World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(REVIEW ARTICLE)

Check for updates

The Impact of Data Breaches in U.S. Healthcare: A Cost-Benefit Analysis of Prevention vs. Recovery

Zeliatu Ahmed [1], Abimbola Filani [2], Adewale Samuel Osifowokan [3] and Nasiru Hutchful [4,*]

[1] *Department of Information Systems, Cybersecurity, Dakota State University, Madison, USA.*
[2] *Department of Business Information Systems, Central Michigan University, Michigan, USA.*
[3] *Regeneron Pharmaceuticals, New York, USA.*
[4] *Department of Computer Science and Engineering, University of Mines and Technology, Ghana.*

World Journal of Advanced Research and Reviews, 2025, 27(03), 1542-1549

Publication history: Received on 12 August 2025; revised on 19 September 2025; accepted on 22 September 2025

Article DOI: https://doi.org/10.30574/wjarr.2025.27.3.3274

Abstract

The healthcare sector in the United States has experienced increased incidences of data breaches which poses significant challenges to patient privacy, financial stability, and organizational integrity. This paper conducts a cost-benefit analysis of the two primary approaches, prevention and recovery, in addressing data breaches. This research leverages both industry reports and statistical analyses to measure the financial and operational implications of the breaches to the US healthcare sector. The study reveals that despite costly investments made towards preventive efforts such as training of the organizational staff, conducting regular system audits and robust cybersecurity frameworks and assessment, they prove more cost effective in mitigating long-term damages. On the other hand, recovery costs such as legal expenses, data restoration, and repair of reputational damage are usually cumulatively higher and erodes public confidence. Through comparative analyses this paper highlights the economic and operational benefits of proactive strategies. Recommendations are given for healthcare organizations to take a proactive stance and focus on balancing resources for cybersecurity infrastructure as well as developing cybersecurity workforce training. This research highlights the importance of moving from reactive to more proactive strategies, while not denying the importance of both in ensuring improved patient security and a decreased risk of financial liability.

Keywords: Data breach; Healthcare; Cost-benefit analysis; Cybersecurity

1. Introduction

Healthcare data breaches in the United States reached more than 40 million victims in 2022 violating the privacy of these victims. More than 500 hospitals lost millions of dollars for ransom, lawsuits, response, and recovery within the year [1]. The increased adoption and reliance on digital infrastructure within the U.S. healthcare industry has created profound changes in the quality of patient treatment, information processing, and operational performance. Nonetheless, this digital transformation has brought about new challenges of cybersecurity risks, with data breaches acting as an inevitable threat to healthcare institutions. Unlike many other industries, the healthcare industry involves handling very sensitive medical data, personal identifiers and even financial information. Consequently, data breaches in health institutions can be very life-threatening emergencies for an entire hospital or, even worse, all the hospitals in a health system that share information system infrastructure.

* Corresponding author: Nasiru Hutchful

A current concern that is being built is the cost and impact of data breaches on business. It is important to consider that the costs of breaches extend beyond just the immediate incidence response and some regulatory penalties, but also the loss of reputation, the risks of legal actions, and the disruptions in patient care. In 2019, A newborn baby died at an Alabama hospital nine months after being delivered because the hospital was locked in a three weeks ransomware IT meltdown. The mother claimed in a negligence lawsuit that she was uninformed about the cyberattack which interrupted essential medical data availability contributing to the death [2]. Industry reports have pointed out that the cost of data breaches within the healthcare sector is among the highest, averaging millions per incident. These breaches often lead to loss of critical patient data exposing these health institutions to fines and compliance violations under regulations like Health Insurance Portability and Accountability Act (HIPAA). While some organizations continue to prioritize a proactive cybersecurity posture to prevent cyber threats from infiltrating their systems, others prefer to invest in mitigative strategies should an attack happen.

Due to the above concerns, this paper aims to analyze the cost-benefit trade-off between prevention and recovery of data breaches in the U.S healthcare system. This study will provide an in depth analysis of whether health institutions should invest more in proactive cybersecurity measures or focus on building better recovery systems by conducting a review and examining breach incidents, trends within the healthcare industry, and their financial consequences. Finally, this research intends to provide healthcare organizations with fact-based evidence on which to base its decisions on future cybersecurity investment, taking cognizance of the fact that while most of these investments are costly, the protection of patient privacy cannot be overemphasized.

