RESEARCH ARTICLE

Organizational Cybersecurity Resilience in Clinical Settings: A Qualitative Analysis of Digital Threat Patterns in U.S. Patient Information Systems

Raymond Mensah[1] (r.mensah@gmu.edu), Lucia Okafor[2], Edmond Vasquez[3]

[1]Department of Cyber Security Engineering, George Mason University, Fairfax, VA, USA
[2]Institute for Health Informatics, Howard University, Washington, DC, USA
[3]Department of Computer Science and Electrical Engineering, University of Maryland Baltimore County, Baltimore, MD, USA

Abstract

Healthcare organizations in the United States now defend patient records, networked medical devices, and shared clinical platforms against a steady stream of cyber threats. Even with greater spending on perimeter controls, breach notifications submitted to the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) have continued to rise. This article examines the organizational and human factors that weaken cybersecurity resilience in clinical environments in the mid-Atlantic region. Using a qualitative exploratory design based on secondary data, the researchers reviewed 762 breach notification records submitted to the OCR breach portal from January 2019 through December 2021. The sample was limited to incidents classified as hacking or information technology (IT) disruptions in the District of Columbia, Maryland, and Virginia. Interpretive thematic coding produced 68 initial codes, which were consolidated into 58 frequency-based categories and three main themes: (1) weak security governance and leadership accountability, (2) supply-chain and third-party data handling vulnerabilities, and (3) persistent gaps in workforce cybersecurity awareness. The analysis is interpreted through Routine Activity Theory, the Swiss Cheese Model of accident causation, and Deterrence Theory. The recommendations emphasize role-based access governance, continuing security education, and enforceable cybersecurity requirements for business associates. Overall, the study shows how organizational, behavioral, and structural weaknesses combine to create exploitable attack surfaces in clinical settings.

Keywords — Healthcare cybersecurity; data breach; organizational resilience; clinical information systems; human factors; thematic analysis

1 Introduction

The digitization of healthcare delivery has resulted in large volumes of sensitive patient data stored across electronic health record (EHR) platforms, cloud repositories, and interconnected medical devices. These technologies can improve clinical workflows and patient outcomes, but they also enlarge the attack surface available to malicious actors. Data breaches in U.S. healthcare settings have risen sharply over the past decade. Between 2009 and 2020, more than 3,700 breaches affecting 500 or more records each were reported to the HHS Office for Civil Rights, collectively exposing over 268 million individual records [1]. The financial and reputational consequences of such incidents are severe; remediation costs per breached record in healthcare remain the highest across all industries, and the downstream effects on patient trust, care continuity, and institutional reputation are difficult to quantify [2].

Yet in many healthcare organizations, cybersecurity is still treated as a technical support issue rather than a core governance responsibility. Perakslis [3] warned over a decade ago that the healthcare sector lagged behind other industries in adopting strong cybersecurity postures, and subsequent scholarship has documented persistent structural weaknesses [4, 5]. The COVID-19 pandemic further complicated this risk environment by accelerating telehealth adoption, remote workforce arrangements, and reliance on third-party cloud services, changes that scholars have associated with new opportunities for unauthorized access [6].

Healthcare organizations are legally obligated under the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act to safeguard protected health information (PHI). Violations can result in significant civil monetary penalties and corrective action plans imposed by the OCR. Yet the volume of reported breaches has climbed steadily. In 2020 alone, the HIPAA Journal documented 642 large-scale breaches, a 25 percent increase over the previous year, with hacking and IT incidents accounting for the majority of compromised records [1].

Prior research has thoroughly cataloged technical threat vectors, including ransomware, phishing, and distributed denial-of-service attacks [5,7]. However, a gap persists in understanding how organizational governance failures, including leadership deficits, inadequate policy enforcement, and weak vendor oversight, create the preconditions for these technical exploits to succeed [4]. Kamoun and Nicho [8] applied the Swiss Cheese Model to healthcare data breaches and concluded that most incidents result from the alignment of multiple organizational lapses rather than a single point of failure. Similarly, Nifakos et al. [9] found that human factors, ranging from insufficient training to poor password practices, remain the predominant enablers of successful attacks.

