Strengthening Compliance with Data Privacy Regulations in U.S. Healthcare Cybersecurity

Abstract

This study evaluates the state of data privacy and cybersecurity compliance within the U.S. healthcare sector, leveraging data from the U.S. Department of Health & Human Services Breach Portal, Verizon Data Breach Investigations Report, and the Health IT Dashboard. A quantitative methodology comprising descriptive statistical analysis, K-means clustering, and multivariate regression was employed to examine healthcare data breaches, categorize cybersecurity threats, and identify compliance challenges. Findings revealed a persistent increase in breaches, with hacking/IT incidents comprising over 80% of breaches in 2020 and a peak of 135 incidents in 2021. Budget allocation emerged as the most significant predictor of compliance ($p = 0.0178$), affirming resource constraints. Malware and ransomware were identified as dominant threats, while insider threats emerged as high-impact vulnerabilities. The study recommends increasing cybersecurity budgets, implementing continuous staff training, harmonizing regulations, and adopting Cybersecurity Maturity Models to systematically enhance security postures. The study provides critical insights into the challenges faced by healthcare organizations in achieving compliance with evolving data privacy regulations such as HIPAA and HITECH. The findings highlight the economic and operational implications of non-compliance, including financial penalties, reputational harm, and patient trust erosion. The study further affirms the importance of strategic investments in advanced cybersecurity tools, policy harmonization, and employee education. Hence, policymakers and healthcare administrators can utilize these insights to foster a robust culture of compliance, ensuring the protection of sensitive patient information and the resilience of healthcare operations against cyber threats. The study suggests that future research explores integrating artificial intelligence, zero-trust architectures, and adaptive risk management frameworks to further enhance cybersecurity strategies and regulatory compliance.

Keywords: cybersecurity, healthcare compliance, HIPAA, K-means clustering, multivariate regression

1. Introduction

The increasing digitization of healthcare services in the United States has profoundly transformed patient care delivery and operational efficiency. However, this technological advancement has concurrently exposed the sector to escalating cybersecurity threats. Data breaches within the U.S. healthcare industry have risen alarmingly, both in frequency and severity. In 2023 alone, 725 breaches were reported, compromising over

133 million records—more than double the 51.9 million records exposed in 2022 (Alder, 2024). These incidents jeopardize sensitive patient data and impose substantial financial, operational, and reputational burdens on healthcare organizations.

The U.S. regulatory framework for safeguarding healthcare data is anchored in the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act. These laws mandate that entities implement administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and availability of protected health information (PHI). Complementing these mandates, cybersecurity frameworks such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework and the HITRUST Common Security Framework (CSF) provide structured methodologies to mitigate cybersecurity risks. These frameworks offer tailored guidance to address the healthcare sector's unique vulnerabilities (Abohatem et al., 2023).

Despite these regulatory and framework-driven efforts, the sector faces a growing array of sophisticated cyber threats. Hacking and IT incidents constituted 80% of reported breaches in 2023, a sharp increase from 49% in 2019 (McKeon, 2023). Common tactics include ransomware attacks, which encrypt critical data and disrupt operations, and phishing schemes, where individuals are deceived into divulging credentials or installing malware. Insider threats—whether malicious or negligent—alongside malware infections further exacerbate the challenges. The proliferation of connected medical devices and reliance on cloud-based systems have expanded the attack surface, introducing complex security risks that healthcare organizations must address (Bala et al., 2024).

Legacy systems remain a critical barrier to cybersecurity resilience. These outdated technologies, often unpatched and lacking modern security features, serve as vulnerable entry points for attackers. Limited financial and technical resources, particularly among smaller providers, compound the difficulty of implementing robust security measures. Human error also remains a persistent challenge, with insufficient training leaving staff ill-prepared to adhere to cybersecurity protocols. Compounding these vulnerabilities is the complexity of regulatory compliance. Only 38% of healthcare providers reportedly meet all HIPAA Security Rule requirements, illustrating systemic struggles in achieving compliance (Bureau, 2021).

Recent high-profile breaches highlight the sector's vulnerabilities. For example, the 2023 Tampa General Hospital breach exposed 2.1 million patient records, resulting in a $6.8 million settlement (Diaz, 2025). Similarly, the HCA Healthcare breach impacted over 11 million patients (Ivanova, 2023). Such incidents underscore the significant financial repercussions, including regulatory fines, legal expenses, breach mitigation costs, and operational disruptions. The average cost of a healthcare data breach reached $10.93

million in 2023, with a per-record cost of $408, far exceeding the cross-industry average of $148 (Ukyab & Beato, 2024). Beyond these direct costs, reputational damage further erodes patient trust, often resulting in patient attrition and long-term financial losses.

Regulatory bodies have taken steps to strengthen enforcement and adapt to evolving threats. In December 2024, the Department of Health and Human Services (HHS) proposed amendments to HIPAA to enhance cybersecurity protections (HHS, 2024). These revisions include requirements for documented security policies and improved safeguards for electronic PHI managed by business associates (HHS, 2024). Similarly, enforcement actions such as the Federal Trade Commission's $7.1 million fine against mental health startup Cerebral for privacy violations emphasize the need for compliance and accountability (Alder, 2024).

Cybersecurity breaches also impose broader economic and reputational consequences. Resources must be redirected to post-breach mitigation efforts, including hiring cybersecurity experts and upgrading security systems. Reputational damage often leads to reduced patient retention and legal actions, as seen in the Children's Healthcare of Atlanta case, where allegations of unauthorized data sharing with Facebook highlighted the risks associated with inadequate data protection (Rodrigues et al., 2024).

Proactive strategies are essential to counteract these risks. A tailored Cybersecurity Maturity Model (CMM), inspired by the Department of Defense's Cybersecurity Maturity Model Certification (CMMC), could provide a structured approach for assessing cybersecurity resilience and guiding investment decisions. Such a framework would enable healthcare organizations to advance through progressive cybersecurity maturity levels, fostering continuous improvement in compliance and operational security (Ngounou et al., 2024). Furthermore, lessons from case studies such as Tampa General Hospital's effective incident response highlight the importance of collaborative crisis management in mitigating the impacts of breaches and preserving stakeholder trust.This study aims to critically analyze the current state of data privacy and cybersecurity within the U.S. healthcare sector, identifying key vulnerabilities and challenges to compliance with relevant regulations. Furthermore, it seeks to propose evidence-based strategies and recommendations for strengthening cybersecurity defenses and fostering a culture of compliance to effectively safeguard protected health information (PHI), by achieving the following objectives:

1. Evaluates the effectiveness of existing data privacy regulations (e.g., HIPAA, HITECH) and cybersecurity frameworks (e.g., NIST Cybersecurity Framework, HITRUST CSF) in mitigating cybersecurity risks within the U.S. healthcare context.

2. Systematically identifies and categorises the primary cybersecurity threats and vulnerabilities currently exploited within U.S. healthcare organizations, drawing upon empirical data from recent breaches and security incidents.
3. Investigates and analyses the multifaceted challenges and barriers that impede effective compliance with data privacy regulations in U.S. healthcare, considering technical, organizational, human, and economic factors.
4. Formulates and proposes practical, actionable strategies and recommendations for diverse stakeholders (healthcare organizations, policymakers, technology providers, etc.) to enhance data protection, strengthen cybersecurity posture, and promote a robust culture of compliance within the U.S. healthcare ecosystem.

This study becomes essential as it addresses the critical and timely issue of data privacy and cybersecurity compliance in the U.S. healthcare sector. Using K-means clustering and multivariate regression, the research provides an in-depth analysis of persistent vulnerabilities such as hacking incidents and insider threats, highlighting the economic and operational implications of data breaches, emphasizing the pivotal role of financial investment in achieving compliance.

2. LITERATURE REVIEW

The regulatory framework governing data privacy in the U.S. healthcare sector is both intricate and constantly evolving, reflecting the critical imperative to protect sensitive patient information. Central to this framework is the Health Insurance Portability and Accountability Act (HIPAA) of 1996, which established national standards for safeguarding protected health information (PHI). According to Subramanian et al. (2024), HIPAA comprises three principal components: the Privacy Rule, delineating permissible uses and disclosures of PHI; the Security Rule, mandating administrative, physical, and technical safeguards to protect electronic PHI (ePHI); and the Breach Notification Rule, which requires notification to affected individuals, the Department of Health and Human Services (HHS), and, in certain circumstances, the media in the event of a breach involving unsecured PHI.

The regulatory scope of HIPAA was significantly enhanced by the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009. As Szalados (2021) posits, this legislation introduced stricter penalties for non-compliance, expanded regulatory oversight to include business associates, and incentivized the adoption of electronic health records. This expansion underscores the increasing emphasis on cybersecurity within the healthcare sector. Recent regulatory initiatives, such as the December 2024 proposed revisions to the HIPAA Security Rule, aim to bolster

cybersecurity measures further by mandating encryption, multifactor authentication, and comprehensive documentation of security policies (Donaldson, 2024; Adigwe et al., 2024). Notably, these revisions eliminate the distinction between "required" and "addressable" safeguards, effectively requiring all specified measures unless alternative solutions providing equivalent security are demonstrated (Fillmore et al., 2023; Alao, Adebiyi and Olaniyi, 2024).

State-level regulations compound the complexity of the compliance landscape. For example, the California Consumer Privacy Act (CCPA), along with its amendments under the California Privacy Rights Act (CPRA), grants residents of California extensive rights over their personal data, including health-related information. Ijaz and Carrie (2023) observes that healthcare organizations operating within California must navigate the interplay between state-specific and federal requirements, addressing overlapping mandates to achieve comprehensive compliance. This dual-layered regulatory environment necessitates adaptive and cohesive data governance strategies among national healthcare providers.