2. Literature Review

Healthcare organizations, compared to other industries, manage highly sensitive data that ideally makes them primary targets of hackers. Health data digitization has direct gains for medical record data holders yet there exist conflicting interests between privacy protection and “data-based technological process” [3]. Information technology enhances the quality of both the healthcare system and the overall ecosystem [4], but as hospitals adopt the usage of information systems, data breaches surface and introduction detrimental effects to patient welfare.

Over the past few years, breaches of healthcare organizations have visibly increased due to new breach reporting regulations under the Health Information Technology for Economic and Clinical Health (HITECH) Act. The HITECH Act of 2009 encouraged the adoption of electronic healthcare records (EHR) by health providers by billions of dollars in financial incentives to these providers. More than 90% of healthcare providers also indicated they have experienced at least one data breach since 2011, as the adoption of these EHRs were increasing [5] . This breach epidemic was partly a result of the new stringent breach notification requirements associated with the HITECH Act. The requirements mandated that the healthcare providers who discovered data breaches, were to inform the affected individuals within 60 days from the date of discovery. Moreover, if the breach impacted more than 500 individuals, it must be disclosed to media outlets and the U.S. Health and Human Services (HHS) which lists such breaches on its website (often referred to as “the Wall of Shame”) [6]. Such notification requirements have been found to have significantly increased visibility of breaches of personal information, which has enhanced the state breach notification laws already in existence.

A study done by Ponemon Institute reveals that healthcare data breaches rank as the most expensive, costing an average of $10.93 million per incident in 2023. This number appears higher than the finance, retail and other critical industries [7]. The causes of these breaches differ but are mostly related to cyberattacks, system misconfigurations, lack of adequate security protocols and insider threats. Also, ransomware and phishing attacks, particularly, have surged, with cyber attackers leveraging on vulnerabilities of legacy systems and human error to gain unauthorized access. The magnitude of breach incidents within the health care industry has grown at an alarming rate. The HIPPA Journal reveals that millions of patient records are exposed each year, with a pattern of significant increase observed during periods of heightened reliance on technology like the COVID-19 pandemic [8]. A report done by IBM Security and Ponemon Institute revealed that more than 700 health care breaches had been reported in 2022 alone, which impacted over 50 million Americans. Particularly, healthcare breaches tend to remain undetected on average of over 200 days which exacerbates the losses caused by these breaches. Furthermore, the research suggests that third-party vendors and supply chain vulnerabilities contribute majorly to expanding attack surface and cybersecurity efforts more challenging [9].

2.1. Cost Implications of Data Breaches

The financial strain from healthcare data breaches goes beyond the cost of containment and remediation processes. Organizations face significant costs in areas such as forensic investigations, regulatory penalties, patient notifications, and legal responsibility. Researchers have established that the costs of post-breach expenses linger for years, as

institutions that have been impacted by these breaches invest in security strategies, public relation management and legal compensation.

Benchmarking the costs of data breaches reveals that the healthcare cost per breached record has risen at a much faster rate compared to the average cost per breached record across other industries. The average record cost recorded $214 in 2010 but in 2011 there was a 10% reduction. In 2012, they reduced by 42.64% from the year 2011. After that, a gradual increase was seen year by year. In 2019, it rose by 1.55% compared to the year before. Healthcare breached record cost from 2010 to 2019 rose by 45.91% from $294 to $429. The cost per record breach in the healthcare industry was $294 in 2010 and this cost reduced until 2012, after which it rose again by 1.11% from 2014 to 2015, 7.04% from 2016 to 2017 and 5.14% from 2018 to 2019. The 2018 Verizon DBIR report revealed that 76% of the data breaches that occurred in 2018 were financially motivated [10]. Regarding that report, it was discovered that 83% of healthcare data breaches had financial motives [11]. Figure 1 below provides a graphical cost comparison of average breached record costs and healthcare breached record costs by each year.

