Scientia Moralitas International Journal of Multidisciplinary Research
ISSN 2472-5331 (Print) | ISSN 2472-5358 (Online) | Vol. 10, No. 2, 2025
DOI: 10.5281/zenodo.18041150

Data Breach Risk Management: Examining Impacts, Strategies, and Cultural Shifts

Samantha Thibodeau
Marymount University, Arlington, VA, USA
s0t82654@marymount.edu
https://orcid.org/0009-0000-4639-9166

ABSTRACT: Data breaches result in realized operational risks that threaten organizational health. Ollaw Health Systems (OHS), a pseudonym for a health system comprising two outpatient clinics and four hospitals, experienced multiple consecutive breaches that exposed Patient Health Information. The impacts left OHS struggling to mitigate the impact on employee morale, sustain operations during incidents, and maintain quality patient care. A narrative literature review was conducted to understand how organizations design enterprise risk management practices that foster a preventative, sustainable cybersecurity culture. The review suggests a bifocal approach, with leaders considering both short and long-term controls. The findings recommend that leaders consider short-term actions, such as managing reputational risk and providing personnel training, while focusing on long-term strategic activities, such as implementing risk registers to build a preventive culture and formalizing the ERM plan within the organization.

KEYWORDS: data breach, cybersecurity, enterprise risk management, risk identification

Introduction

For the 14th consecutive year, hospitals have experienced the most expensive data breaches resulting in average cost of $7.42 million per breach (Khalil, 2025). Personal Health Information (PHI) represents a valuable commodity that attracts malicious actors attempting to profit off the information (Priestman et al., 2019). Phishing, a subcategory of malicious cyberattacks, utilizes human factors to gain access to such PHI. Hospital's falling victim to data breaches face personnel, organizational, and stakeholder impacts that have long term impacts on their operational stability.

Repeat attacks plague hospitals as cybercriminals continually evolve their practices and target knowingly vulnerable systems (Dean, 2023). Robust prevention strategies require considerations, including change management models, problem-solving frameworks, and cultural models. Clinical leaders build disaster recovery processes to respond to data breaches. These efforts focus on short-term resolutions and plan for long-term preventative methods (Ramos, 2024). Frequent breaches require purposeful diagnosis, triaging, and strategic risk mitigation planning. Without such interventions hospital stability diminishes which threatens operations and hinders quality patient care. Repetitious data breaches pose a significant risk to all hospitals.

Situational Analysis

Ollaw Health Systems (OHS) represents an urban-based hospital that serves patients from diverse health backgrounds. The hospital has experienced three cybersecurity breaches within the last five years, exposing over 5,000 patient records. The information includes patient names, Social Security numbers, and prescription details. Frequent data breaches have impacted the hospital's reputation within the community, with many former patients wary of returning to a hospital that lacks proper cybersecurity risk management. Organizational leaders have attempted various mitigation plans, but have lacked a formal Enterprise Risk Management plan. Previous attempts to manage risk resulted in scattered information for clinicians, lacked formal training to establish a proper cybersecurity posture within the hospital, and resulted in susceptibility to phishing attacks. As a result, high turnover rates following breaches have led to a demoralized workforce that lacks stability. The mounting pressure to secure its data has left OHS with critical decisions that will directly impact the hospital's survival within the community.

Problem Statement

In July 2025, during a 31-day span, 37 healthcare providers were breached, affecting over 3.7 million patients and exposing their Patient Health Information (PHI) (Alder, 2025). Furthermore, in 2024, the Healthcare Information and Management Systems Society found that only 44% of clinicians and 48% of compliance professionals in hospitals had undergone proper tabletop exercises in the event of a breach (HIMSS, 2025). The generic problem is that hospitals continue to be plagued by cybersecurity attacks, exposing patient data and eroding trust in the healthcare system. The specific problem focuses on OHS's lack of proper risk management practices, which increases its susceptibility to cybersecurity attacks and threatens its operational health. To effectively pilot enterprise risk management plans, leaders must utilize ERM planning models and proper change management to build a team armed with secure practices.

Significance

The significance of the study lies in designing proper ERM practices that promote proper cybersecurity practices to safeguard patient data and reduce reputational risk from data exposure. The importance of ERM process design lies in designing a process that anticipates risk and designs mitigation strategies. Hospitals must stay vigilant in a technology-based era where hackers seek daily attacks to gain patient health information and sell it for profit (Pool et al., 2019). Healthcare organizations that prioritize risk identification, triaging, and mitigation plans find themselves proactive in cyber threats and better able to respond to changes (Choi & Johnson, 2021). The development of an ERM plan strengthens team-internal skills to make all individuals within the hospital able to identify risk. Furthermore, change management process significantly aids ERM plan adoption. Effective adherence to an ERM plan requires adoption (Sufi, 2023). Hospital leaders must understand how to drive adoption of risk management and educate the team on the importance of cybersecurity practices outlined in the ERM plan (Pool et al., 2019). The study's findings are applicable to hospitals looking to prevent cybersecurity breaches and educate their personnel on risk management.

