healthcare networks, including the notorious 'NotPetya' malware, mirroring the WannaCry incident and impacting numerous computers worldwide.

The pharmaceutical sector is actively investing in identity and access management (IAM), driven by the necessity to efficiently manage user identities and grant appropriate access to sensitive business data when needed. The main concerns in these sectors revolve around intellectual property, personal identifiable information, and protected health information. This includes the protection of formulas, contracts, clinical research, and PII. Additionally, addressing risks, compliance, IoT, cloud usage, supply chain security, and clinical trial data security is crucial for ensuring industry-wide cyber security.

India is still in early stage with significant efforts being underway in India, driven by the Digital India initiative, to advance cyber security. Recognizing the strategic importance of this sector, the Ministry of Electronics and Information Technology (MeitY) has directed government entities to prioritize domestically manufactured cyber security products, promoting the "Make in India" approach to stimulate economic growth and employment [12]. Both the National Cyber Security Policy (NCSP) and the Joint Working Group (JWG) highlight the importance of developing cyber security products within the country. DSCI , a non-profit organization and NASSCOM initiative, has established the India Cyber Security Product forum to facilitate collaboration, providing a boost to Indian cyber security product companies and fostering local product development. If effectively implemented, this initiative promises significant benefits.

4.2. Cases Involving Threats from Pharmaceutical Products

On the 20th of September 2022, the FDA issued an alert regarding a potential cybersecurity risk associated with the Medtronic MiniMed 600 Series Insulin Pump System. This includes models like MiniMed 630G and MiniMed 670G. The concern lies in a vulnerability related to the pump system's communication protocol, which could potentially allow unauthorized access. If unauthorized access occurs, it might compromise the pump's communication and result in incorrect insulin delivery, either too much or too little.

The system components of the MiniMed 600 series communicate wirelessly, which includes the insulin pump, continuous glucose monitoring (CGM) transmitter, blood glucose meter, and CareLink USB device. Unauthorized access would require a nearby unauthorized person to gain access to the pump during the pairing process with other system components. It's important to note that the FDA has not received any reports of this vulnerability being exploited. Medtronic has issued an Urgent Medical Device Correction, offering recommendations to address this risk. The FDA is collaborating with Medtronic to address and prevent potential adverse events related to this cyber security concern, with a commitment to keeping the public informed of any significant updates.

The FDA is actively collaborating with federal partners, private sector entities, and medical device manufacturers to address cyber security vulnerabilities related to BlackBerry's QNX Real Time Operating System (RTOS) version 6.5 Service Pack 1 and earlier. These vulnerabilities have the

 | DOI: 10.20533/ijisr.2042.4639.2024.0123

potential to pose risks to specific medical devices and pharmaceutical or medical manufacturing equipment. It's worth noting that the FDA has not received reports of confirmed adverse events associated with these vulnerabilities. The FDA has provided guidance to medical device and pharmaceutical manufacturers, outlining steps to mitigate cyber security concerns and what actions to take in the event of a cyber security incident. Manufacturers are diligently assessing whether their systems are impacted by these vulnerabilities, evaluating associated risks, and developing strategies for remediation. Those manufacturers affected by these issues are encouraged to communicate with their customers and collaborate with the Cyber security and Infrastructure Agency (CISA) to address the matter effectively.

4.3. Global Cybersecurity Regulations and Guidelines for the Pharmaceutical Industry DPDP Act 2023

Following the recent enactment of the DPDP Act 2023, the pharmaceutical sector falls within its regulatory framework. The Act's Section 8 , specifically subsections 5 and 6 which stipulate the obligations of data fiduciaries. These provisions emphasize the necessity of comprehensive security measures to avert data breaches and in the event of a data breach, the data fiduciary must adhere to the Act by promptly notifying both the Data Protection Board and each affected data principal. In the case of the Sun Pharma data breach incident, the data fiduciary responsible for employee and customer data processing is bound by the obligations articulated in this section of the Act.

Section 27 of the DPDP Act 2023 outlines the ‘powers and functions of the Data Protection Board’, which plays a crucial role in upholding data protection standards. The Board is granted authority to respond to personal data breaches swiftly and effectively. It can direct urgent remedial measures in the event of a data breach, investigate the breach thoroughly, and impose penalties as specified in the Act which is given in schedule of DPDP Act 2023 which imposes penalty which may extend to two hundred and fifty crore rupees.