Regulatory enforcement is primarily overseen by the Office for Civil Rights (OCR) within HHS; the OCR investigates complaints, conducts compliance reviews, and imposes monetary penalties for violations, as evidenced by its resolution of 13 enforcement actions in 2023, reflecting its ongoing commitment to upholding HIPAA standards (Davis, 2023; Arigbabu et al., 2024). In addition to the OCR, the Federal Trade Commission (FTC) addresses broader consumer privacy concerns. High-profile enforcement actions, such as the $7.1 million fine levied against the mental health startup Cerebral for alleged privacy violations, highlight the FTC’s significant role in addressing consumer data protection issues beyond HIPAA's jurisdiction (Alder, 2024; Fabuyi et al., 2024).

This multifaceted regulatory framework requires healthcare organizations to remain vigilant and proactive in their compliance efforts. Organizations must address the interplay of federal and state mandates while adapting to emerging cybersecurity challenges and enforcement priorities, as emphasized by Adegbite et al. (2023). A cohesive approach to data governance and privacy is essential for maintaining compliance and safeguarding patient information in an increasingly complex regulatory environment.

Cybersecurity Threats and Vulnerabilities in Healthcare

The U.S. healthcare sector faces a diverse and escalating range of cybersecurity threats, requiring comprehensive strategies to mitigate risks and safeguard sensitive patient data. Among the most significant challenges are hacking incidents, including ransomware, phishing, and malware attacks (Neprash et al., 2022; Gbadebo et al., 2024). Ransomware, which encrypts critical data and disrupts operations, has seen a dramatic rise, with incidents increasing by over 100% since 2019 (Benmalek, 2024; Joeaneke et al., 2024). Teichmann and Boticiu (2024) notes that these attacks often result in substantial financial losses and operational disruptions, as demonstrated by the 2023 breaches at Tampa General Hospital and HCA Healthcare, which affected millions of patients and led to significant settlements. Phishing campaigns, which exploit human vulnerabilities through deceptive communications, remain a prevalent entry point for attackers, frequently serving as precursors to malware deployment aimed at data exfiltration and system compromise (Bardin, 2024; Joeaneke et al., 2024).

Insider threats exacerbate cybersecurity risks within healthcare organizations. These threats may stem from malicious insiders intentionally breaching systems for financial gain or inadvertent errors caused by insufficient training or negligence (Al-Mhiqani et al., 2024; John-Otumu et al., 2024). Human errors, such as misconfigured system settings or unintended data sharing, often lead to breaches (El-Bably, 2021; Joseph, 2024). Ugbebor et al. (2024) posits that addressing insider threats necessitates a dual approach, combining stringent access controls with continuous employee education to cultivate a culture of security awareness.

The growing integration of connected medical devices and Internet of Things (IoT) technologies introduces additional vulnerabilities. IoT devices, including patient monitoring systems and implantable medical devices, often lack robust security features, rendering them susceptible to exploitation (Jaime et al., 2023; Kolade et al., 2024). Recent studies underscore these risks, highlighting the potential for such devices to act as entry points for attackers to access broader healthcare networks or disrupt critical services (Affia et al., 2023; Djenna et al., 2021; Staddon et al., 2021; Okon et al., 2024). Securing this interconnected ecosystem requires device-level protections combined with comprehensive network security measures, as Mustafa et al. (2024) observes.

Legacy systems present yet another significant challenge; outdated technologies frequently lack critical updates and patches, creating exploitable vulnerabilities (Dissanayake et al., 2021; Olabanji et al., 2024). Budgetary constraints and compatibility issues often hinder system upgrades, leaving organizations exposed to attacks (George et al., 2024; Olabanji, Olaniyi and Olagbaju, 2024). According to Ebong et al. (2024), mitigation strategies include network segmentation, intrusion detection systems, and virtual patching to address known vulnerabilities. However, a sustainable solution involves the phased replacement of legacy systems with secure, modern infrastructure (Irani et al., 2023; Olabanji, Olaniyi and Olaoye, 2024).

The convergence of external attacks, internal vulnerabilities, and technological challenges highlights the urgency for healthcare organizations to adopt proactive, layered security measures. Shahid et al. (2022) asserts that only through comprehensive risk management strategies can the healthcare sector effectively protect patient data and ensure the reliability of critical services.

Barriers to Compliance with Data Privacy Regulations

Compliance with data privacy regulations in the U.S. healthcare sector is hindered by a complex interaction of technical, organizational, human, and economic barriers (Williamson & Prybutok, 2024; Oladoyinbo et al., 2024). Technically, healthcare organizations face significant challenges in implementing robust safeguards such as encryption, access controls, and anomaly detection tools (Bala et al., 2024; Olaniyi, 2024). While these measures are mandated under regulations like HIPAA's Security Rule, their integration often demands specialized expertise that many organizations, particularly smaller providers, lack. George et al. (2023) argues that the rapidly evolving nature of cyber threats necessitates frequent updates and adaptations, placing additional strain on already limited IT resources.

Organizational constraints further compound technical challenges. Limited budgets, especially in smaller healthcare organizations and rural facilities, often restrict investments in cybersecurity infrastructure and skilled personnel (Abdul et al., 2024; Olaniyi, Olaoye and Okunleye, 2023). Mahboubi et al. (2024) notes that this scarcity of resources typically results in reactive security measures, rather than proactive approaches. Moreover, a lack of executive buy-in exacerbates the problem, as

cybersecurity is often deprioritized at the leadership level, receiving inadequate funding and attention (Anderson et al., 2024; Olaniyi et al., 2024). This absence of prioritization frequently leads to fragmented accountability and poorly coordinated security efforts, weakening the organization's compliance capabilities (Lægreid & Rykkja, 2021; Olateju et al., 2024).

Human factors also contribute significantly to compliance failures. Inadequate staff training and awareness remain persistent vulnerabilities, with human error—such as falling for phishing attacks or mishandling sensitive data—posing a substantial threat (Sarker et al., 2024; Olateju et al., 2024). Even the most advanced technical safeguards cannot fully mitigate these risks, as Jamal et al. (2024) observes. This underscores the importance of regular, comprehensive security training programs that educate employees on data privacy, common cyberattack methods, and best practices for managing sensitive information. Cultivating a culture of security consciousness throughout the organization is essential to mitigating these risks effectively (Khando et al., 2021; Tejay & Mohammed, 2022; Salako et al., 2024).

Economic barriers represent another critical challenge; implementing and maintaining effective cybersecurity measures, such as acquiring advanced technology, hiring skilled personnel, and conducting ongoing training, require significant financial investment. Firoozi et al. (2024) highlights that for many organizations, these costs are difficult to justify amid competing operational priorities. However, the economic consequences of non-compliance—including regulatory fines, legal penalties, reputational harm, and breach recovery costs—often far exceed the costs of proactive cybersecurity investments (Shandilya et al., 2024; Samuel-Okon et al., 2024). Recent data illustrates a rising trend in the average cost of healthcare data breaches, emphasizing the financial prudence of treating cybersecurity as a strategic investment rather than an expense (Prakash & Garg, 2024; Elendu et al., 2024; Selesi-Aina et al., 2024).

Addressing these multifaceted barriers necessitates a holistic strategy that integrates technological innovation, organizational leadership, staff education, and efficient resource allocation to safeguard patient data and achieve regulatory compliance effectively.

Economic Impact of Cybersecurity Breaches

The economic repercussions of cybersecurity breaches in the U.S. healthcare sector are extensive, encompassing both direct and indirect costs that strain organizational resources and jeopardize long-term sustainability. Direct costs include regulatory fines, legal expenses, and expenses related to breach mitigation efforts. For instance, Anthem Inc.'s 2015 data breach, which compromised approximately 79 million records, resulted in a $16 million settlement with the Office for Civil Rights (OCR) and an additional $115 million class-action settlement (Tweh, 2017). Similarly, Tampa General Hospital's 2023 breach, which affected 2.1 million individuals, culminated in a $6.8 million settlement (Alder, 2024). These examples underscore the financial consequences associated with regulatory penalties, legal actions, and operational recovery measures, collectively imposing significant burdens on healthcare organizations.

Indirect costs, although less immediately quantifiable, have equally detrimental effects. Reputational damage remains a primary concern, as data breaches undermine patient trust and public confidence. Eriks-Hoogland et al. (2024) contends that a substantial proportion of patients are inclined to switch healthcare providers following a breach, leading to patient attrition and sustained revenue losses. Additionally, operational disruptions exacerbate the impact of these incidents. Breaches often necessitate reallocating resources from core healthcare functions to incident response, forensic investigations, and system restoration, thereby compromising patient care and diminishing organizational efficiency (Kwon & Johnson, 2024; Val et al., 2024). These indirect costs frequently exceed direct financial penalties, emphasizing the multifaceted ramifications of cybersecurity breaches (Larsson & Sigholm, 2024; Val et al., 2024).

Investing in proactive cybersecurity measures offers a compelling economic rationale by mitigating these risks. The deployment of artificial intelligence (AI)-driven tools significantly enhances threat detection and response capabilities. AI-powered systems, as Akhtar and Tajbiul Rawol (2024) argues, can monitor networks in real time, identify anomalies indicative of cyber threats, and facilitate swift intervention to prevent breaches. These technologies also reduce reliance on manual processes, streamlining compliance with regulatory standards and minimizing the likelihood of fines for non-compliance. Furthermore, automated compliance systems ensure adherence to complex regulatory frameworks, alleviating administrative burdens and improving organizational efficiency (Oguejiofor et al., 2023).

Healthcare organizations that integrate advanced cybersecurity measures frequently realize substantial cost savings. Studies consistently demonstrate that entities employing AI-driven security solutions incur lower breach-related expenses than those relying on traditional methods (Usman, 2024; Larsson & Sigholm, 2024; Prakash & Garg, 2024). Although the initial investment in these technologies can be substantial, the long-term financial benefits—derived from avoiding breaches, maintaining operational continuity, and preserving patient trust—justify the expenditure. This strategic, proactive approach not only responds to the evolving cybersecurity threat landscape but also represents a prudent economic decision, reinforcing the necessity of robust cybersecurity infrastructure within the healthcare sector (Mallick & Nath, 2024; Kianpour & Raza, 2024).