Employee Impact

The breach at OHS had a significant impact on the employees. Specifically, the individual who feels victim to the phishing scam and the staff attempting to prevent future breaches found themselves disengaged. Low morale among employees leads to turnover and reduced motivation to improve processes. The resulting employee impact bolstered OHS's ability to create an Enterprise Risk Management (ERM) plan that focused on preventing data breaches.

Employee Morale

Hospitals that fall victim to data breaches experience psychological shame, which directly impacts employee morale. Individuals who expose data unintentionally face feelings of vulnerability, frustration, and diminished trust within their team (Al Kinoon, 2024). The insecurity in their own cyber threat detection skills can manifest into insecurities within their job (Pool et al., 2019). After the breach, hospitals must conduct a set of remediation processes that increase the workload on those who have fallen victim to the phishing scam (Al Kinoon, 2024). The combination of increased work and lack of confidence leads to low employee morale (Pool et al., 2019). OHS's third data breach resulted from a phishing scam that targeted a set of individuals who were previously victims. The vulnerable state of those individuals causes them to second-guess their instincts and fall for another cyberattack tactic. Overall, those who have fallen victim to the threats experience lowered employee morale, which manifests in susceptibility to future cyberattacks.

Lack of Preparedness and Demotivation

OHS faced multiple breaches within a five-year span, resulting in employees feeling ill-prepared for cyber threats and demotivated to report risks. Phishing exploits employee trust, causing individuals to inadvertently click on a link they believe to be valid (Priestman et al., 2019). When hospital employees have a false sense of security or become complacent in their day-to-day work, threats arise that make them vulnerable (Priestman et al., 2019). This results in employees who fall victim to a scam often feeling that organizations have failed to implement adequate protection measures to prevent recurrence (Al Kinoon, 2024). Ill-preparedness leads to a demotivated workforce that lacks empowerment to take action against cybersecurity threats (Al Kinoon, 2024). Thus, leading to a reactive cybersecurity culture that risks exposing PHI due to human error (Choi & Johnson, 2021). Overall, data breaches highlight the gaps in cybersecurity practices within hospitals which directly impacts the confidence and motivation within employees to stay vigilant.

Turnover

Hospitals experiencing data breaches often face higher turnover rates due to increased personnel workload and stress. After an incident has occurred, hospital personnel assume responsibility for implementing the risk management plan to secure data and personnel and attempt to restore trust with patients (Clement, 2023). The increase in responsibilities leads to stress, longer workdays, and unknown challenges in the face of crises, which contribute to burnout among employees (Clement, 2023). This additional stress directly results in high turnover rates. The cycling of new staff who lack training increases the hospital's susceptibility to additional attacks (Gordon et al., 2019). A cyclical pattern of breaches, followed by higher turnover and the hiring of inexperienced new employees, results in a culture that is ill-prepared to face cyberattacks (Clement, 2023; Gordon et al., 2019). OHS attackers targeted both seasoned staff with low morale and new staff with no training, which were effective tactics that led to the third data breach. Ultimately, personnel turnover and high stress reactions impact a hospital's ability to prevent subsequent data breaches.

Impacts on the Organization

Hospitals that incur a data breach, such as OHS, experience organizational impacts that affect their future success. After an incident occurs, hospitals must address a lack of community trust, face increased operating costs, and legal ramifications, all of which impact their organizational success. Hospitals that fail to address critical operational threats find themselves out of business due to funding concerns and loss of patient trust.

Business Continuity Impacts

Upon experiencing a data breach, a hospital may be forced to temporarily cease operations to restore its business functions. Any halt of functioning within the hospital can have drastic impacts on the organization's operational plan (Gordon et al. 2019). Scheduled procedures, treatment plans, and prescription orders may be halted during the incident period, which can directly impact the trust between patients and clinicians. In extreme cases, prolonged outages within hospitals increase the risk to patient safety and lead to overall system failure in critical hospital systems (Bozic, 2025). Many hospitals employ a disaster recovery plan designed to mitigate risks and ensure continuous operations in the event of a cyberattack (Raisel & Friga, 2013). A hospital's organizational resilience symbolizes the commitment to its community, which helps restore trust and minimize reputational damage (Pool et al., 2019). OHS could have benefited from more operational resilience as they were forced to halt operations after identifying the breach. This period significantly lowered their reputation within the clinical community and impacted patient care operations. Overall, business continuity has a significant impact on an organization's success following a data breach.