Figure 1 Graphical Comparison of Average Record Cost and Healthcare Record Cost

In response to this increasing problem, institutions have concentrated on both preventive and reactive strategies, but the cost effectiveness of these measures continues to be a subject of debate. Preventive measures that include advanced security cybersecurity tools, employee training and compliance with industry standards come with high upfront costs. For instance, expenses required to protect sensitive information of patients via multifactor authentication and encryption especially for small-scale organizations can be substantial. According to a 2024 survey conducted, over 70% of the medical group practices revealed that they had embarked on increasing their cybersecurity budget due to emerging risks with most of them opting to strengthen employee training, in order to mitigate be address the human factor that often leads to breaches (Janakiraman et al, 2023).

On the other hand, the global average cost of a data breach in 2023 reached $4.45 million, with the cost of data breach in the US considerably higher at $9.48 million (IBM Security, 2023). These numbers highlight the significant financial burdens that healthcare organizations endure when breaches occur, even when they have the best recovery plans in place. While some researchers are optimistic about recovery and inevitability and suggest that it should be made priority, others look out to the higher long-term costs of recovery, which in many cases are aggravated by delayed responses and inefficiency in managing the breach.

This research will contribute to ongoing studies by examining the cost-benefit tradeoffs of prevention as opposed to recovery regarding healthcare data breaches. By analyzing the immediate and long-term impacts for each, this research aims to present data-driven insights to contribute to more informed decisions on how best to invest and allocate resources. These findings will provide a better understanding of the cost implications on prevention and mitigative strategies to guide the healthcare institutions and decision makers in achieving a better balance and cost-effective approach for managing risks associated with data breach

3. Methodology

This research uses a cost-benefit analysis approach to assess the economic consequences of prevention rather than recovery strategies in addressing the data breaches within the healthcare sector in the U.S. To accomplish this, the research will employ secondary data from case fillings, industry reports and case studies of past security breaches. The IBM Cost of a Data Breach Report which will provide empirical insights into the average costs associated with breaches and the HIPAA Journal which documents healthcare data breaches, regulatory fines, and compliance trends will be the main sources for collecting the primary data since they offer the actual costs of breaches and practical examples. In addition, surveys from Medical Group Management Association (MGMA) will be analyzed to compute the amount spent on cybersecurity by the healthcare providers while reports from security intelligence supports by offering comparative insights across industries. Together, these sources can be said to form a strong basis for evaluating the financial costs and benefits of prevention and recovery.

However, apart from financial metrics, each of the approaches is assessed in terms of its wider impact. Operational efficiency is measured by assessing the impact of disruptions in services, workforce unavailability, and efforts required to recover patient data after a breach. Also, regulatory and reputational implications and legal sanctions together with the future effects on the credibility of healthcare organizations is further analyzed. Through the synthesis of these factors, this research seeks to deliver a concise and empirical comparative analysis to inform health institutions and decision-makers in optimizing cybersecurity investments while at the same time developing long-lasting sustainable solutions.

4. Findings and Discussion

Based on Ponemon Institute research, the IBM Cost of a Data Breach Report [14], highlights the financial strain of cyberattacks which continues to increase as the average cost on data breaches grows to $4.88 million, up by 10% from the previous year, 2023, and the highest increase since the pandemic. This increase was mainly attributed to lost business costs, which include operational downtime, customers churn along with regulatory fines which estimated to $2.8 million, making it the highest in six years. In spite of the 10.6% decline in costs of healthcare data breach to $9.77 million, the health sector still remains the most costly industry for data breaches, holding this position since 2011 due of its reliance on existing technology systems that are vulnerable to disruption. However, IBM discovered the acceptance of AI driven security and automation has been a game changer in lowering the costs of breaches. Amongst the organizations that adopted AI in attack surface management (ASM), red teaming, and posture management, these organizations who heavily invested in these technologies saved an average of $2.2 million compared to their counterparts without AI integration. At the same time, the cybersecurity skills gap remains a significant issue and is leading in increased financial losses as most organizations experience a high staffing gap which further introduces an extra $1.76 million in breaches, contributing to a 26.2% rise from the previous year. Despite the fact that 20% of organizations have adopted generative AI security tools to improve efficiency, the talent deficit remains a major persisting issue. In addition, active engagement of law enforcement in ransomware attacks has proven another major cost saving, decreasing expenses related to breaches by nearly $1 million, and decreasing containment duration from 297 to 281 days, which further emphasizes the relevance of implementing proactive security strategies and comprehensive response planning [14].