Strategies for Strengthening Compliance and Cybersecurity

Enhancing compliance and cybersecurity in the U.S. healthcare sector requires a multifaceted approach, integrating organizational, technological, and policy-level strategies. At the organizational level, conducting comprehensive and regular risk assessments is essential for identifying vulnerabilities and prioritizing mitigation measures based on potential impacts. These assessments serve as the foundation for developing incident response plans, which ensure that healthcare organizations can manage breaches effectively and sustain operational continuity (Hassel & Cedergren, 2021). In addition, employee training plays a pivotal role in mitigating risks associated with human error, including susceptibility to phishing attacks. Training programs should emphasize common attack vectors, best practices for handling sensitive data, and strict adherence to security protocols (Aslan et al., 2023). Furthermore, the adoption of data minimization practices, which involve collecting and retaining only essential information, enhances security by reducing the volume of sensitive data susceptible to breaches (Jamal et al., 2024).

From a technological perspective, advanced tools such as artificial intelligence (AI) and machine learning (ML) significantly enhance cybersecurity defenses. Nassar and Kamal (2021) asserts that these technologies enable real-time threat detection by analyzing large datasets to identify anomalies indicative of cyber threats. AI-driven systems can detect and neutralize potential intrusions proactively, thereby minimizing damage. The implementation of zero-trust security models further strengthens defenses by requiring strict authentication and authorization for all access requests, regardless of user location

or device. As healthcare organizations increasingly adopt cloud-based services, improving cloud security becomes critical. Encrypting data, implementing robust access controls, and conducting regular security audits are necessary measures to ensure the integrity and confidentiality of sensitive patient information stored in the cloud environment (Kommidi & Padakanti, 2024).

At the policy level, the development of a Healthcare Cybersecurity Maturity Model (HCMM) could provide a structured framework for enhancing cybersecurity capabilities systematically. Inspired by established frameworks such as the Department of Defense's Cybersecurity Maturity Model Certification, the HCMM would guide organizations through progressive stages of cybersecurity maturity. This model would enable tailored investments based on risk profiles, ensuring that resources are allocated efficiently and effectively (Raju & Kondle, 2024). Furthermore, harmonizing federal and state regulations is crucial for reducing compliance challenges. The current fragmented regulatory landscape diverts significant resources from proactive security measures to address varying requirements. Establishing unified national standards would streamline compliance efforts and promote a consistent approach to data privacy and protection across the healthcare sector (Silva & Soto, 2022).

By integrating comprehensive risk assessments, targeted employee training, advanced technological tools, and cohesive policy frameworks, healthcare organizations can address cybersecurity challenges more effectively. These strategies not only safeguard sensitive patient information but also enhance the sector's capacity to navigate a complex and evolving regulatory environment.

3. Methodology

This study utilized a quantitative research design, leveraging publicly available datasets to analyze cybersecurity in the U.S. healthcare sector. The data sources were the Breach Portal from the U.S. Department of Health & Human Services, the Verizon Data Breach Investigations Report (DBIR), and the Health IT Dashboard from the Office of the National Coordinator for Health Information Technology.

All continuous variables were standardized to ensure comparability using the formula:

$$X_{scaled} = \frac{X - \mu}{(\sigma)}$$

where $X_{(scaled)}$ represents the standardized value, X is the raw variable, μ is the mean, and σ is the standard deviation.

To evaluate the effectiveness of existing regulations, descriptive statistics and trend analysis were applied. The temporal trends in breach frequency and penalties were modelled using linear regression:

$$Y_t = \beta_0 + \beta_1 t + \epsilon$$

where Y_t is the outcome (e.g., number of breaches) at time t, β_0 is the intercept, β_1 captures the trend, and ϵ represents the error term.

To categorize cybersecurity threats and vulnerabilities, K-means clustering was employed to group incidents based on characteristics - attack type and frequency. The clustering objective function minimized within-cluster variance:

$$J = \sum_{\{i=1\}}^{k} \sum_{\{x \in C_i\}} \|x - \mu_i\|^2$$

Where k is the number of clusters, C_i is the set of points in cluster i, x represents a data point, and μ_i is the centroid of cluster i. The optimal k was determined using the elbow method, plotting k against J.

For analyzing barriers to compliance, multivariate regression was used to quantify the impact of various factors (budget allocation, training hours, and EHR adoption rates).

The model is expressed as:

$$Y = \beta_0 + \beta_1 X_1 + \beta_2 X_2 + \cdots + \beta_n X_n + \epsilon$$

Where Y represents compliance levels, X_1, X_2,,X_n are independent variables, and β_1,β_2,…,β_n are their respective coefficients. Statistical significance was determined by p-values, with variables below 0.05 considered impactful.

4. Results

Evaluation of the Effectiveness of Existing Data Privacy Regulations and Cybersecurity Frameworks

To evaluate the trends in healthcare data breaches, their types, and the associated financial penalties to assess the impact of data privacy regulations and cybersecurity frameworks in the U.S. healthcare sector from 2019 to 2023, a descriptive statistics analysis was performed. Figure 1 below illustrates the trends in total healthcare data breaches from 2019 to 2023. A fluctuating pattern is observed, with breaches peaking in 2021 (135 incidents) and showing a slight decline by 2023 (128 incidents). The overall trend highlights persistent vulnerabilities despite regulatory efforts like HIPAA and HITECH. This consistency suggests limited impact of regulations in significantly reducing breach occurrences.

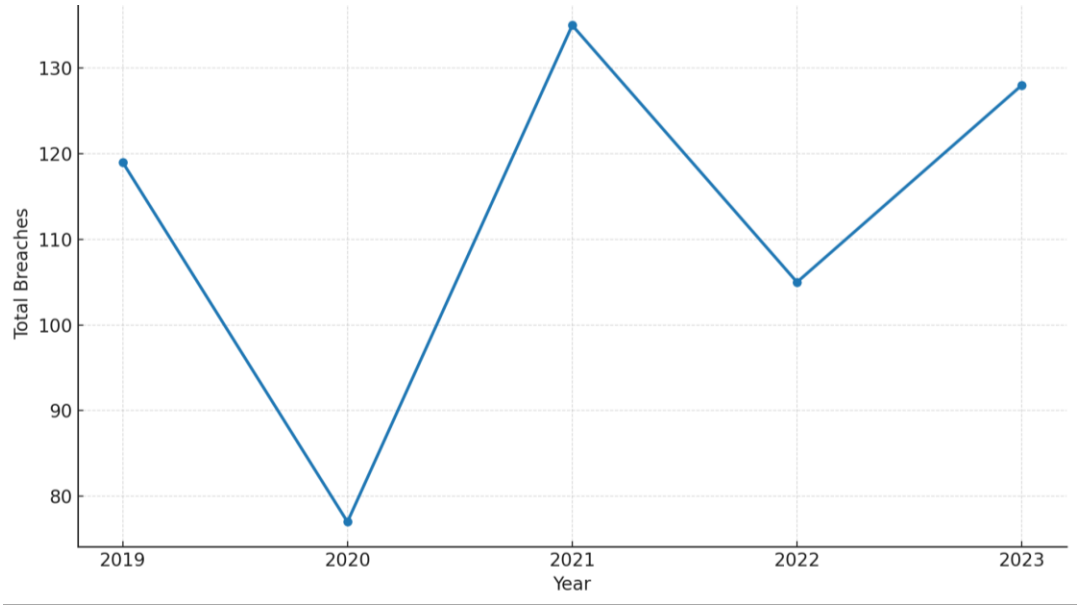

Figure 1: Line Chart for Total Breaches Over Time

Proportions of Breach Types

The proportions of breach types across the years, as shown in Figure 2, reveal critical insights. Hacking/IT incidents consistently dominated, ranging from 36.3% (2021) to 84.4% (2020). Unauthorized access followed, with a notable peak in 2022 at 40%. The dominance of Hacking/IT breaches indicates a continued focus of attackers on exploiting technological vulnerabilities. These findings align with the growing sophistication of cyber threats and emphasize the need for strengthened technological safeguards. Other breach types, such as theft and improper disposal, contributed marginally but underscore areas for improvement in data handling practices.

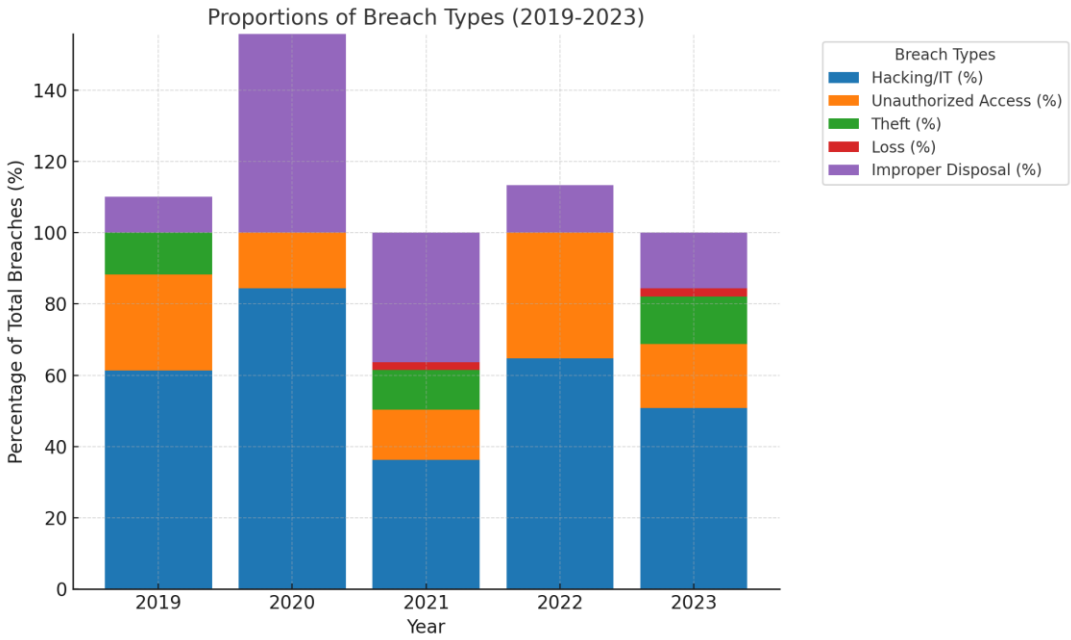

Figure 2: Stacked Bar Chart for Proportions of Breach Types

Year	Hacking/IT (%)	Unauthorized Access (%)	Theft (%)	Loss (%)	Improper Disposal (%)
2019	61.34	26.89	15.13	6.72	-10.08
2020	84.42	42.86	22.08	6.49	-55.84
2021	36.30	14.07	11.11	2.22	36.30
2022	64.76	40.00	5.71	2.86	-13.33
2023	50.78	17.97	13.28	2.34	15.63

Table 1: Proportions of breach types for the 2019 to 2023

The table above (Table 1) further breaks down the proportions of breach types for each year, providing detailed insights into the relative dominance of each type. For example, hacking/IT incidents consistently comprise a significant portion of total breaches, underscoring the need for enhanced cybersecurity measures. Unauthorized access breaches peaked at 40% in 2022, highlighting gaps in access control mechanisms.