The research problem is therefore this: publicly available federal reporting data describe breach events in standardized categories but provide limited direct evidence about the organizational and human-factors conditions surrounding those events. This gap matters because policy and institutional reforms need evidence that

Submitted: February 6, 2023 Accepted: February 21, 2023 Published: March 15, 2023
www.pearlacademicpublishing.com

goes beyond technical vulnerability assessments and avoids unsupported claims about internal organizational causes.

This study focuses on the organizational side of cybersecurity in clinical environments. Instead of focusing solely on technical controls such as firewalls or intrusion detection systems, it examines the governance structures, workforce behaviors, and supply-chain relationships that determine whether a clinical organization can withstand, detect, and recover from cyber incidents. The investigation draws on publicly available breach notification data submitted to the OCR by covered entities and their business associates in the mid-Atlantic region of the United States. By analyzing these records through a qualitative thematic lens, the study identifies recurring organizational patterns that contribute to the occurrence and persistence of breaches.

This article makes three contributions. First, it presents a qualitative thematic analysis of 762 breach notification records from the OCR breach portal, offering an evidence-based account of how organizational factors precipitate data breaches in clinical settings. Second, it develops a multi-theory conceptual framework that integrates Routine Activity Theory, the Swiss Cheese Model, and Deterrence Theory to explain the interplay between human behavior, organizational structure, and threat actor motivation. Third, it offers actionable recommendations for healthcare administrators and information security officers seeking to strengthen cybersecurity resilience through governance reform, workforce training, and third-party risk management.

2 Literature Review

Healthcare is now among the sectors most frequently targeted by cyberattacks. Coventry and Branley [10] conducted a narrative review of cybersecurity trends in healthcare and identified four principal threat categories: ransomware campaigns targeting hospital networks, phishing attacks aimed at clinical staff, vulnerabilities in legacy medical devices, and insider threats from disgruntled or negligent employees. Their review stressed that, because modern clinical information systems are deeply interconnected, a breach in one subsystem can spread across the care delivery infrastructure.

Kruse et al. [5] performed a systematic review of 31 peer-reviewed articles published between 2006 and 2016, reporting that the most common breach vectors in healthcare were hacking, loss or theft of portable devices, and unauthorized access by internal actors. Their analysis found that smaller healthcare organizations, often operating without dedicated security teams, were disproportionately affected. Luna et al. [7] reached similar conclusions in an earlier systematic review, noting that healthcare entities frequently underestimate the sophistication of threat actors and overestimate the protective value of compliance-oriented security measures.

The OCR breach portal, colloquially known as the “Wall of Shame,” provides a publicly accessible database of all breaches involving 500 or more records reported under HIPAA. Ronquillo et al. [11] analyzed trends in this database from 2010 to 2017 and found that hacking incidents increased by more than 300 percent over the study period, while simultaneously accounting for an increasing share of total compromised records. Seh et al. [1] extended this line of inquiry through 2019 and confirmed that hacking and IT incidents had become the dominant breach category, surpassing theft, unauthorized access, and improper disposal.

Choi et al. [2] examined the downstream effects of reported breaches on hospital quality indicators, finding that hospitals that experienced data breaches subsequently exhibited declines in patient satisfaction scores and timeliness-of-care metrics. These findings indicate that breaches can impose costs beyond immediate penalties and remediation expenses.

Recent scholarship increasingly treats healthcare cybersecurity as an organizational problem, not only a technical one. Jalali and Kaiser [4] developed a systematic framework for understanding hospital cybersecurity from an organizational perspective, identifying leadership commitment, resource allocation, security culture, and inter-departmental coordination as critical determinants of security posture. They argued that hospitals with fragmented governance structures, where security responsibilities are distributed across IT, compliance, and clinical departments without clear accountability, are particularly vulnerable.

Nifakos et al. [9] conducted a systematic review of human factors in healthcare cybersecurity and found that the most frequently cited contributors to security incidents were inadequate training, poor password hygiene, susceptibility to social engineering, and lack of awareness regarding organizational security policies. Priestman et al. [12] specifically examined phishing in healthcare organizations and linked susceptibility to phishing to time pressure, multitasking demands, and a clinical culture that prioritizes information sharing over information guarding.