March 2024 broke the record of healthcare data breaches. HIPAA Journal reported a massive increase highlighting 93 breaches of 500 or more records reported to the U.S. Department of Health and Human Services (HHS), indicating a 50% uptick from February 2024, and a 41% increase YoY from March 2023. This signified the highest number of breaches recorded in a specific month since before the COVID-19 breakout in 2020 [15]. Even though HHS does not directly mandate which electronic platforms should be used in healthcare organizations, they are encouraged to adopt the NIST's guidance documents when selecting secure platform providers. Any violation of the HIPAA regulations attracts fines that are steep. The HIPAA violation penalty structure consists of four tiers that reflect the level of negligence and reasonable knowledge of potential violations prior or post a data breach of healthcare institutions, with the annual penalty limit of $1,919,173 for the violations that fall under each tier [16].

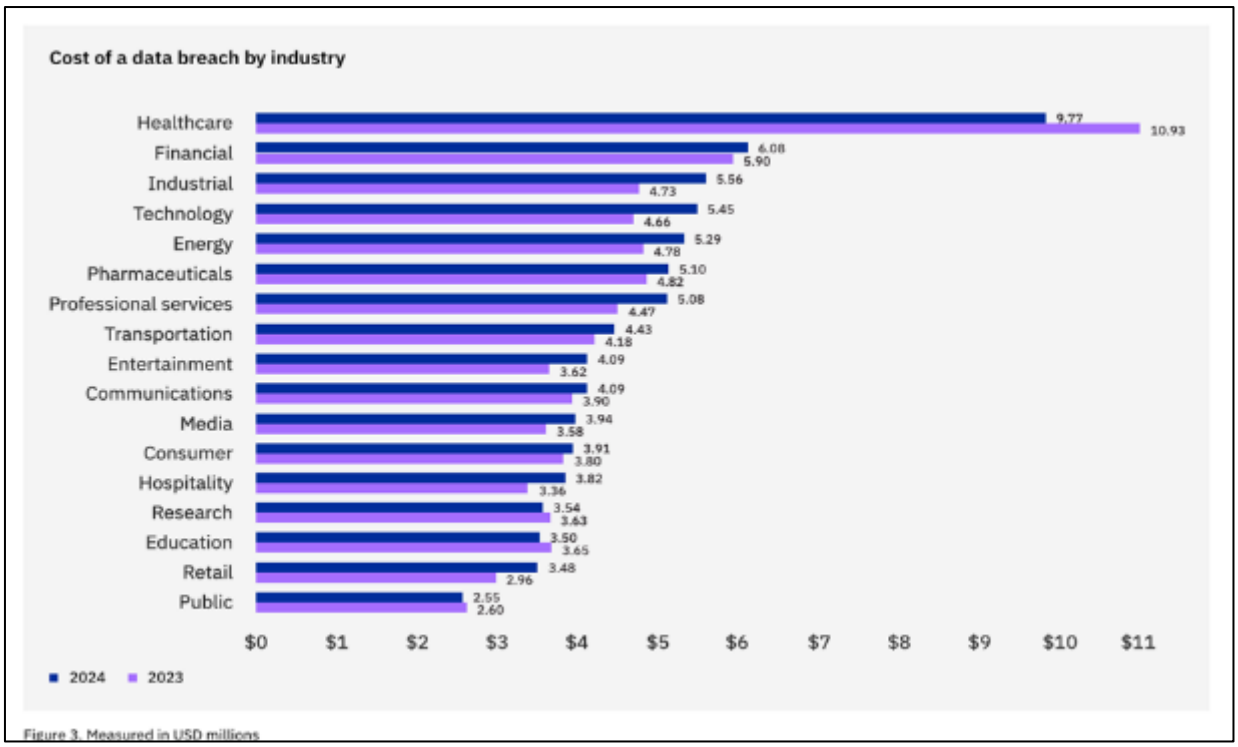

Figure 2 Cost of Data breach by Industry [14]

4.1. Lagging security approaches

The Healthcare sector tends to lag behind other industries with respect to cybersecurity investments. According to *Security Intelligence,* it is reported that 6% to 10% is spent off the overall IT budget by the healthcare industry on cybersecurity, where the average spend remains at 6%. A forecasted rise in cybersecurity investments after a data breach was considered by 51% of all the industries surveyed, despite the cost of data breaches escalating each year [16]. Additionally, *Security Intelligence* highlighted a recent Gartner report which shows that IT security and data protection remain the top priorities for only 28% of healthcare leaders in 2024.