Financial Penalties and Regulatory Enforcement

The trends in financial penalties, displayed in Figure 3, reflect the enforcement efforts and financial consequences of non-compliance. The penalties fluctuated from approximately $529,000 in 2020 to $863,000 in 2023, indicating variability in the severity of breaches and enforcement actions. The data suggests an increasing focus on imposing financial consequences for breaches, which aligns with HIPAA's enforcement measures.

However, the variations may reflect inconsistencies in compliance levels or regulatory prioritization.

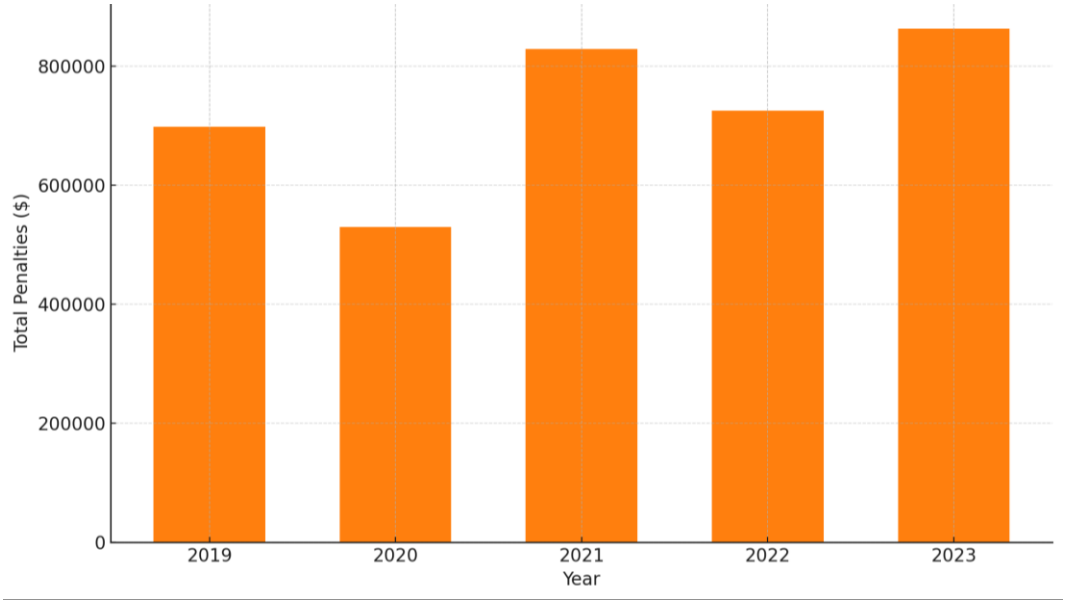

Figure 3: Bar Chart for Total Financial Penalties Over Time

The significant financial penalties indicate the financial risks of non-compliance but also suggest room for more consistent enforcement to incentivize stronger adherence to regulations. Unauthorized access breaches reveal gaps in organizational policies, including access controls and employee training.

Identification and Categorization of Primary Cybersecurity Threats and Vulnerabilities

To explore and categorise the primary cybersecurity threats and vulnerabilities in the U.S. healthcare sector, a K-means cluster analysis was performed. The result of the analysis identifies clusters of threats based on frequency, success rates, and financial impacts, offering insights into dominant patterns.

The clustering analysis revealed three distinct groups of threats, each characterized by unique attributes. Table 2 summarizes the average frequency, success rate, financial impact, and dominant threat types for each cluster.

Cluster	Avg. Frequency	Avg. Success Rate (%)	Avg. Financial Impact ($M)	Dominant Threat Types
0	118.38	43.80	2.60	Ransomware, Phishing, Insider Threat, Malware, Other
1	96.41	39.06	7.75	Insider Threat, Ransomware, Malware, Phishing, Other
2	149.11	67.57	5.86	Malware, Other, Phishing, Ransomware, Insider Threat

Table 2: Average frequency, success rate, financial impact, and dominant threat types for each cluster

Cluster 0 represents threats with moderate frequency, success rates, and financial impacts. This group includes ransomware and phishing, highlighting the widespread yet relatively contained nature of these attacks. Cluster 1 is characterized by lower frequency but significantly higher financial impact, likely reflecting high-cost but less frequent incidents such as insider threats. Cluster 2, the most severe, includes threats with the highest frequency and success rates, notably malware, which often leads to substantial operational and financial losses.

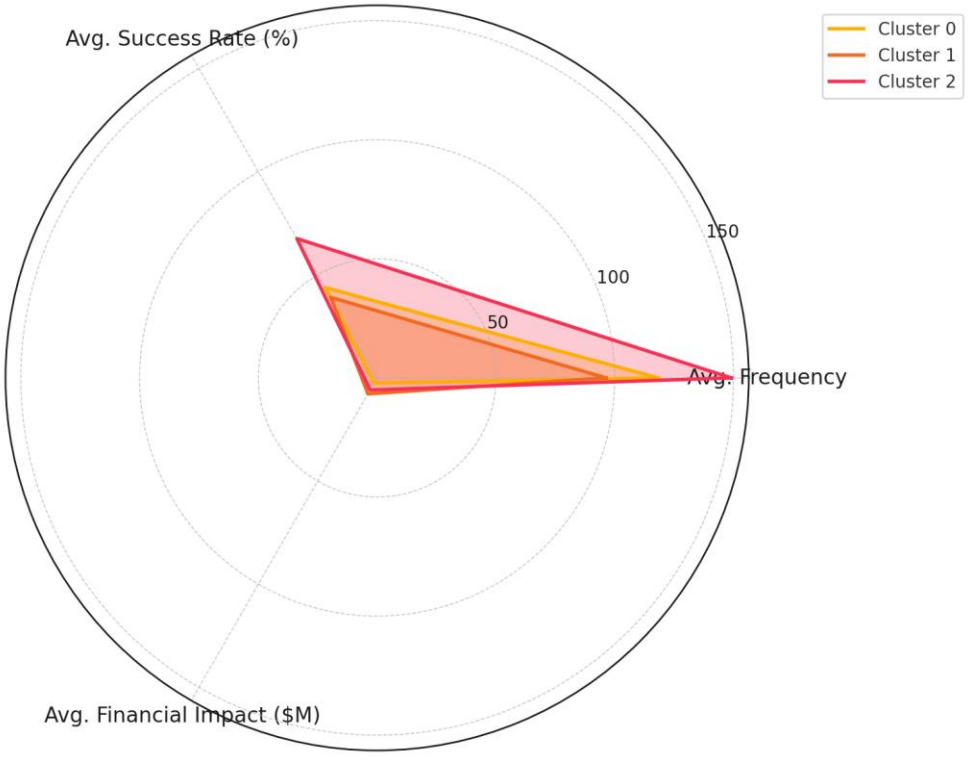

Figure 4: Radar Chart of Cybersecurity Threat Clusters

Figure 4 illustrates the characteristics of each cluster using a radar chart. Cluster 2 exhibits the highest values across all metrics, emphasizing its dominance in frequency, success, and financial impact. Cluster 1 stands out for its disproportionate financial impact despite lower frequency and success rates. Cluster 0 displays more balanced attributes, signifying moderate risks.

Emerging technologies such as artificial intelligence (AI) and zero-trust architectures offer significant potential to transform healthcare cybersecurity and compliance. AI-powered systems can monitor network activities in real time, detect anomalies indicative of cyber threats, and automate responses to mitigate breaches, thereby enhancing regulatory compliance. Similarly, zero-trust security models, which enforce strict authentication and authorization protocols, strengthen access controls and reduce the risks associated with insider threats and unauthorized access. Machine learning (ML), a subset of AI, can analyze patterns in large datasets to predict vulnerabilities, detect fraud, and streamline compliance efforts. By automating processes such as auditing and anomaly detection, ML minimizes human error and optimizes resource allocation, ensuring that healthcare organizations can better adhere to frameworks like HIPAA and HITECH. These technologies present promising avenues for addressing persistent challenges in healthcare cybersecurity.

Comparative Analysis Across Metrics

A parallel coordinates plot (Figure 5) provides a comprehensive view of the clusters' performance across all metrics. The distinct trajectories highlight the variation between clusters, emphasizing the need for tailored mitigation strategies for each threat type.