Lack of Community Trust

A data breach results in the exposure of Patient Health Information, which can lead to a lack of trust between the patient and the hospital. Data breaches result in the theft, exposure, or modification of data, all of which directly impact patient safety regarding diagnoses and treatment plans (Bozic, 2025). The loss of trust between patients and hospitals further diminishes with multiple breaches, as seen with OHS. Skepticism mounts when the community sees multiple cybersecurity incidents indicating a lack of preparedness within the hospital and its staff (Choi et al., 2019). Failure to initially protect patient health data erodes confidence in the hospital's ability to protect future data (Bozic, 2025; Choi et al., 2019). Data breaches compromise patient health information and the quality of care, raising concerns about trust within the patient community.

Increased Cost for Operations

Data breaches from phishing attacks, such as the one that occurred at OHS, leave lasting operational cost impacts. Post-incident hospital leaders spend significant funds to investigate the breach, conduct necessary remediation that requires immediate action, and provide patient protection services (Mesiner, 2017). Hospital leaders must also invest in preventive measures, such as comprehensive training related to data protection and additional security measures, including software and personnel (Bozic, 2025). The fallout from the data breach results in increased operational costs associated with implementing a cyber defense strategy (Meisner, 2017). This can directly impact resourcing requirements for implementing new practices, requiring individuals to work longer hours and assume additional responsibilities within their roles (Bozic, 2025). The operational costs are investments in reestablishing trust and secure practices to build back trust within the community (Herisasono, 2024). With any major breach, companies must dedicate additional funds to remediation efforts to improve practices on a heightened timeframe (Herisasono, 2024). Lasting operational cost impacts remain a pivotal concern when hospitals experience data breaches, which can undermine trust but also cause operational stress.

Liability Impacts

Hospitals face significant liability concerns when a data breach occurs. The exposure of sensitive Patient Health Information poses legal ramifications (Seh et al., 2020). Legal action, such as class action lawsuits, penalties, and fines associated with regulatory violations, can amount to significant fees owed to individuals impacted by the breach or the U.S. government (Seh et al., 2020). Moreover, specifically for healthcare-related organizations, HIPAA outlines legal obligations to protect patient data by following a set of standards (Choi & Johnson, 2019).OHS did not follow all of HIPAA's data privacy standards, resulting in negligence and fines. The increased distrust within the community led to a class action lawsuit, in which former patients sued for damages incurred due to the exposure of their PHI. The culmination of various liabilities imposes threats to a hospital's operations and financial stability (Meisner, 2017). Such legal suits can financially bankrupt a clinical system, impact operational stability, and impact reputation (Sharm et al., 2020). Reputational damage stemming from legalities further complicates recovery efforts, as hospitals struggle to reassure patients about the quality of their care and the protection of their data (Sharma et al., 2020). Ultimately, hospitals impacted by data breaches experience liability ramifications that last beyond the initial remediation period.

Impacts on Stakeholders

Resource Diversion

Hospitals experiencing a data breach often find resources diverted to risk mitigation planning, away from their standard duties. Leaders will shift personnel to focus on critical remediations to secure the remaining data and assess the organizational impact (Choi & Johnson, 2017). This will cause funding to shift away from patient improvement initiatives and towards cybersecurity (Choi & Johnson, 2017). The resulting monetary and resource diversion leads to clinical staff feeling overwhelmed in their duties and assuming additional responsibilities to maintain patient operations (Branch, 2018; Choi & Johnson, 2017). The shift in resourcing can also cause a slowdown in staff availability, halting forward-thinking initiatives aimed at maturing the hospital's operations (Branch, 2018). The shift from strategic operations to tactical actions hinders leaders' ability to plan for the future (Choi & Johnson, 2017). OHS experienced a similar pattern in which resources were routed away from an initiative to modernize treatment plan reporting and towards cybersecurity remediation. Stakeholder responsibilities that shift directly impact the trajectory of the hospital, resulting in deprioritized initiatives that could negatively affect patient care quality and safety (Moffit & Steffen, 2017). Hospital leaders must recognize the impacts of resource diversion on stakeholders, including clinical staff and patients.