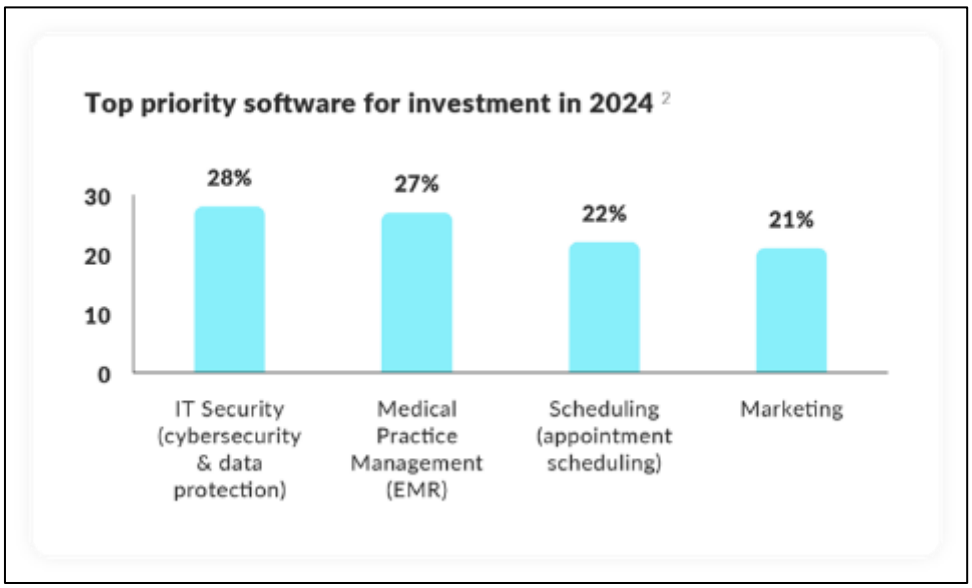

Figure 3 Top Investment priorities of health organizations [15]

Furthermore, as reported in IBM's 2023 Cost of a Data Breach, data breach costs remain significantly lower when organizations have dedicated tools and teams to protect and manage data breaches. The overall cost savings for the

healthcare industry in this study amounted to $2 million with incident response (IR) and testing teams established, unlike places with no IR or testing. Health organizations using artificial intelligence and automation massively saved $850,000 than the global average cost of a breach [16]. Likewise, in their 2024 Cost of a Data Breach report, IBM states that organizations that have highly adopted and integrated AI and automation in their security operations, especially in attack surface management (ASM), red teaming and posture management reported the most significant loss cutting of $2.2 million on breach expenses. This trend reveals a 10% increase compared to the previous year in AI adoption. Nonetheless, with the increased application of AI in cybersecurity, about half of breached organizations are struggling with a shortage of security staffing, representing an increase of 26.2% compared to the previous year. This shortage has led to an additional $1.76 million required to mitigate breaches, underscoring the criticality of the cybersecurity skills gap despite 1 in 5 organizations adopting generative AI tools to improve productivity and address workforce gaps [16].

The findings of this research reveal a paradox in the U.S. healthcare sector. Unsurprisingly, the costs of breaches continue to rise, even as organizations are investing more in cybersecurity. Increasing costs of data breaches, reaching an average $4.88 million, indicate that many organizations remain far from proactive security strategies and operate in reactive measures. Lost business costs accounting for the greatest financial impact driven by operational disruption, customer attrition, and regulatory fines allow the conclusion that recovering from breaches goes beyond straightforward financial losses. This also supports the call that organizations should consider more proactive measures rather than relying on post-breach remediation.