Williams and Woodward [13] provided a comprehensive analysis of cybersecurity vulnerabilities in networked medical devices, noting that many devices in active clinical use were designed before modern cybersecurity standards existed and cannot be easily patched or updated. The proliferation of Internet of Things (IoT) devices in clinical environments further compounds this risk. Argaw et al. [14] discussed the supply-chain dimension of hospital cybersecurity, noting that healthcare organizations routinely share patient data with dozens of business associates, including billing companies, laboratory services, cloud storage providers, and electronic health record vendors, each of which can be a potential point of compromise.

He et al. [6] documented a marked increase in healthcare-targeted cyberattacks during the COVID-19 pandemic. Hospitals operating at surge capacity diverted resources from IT security to clinical operations, remote

access configurations were deployed hastily, and telehealth platforms were adopted without thorough security vetting. The authors noted that threat actors exploited pandemic-related anxiety through COVID-themed phishing campaigns that achieved unusually high success rates among healthcare workers.

3 Study

The goal of the present study is to examine breach notification records from the U.S. Department of Health and Human Services Office for Civil Rights breach portal to identify organizational patterns associated with cybersecurity incidents in healthcare settings. Our analysis focuses on the administrative, workforce, vendor, and governance conditions reflected in the reported incidents. The central research question was the following. What organizational and human factors contribute most significantly to cybersecurity breach incidents in clinical healthcare settings in the mid-Atlantic United States? To this end, four supporting questions guided the analysis. What categories of breach incidents appear most frequently in the OCR breach portal data for the selected region and timeframe? What role do third-party business associates and supply-chain partners play in the occurrence of reported breach events? How do workforce-related factors, including training deficiencies and credential management practices, manifest in the reported breach data? What governance and leadership patterns are associated with organizations that experience repeated breach events?

3.1 Methodology

The conceptual framework combines three perspectives that help explain the organizational dynamics behind healthcare data breaches.

Routine Activity Theory (RAT), originally proposed by Cohen and Felson in 1979, posits that criminal events occur at the convergence of three elements: a motivated offender, a suitable target, and the absence of a capable guardian. In the healthcare cybersecurity context, the motivated offender is the threat actor (whether an external hacker or a malicious insider); the suitable target is the repository of electronic protected health information (ePHI), which carries high resale value on illicit markets; and the capable guardian is the combination of technical controls, governance structures, and trained personnel that can detect and prevent unauthorized access [10].

RAT is particularly useful for explaining why routine organizational behaviors, such as daily login patterns, data transfer practices, and remote access habits, can create predictable windows of vulnerability. The theory is used here as an interpretive framework rather than as evidence that any specific breach in the dataset resulted from a particular staffing pattern or operational decision [9].

Kamoun and Nicho [8] adapted Reason's Swiss Cheese Model of accident causation to the domain of healthcare data breaches. In this model, each layer of organizational defense, including policy, technology, training, and monitoring, is represented as a slice of cheese containing holes that represent weaknesses. A breach occurs when the holes in multiple layers align, allowing a threat to pass through all defenses. This perspective emphasizes that data breaches are rarely the result of a single catastrophic failure; rather, they emerge from the coincidental alignment of multiple, often minor, organizational lapses.

The Swiss Cheese Model is well-suited for analyzing the OCR breach portal data because it encourages the researcher to look beyond the proximate technical cause of a breach (e.g., a phishing email) and investigate the upstream organizational conditions that allowed the phishing email to reach the target, the training gaps that prevented the recipient from recognizing it, and the monitoring failures that delayed detection.

Deterrence Theory, rooted in criminological scholarship, holds that individuals are less likely to engage in prohibited behavior when they perceive a high probability of detection and severe consequences. In the organizational cybersecurity domain, deterrence operates along two axes: external deterrence, which concerns the penalties imposed by regulatory bodies such as the OCR, and internal deterrence, which encompasses the sanctions an organization imposes on employees who violate security policies [15].