Information Flow

Data breaches have a significant impact on the flow of patient information, affecting clinicians' ability to provide care and raising concerns about the current state of data privacy policies. Hospitals, such as OHS, experience data continuity concerns when breaches halt the update of patient health data. This can result in out-of-date patient histories, missing diagnoses, and incomplete clinical information (Branch, 2018). At the extreme, clinical staff can misdiagnose patients or establish irrelevant treatment plans based on outdated information (Choi & Johnson, 2017). The decreased accuracy of the information raises concerns among stakeholders regarding the trustworthiness of data integrity (Branch, 2018). Distortion of information has lasting impacts on clinicians' confidence in providing relevant care to patients (Branch, 2018; Choi & Johnson, 2017). Such feelings impact the stability of the staff and reduce stakeholders' willingness to use the data to inform their clinical decisions (Choi & Johnson, 2017). All of which can hinder a hospital's ability to adopt new cybersecurity practices due to a lack of belief in the system (Yeng et al., 2019; Choi & Johnson, 2017). Overall, data breaches undermine information flows, resulting in less confident diagnoses and care from clinical staff, which leads to resistance to process changes.

Problem-Solving Models Application

OHS faced a data breach that culminated in a substantial exposure of PHI. During the incident, leaders should employ problem-solving models to help understand and assess the impacts of the vulnerability. Lean Six Sigma and the NIST Incident Response Framework guide leaders into a problem-solving process. The streamlining of investigation, diagnosis, action, and review helps ensure the effectiveness of implemented controls.

Lean Six Sigma Process

A Lean Six Sigma process within a cybersecurity framework focuses on key steps to enhance secure practices and minimize operational waste. The process of define, measure, act, implement, and control allows leadership to foster continuous quality improvements, which strengthen cybersecurity practices (Afriyie, 2025). The OHS data breach could have benefited from a continuous improvement framework to help guide prevention efforts. and post-incident response. Iterative processes, such as DMAIC, offer clinical leaders the ability to reassess processes and measure the effectiveness of change, staying vigilant against cybersecurity threats (Afriyie, 2025). Clinical organizations that fail to mature their cybersecurity practices experience increased risk of attack (Farahbod et al., 2022). This can result in data breaches, inefficient risk management processes, and instability in cybersecurity posture (Alduaibi, 2023). Systemic framework implementations garnish a structured approach to ensuring organizational maturity of cyber practices (Farahbod et al., 2022). The use of DMAIC holds a significant role in improving a hospital's ability to remain vigilant against data breaches.

Lean Six Sigma also aids individuals during the post-incident response period. After a data breach occurs, hospitals must employ an incident response plan to assess the impact of the breach and restore hospital operations to normal function using the safest methods possible (Moffit & Steffen, 2017). The emergency post-breach period requires a structured process of assessment and improvement (Abrahams et al., 2024). DMAIC streamlines response activities, incorporates key lessons learned into controls, and measures the effectiveness of controls in mitigating risk (Farahbod et al., 2022). Utilizing a problem-solving framework centered around cyclical improvements helps a hospital evolve its practices in a measurable manner (Abrahams et al., 2024). Incorporating a continuous improvement framework fosters an iterative cybersecurity culture that evolves in tandem with the organization, bringing it one step closer to a proactive practice (Abrahams et al., 2024). Ultimately, utilizing a Lean Six Sigma approach enables clinical leaders to respond effectively to critical incidents and refine their processes based on lessons learned.

SWOT Problem-Solving Model

Strengths, weaknesses, opportunities, and threats analysis (SWOT) aids clinical leaders in the diagnosis of cybersecurity vulnerabilities related to storing digital PHI. The process promotes strategic evaluation of risks associated with digitizing health information. Daman (2016) identified threats such as data security breaches, privacy risks, unauthorized access, and malware, all of which can compromise a hospital's data hosting. Moreover, the weaknesses included data security operations and clinician apprehension to the adoption of the feature of data misuse. Prasuna and Rachh (2023) identified the strengths of current strategies that successfully protect healthcare data and opportunities to strengthen defenses. After the first breach, OHS struggled to identify the vulnerabilities plaguing its hospital. They lacked clear direction, which resulted in increased risk and subsequent security attacks. Employing a technique such as SWOT analysis would have helped identify vulnerabilities, prioritizing tangible threats, and guiding resource allocation to promote sustainable security operations (Prasuna & Rachh, 2023). Ultimately, clinical leaders should employ a SWOT analysis as a problem-solving method to strategically improve their security procedures and stay vigilant against data breaches.

Organizational Cultural Models

Hospital systems that have incurred data breaches must assess their cybersecurity culture. Organizational cultural models guide clinical leaders in understanding their current cybersecurity environment and making impactful improvements within their clinical system. Structured approaches, such as the competing values model and the cultural iceberg model, inform leaders of the next steps to take in improving security-based cultural practices.