Arguably, the most compelling finding is the cost-benefit analysis of artificial intelligence in security and automation. Organizations that adopted AI across attack surface management, posture management, and red teaming saved $2.2 million in breach costs. This means that the future is not simply in AI as a trend but in the definite factor as a way of mitigating financial losses. However, the increase in cybersecurity skills deficit simultaneously, leading to a further $ 1.76 million in breach costs questions whether technology alone can resolve security risks. While AI ushers in improved efficiency, security solutions can only be optimally utilized if professionals skilled in the execution and management of security frameworks are hired. This finding proves that AI introduction has to be accompanied by investments in the workforce correspondingly and should not be treated as a standalone measure.

Another major concern is the healthcare sector's lagging investment in cybersecurity. With 6% to 10% of its IT budgets going into security, the healthcare industry ranks poorly despite being the industry most targeted for data breaches. With just 28% of healthcare leaders considering security and data protection in 2024 reveals organizational complacency which leaves healthcare institutions most vulnerable. This discovery directly contradicts the assumption that as breach costs increase over time, so will security investments. Rather, the opposite is seen in healthcare as they seem to appear more reactive than incorporating cybersecurity as a strategic priority.

Another important observation is the record-breaking spike in the number of healthcare data breaches in March 2024, which highlights a 50% increase from February 2024. This indicates that while there has been a progressive advancement of improved security technologies, threats are evolving even more. HIPAA establishes regulatory standards rules protecting healthcare information and its penalties are objective to incentivize organizations to follow these regulations. Yet, this record-breaking number of breaches in March 2024, suggests that, even with these severe penalties, just strictly following compliance standards isn't the same as having strong cybersecurity. This increase coupled with the HIPAA's strict regulatory fines up to a staggering $1.92 million for each violation, infers that compliance-driven security models may not be entirely adequate as compliance is not equal to security. Organizations can meet basic compliance and regulations and may have still not achieved a robust, risk driven security posture that mitigates breaches efficiently. This difference between mere compliance and security readiness is a critical factor that should not be underestimated and must be considered by the policy makers and healthcare organization leaders [17].

In addition, the efficiency of the incident response (IR) teams supports the argument for proactive security investments. Organizations with well-established IR frameworks made $2,000,000 savings in comparison to those who did not. Also, the findings reveal that collaboration with law enforcement decreased containment time from 297 to 281 days and cut nearly $100,000 on expenses. This shows that although breaches seem unavoidable, their financial impact is not fixed or predictable. Well established response strategies can significantly save cost and recovery time for organizations. The comparison between organizations who incorporate AI into their preventive measures and those lacking in incidence response readiness implies that prevention and response are not mutually exclusive. A comprehensive security needs to be managed proactively as well as contingently to be cost effective. Findings from this research indicate that maximum cost reduction can be achieved when organizations engage in both proactive and reactive strategies. The health care industry's reluctance to prioritize security investments, over-reliance on regulatory compliance, along with workforce deficits exacerbates financial risks, moving breaches from the inevitable to excessively costly. Hence, the real

issue lies not in whether it is more cost effective to focus on prevention or recovery, but rather how organizations can effectively integrate both to maximize their financial cost and reinforce operational resilience.

Recommendations

To mitigate the future occurrence of breaches effectively, healthcare organizations must implement more proactive risk-based security frameworks than compliance-based security risk management frameworks. Real time threat intelligence adaptive security policies and continuous monitoring cannot be overemphasized to counter emerging attack vectors. Making investments in cybersecurity talents is equally important as AI and automation can't compensate for the increased skills gap. Healthcare institutions have to develop highly efficient and robust approaches to manage incidents through structured teams and simulations in order to contain incidents in a short time and decrease costs. Furthermore, increased cooperation with the law enforcement as evidenced will contribute effectively by shortening the time to resolve breaches and minimizing financial losses. We also find that financial commitment remains an essential indicator of cybersecurity readiness. The current level of investment of the healthcare industry towards cybersecurity is insufficient given the high stakes associated with healthcare data breaches. Increased investment in advanced threat detection, vendor risk management and end point security are imperative. Third-party providers must also ensure strict compliance with security standards before they integrate with healthcare systems. Cybersecurity needs to be viewed as an organizational priority than a compliance requirement.