Gordon et al. [16] argued that many healthcare organizations lack meaningful internal deterrence mechanisms; security policy violations frequently go undetected or are treated as minor infractions rather than serious governance failures. When employees perceive that non-compliance carries few consequences, the deterrent effect of formal policies diminishes, and risky behaviors, such as sharing login credentials or circumventing multifactor authentication, persist.

Taken together, the three theories help interpret the patterns observed in the OCR breach data. RAT explains the situational dynamics that create opportunities for attack; the Swiss Cheese Model explains how multiple organizational weaknesses converge to enable a breach; and Deterrence Theory explains why inadequate enforcement and oversight fail to prevent the risky behaviors that initiate the causal chain.

3.2 Procedures

The study used a qualitative exploratory design based on secondary data analysis. An exploratory approach was appropriate because the research questions concern organizational patterns that are difficult to capture through hypothesis-driven quantitative testing alone. The use of secondary data, specifically publicly available breach

notification records, was appropriate given the sensitivity of the subject matter and the impracticality of obtaining primary interview data from healthcare security professionals across a large geographic region within the study timeframe. The analysis was guided by an interpretivist stance. The aim was to identify meanings and patterns in breach notification records rather than test predetermined causal hypotheses.

The primary data source was the HHS Office for Civil Rights Breach Portal, a publicly accessible database maintained under the HIPAA Breach Notification Rule. This portal lists reported breaches of unsecured PHI affecting 500 or more individuals submitted by covered entities and their business associates. Each record in the portal contains standardized fields such as the name of the covered entity, state, type of covered entity, number of individuals affected, date of breach, type of breach, and location of breached information. The portal does not, by itself, identify root causes, internal governance structures, training completion rates, or the specific security controls in place at the affected organization.

The researchers downloaded the complete breach portal dataset in spreadsheet format and applied these inclusion criteria:

1. Geographic scope: Incidents occurring in the District of Columbia, Virginia, and Maryland (i.e., the mid-Atlantic / Washington metropolitan region).

2. Temporal scope: Incidents with reported breach dates between January 1, 2019, and December 31, 2021.

3. Breach type: Incidents classified as “Hacking/IT Incident” in the portal’s breach-type taxonomy.

After these filters were applied, the study dataset contained 762 unique breach notification records. This count refers to the authors’ filtered working dataset and should be reproducible from the archived data file used for analysis. The geographic restriction to the mid-Atlantic region had two purposes: first, the concentration of federal healthcare agencies and major health systems in this area provides a useful setting for analysis; second, limiting the geographic scope keeps the contextual interpretation more consistent, as organizations in the same regulatory and labor-market environment face broadly similar structural conditions.

All data used in the study are publicly available and contain no individually identifiable patient information. Because the analysis relied on public, de-identified government records, the study did not involve direct interaction with human participants. Any institutional review board (IRB) determination should be documented in accordance with the authors’ institutional requirements.

The analysis followed an interpretation-focused coding strategy adapted from established qualitative protocols. To avoid inferring facts not present in the source material, coding was limited to information contained in the breach portal or in linked public materials such as OCR enforcement documents and official organizational notices. It proceeded in five phases:

1. Data transcription and organization. The filtered dataset was organized in a structured spreadsheet, and supplementary contextual information (e.g., OCR settlement announcements, corrective action plans, and annual breach trend reports published by HHS) was compiled in a separate document to support triangulation.

2. Open coding. Each breach record was examined in conjunction with publicly available contextual information, and initial descriptive codes were assigned. Codes captured attributes such as the organizational setting (hospital, health plan, business associate), the breach vector (network server, email, portable device), and, where available, contributing factors identified in OCR resolution agreements.

3. Axial coding. Related initial codes were grouped into categories reflecting higher-order organizational patterns. During this phase, the researchers conducted constant comparison across categories to ensure internal consistency and to identify relationships among categories.

4. Thematic synthesis. Categories were consolidated into main themes that addressed the research questions. Each theme was evaluated against the theoretical framework to ensure analytical coherence.

5. Triangulation.s Findings derived from the breach portal data were cross-referenced with OCR annual reports, published enforcement actions, and peer-reviewed literature to enhance trustworthiness and reduce interpretive bias.