FDA's Recommendation for Comprehensive Cybersecurity Risk Management Programs

The integration of cybersecurity risk management is crucial for medical device systems to ensure the safety and security of patients and the larger healthcare infrastructure. This involves assessing the security risks of each device within the context of the entire system to identify vulnerabilities and potential threats.

Unlike safety risk management outlined in ISO 14971, security risk management addresses cybersecurity threats and potential risks related to patient harm. It also extends beyond physical injury to include indirect or direct patient harm, business, and reputational risks. Security risk management should be integrated into a manufacturer's quality system processes, covering design, manufacturing, distribution, and updates. Comprehensive design mitigations should address known vulnerabilities, and compensating controls should be considered when necessary. Manufacturers should document security risk management activities in a security risk management plan and report, which should be included in premarket submissions to demonstrate the device's safety and effectiveness. These reports should summarize risk evaluation methods, detail residual risk conclusions, describe risk mitigation activities, and provide traceability between threat modeling, cybersecurity risk assessment, and testing documentation. This comprehensive approach ensures that both safety and security risks are addressed in medical device systems, promoting patient safety and data security.

FDA Guidance for Industry Part 11 of Title 21 of the Code of Federal Regulations regarding electronic records and signatures.

The FDA has adopted an approach to specific Part 11 requirements related to computerized systems, focusing on validation, audit trails, legacy systems, copies of records, and record retention. For validation, the agency recommends exercising enforcement in discretion, with a strong emphasis on considering the impact of these systems on predicate rule requirements, the integrity of records and signatures, and the potential effect on product quality and safety. It advises basing decisions on documented risk assessments. Regarding audit trails, the FDA exercises enforcement discretion while emphasizing the importance of ensuring trustworthiness and reliability of records through appropriate controls based on risk assessments. Audit trails are particularly relevant when users create, modify, or delete regulated records during normal operations. For legacy systems operational before August 20, 1997, the FDA will not enforce Part 11 requirements if specific criteria are met, including documented evidence of fitness for intended use. In the case of copies of records, the FDA suggests providing reasonable access during inspections and preserving content and meaning in copies, allowing the same capabilities as the original records. Regarding record retention, the FDA exercises enforcement discretion and recommends a decision based on predicate rule requirements, justified and documented risk assessments, and value over time. Electronic records can be archived to non electronic

 | DOI: 10.20533/ijisr.2042.4639.2024.0123

media or standard electronic formats, provided predicate rule requirements are met. Overall, this approach focuses on risk-based decision-making and emphasizes the importance of maintaining data integrity and accessibility throughout the record lifecycle.

The HITECH Act

Enacted in 2009, was designed to encourage the use of health information technology. Subtitle D of the act focused on addressing privacy and security concerns in the electronic transmission of health information. It introduced stricter enforcement of HIPAA rules, with penalties categorized into four levels of culpability and corresponding tiers of fines, reaching a maximum of $1.5 million for identical violations. The Act also removed the provision that protected covered entities from penalties if they were unaware of a violation, unless it was due to wilful neglect. Additionally, it allowed for the correction of violations within 30 days without penalties. An interim final rule was introduced to align HIPAA enforcement regulations with these HITECH Act revisions effective since February 2009. The rule took effect on November 30, 2009, and the Department of Health and Human Services invited public comments on it until December 29, 2009.

Health Insurance Portability and Accountability Act (HIPAA)

Pharmaceutical companies themselves are not directly regulated by HIPAA, but they may come into contact with HIPAA requirements when they work with covered entities or interact with protected health information in the context of clinical trials or electronic health record systems. In such cases, compliance with HIPAA rules is essential to protect patient privacy and ensure legal and ethical data handling. The Privacy Rule set BY HIPAA limits on using and disclosing PHI without an individual's authorization, especially for marketing purposes. Highlights include obtaining a signed authorization before disclosure, using plain language, specifying the purpose, and disclosing financial gain if applicable. Business associates require permission from covered entities via a business associate agreement before seeking HIPAA authorizations. The Security Rule mandates safeguards for electronic PHI, covering risk identification, training, contingency planning, security incident response, access controls, encryption, and audit controls. The Breach Notification Rule requires notifying affected parties, HHS, and, sometimes, the media after a breach of unsecured PHI. Business associates must notify covered entities of such breaches. Reports go through OCR's breach portal, which lists major breaches.