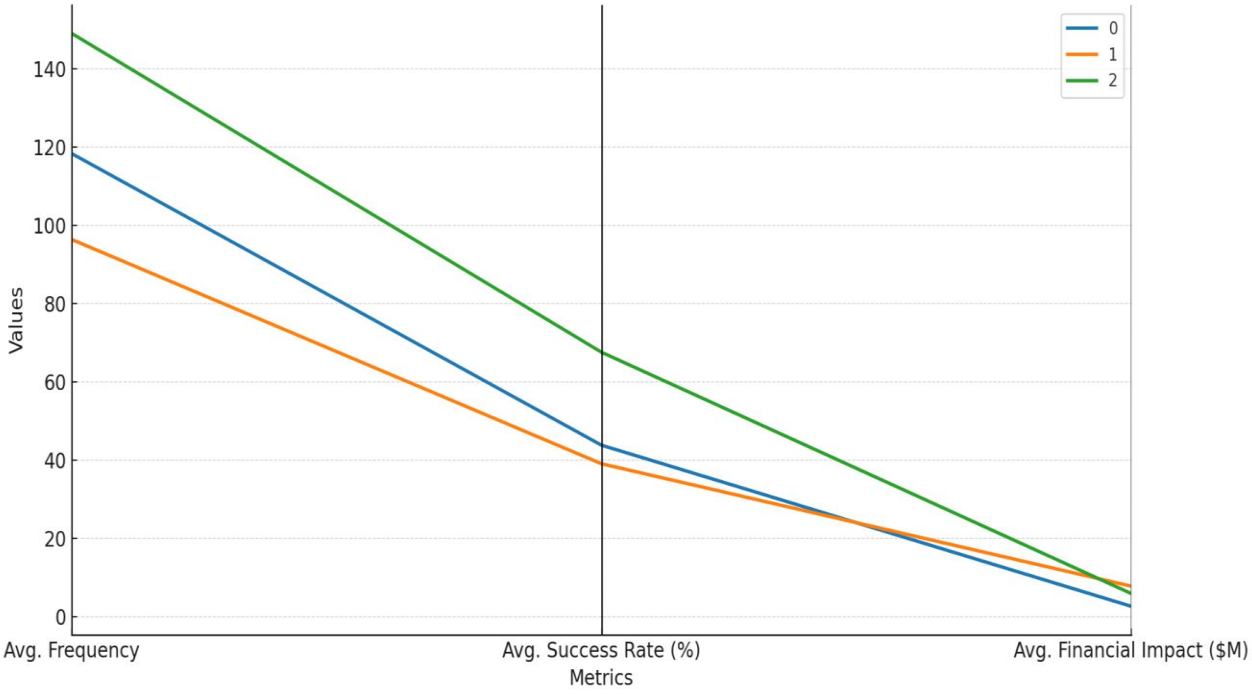

Figure 5: Parallel Coordinates Plot for Clusters

The findings highlight the dominance of malware and ransomware, which are characterized by high frequency and success rates, necessitating stronger technological safeguards.

Investigation of Challenges Impeding Compliance with Data Privacy Regulations

To examine the factors that influence compliance with data privacy regulations in the U.S. healthcare sector, a multivariate regression analysis was performed. During the analysis, the study identifies technical, organizational, human, and economic factors that impede effective adherence to these regulations.

Findings and Discussion

The regression analysis reveals the relationship between compliance levels and various predictors, as summarized in Table 3.

Variable	Coefficient	P-value
Constant	0.8387	0.0000
EHR Adoption Rate (%)	-0.0003	0.7757
Use of Encryption (%)	-0.0009	0.3805
Budget Allocation ($M)	-0.0289	0.0178
Staff Training Hours	0.0009	0.1232
Organizational Size ($B)	0.0015	0.8043
Revenue ($M)	0.0000	0.9424

Table 3: Compliance levels and various predictors values

The analysis highlights Budget Allocation ($M) as the only statistically significant predictor ($p = 0.0178$), suggesting that higher financial investments in cybersecurity are directly associated with better compliance.

Figure 6 presents the regression coefficients, showcasing the magnitude and direction of each variable's impact. Budget allocation exhibits the most pronounced influence, while other variables, such as EHR adoption rate and encryption usage, display minimal effects.

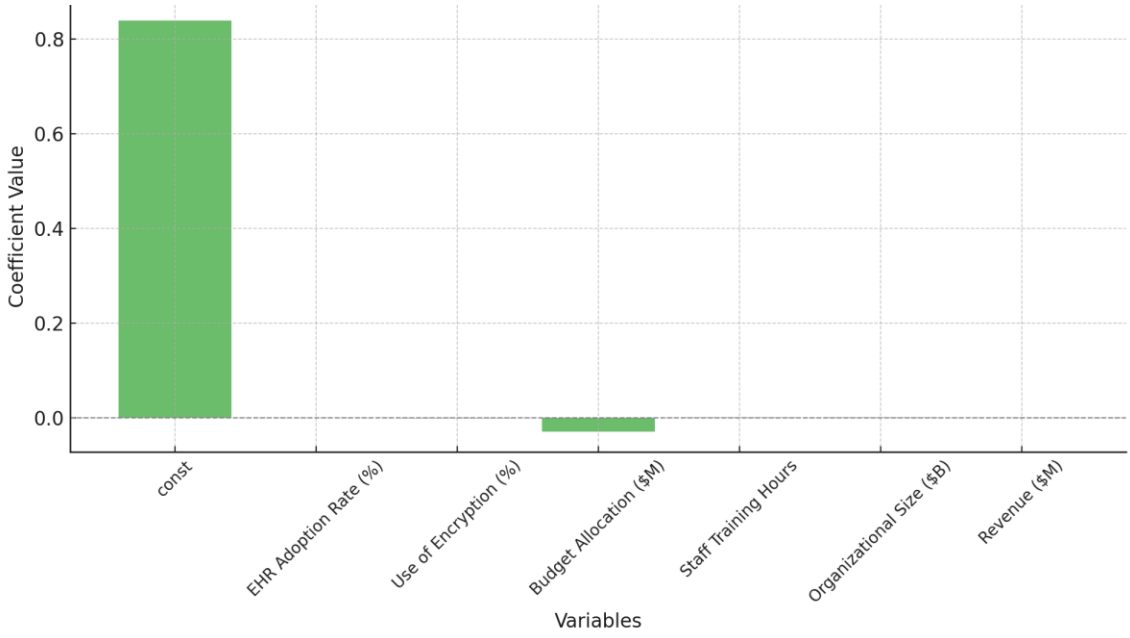

Figure 6: Regression Coefficients for Compliance Challenges

Statistical Significance of Predictors

The statistical significance of each variable is further analyzed in Figure 7, where variables are plotted against the p-value threshold of 0.05. Budget allocation is the sole significant predictor, reinforcing its critical role in driving compliance.

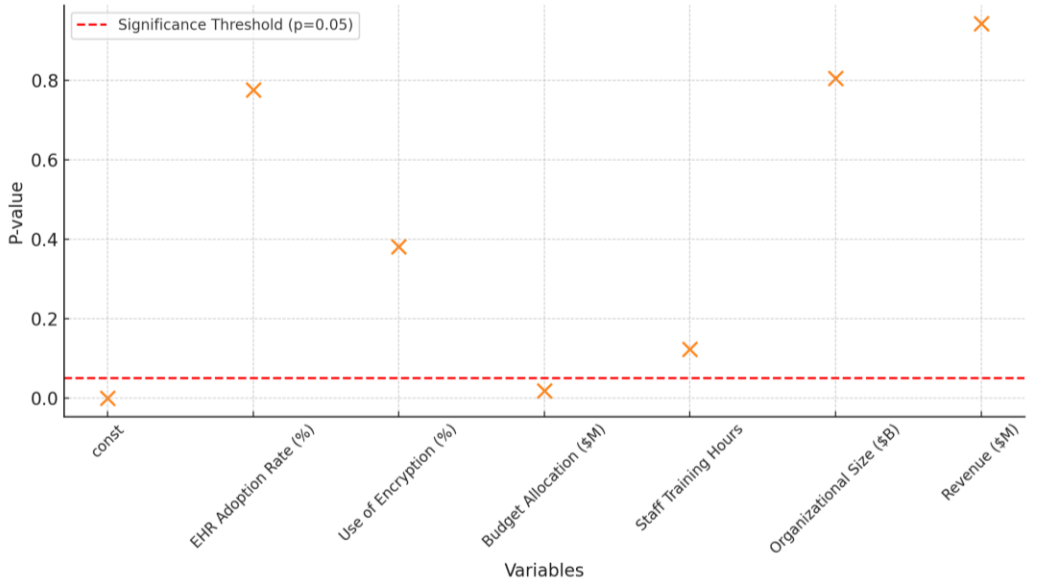

Figure 7: P-values of Regression Variables

Comparison of Predictors

Figure 8 uses a horizontal bar chart to emphasize the statistical significance of the variables. Variables with p-values below 0.05 are marked distinctly, highlighting the pivotal role of financial investments in compliance outcomes.

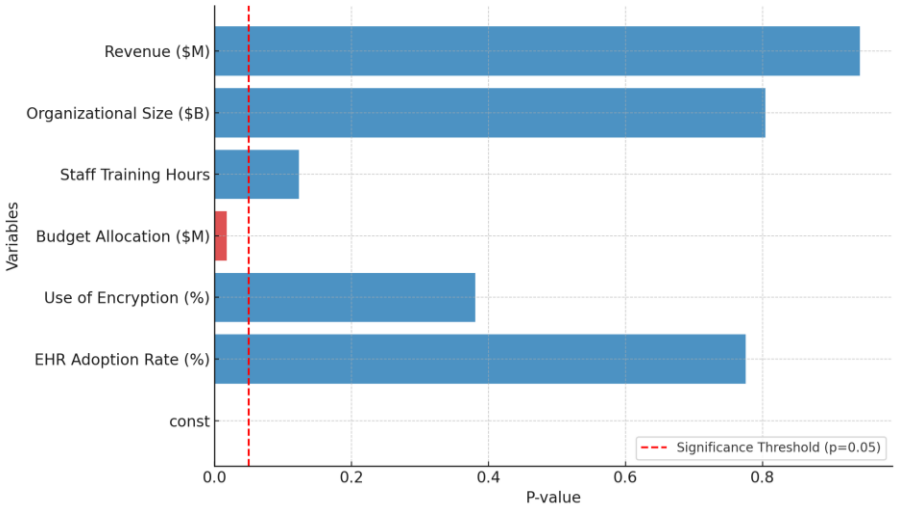

Figure 8: P-value Analysis of Regression Variables

The findings indicate that budget allocation is the most impactful factor influencing compliance. This result emphasizes the need for healthcare organizations to prioritize cybersecurity funding.