Competing Values Model

The competing values model examines the organizational culture of a given topic using four key dimensions. The four quadrants of consideration include clan culture, focusing on cohesion; adhocracy, valuing innovation; market culture, favoring competitiveness; and hierarch, lending towards consistency (Triplett, 2021). The model enables organizations to balance strategic goals with environmental demands, creating an adaptable cybersecurity culture that can protect against cyberattacks and maintain the data privacy of PHI (Triplett, 2021). A phishing scheme led to a significant data breach, prompting OHS to reassess its cybersecurity culture. Applying the competing values model helps to understand the multifaceted dimensions of cybersecurity and supports the redefinition of culture within a hospital (Kam et al., 2020). However, each value has both significant benefits and drawbacks for cybersecurity practices within hospitals. Clan culture favors teamwork, but an overemphasis can lead to a lenient attitude towards security practices (Adamu et al., 2025). Conversely, adhocracy favors creativity and flexibility in cybersecurity practices but can make standardization and implementing controls difficult (Triplett, 2021). Market culture emphasizes competitiveness, which can prioritize quick security remediation without considering data-driven decisions (Adamu et al., 2025). Finally, the hierarchical culture values stability, which promotes a strict culture that hinders adaptive cybersecurity responses (Triplett, 2021). Applicable to OHS, the clinical leader's assessment of cultural norms could have presented a clear direction for iterations to their security practices. Overall, the model helps determine how flexible or strict an organizational culture remains towards cybersecurity and allows clinical leaders to shift cultures towards a strategic alignment.

Cultural Iceberg Model

The cultural iceberg model explains the complexity of cybersecurity practices within an organization. The model highlights that only a tip of information can be seen, but complexities beneath the surface continue to impact culture (Bisogni et al., 2016). The process consists of key steps, including understanding the levels of culture that impact the current cybersecurity strategy, the cultural substructures that determine knowledge creation and sharing, implementing centralized learning activities, and promoting a continuous culture of support regarding cybersecurity vigilance (Haider, 2009). OHS should have considered a cultural model to identify the staff's immediate understanding of phishing prevention and deepen cybersecurity knowledge within the hospital. By using the culture iceberg model, clinical leaders can expose hidden knowledge and reveal more surface-level knowledge to their clinicians (Haider, 2009). The findings from the initial cultural evaluation would have identified areas for improvement, enabling clinical leaders to implement targeted training to protect PHI (Holloway, 2025). The creation of cultural knowledge, norms, and workflows regarding data protection and phishing prevention can equip clinicians with the proper tools to prevent future breaches (Haider, 2009; Holloway, 2025). The cultural iceberg model can help clinicians establish a systemic and holistic approach to improving the cybersecurity culture within OHS.

Change Management Theory Application

Bridges' Transition Change Management Model

Bridges' Transition Change Management Model directly applies to the case study at OHS, highlighting the need for a systematic approach to measuring cultural shifts. The model focuses on the psychological and emotional resistance individuals encounter regarding work habits, consisting of three steps: ending, the neutral zone, and a new beginning (Heckelmen, 2017). Each step simulates the broader emotional complexities that change imparts on individuals (Bridges, 2009). OHS experienced an increase in cyber risk associated with high turnover and persistence of unfavorable security practices. Several breaches left an emotional impact on the hospital staff, leaving them with feelings of self-doubt, fear, and confusion regarding behavioral changes. The psychological and emotional impact on individuals within the hospital justifies the application of this transition change model (Mbarek, 2024). The use of a systemic approach ensures that leaders reduce resistance to change, promoting sustainable, adoptable practices that persist across the workforce (Mbarek, 2024). During each step, employees are psychologically prepared, emotionally supported, and engaged throughout the process (Bridges & Mitchell, 2000). These considerations reduce defensive resistance, promote the creation of collaborative processes, and foster empathy during process change. The human-centric process ensures that changes are sustained and prevent reversion to outdated cybersecurity practices (Heckelmen, 2017).

Bridges' transition Model begins with "endings". The concept regards letting go of old behaviors, practices, identities, and the current understanding of the organizational culture (Bridges & Mitchell, 2000). Employees often tie their work roles to their identities, which makes the ending phase of their careers difficult (Bridges & Mitchell, 2000). OHS attempted numerous times to improve cybersecurity practices, requiring all clinical staff to shift daily work routines to incorporate enhanced security practices. However, leaders continually found employee resistance. The deep tie of the clinical staff to their role within the hospital left individuals feeling that it was not their responsibility to uphold security (Yeng et al., 2019). Staff resisted relinquishing familiar practices which bred resistance (Bridges & Mitchell, 2000). Instead, Bridges and Mitchell (2000) define the ending as a recognition of past practices, a basis for new practices, and a collaborative effort between leaders and staff to implement the change. The ending phase fundamentally reduces defenses around tying worth of the individual to the role, within the workplace, which establishes the psychological and emotional opportunity for the next phase: the neutral zone.