Federal Trade Commission (FTC)

Pharmaceutical industries are related to the FTC in terms of compliance with various regulations, particularly those related to advertising practices, competition, consumer privacy, data breach notification, and consumer protection. The FTC plays a vital role in overseeing and enforcing these regulations to safeguard the interests of consumers. The FTC's Health Breach Notification Rule applies to specific businesses not covered by HIPAA, such as personal health record vendors, related entities, and third-party service providers. If your business deals with electronic health information in personal health records or offers services related to such products, you may need to comply with this rule. This rule mandates that companies notify affected consumers, the FTC, and possibly the media in the event of a security breach involving consumers' identifiable health information. A security breach can result from unauthorized acquisition or disclosure of health information, except when it's protected by HHS-specified technologies. To comply with this rule, businesses should understand their obligations, report breaches promptly to the FTC, and follow guidance provided by the FTC and HHS, especially if they have health apps. When disclosing health information practices to consumers, they must consider the FTC Act, the Health Breach Notification Rule, and HIPAA Rules.

5. Suggestions

The pharmaceutical companies should conduct a comprehensive inventory of their computer systems, including servers, desktops, laptops, and portable devices like USB drives and CDs. It's advisable to limit access to social media and emphasize the importance of safeguarding intellectual property, even in social media usage. For computers containing sensitive data, the IT department should establish controlled access using usernames and passwords, enforce restricted permissions by disabling copying, printing, and unauthorized software installation. They should also control access to email, FTP, and public ports, segregate sensitive information, maintain activity logs, and regularly update antivirus and spam filters. These steps are crucial for ensuring strong security on both individual computers and network systems.

Laptops and portable devices require distinct safety measures. Chief Information Officers (CIOs) and technical services should establish policies prohibiting the transfer of files to personal computers, whether through remote desktop, CitrixTM, or other remote file access services. For confidential matters, only company-issued laptops should be allowed. Moreover, the use of portable drives should be restricted. Portable drives pose

 | DOI: 10.20533/ijisr.2042.4639.2024.0123

significant cybersecurity risks due to their high storage capacity and small size. For particularly sensitive matters, it's advisable to regularly review logs of mounted drives and copied files to ensure data security. When it comes to portable electronic devices like smartphones and tablets, having a well-defined Bring Your Own Device (BYOD) policy is essential. This policy should outline when it's appropriate to use personal devices versus company-issued ones. Monitoring file copies and email access to remote or personal devices is crucial. Personal and remote devices may require specific security measures, including separate passwords, tracking software in case the device is lost, and the ability to remotely delete data. Furthermore, any temporary devices provided to employees containing sensitive information should be returned when they leave the company, and there may be a need for forensic examination of these devices to ensure data security.

Managing Third-Party Access to Critical Data: As more companies extend network access to external vendors and Contract Research Organizations (CROs) for data exchange, there's an inherent security risk. If a vendor's network lacks robust security, it can be a gateway for breaches into the company's own network. The Target security breach, for instance, stemmed from a subcontractor in heating and air conditioning with access to Target's network. Effective risk mitigation involves thorough vendor due diligence and clear contractual restrictions on the type and circumstances of network access granted to CROs or vendors.

Indemnification and Cyber security Insurance: Indemnification clauses in service contracts ensure that one party covers monetary losses incurred by the other due to potential security vulnerabilities introduced by granting network access to vendors or CROs. Additionally, companies can minimize financial impact through cybersecurity insurance policies, covering various incidents like hacking, data theft, and viruses. It's important to comply with policy requirements, including maintaining a baseline level of data security within the organization. Vendor due diligence should verify that vendors handling sensitive information possess adequate cyber security insurance.

Incident and Data Breach Response Plans: Most states have laws mandating security breach notifications to consumers and authorities. Federal regulations, including those by the FTC and HHS, impose notification requirements, especially for entities managing health data under HIPAA. Developing comprehensive incident and data breach response plans tailored to state and federal laws is crucial to effectively manage and mitigate the aftermath of security breaches, ensuring compliance with notification obligations and protecting affected individuals.

6. Conclusion

The research findings support the hypothesis. A connection exists between Sun Pharma's response to the security incident and the severity of financial losses and legal consequences. Unexpected consequences do influence cybersecurity strategies in the pharmaceutical industry. The pharmaceutical industry, crucial for healthcare, faces significant cybersecurity challenges to protect sensitive data. Recent incidents, like the Sun Pharma data breach, highlight the industry's vulnerability to cyber threats. It's essential for companies to invest in robust cyber security measures and follow global regulations like the DPDP Act and FDA guidelines. Compliance with privacy and data security laws, such as HIPAA and FTC regulations, is vital. Furthermore, India's push for domestically manufactured cybersecurity products and the development of security risk management programs demonstrates the industry's commitment to enhancing data protection. Ensuring cybersecurity is a paramount concern in the pharmaceutical sector to safeguard critical information and maintain patient trust.