Discussion

The findings of this study underscore critical insights into the current state of cybersecurity in the U.S. healthcare sector, revealing both persistent vulnerabilities and the multifaceted challenges to compliance with data privacy regulations. Evaluating data privacy regulations, including HIPAA and HITECH, alongside cybersecurity frameworks such as the NIST Cybersecurity Framework, highlights a limited impact in curbing the frequency and severity of breaches. Despite regulatory efforts, the consistent trends in total breaches observed in Figure 1 suggest that existing safeguards have not sufficiently addressed the evolving nature of threats. This aligns with the literature indicating that the healthcare sector's unique vulnerabilities, such as legacy systems and resource constraints, continue to outpace the protective measures enforced by current frameworks (Bala et al., 2024; Abohatem et al., 2023).

The analysis of breach types further emphasizes the dominance of hacking and IT incidents, which constituted the majority of breaches across all years. Figure 2 and Table 1 reveal the recurring nature of these threats, with hacking incidents peaking at 84.4% in 2020. These findings resonate with prior studies suggesting the increasing sophistication of cyberattacks targeting healthcare organizations, particularly through ransomware and phishing schemes (Neprash et al., 2022; Joeaneke et al., 2024). Unauthorized access breaches, which spiked at 40% in 2022, highlight ongoing gaps in organizational policies, including access controls and staff training. These patterns reflect a need for enhanced technical safeguards and organizational strategies, as John-Otumu et al. (2024) and Kolade et al. (2024) emphasized.

The financial penalties associated with breaches, as illustrated in Figure 3, reinforce the economic risks of non-compliance. The variability in penalties, ranging from $529,000 in 2020 to $863,000 in 2023, suggests inconsistencies in enforcement or compliance levels across organizations. This observation aligns with reports of systemic struggles among healthcare providers, with only 38% reportedly meeting all HIPAA Security Rule requirements (Bureau, 2021). While financial penalties effectively highlight accountability,

their deterrence value remains questionable, given the persistence of breaches and the limited resources available to smaller providers (Adegbite et al., 2023).

The categorization of cybersecurity threats through cluster analysis provides further depth into understanding the scope of vulnerabilities. Table 2 and Figure 4 illustrate distinct clusters of threats, with Cluster 2 emerging as the most severe due to its high frequency, success rates, and financial impact. The dominance of malware within this cluster corroborates findings by Affia et al. (2023), who emphasized the rising risks of interconnected medical devices and cloud systems. Cluster 1, characterized by lower frequency but disproportionately high financial impact, underscores the costly nature of insider threats, as reflected in earlier studies highlighting the challenges of mitigating human error and malicious insider activities (Al-Mhiqani et al., 2024; Sarker et al., 2024). The balanced attributes of Cluster 0 signify widespread yet manageable risks, emphasizing the need for proactive, tailored strategies to address each category effectively.

The regression analysis examining compliance challenges reinforces the pivotal role of financial investments in achieving regulatory adherence. Budget allocation emerged as the only statistically significant predictor of compliance levels, as shown in Table 3 and Figures 6 to 8. This finding is consistent with earlier reports emphasizing resource limitations as a critical barrier to implementing robust cybersecurity measures (Olaniyi et al., 2024; Abdul et al., 2024). Despite the emphasis on technical safeguards such as encryption and EHR adoption, their lack of statistical significance highlights the need for a more holistic and integrated approach that balances technical, organizational, and human factors. These results underscore the urgency for healthcare organizations to prioritize funding and strategic planning, ensuring the alignment of resource allocation with emerging threats and compliance demands.

The findings provide a unique understanding of the interplay between regulatory efforts, organizational capacities, and the evolving nature of cybersecurity threats. The persistent challenges observed, including the dominance of advanced threat vectors like malware and the economic strain of breaches, align with the broader literature emphasizing the healthcare sector's struggle to balance innovation with security (Benmalek, 2024; Rodrigues et al., 2024). Addressing these challenges requires a concerted effort among stakeholders to enhance compliance frameworks, invest in advanced technological tools, and foster a culture of security awareness across all levels of the organization.

5. Conclusion and Recommendation

This study highlights the critical need for enhanced cybersecurity measures and robust compliance frameworks in the U.S. healthcare sector. Persistent vulnerabilities, including the dominance of hacking incidents, access control gaps, and the financial burden of insider threats, demonstrate the limited impact of existing frameworks like HIPAA and HITECH. The findings further emphasize the pivotal role of financial investment, with budget allocation identified as the most significant predictor of compliance. Addressing these challenges requires a unified effort among stakeholders to strengthen safeguards, streamline compliance, and promote proactive risk management. To achieve these goals, the following concise recommendations are proposed:

1. Allocate sufficient budgets for advanced cybersecurity tools, including AI-driven threat detection and encrypted data transmission, to improve real-time monitoring and mitigate breaches.
2. Implement continuous staff training on phishing detection, secure data handling, and adherence to security protocols to reduce human error and enhance organizational resilience.
3. Harmonize federal and state cybersecurity regulations to simplify compliance and ensure a unified national framework tailored to technological advancements.
4. Conduct regular risk assessments and adopt a Cybersecurity Maturity Model (CMM) to improve security postures and prioritize critical vulnerabilities systematically.
5. Future studies should focus on integrating emerging technologies like artificial intelligence, zero-trust architectures, and adaptive risk management frameworks to enhance cybersecurity strategies and address compliance challenges. These technologies hold the potential for improving threat detection, streamlining compliance processes, and mitigating the financial and operational impacts of breaches. Additionally, exploring sector-specific applications of machine learning and the role of predictive analytics in compliance forecasting could provide further advancements in healthcare cybersecurity.

Disclaimer (Artificial intelligence)

Author(s) hereby declare that NO generative AI technologies such as Large Language Models (ChatGPT, COPILOT, etc.) and text-to-image generators have been used during the writing or editing of this manuscript.

References

Adigwe, C. S., Olaniyi, O. O., Olabanji, S. O., Okunleye, O. J., Mayeke, N. R., & Ajayi, S. A. (2024). Forecasting the Future: The Interplay of Artificial Intelligence, Innovation, and Competitiveness and its Effect on the Global Economy. *Asian Journal of Economics, Business and Accounting*, *24*(4), 126–146. https://doi.org/10.9734/ajeba/2024/v24i41269

Alao, A. I., Adebiyi, O. O., & Olaniyi, O. O. (2024). The Interconnectedness of Earnings Management, Corporate Governance Failures, and Global Economic Stability: A Critical Examination of the Impact of Earnings Manipulation on Financial Crises and Investor Trust in Global Markets. *Asian Journal of Economics Business and Accounting*, *24*(11), 47–73. https://doi.org/10.9734/ajeba/2024/v24i111542

Arigbabu, A. T., Olaniyi, O. O., Adigwe, C. S., Adebiyi, O. O., & Ajayi, S. A. (2024). Data Governance in AI - Enabled Healthcare Systems: A Case of the Project Nightingale. *Asian Journal of Research in Computer Science*, *17*(5), 85–107. https://doi.org/10.9734/ajrcos/2024/v17i5441

Azubuike, C. F. (2023). Cyber Security and International Conflicts: An Analysis of State-Sponsored Cyber Attacks. *Nnamdi Azikiwe Journal of Political Science*, *8*(3), 101–114. https://najops.org.ng/index.php/najops/article/view/70

Baram, G. (2024). Cyber Diplomacy through Official Public Attribution: Paving the Way for Global Norms. *International Studies Perspectives*. https://doi.org/10.1093/isp/ekae022

Bardin, J. S. (2024). Cyber Warfare. *Elsevier EBooks*, 1345–1380. https://doi.org/10.1016/b978-0-443-13223-0.00087-4

BBC News. (2014). Edward Snowden: Leaks that Exposed US Spy Programme. *BBC News*. https://www.bbc.com/news/world-us-canada-23123964

Bolsinger, D. I. (2023). Overt Action: Congressional oversight, private activism, and Afghan Covert Action policy in the Reagan administration. *Intelligence & National Security*, *39*(5), 1–17. https://doi.org/10.1080/02684527.2023.2287793

Brotherton-Bunch, E. (2018). *China's Cyber Espionage Continues, and There's a Big Cost - Alliance for American Manufacturing*. Alliance for American Manufacturing.

https://www.americanmanufacturing.org/blog/chinas-cyber-espionage-continues-and-theres-a-big-cost/

Burgess, M. (2017). *Hacking the hackers: everything you need to know about Shadow Brokers' attack on the NSA*. Wired. https://www.wired.com/story/nsa-hacking-tools-stolen-hackers/

Burt, S. K. (2023). President Obama and China: cyber diplomacy and strategy for a new era. *Journal of Cyber Policy*, *8*(1), 48–66. https://doi.org/10.1080/23738871.2023.2282688

Cheng, J., & Zeng, J. (2022). Shaping AI's Future? China in Global AI Governance. *Journal of Contemporary China*, *32*(143), 1–17. https://doi.org/10.1080/10670564.2022.2107391

CISA. (2024). *National Security Memorandum on Critical Infrastructure Security and Resilience | CISA*. Www.cisa.gov. https://www.cisa.gov/national-security-memorandum-critical-infrastructure-security-and-resilience

Clark, J. (2023). *U.S. Focuses on Deterrence as China Raises Stakes in Indo-Pacific*. U.S. Department of Defense. https://www.defense.gov/News/News-Stories/Article/Article/3566970/us-focuses-on-deterrence-as-china-raises-stakes-in-indo-pacific/