4 Results

The thematic coding produced 68 initial codes, which were consolidated through axial coding into 58 frequency-based categories. These categories were further synthesized into three main themes that address the central research question. Table 1 summarizes the three themes along with their frequency distributions and representative sub-categories. The frequencies refer to coded categories, not verified counts of root causes across all incidents.

Table 1: Summary of main themes, frequency counts, and representative sub-categories derived from thematic analysis of 762 breach notification records (OCR Breach Portal, 2019–2021, DC/MD/VA).

Theme	Frequency	Representative Sub-categories
Deficiencies in security governance and leadership accountability	31	Documented governance gaps; inconsistent policy enforcement where publicly reported; delayed detection or notification; fragmented incident-response planning
Supply-chain and third-party data handling vulnerabilities	18	Business associate involvement; vendor-managed systems; cloud or hosted-service exposure; third-party data handling noted in public records
Persistent gaps in workforce cybersecurity awareness	9	Email compromise; phishing-related indicators where publicly documented; credential-management concerns; workforce-facing security controls

4.1 Theme 1: Deficiencies in Security Governance and Leadership Accountability

The most common theme, appearing in 31 of the 58 frequency-based categories, involved governance and leadership accountability. The breach portal did not provide direct information about whether a given entity had a designated Chief Information Security Officer (CISO) or equivalent role. Accordingly, this theme was coded only when public source material pointed to governance-related issues such as delayed detection, prior corrective action, incomplete policy implementation, or incident-response weaknesses.

Some records were associated with entities or entity types that have appeared in OCR enforcement materials or corrective action discussions. Where such public materials were available, they were treated as contextual evidence rather than as proof that the same deficiency caused every related breach. This cautious interpretation fits the Swiss Cheese Model by treating repeated or overlapping weaknesses as possible layers of vulnerability rather than as verified single causes.

The governance theme also encompassed deficiencies in incident-response planning. Several records showed long intervals between breach dates and notification dates, a pattern that may indicate challenges in detection, investigation, or reporting. Jalali and Kaiser [4] have argued that delayed detection is a hallmark of organizations where security monitoring is treated as a peripheral function rather than a core operational capability.

4.2 Theme 2: Supply-Chain and Third-Party Data Handling Vulnerabilities

The second theme, represented by 18 frequency-based categories, concerned business associates, subcontractors, and technology vendors. Under HIPAA, covered entities are required to execute Business Associate Agreements (BAAs) with all third parties that create, receive, maintain, or transmit PHI on their behalf. In the dataset, some records identified a business associate as the reporting or involved entity, showing that third-party relationships are part of the breach landscape.

Common patterns within this theme included breach locations or public notices involving vendor-managed systems, cloud or hosted services, and third-party handling of electronic health information. These findings are consistent with those reported by Argaw et al. [14], who observed that the healthcare supply chain is a particularly vulnerable link because healthcare organizations often lack visibility into the security practices of their business associates.

The supply-chain theme also highlighted the challenge of maintaining security standards across organizational boundaries. Even when a covered entity maintains internal security controls, a breach at a business associate can expose patient data maintained or transmitted on the covered entity's behalf. This dynamic reflects the suitable-target element of Routine Activity Theory: the distributed nature of health information exchange means that patient data resides simultaneously in multiple locations with varying levels of guardianship.

4.3 Theme 3: Persistent Gaps in Workforce Cybersecurity Awareness

The third theme, represented by 9 frequency-based categories, concerned workforce-related factors. Although this theme had the lowest frequency count, it remains important because workforce behavior is often the immediate mechanism through which governance and supply-chain weaknesses become actual breaches.

The most common workforce-related pattern involved email compromise and public descriptions consistent with phishing or credential-related access. Priestman et al. [12] have documented that healthcare workers are particularly vulnerable to phishing because the clinical workflow demands rapid information exchange and creates a culture in which opening emails and clicking links is routine rather than suspect. The breach records

Table 2: Distribution of breach incidents by type of covered entity and breach location among 762 hacking/IT incident records (OCR Breach Portal, 2019–2021, DC/MD/VA).