7. References

[1] Datta, P. J. (2023). Ransomware Attack: Sun Pharma Says Business Operations Impacted. https://www.thehindubusinessline.com/companies/ransomware-attack-sun-pharma-says-business-operatio ns-impacted/article66667349.ece (Access Date: 1 October 2023).

[2] Marino, D. (2022). Cybersecurity - Why Pharma ceutical Companies Are Vulnerable to Cyberattacks and What You Can Do to Protect Your Company. https://drug-dev.com/cybersecurity-why-pharm aceutical-companies-are-vulnerable-to-cyberattacks-what-you-can-do-to-protect-your-company/ (A ccess Date: 1 October 2023).

[3] Alzoubi YI, Gill A. Q., and Anwar M. J. (2202). Cybersecurity Enterprises Policies: A Comparative Study. https://www.mdpi.com/1424-8220/22/2/538 (Access Date: 1 October 2023).

[4] Data Integrity and Compliance with CGMP Guidance for Industry. (2022). U.S. Department of Health and Human Services Food and Drug Administration Center for Drug Evaluation and Research (CDER) Center for Biologics Evaluation and Research (CBER) Center for Veterinary Medicine (CVM). https://www.fda.gov/files/drugs/published/Data-Integrity-and-Compliance-With-Current-Good-Manufacturing-Practice-Guidance-for-Industry.pdf (Access Date: 1 October 2023).

[5] Venkateswaran, V. (2022). Cybersecurity Is a Top Priority for Pharmaceutical Organizations. https://www.isaca.org/resources/news-and-trends/industry-news/2022/cybersecurity-is-a-top-priority-for-pharmaceutical-organizations (Access Date: 1 October 2023).

 | DOI: 10.20533/ijisr.2042.4639.2024.0123

[6] Perlroth, N. (2020). Clinical Trials Hit by Ransomware Attack on Health Tech Firm. https://www.nytimes.com/2020/10/03/technology/clinical-trials-ransomware-attack-drugmakers.html (A ccess Date: 1 October 2023).

[7] Amlegals A, (2022). Data Privacy in Pharmaceutical Industry in India' https://amlegals. com/data-privacy-in-pharmaceutical-industry-in-india/# (Access Date: 2 Octo ber 2023).

[8] FDA. (2023). Commissioner O of the 'Part 11 Electronic Records Electronic Signatures Scope and Application. https://www.fda.gov/regulatory-inform ation/search-fda-guidance-documents/part-11-electronic-records-electronic-signatures-scope-and-application (Access Date : 10 October 2023).

[9] Networks, N. (2023). Ensuring Cybersecurity of Medical Devices: What Changed in the FD and C Act? https://www.nozominetworks.com/blog/ensuring-cybersecurity-of-medical-devices-fdc-act, (Access Date: 2 October 2023).

[10] Khaitan, A., and Pandagle, V. (2023). Sun Pharmaceutical Cyber Attack Confirmed, ALPHV Ransomware Claims Responsibility. https://thecyberexpress.com/sun-pharma-cyber-attack/ (Access Date: 3 October 2023).

[11] Subramanian, S. (2023). Corporate Governance issues Sun Pharmaceutical Industries Ltd https:// iimk.ac.in/uploads/publications/IIMKCS201FIN202309.pdf (Access Date: 3 October 2023).

[12] Meity. (2013). National Cyber Security Policy (Draft V1 - Ministry of Electronics And ...' (National cyber security policy 2013). https://www.meity.gov.in/writereaddata/files/downloads/National_cyber_security_policy-2013%281%29.pdf (Access Date: 4 October 2023).

[13] Pharmabiz. (2019). Cyber security key in pharma and healthcare to ensure protection of information. http://www.pharmabiz.com/ArticleDetails.aspx?aid=113648andsid=11 (Access Date: 4 October 2023).

[14] HHS. (2021). OCR O for CR, 'Hitech Act Enforcement Interim Final Rule. https://www.hhs.gov/hipaa/for-professionals/special-topics/hitech-act-enforcement-interim-final-rule/index.html#:~:text= S ubtitle%20D%20of%20the%20HITECH,enforcement%20of%20the%20HIPAA%20rules. (Access Date: 5 October 2023).

 | DOI: 10.20533/ijisr.2042.4639.2024.0123