Coetzee, S., Ivánová, I., Mitasova, H., & Brovelli, M. (2020). Open Geospatial Software and Data: A Review of the Current State and A Perspective into the Future. *ISPRS International Journal of Geo-Information*, *9*(2), 90. https://doi.org/10.3390/ijgi9020090

Council on Foreign Relations. (2005). *Connect the Dots on State-Sponsored Cyber Incidents - Titan Rain*. Council on Foreign Relations. https://www.cfr.org/cyber-operations/titan-rain

Council on Foreign Relations. (2016). *The Top Five Cyber Policy Developments of 2015: United States-China Cyber Agreement*. Council on Foreign Relations. https://www.cfr.org/blog/top-five-cyber-policy-developments-2015-united-states-china-cyber-agreement

Davenport, S. W., & Rentsch, J. R. (2021). Managing conflict through team member schema accuracy: A fresh perspective on perspective taking. *Journal of Theoretical Social Psychology*. https://doi.org/10.1002/jts5.110

Drake, F. (2018). Risk Society and Anti-Politics in the Fracking Debate. *Social Sciences*, *7*(11), 222. https://doi.org/10.3390/socsci7110222

Egloff, F. J., & Smeets, M. (2021). Publicly attributing cyber attacks: a framework. *Journal of Strategic Studies*, *46*(3), 1–32. https://doi.org/10.1080/01402390.2021.1895117

Fabuyi, J. A., Oluwaseun Oladeji Olaniyi, O. O., Olateju, O. O., Aideyan, N. T., & Olaniyi, F. G. (2024). Deepfake Regulations and Their Impact on Content Creation in the Entertainment Industry. *Archives of Current Research International*, *24*(12), 52–74. https://doi.org/10.9734/acri/2024/v24i12997

Fenster, M. (2023). How Reputational Nondisclosure Agreements Fail (Or, In Praise of Breach). *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4332257

Finnemore, M., & Hollis, D. B. (2020). Beyond Naming and Shaming: Accusations and International Law in Cybersecurity. *European Journal of International Law*, *31*(3). https://doi.org/10.1093/ejil/chaa056

Fratini, S., Hine, E., Novelli, C., Roberts, H., & Floridi, L. (2024). Digital Sovereignty: A Descriptive Analysis and a Critical Evaluation of Existing Models. *Deleted Journal*, *3*(3). https://doi.org/10.1007/s44206-024-00146-7

Fruhlinger, J. (2020a). *Equifax data breach FAQ: What happened, who was affected, what was the impact?* CSO Online. https://www.csoonline.com/article/567833/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html

Fruhlinger, J. (2020b). *The OPM hack explained: Bad security practices meet China's Captain America*. CSO Online. https://www.csoonline.com/article/566509/the-opm-hack-explained-bad-security-practices-meet-chinas-captain-america.html

Gale, M., Bongiovanni, I., & Slapnicar, S. (2022). Governing cybersecurity from the boardroom: Challenges, drivers, and ways ahead. *Computers & Security*, *121*(1), 102840. https://doi.org/10.1016/j.cose.2022.102840

Gbadebo, M. O., Salako, A. O., Selesi-Aina, O., Ogungbemi, O. S., Olateju, O. O., & Olaniyi, O. O. (2024). Augmenting Data Privacy Protocols and Enacting Regulatory Frameworks for Cryptocurrencies via Advanced Blockchain Methodologies and Artificial Intelligence. *Journal of Engineering Research and Reports*, *26*(11), 7–27. https://doi.org/10.9734/jerr/2024/v26i111311

Hanlon, R. J., & Christie, K. (2023). *Building a Human Security Diplomacy*. SpringerLink. https://doi.org/10.1007/978-3-031-48266-3

Hansel, M., & Silomon, J. (2024). Ransomware as a threat to peace and security: understanding and avoiding political worst-case scenarios. *Journal of Cyber Policy*, 1–20. https://doi.org/10.1080/23738871.2024.2357092

Harold, S. W. (2016). *The U.S.-China Cyber Agreement: A Good First Step*. Rand.org; The Cipher Brief. https://www.rand.org/pubs/commentary/2016/08/the-us-china-cyber-agreement-a-good-first-step.html

Huang, H. (2024). "Digital Diplomacy" in Cyberspace Governance. *Modern China and International Economic Law*, 269–310. https://doi.org/10.1007/978-981-97-1968-6_8

Hunter, L. Y., Albert, C. D., Rutland, J., Topping, K., & Hennigan, C. (2024). Artificial intelligence and information warfare in major power states: how the US, China, and Russia are using artificial intelligence in their information warfare and influence operations. *Defense & Security Analysis*, *40*(2), 1–35. https://doi.org/10.1080/14751798.2024.2321736

Jiang, M. (2023). Chinese Cybersecurity Policies in the Age of Cyber Sovereignty. *Philosophical Studies Series*, *154*, 77–90. https://doi.org/10.1007/978-3-031-41566-1_5

Jiangtao, S. (2019). *How China's surveillance state was a mirror to the US for Snowden*. South China Morning Post. https://www.scmp.com/news/china/diplomacy/article/3027598/us-whistleblower-edward-snowden-left-hong-kong-because

Joeaneke, P. C., Kolade, T. M., Val, O. O., Olisa, A. O., Joseph, S. A., & Olaniyi, O. O. (2024). Enhancing Security and Traceability in Aerospace Supply Chains through Block Chain Technology. *Journal of Engineering Research and Reports*, *26*(10), 114–135. https://doi.org/10.9734/jerr/2024/v26i101294

Joeaneke, P. C., Val, O. O., Olaniyi, O. O., Ogungbemi, O. S., Olisa, A. O., & Akinola, O. I. (2024). Protecting Autonomous UAVs from GPS Spoofing and Jamming: A Comparative Analysis of Detection and Mitigation Techniques. *Journal of Engineering Research and Reports*, *26*(10), 71–92. https://doi.org/10.9734/jerr/2024/v26i101291

John-Otumu, A. M., Ikerionwu, C., Olaniyi, O. O., Dokun, O., Eze, U. F., & Nwokonkwo, O. C. (2024). Advancing COVID-19 Prediction with Deep Learning Models: A Review. *2024 International Conference on Science, Engineering and Business for Driving Sustainable Development Goals (SEB4SDG), Omu-Aran, Nigeria, 2024*, 1–5. https://doi.org/10.1109/seb4sdg60871.2024.10630186

Joseph, S. A. (2024). Balancing Data Privacy and Compliance in Blockchain-Based Financial Systems. *Journal of Engineering Research and Reports*, *26*(9), 169–189. https://doi.org/10.9734/jerr/2024/v26i91271

Jung, Y. J. (2024). Cyber Shadows over Nuclear Peace: Understanding and Mitigating Digital Threats to Global Security. *Journal of Asian Security and International Affairs*, *11*(2), 233–253. https://doi.org/10.1177/23477970241250102

Karlén, N. (2020). Escalate to De-Escalate? External State Support and Governments' Willingness to Negotiate. *Studies in Conflict & Terrorism*, *46*(8), 1–22. https://doi.org/10.1080/1057610x.2020.1835002

Khalid Khan, S., Shiwakoti, N., & Stasinopoulos, P. (2022). A conceptual system dynamics model for cybersecurity assessment of connected and autonomous vehicles. *Accident Analysis & Prevention*, *165*, 106515. https://doi.org/10.1016/j.aap.2021.106515

Kolade, T. M., Aideyan, N. T., Oyekunle, S. M., Ogungbemi, O. S., & Olaniyi, O. O. (2024). Artificial Intelligence and Information Governance: Strengthening Global Security, through Compliance Frameworks, and Data Security. *Asian Journal of Research in Computer Science*, *17*(12), 36–57. https://doi.org/10.9734/ajrcos/2024/v17i12528

Lorci, E. (2024). Thucydides Trap Revisited. *Perspectives on Global Development and Technology*, *22*(3-4), 190–216. https://doi.org/10.1163/15691497-12341658

Malmio, I. (2023). Ethics as an enabler and a constraint – Narratives on technology development and artificial intelligence in military affairs through the case of Project Maven. *Technology in Society*, *72*, 102193. https://doi.org/10.1016/j.techsoc.2022.102193

Manantan, M. B. F. (2021). Advancing cyber diplomacy in the Asia Pacific: Japan and Australia. *Australian Journal of International Affairs*, *75*(4), 432–459. https://doi.org/10.1080/10357718.2021.1926423

Mokdad, M. (2024). The Rise of Soft Power in Modern Diplomacy. *Advances in Public Policy and Administration (APPA) Book Series*, 29–50. https://doi.org/10.4018/979-8-3693-6074-3.ch002

Molokomme, D. N., Onumanyi, A. J., & Abu-Mahfouz, A. M. (2022). Edge Intelligence in Smart Grids: A Survey on Architectures, Offloading Models, Cyber Security Measures, and Challenges. *Journal of Sensor and Actuator Networks*, *11*(3), 47. https://doi.org/10.3390/jsan11030047

Mori, S. (2019). US Technological Competition with China: The Military, Industrial and Digital Network Dimensions. *Asia-Pacific Review*, *26*(1), 77–120. https://doi.org/10.1080/13439006.2019.1622871

Nexon, D. H. (2009). The Balance of Power in the Balance. *World Politics*, *61*(2), 330–359. https://doi.org/10.1017/s0043887109000124

Obi, C., Akagha, V., Onimisi, S., Chigozie, A., Onwusinkwue, S., & Ibrahim, A. (2024). COMPREHENSIVE REVIEW ON CYBERSECURITY: MODERN THREATS AND ADVANCED DEFENSE STRATEGIES. *Computer Science & IT Research Journal*, *5*(2), 293–310. https://doi.org/10.51594/csitrj.v5i2.758