Entity Type / Breach Location	**Count**	**Percentage**
By Type of Covered Entity		
Healthcare Provider	487	63.9%
Health Plan	138	18.1%
Business Associate	104	13.6%
Healthcare Clearinghouse	33	4.3%
By Breach Location		
Network Server	341	44.8%
Email	256	33.6%
Electronic Medical Record	89	11.7%
Other / Multiple	76	10.0%

analyzed in this study included incidents in which email was listed as the breach location, and some related public notices described compromised email accounts.

Credential management practices formed another important sub-category. Credential-management concerns were coded only when public materials specifically discussed shared credentials, weak passwords, or the absence or non-enforcement of multi-factor authentication. Nifakos et al. [9] identified poor credential management as one of the most persistent human-factor vulnerabilities in healthcare cybersecurity.

Table 2 shows the distribution of the 762 breach incidents by type of covered entity and by breach location. Healthcare providers accounted for nearly two-thirds of all incidents, which is consistent with national trends documented by Ronquillo et al. [11]. Network servers and email systems together constituted the breach location in more than 78 percent of cases, indicating that network infrastructure and electronic communication channels were the most commonly reported breach locations.

5 Discussion

The three themes connect to the conceptual framework in several ways. Routine Activity Theory explains how the daily operations of clinical organizations, including routine data exchanges, remote access sessions, and email communications, create predictable opportunities for motivated offenders. The absence of capable guardianship, whether through leadership inattention (Theme 1), unmonitored vendor access (Theme 2), or untrained staff (Theme 3), allows these opportunities to become breach events.

The Swiss Cheese Model helps explain why single-layer defenses are insufficient. Each theme represents a distinct defensive layer: governance policy, supply-chain management, and workforce behavior. When weaknesses in all three layers coincide, for example, when vendor oversight, phishing awareness, and incident-response planning are all weak, the conditions for a breach may become more favorable. The breach portal data alone do not prove such cascading failures, but public contextual materials support the use of this model as an interpretive lens.

Deterrence Theory helps explain why risky behaviors persist inside organizations. When security policy violations carry minimal internal consequences, and when regulatory enforcement is perceived as slow or unlikely, both employees and business associates have diminished incentive to comply with security requirements. Repeated breach reports by the same or similar entities may suggest limits in internal and external deterrence mechanisms, although the dataset does not by itself establish why recurrence occurred.

Figure 1 depicts how the three theories and three themes interrelate within the analytical framework.

The findings reinforce several conclusions from prior scholarship and add regional detail from the OCR records. The prominence of governance-related factors is consistent with Jalali and Kaiser's [4] argument that cybersecurity in hospitals must be understood as an organizational management challenge. The governance theme suggests that the problem is not merely a matter of technical capability but also of institutional priority-setting. The source material did not consistently disclose internal reporting structures, so the analysis does not claim that all breached organizations lacked dedicated security leadership.

The supply-chain findings echo concerns raised by Argaw et al. [14] and Williams and Woodward [13]. Healthcare organizations operate within a complex ecosystem of vendors, contractors, and affiliated entities. Each data-sharing relationship introduces potential points of compromise. The finding that business associates accounted for 13.6 percent of reported entity types in the dataset highlights the limits of relying on contractual BAA provisions without actively monitoring vendor security practices. The dataset does not establish the full extent of business associates' contributions to provider-reported breaches.

The workforce awareness theme, although it has the lowest frequency count, should not be treated as secondary. As Blanke and McGrady [15] observed, human error remains the most common proximate cause of data breaches, even when deeper organizational failures set the stage. The finding that email compromise and