The neutral zone represents the period of reorganization. Neutrality dictates the release of old ways and the repatterning of behaviors, practices, and processes within the organization (Miller, 2017). Psychologically, during this phase, individuals face uncertainty, leaving them feeling apprehensive about the future direction of the culture. OHS would benefit from the neutral zone by supporting its clinical staff during times of necessary change. Cultural resistance may increase during this period due to a lack of clear direction, apprehension about developing new skills, and fear of uncertainty (Mbarek, 2024; Miller, 2017). OHS clinical leaders play a critical role during this phase, supporting their staff, communicating transparency about additional changes, and engaging employees in helping redefine their working roles in the face of changing cultural practices (Miller, 2017). Framing this phase as an opportunity to explore and embrace changes remains critical to prevent employees from reverting to old behaviors (Mbarek, 2024). The ability to effectively drive a neutral zone focuses on designing, learning, and embracing new changes, which allows the hospital to transition to the final phase.

The final phase of the model, the new beginning, represents employees settling into their new operational reality. Individuals should feel established in their new roles, develop new routines, and embrace the organizational cultural shifts (Sharma, 2025). The significance of the final phase lies in reaching stability that benefits an individual's sense of confidence in their role and ability to deliver (Sharma, 2025). OHS could directly benefit from a sense of ownership within the clinical staff regarding cybersecurity practices. Those who feel directly tied to the process change will persist in habits that uphold the systems they help build (Bridges & Mitchell, 2000). Clinical staff will develop an emotional connection to the culture, which creates a cyclical pattern of supporting leadership in iterations that continue to improve the cybersecurity culture within a hospital (Yeng et al., 2019). Leadership also plays a critical role in establishing the emotional connection necessary to sustain adoption by recognizing positive outcomes from employees, further reinforcing employees' direct impact on the culture (Mbarek, 2024). A strong psychological connection to cultural change strengthens adoption, promotes long-term behavioral improvements, and reduces the risk of reversion (Sharma, 2025). Overall, the Bridges Transition Model focuses on the necessary emotional considerations within staff and leadership to introduce sustainable cultural shifts.

Nudge Theory

The Nudge Theory focuses on crafting effective decision-making patterns within an organization. The theory utilizes an individual's behavioral patterns. System 1 focuses on the automatic, immediate human responses, and system 2 focuses on the slower, deliberate decision-making patterns of individuals (Sharma et al., 2021). The Nudge Theory within cybersecurity helps balance individuals' autonomy and adoption of secure practices by considering both conscious and unconscious decision-making (Mersinas & Bada, 2024). In the case of OHS, clinical leaders focused on implementing new processes but did little to understand the logic behind their clinical staff's decisions. Utilizing the system 1 and system 2 approach allows each mechanism of human cognitive decision-making to be influenced by nudging individuals toward the correct decisions (Van Steen, 2025). Priming involves exposing individuals to past occurrences (Sharma et al., 2021). Framing focuses on depicting cybersecurity threats to influence the perception and decisions (Sharma et al., 2021). Implementing Nudge Theory benefits hospitals by routing System 1 decisions to System 2, thereby forcing a critical evaluation of decisions related to cybersecurity (Mersinas & Bada, 2024; Sharma et al., 2021). The practice enables informed decision-making across the entire clinical staff, reducing risky behavior related to cyber threats, and helps evaluate potential consequences of a breach (Mersinas & Bada, 2024). The internalization of choices regarding phishing incidents enables each employee to confidently ward off cyber breaches and halt the recurrence of such incidents (Sharma et al., 2021). Ultimately, the application of Nudge's Theory serves to shift decision patterns from hasty to informed, allowing hospitals to increase their resistance to data breaches from phishing.

Enterprise Risk Management Frameworks

PESTLE Analysis

A PESTLE analysis focuses on holistic identification of threats that plague an organization. Regarding cybersecurity, the framework examines the Political, Economic, Social, Technological, Legal, and Environmental dimensions of risk that inhibit the implementation of cybersecurity strategies (Balzano & Marzi, 2024). Political considerations encompass the regulatory frameworks that govern cybersecurity practices and the coordination among stakeholders within an organization to facilitate adoption. Economics focuses upon challenges such as personnel shortages, lack of skills, and associated costs for adoption. Social aspects encompass societal awareness and cultural attitudes towards the adoption of cybersecurity strategies. Centers focus on training tools, innovation, and necessary technology to support secure operations. Legal investigates frameworks and barriers that govern cybersecurity process design; environmental considers the impact of cyberattacks (Ricci et al., 2021). At OHS, leadership could have benefited from employing the PESTLE framework to establish a proper risk mitigation framework. The importance of PESTLE lies in creating a strategic means of determining macro risks to the security of the data within the hospital