Okon, S. U., Olateju, O. O., Ogungbemi, O. S., Joseph, S. A., Olisa, A. O., & Olaniyi, O. O. (2024). Incorporating Privacy by Design Principles in the Modification of AI Systems in Preventing Breaches across Multiple Environments, Including Public Cloud, Private Cloud, and On-prem. *Journal of Engineering Research and Reports*, *26*(9), 136–158. https://doi.org/10.9734/jerr/2024/v26i91269

Olabanji, S. O., Marquis, Y. A., Adigwe, C. S., Abidemi, A. S., Oladoyinbo, T. O., & Olaniyi, O. O. (2024). AI-Driven Cloud Security: Examining the Impact of User Behavior Analysis on Threat Detection. *Asian Journal of Research in Computer Science*, *17*(3), 57–74. https://doi.org/10.9734/ajrcos/2024/v17i3424

Olabanji, S. O., Olaniyi, O. O., & Olagbaju, O. O. (2024). Leveraging Artificial Intelligence (AI) and Blockchain for Enhanced Tax Compliance and Revenue Generation in Public Finance. *Asian*

Journal of Economics, Business and Accounting, *24*(11), 577–587. https://doi.org/10.9734/ajeba/2024/v24i111577

Olabanji, S. O., Oluwaseun Oladeji Olaniyi, O. O., & Olaoye, O. O. (2024). Transforming Tax Compliance with Machine Learning: Reducing Fraud and Enhancing Revenue Collection. *Asian Journal of Economics Business and Accounting*, *24*(11), 503–513. https://doi.org/10.9734/ajeba/2024/v24i111572

Oladoyinbo, T. O., Olabanji, S. O., Olaniyi, O. O., Adebiyi, O. O., Okunleye, O. J., & Alao, A. I. (2024). Exploring the Challenges of Artificial Intelligence in Data Integrity and its Influence on Social Dynamics. *Asian Journal of Advanced Research and Reports*, *18*(2), 1–23. https://doi.org/10.9734/ajarr/2024/v18i2601

Olaniyi, O. O. (2024). Ballots and Padlocks: Building Digital Trust and Security in Democracy through Information Governance Strategies and Blockchain Technologies. *Asian Journal of Research in Computer Science*, *17*(5), 172–189. https://doi.org/10.9734/ajrcos/2024/v17i5447

Olaniyi, O. O., Olaoye, O. O., & Okunleye, O. J. (2023). Effects of Information Governance (IG) on Profitability in the Nigerian Banking Sector. *Asian Journal of Economics, Business and Accounting*, *23*(18), 22–35. https://doi.org/10.9734/ajeba/2023/v23i181055

Olaniyi, O. O., Omogoroye, O. O., Olaniyi, F. G., Alao, A. I., & Oladoyinbo, T. O. (2024). CyberFusion Protocols: Strategic Integration of Enterprise Risk Management, ISO 27001, and Mobile Forensics for Advanced Digital Security in the Modern Business Ecosystem. *Journal of Engineering Research and Reports*, *26*(6), 32. https://doi.org/10.9734/JERR/2024/v26i61160

Olateju, O. O., Okon, S. U., Igwenagu, U. T. I., Salami, A. A., Oladoyinbo, T. O., & Olaniyi, O. O. (2024). Combating the Challenges of False Positives in AI-Driven Anomaly Detection Systems and Enhancing Data Security in the Cloud. *Asian Journal of Research in Computer Science*, *17*(6), 264–292. https://doi.org/10.9734/ajrcos/2024/v17i6472

Olateju, O. O., Okon, S. U., Olaniyi, O. O., Samuel-Okon, A. D., & Asonze, C. U. (2024). Exploring the Concept of Explainable AI and Developing Information Governance Standards for Enhancing Trust and Transparency in Handling Customer Data. *Journal of Engineering Research and Reports*, *26*(7), 244–268. https://doi.org/10.9734/jerr/2024/v26i71206

Patz, R. (2017). Leaking, leak prevention, and decoupling in public administrations: the case of the European Commission. *West European Politics*, *41*(4), 1049–1071. https://doi.org/10.1080/01402382.2017.1394103

Pollak, C. (2021). Legitimation and Textual Evidence: How the Snowden Leaks Reshaped the ACLU's Online Writing About NSA Surveillance. *Written Communication*, *38*(3), 074108832110078. https://doi.org/10.1177/07410883211007870

Qian, X. (2024). Redefining International Law Paradigms: Charting Cybersecurity, Trade, and Investment Trajectories within Global Legal Boundaries. *The Journal of World Investment & Trade*, *25*(3), 295–333. https://doi.org/10.1163/22119000-12340327

Riordan, S. (2018). The Geopolitics of Cyberspace: a Diplomatic Perspective. *Brill Research Perspectives in Diplomacy and Foreign Policy*, *3*(3), 1–84. https://doi.org/10.1163/24056006-12340011

Salako, A. O., Fabuyi, J. A., Aideyan, N. T., Selesi-Aina, O., Dapo-Oyewole, D. L., & Olaniyi, O. O. (2024). Advancing Information Governance in AI-Driven Cloud Ecosystem: Strategies for Enhancing Data Security and Meeting Regulatory Compliance. *Asian Journal of Research in Computer Science*, *17*(12), 66–88. https://doi.org/10.9734/ajrcos/2024/v17i12530

Samuel-Okon, A. D., Akinola, O. I., Olaniyi, O. O., Olateju, O. O., & Ajayi, S. A. (2024). Assessing the Effectiveness of Network Security Tools in Mitigating the Impact of Deepfakes AI on Public Trust in Media. *Archives of Current Research International*, *24*(6), 355–375. https://doi.org/10.9734/acri/2024/v24i6794

Selesi-Aina, O., Obot, N. E., Olisa, A. O., Gbadebo, M. O., Olateju, O. O., & Olaniyi, O. O. (2024). The Future of Work: A Human-centric Approach to AI, Robotics, and Cloud Computing. *Journal of Engineering Research and Reports*, *26*(11), 62–87. https://doi.org/10.9734/jerr/2024/v26i111315

Shires, J. (2024). Civil society in cyberwarfare: hack-and-leaks, attribution and mobilization. *Edward Elgar Publishing EBooks*, 167–182. https://doi.org/10.4337/9781803924854.00018

Sukumar, A., Broeders, D., & Kello, M. (2024). The pervasive informality of the international cybersecurity regime: Geopolitics, non-state actors and diplomacy. *Contemporary Security Policy*, *45*(1), 7–44. https://doi.org/10.1080/13523260.2023.2296739

Teo, V. (2024). The United States' Neoconservative Turn: America First, Preserving U.S. Hegemony and the Containment of China. *SpringerLink*, 123–217. https://doi.org/10.1007/978-981-97-3733-8_3

Thumfart, J. (2024). The Construction of Digital Sovereignty in Struggles for Recognition. *SpringerLink*, 55–140. https://doi.org/10.1007/978-3-031-63426-0_3

Tucker, E. (2021, July 19). *Microsoft Exchange hack caused by China, US and allies say*. AP NEWS. https://apnews.com/article/microsoft-exchange-hack-biden-china-d533f5361cbc3374fdea58d3fb059f35

US Department of Justice. (2020). *Two Chinese Hackers Working with the Ministry of State Security Charged with Global Computer Intrusion Campaign Targeting Intellectual Property and Confidential Business Information, Including COVID-19 Research*. Www.justice.gov. https://www.justice.gov/opa/pr/two-chinese-hackers-working-ministry-state-security-charged-global-computer-intrusion

Usman, H., Showkat Ahmad, M., & Rehman, A. U. (2023). Beyond Conventional War: Cyber Attacks and the Interpretation of Article 2(4) of the UN Charter. *Global Legal Studies Review*, *VIII*(II), 16–26. https://doi.org/10.31703/glsr.2023(VIII-II).03

Val, O. O., Kolade, T. M., Gbadebo, M. O., Selesi-Aina, O., Olateju, O. O., & Olaniyi, O. O. (2024). Strengthening Cybersecurity Measures for the Defense of Critical Infrastructure in the United States. *Asian Journal of Research in Computer Science*, *17*(11), 25–45. https://doi.org/10.9734/ajrcos/2024/v17i11517

Val, O. O., Olaniyi, O. O., Selesi-Aina, O., Gbadebo, M. O., & Kolade, T. M. (2024). Machine Learning-enabled Smart Sensors for Real-time Industrial Monitoring: Revolutionizing Predictive Analytics and Decision-making in Diverse Sector. *Asian Journal of Research in Computer Science*, *17*(11), 92–113. https://doi.org/10.9734/ajrcos/2024/v17i11522

Vergun, D. (2020, September 17). *DOD Works to Increase Cybersecurity for U.S., Allies*. U.S. Department of Defense. https://www.defense.gov/News/News-Stories/Article/Article/2351916/dod-works-to-increase-cybersecurity-for-us-allies/

Wang, R., Zhang, C., & Lei, Y. (2024). Justifying a Privacy Guardian in Discourse and Behaviour: The People's Republic of China's Strategic Framing in Data Governance. *The International Spectator*, *59*(2), 58–76. https://doi.org/10.1080/03932729.2024.2315064

Yang, Z., & Li, L. (2021). Positioning Religion in International Relations: The Performative, Discursive, and Relational Dimension of Religious Soft Power. *Religions*, *12*(11), 940. https://doi.org/10.3390/rel12110940

Yun, H. (2024). China's Data Sovereignty and Security: Implications for Global Digital Borders and Governance. *Chinese Political Science Review*. https://doi.org/10.1007/s41111-024-00269-9

Yusif, S., & Hafeez-Baig, A. (2021). A Conceptual Model for Cybersecurity Governance. *Journal of Applied Security Research*, *16*(4), 1–24. https://doi.org/10.1080/19361610.2021.1918995

Zembylas, M. (2024). On the entanglement of epistemic violence and affective injustice in higher education: a conceptual analysis. *Higher Education*. https://doi.org/10.1007/s10734-024-01247-5