5. Conclusion

The increased financial and operational associated with data breaches in the U.S. healthcare sector highlight the inefficiency of compliance- driven security model. As regulations like HIPAA set the necessary standards, they do not entirely translate into holistic risk mitigation. The unprecedented breaches in 2024 show that cyber attacks are increasing at a faster rate than security solutions are being discovered, threatening the basic infrastructures of corporate organizations and outcompeting poorly funded cyber security departments. More so, security professionals remain scarce resulting in heightened breach expenses even with improvements in AI security solutions which underlines the current need for both technological investment and skilled expertise. Failing to adopt proactive risk-based security measures and rather than continuing with reactive security models exposes the health sector to more costly disruptions patients record compromises and damages the reputation of these targeted organizations. A paradigm shift is needed which handles cybersecurity as a strategic imperative rather than an IT expense.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Clement, N., (2023), July. M&A Effect on Data Breaches in Hospitals: 2010–2022. In Proceedings of the 22nd Workshop on the Economics of Information Security, Geneva, Switzerland (pp. 5-8).

[2] Choi, S. J., & Johnson, M. E. (2019). Do hospital data breaches reduce patient care quality? arXiv preprint, arXiv:1904.02058.

[3] Acquisti, Alessandro, Allan Friedman, and Rahul Telang, "Is there a cost to privacy breaches? An event study," ICIS 2006 proceedings, 2006, p. 94.

[4] Yuan, Bocong, Jiannan Li, and Peiguan Wu, "The effectiveness of electronic health record promotion for healthcare providers in the United States since the Health Information Technology for Economic and Clinical Health Act: An empirical investigation," The International Journal of Health Planning and Management, 2021, 36 (2), 334–352.

[5] Ponemon Institute. (2013). 2013 survey on medical identity theft. Ponemon Institute. Retrieved from https://clearwatercompliance.com/wp-content/uploads/2013/10/2013-Medical-IdentityTheft-Report-FINAL.pdf

[6] U.S. Department of Health and Human Services (HHS). (2009). Breach notification for unsecured protected health information; Interim final rule. Federal Register, 74(162), 42740-42770.

[7] Oslen E. (2023) Average cost of healthcare data breach reaches $11M, report finds. Cybersecurity Dive. Retrieved from: https://www.cybersecuritydive.com/news/healthcare-data-breach-costs/688889/#:~:text=Dive%20Brief:%20*%20Healthcare%20continues%20to%20be,second%2Dmost%20expensive%20data%20breaches%20at%20$5.9%20million

[8] Alder S. (2024) Healthcare Data Breach Statistics. Retrieved from: https://www.hipaajournal.com/healthcare-data-breach-statistics/

[9] IBM (2022) Cost of a Data Breach Report 2022. Retrieved from: https://www.key4biz.it/wp-content/uploads/2022/07/Cost-of-a-Data-Breach-Full-Report-2022.pdf

[10] Verizon. (2018). Data Breach Investigations Report. Retrieved from https://enterprise.verizon.com/resources/reports/DBIR_2018_Report.pdf

[11] Verizon. (2019). Data Breach Investigations Report. Retrieved from https://enterprise.verizon.com/resources/executivebriefs/2019-dbir-executive-brief.pdf

[12] Janakiraman, R., Park, E., M. Demirezen, E. and Kumar, S., 2023. The effects of health information exchange access on healthcare quality and efficiency: An empirical investigation. Management Science, 69(2), pp.791-811.

[13] IBM Security. (2023). Cost of a Data Breach Report 2023. IBM.

[14] IBM (2024) Cost of a Data Breach Report 2024. Available at: https://www.ibm.com/downloads/documents/us-en/107a02e94948f4ec

[15] Tricerat (2024) Health IT Security Report: Top 7 Causes of HIPAA Breaches in 2024. Available at: https://www.tricerat.com/blog/causes-of-hipaa-breaches-in-2024#:~:text=Written%20byTricerat,affecting%20over%2013%20million%20individuals.

[16] Greenlee M. (2023) Cost of a data breach 2023: Healthcare industry impacts. Security Intelligence Available at: https://securityintelligence.com/articles/cost-of-a-data-breach-2023-healthcare-industry-impacts/

[17] Ahmed, Z., Osifowokan, A. S., Filani, A., & Donkor, A. A. Comprehensive analysis of cyber attacks and data breaches in the US health sector: Identifying vulnerabilities and developing proactive defense strategies.