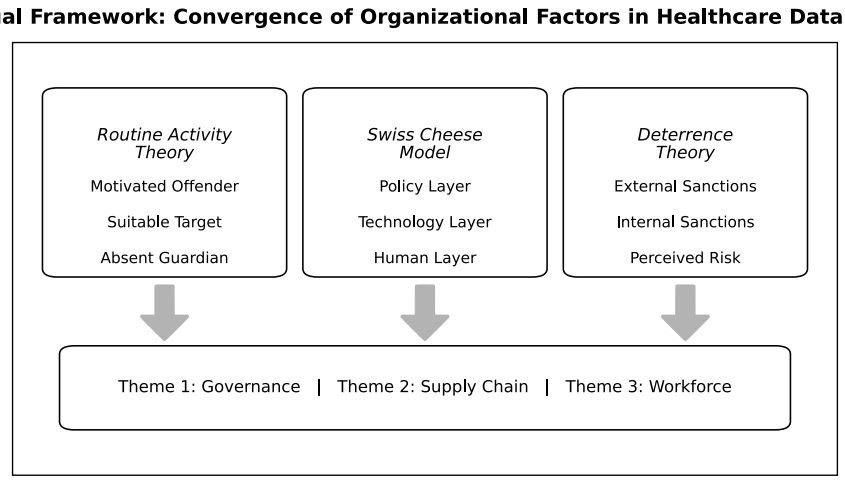

Figure 1: Conceptual framework illustrating the convergence of three theoretical perspectives and the three empirically derived themes. A breach event materializes when weaknesses across the governance, supply chain, and workforce layers align in the presence of a motivated offender and insufficient deterrence.

credential-related concerns appeared in the coded material is consistent with Priestman et al. [12] and Nifakos et al. [9], both of whom documented healthcare workers' exposure to social engineering risks.

The temporal dimension of the study period (2019–2021) is also important. The COVID-19 pandemic, which intensified beginning in early 2020, had a documented effect on healthcare cybersecurity. He et al. [6] reported that threat actors exploited pandemic-related disruptions through targeted phishing campaigns, ransomware attacks on overwhelmed hospitals, and exploitation of hastily deployed telehealth platforms. The breach data analyzed in this study are consistent with that broader context, but the study does not attribute individual incidents to the pandemic unless a public notice or enforcement document explicitly does so.

Several limitations qualify the findings. First, the OCR breach portal captures only breaches affecting 500 or more individuals; smaller breaches, which may exhibit different organizational patterns, are excluded from the dataset. Second, the portal provides limited contextual detail about each incident; the thematic analysis was therefore supplemented with publicly available enforcement actions and settlement documents, but these are available for only a subset of breaches. Third, the geographic restriction to the mid-Atlantic region, while enhancing contextual coherence, limits the generalizability of the findings to other U.S. regions or international healthcare systems. Fourth, the qualitative interpretive methodology, while well-suited to exploratory research, does not support causal inference; the identified themes represent co-occurring patterns rather than verified causal mechanisms. Finally, the study relies exclusively on secondary data; direct engagement with organizational stakeholders through interviews or surveys would provide richer contextual detail but was outside the scope of this study.

6 Conclusion

This study examined organizational and human factors associated with cybersecurity breach incidents in clinical healthcare settings across the mid-Atlantic United States. Through a qualitative thematic analysis of 762 breach notification records submitted to the HHS Office for Civil Rights between 2019 and 2021, the research identified three main themes: deficiencies in security governance and leadership accountability, supply chain and third-party data-handling vulnerabilities, and persistent gaps in workforce cybersecurity awareness. These findings were interpreted through a multi-theory framework integrating Routine Activity Theory, the Swiss Cheese Model, and Deterrence Theory, which collectively explain how organizational weaknesses, routine behaviors, and inadequate enforcement create the conditions for successful cyberattacks.

A practical implication is that healthcare organizations cannot build cybersecurity resilience through technical controls alone. Governance reforms, supply chain oversight, and continuing workforce education must work together to reduce the attack surface. The recommendations offered in this study, spanning leadership structure, access governance, vendor management, training design, incident-response preparedness, and internal enforcement, provide a coordinated framework for strengthening organizational cybersecurity postures in clinical environments without overstating what the breach portal alone can prove.

The rising frequency and severity of healthcare data breaches threaten patient privacy, clinical operations, and institutional trust. Addressing this threat requires healthcare leaders to treat cybersecurity as a strategic organizational responsibility, not simply a technical compliance obligation.