(Ciuperca et al., 2022). Leader can capture the interaction between the macro risks and the cultural characteristics of their hospital to effectively implement cybersecurity strategies (Ciuperca et al., 2022). This action allows enhanced adoption of cyber practices, reduces threats to change management, and supports informed decision-making (Sufi, 2023). The process also facilitates stakeholder alignment, necessary to combat the complexity of cyberattacks, by outlining threats and proactively developing an Enterprise Risk Management (ERM) strategy to prevent their occurrence (Sufi, 2023). In the case of OHS, clinical leaders needed this information to properly strategize preventative measures. By the time leaders collected the necessary data, another attack had already taken place. A more effective approach would have been to conduct the PESTLE analysis proactively and implement the ERM strategies earlier to mitigate the risk of future incidents (Sufi, 2023). The use of the PESTLE analysis helps identify external risks to the organization, enabling the development of proactive risk management strategies to prevent cyberattacks and minimize their impact.

RIMS Risk Maturity Model

The RIMS Risk Maturity Model (RMM) identifies risks inherent within an organization and introduces controls to mitigate effects. Attributes include Enterprise Risk Management (ERM) adoption, effectiveness of process ERM, Risk appetite, problem identification, risk disclosure, performance determination, and business sustainability (Nikolaenko & Sidorov, 2023). Examining the seven attributes allows organizational leaders to assess the ERM maturity of operations (Gallagher & Farrell, 2014). Clinical leaders at OHS could benefit from using RMM to identify process improvements and benchmark current practices. The lack of iterative reflection in OHS cybersecurity practices resulted in unidentified risks. Had leaders understood the overall risk maturity of their organization, they could have developed strategies to enhance EMR strategy, increase risk awareness to promote cultural practices, and create value by mitigating surprise risks (Farrell & Gallagher, 2015). The difficulty of adoption lies in cultural resistance. Organizations deeply ingrained in legacy practices struggle to accept lower-than-expected maturity levels (Farrell & Gallagher, 2015). OHS would need to not only gain leadership engagement to champion RMM adoption but also to persist with the resulting strategic changes thereafter, using a change management model. Both of which are achievable when individuals understand risk and its relationship to their success (Nikolaenko & Sidorov, 2023). The RIMS RMM model emphasizes the importance of systemic risk management in preventing data breaches and promoting enhanced preventive ERM practices.

Comprehensive Solution Proposal

OHS faced a variety of challenges that led to multiple data breaches, resulting from phishing, within a span of 1 year. The problems can be categorized into people, process, and planning. Regarding personnel, a lack of training, improper procedures, and rapid staff turnover resulted in unstable working conditions, making OHS susceptible to data breaches. The hospital's processes also suffered from a lack of ownership, unclear direction, and inaccurately focused ERMs. Finally, the hospital fell out of a proactive culture due to a lack of anticipatory risk identification and planning. The following recommendations have been developed to reestablish a risk-conscious culture that prevents future data breaches at OHS and empowers staff to remain vigilant in the face of threats.

Owning Failures

The first recommendation lies in reestablishing trust between the hospital staff and leadership. Phishing risk magnifies when individuals lack trust in the security practices in place (Kinoon, 2024). As individuals lack confidence in their role, it increases the chances of human error, which can magnify the probability that someone will accidentally expose Patient Health Information (Pool et al., 2019). To properly instill confidence within the staff, especially after multiple breaches, OHS leadership must be transparent about the wrongdoings that occurred (Smith, 2016). The vulnerability will foster in-depth conversations that allow all those involved with the data breach to learn from the error (Smith, 2016). OHS can garnish collaboration by accepting responsibility, as employees post-incident will be open to improvements (Pool et al., 2019). Owning failures is the first step of communication after a breach, followed by announcing the next steps.

Provide Training

Comprehensive cybersecurity training remains critical for vigilant efforts to prevent cyberattacks. Trainings help upskill individuals on the latest cybersecurity practices, discuss cybercriminal trends, and incorporate targeted simulations (Gordon et al., 2019; Priestman et al., 2019). Moreover, implementing regular training helps foster a sense of equal responsibility across all individuals to protect patient health data (Priestman et al., 2019). All factors empower individuals to vigilantly protect themselves against cyberattacks and build confidence in their ability to report risks, act responsibly, and educate one another (Afriyie, 2025). In the case of OHS, training occurred yearly but was not reinforced with awareness programs. Instead, OHS needs to craft a training that focuses on employee education, cybersecurity risks to the hospital, and includes all individuals regardless of their existing awareness levels (Priestman et al., 2019). Preparing individuals throughout the entire process, from prevention to mitigation, will reduce susceptibility to phishing schemes and protect patient data (Gordon et al., 2019). Overall, leadership can support clinical staff through training that addresses current issues and the risks that exist to the hospital.