The exploratory findings point to several directions for future research. First, a quantitative analysis using regression or machine-learning classification models could be applied to a national-level OCR breach dataset

to identify organizational predictors of breach occurrence and severity. Second, primary qualitative research involving interviews with CISOs, compliance officers, and clinical staff at healthcare organizations that have experienced breaches would complement the secondary data analysis by providing insider perspectives on the governance and cultural dynamics that contribute to vulnerability. Third, comparative studies across different national healthcare systems, particularly those with different regulatory frameworks such as the European Union's General Data Protection Regulation (GDPR), could illuminate how policy design influences organizational security behavior. Finally, longitudinal studies tracking the same organizations over time would clarify whether post-breach corrective actions effectively prevent recurrence or whether structural vulnerabilities persist despite regulatory intervention.

Data Availability

All data used in this study are publicly available through the HHS Office for Civil Rights Breach Portal at https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.

References

[1] A. H. Seh, M. Zarour, M. Alenezi, *et al.*, "Healthcare data breaches: Insights and implications," *Healthcare*, vol. 8, no. 2, p. 133, 2020.

[2] S. J. Choi, M. E. Johnson, and C. U. Lehmann, "Data breach remediation efforts and their implications for hospital quality," *Health Services Research*, vol. 54, no. 5, pp. 971–980, 2019.

[3] E. D. Perakslis, "Cybersecurity in health care," *New England Journal of Medicine*, vol. 371, no. 5, pp. 395–397, 2014.

[4] M. S. Jalali and J. P. Kaiser, "Cybersecurity in hospitals: A systematic, organizational perspective," *Journal of Medical Internet Research*, vol. 20, no. 5, p. e10059, 2018.

[5] C. S. Kruse, B. Frederick, T. Jacobson, and D. K. Monticone, "Cybersecurity in healthcare: A systematic review of modern threats and trends," *Technology and Health Care*, vol. 25, no. 1, pp. 1–10, 2017.

[6] Y. He, A. Aliyu, M. Evans, and C. Luo, "Health care cybersecurity challenges and solutions under the climate of COVID-19," *Journal of Medical Internet Research*, vol. 23, no. 4, p. e21915, 2021.

[7] R. Luna, E. Rhine, M. Myhra, R. Sullivan, and C. S. Kruse, "Cyber threats to health information systems: A systematic review," *Technology and Health Care*, vol. 24, no. 1, pp. 1–9, 2016.

[8] F. Kamoun and M. Nicho, "Human and organizational factors of healthcare data breaches: The swiss cheese model of data breach causation," *International Journal of Healthcare Information Systems and Informatics*, vol. 9, no. 1, pp. 42–60, 2014.

[9] S. Nifakos, K. Chandramouli, C. K. Nikolaou, *et al.*, "Influence of human factors on cyber security within healthcare organisations: A systematic review," *Sensors*, vol. 21, no. 15, p. 5119, 2021.

[10] L. Coventry and D. Branley, "Cybersecurity in healthcare: A narrative review of trends, threats and ways forward," *Maturitas*, vol. 113, pp. 48–52, 2018.

[11] J. G. Ronquillo, J. E. Winterholler, K. Carey, *et al.*, "Health IT, hacking, and cybersecurity: national trends in data breaches of protected health information," *JAMIA Open*, vol. 1, no. 1, pp. 15–19, 2018.

[12] W. Priestman, T. Anstis, I. G. Sebire, S. Sridharan, and N. J. Sebire, "Phishing in healthcare organisations: threats, mitigation and approaches," *BMJ Health & Care Informatics*, vol. 26, no. 1, 2019.

[13] P. A. H. Williams and A. J. Woodward, "Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem," *Medical Devices: Evidence and Research*, vol. 8, pp. 305–316, 2015.

[14] S. T. Argaw, J. R. Troncoso-Pastoriza, D. Lacber, *et al.*, "Cybersecurity of hospitals: discussing the challenges and working towards mitigating the risks," *BMC Medical Informatics and Decision Making*, vol. 20, no. 1, p. 146, 2020.

[15] S. J. Blanke and E. McGrady, "When it comes to securing patient health information from breaches, your best medicine is a dose of prevention: A cybersecurity risk assessment approach," *Journal of Healthcare Risk Management*, vol. 36, no. 1, pp. 30–38, 2016.

[16] W. J. Gordon, A. Fairhall, and A. Landman, "Threats to information security — public health implications," *New England Journal of Medicine*, vol. 377, no. 8, pp. 707–709, 2017.