Manage Reputational Risk

OHS needs to manage reputational risk as part of a holistic risk management strategy. Reputation risk manifests when PHI is released during a data breach.

This leaves patients, physicians, and clinical staff lacking confidence in the hospital's security practices Clement, 2023). The breach can also raise concerns around the quality of patient care when data is exposed or missing, resulting in false diagnoses, inaccurate information, and lapses in treatments (Bozic, 2025). Following the first data breach, OHS lost the trust of the community. Subsequent breaches further bolstered any remaining trust and have left the hospital in a fragile position (Kinoon, 2024). Clinical leaders should publish a statement taking accountability for the breach, including details of the incident, and corrective actions taken (Choi et al., 2025). All three components provide transparency that helps reestablish trust (Masuch et al., 2021). OHS will need to communicate regularly, focus on specific actions taken since the last updates, and offer long-term support to victims (Choi et al., 2025). The continual commitment to those impacted will be critical to rebuilding a relationship with patients (Masuch et al., 2021). OHS must mitigate reputational risks, which requires a risk management strategy encompassing transparency and targeted actions.

Generate a Risk Register

Awareness of existing and emerging risks represents strategic conversation facilitators needed to safeguard OHS's patient data. Risk registers are pivotal artifacts that guide the cybersecurity strategy to prevent repeated attacks (Mayer et al., 2023). Instead, OHS should examine the cultural characteristics that drive the system's inability to identify, protect against, and prevent known risks. One application occurs by employing the iceberg model to understand that surface-level risk exhibits the initial threat, but the core cause of any risk lies beneath the surface (Bisogni et al., 2016). OHS can only successfully build a risk mitigation plan if leaders understand the risks, the complexity of those risks, and the cultural and behavioral shifts that will be necessary to prevent the risk from occurring (Quinn et al., 2021). Gathering this information into a holistic risk register will directly inform the mitigation plans, targeting highly probable threats to the organization (Quinn et al., 2021). If OHS had implemented this process, it would have established a preventive, informed culture focused on risk, rather than a reactive culture unaware of existing threats (Bisogni et al., 2016; Quinn et al., 2021). Ultimately, risk registers aid in designing focused risk mitigation plans by utilizing cultural models to understand risk complexity and creating a comprehensive risk mitigation plan.

Formulate an Enterprise Risk Management Plan

Considering the long-term sustainability of organizational data vigilance requires assessing the risks that plague an organization at a systemic level (Sufi, 2023). These practices require utilizing a process such as SWOT Analysis or PESTLE to investigate and report the identified risks. Regarding SWOT Analysis, the methodology focuses on the internal and external risk factors that plague an organization's cybersecurity preparedness (Prasuna & Rachh, 2023). PESTLE focuses on a series of organizational inner dynamics that result in risk identification (Ricci et al., 2021). The importance of both processes lies in the efficiency of identifying threats to an organization that can manifest into risks. Since OHS is primarily concerned with restoring its reputation and implementing a solution quickly, it should utilize a SWOT analysis (Prasuna & Rachh, 2023). The process facilitates a broader identification of risk, in contrast to PESTLE's comprehensive breadth and depth of risk topics that may extend timelines. The benefit of SWOT for OHS lies in ensuring that risks are identified efficiently and a direction is mapped out for a strong risk mitigation plan (Prasuna & Rachh, 2023). A targeted risk mitigation plan aligned with likely risks enables leaders to invest in the personnel, skills, and funds necessary to implement a preventive culture focused on data protection. These practices will directly improve OHS's relationship within the community by reducing reputational risk incurred by repeated breaches. Strengthening patient and provider trust will help restore operations and make a risk-aware culture ready in the event of future incidents. OHS's utilization of a sustainable identification process will ensure a relevant risk mitigation plan to protect organizational operations from and during a data breach.

Implement Controls

After a risk mitigation plan has been established, organizational leaders must implement security controls to ensure long-term protection of data and promote a sustainable cybersecurity culture (Meisner, 2017). Controls should include new practices that focus on education and prevention of data breaches, ongoing training to support vigilance against arising threats, and dedicated personnel monitoring threats to reduce risk for cyberattacks (Afriyie, 2025). To implement controls effectively, leaders must understand change management and tailor their processes to the current organizational culture. The use of Bridges' transition model can account for the psychological and emotional resistance leaders will face when attempting to change cultural dynamics towards secure practices (Heckelman, 2017). The three phases symbolize a gradual process of ending current viewpoints on cybersecurity, entering into a neutral zone that promotes learning and growth of proper cyber-aware practices, and embracing a new beginning that carries forth proper risk mitigation practices. By adopting a gradual process, OHS clinical leaders will establish an emotional connection with the staff (Bridges & Mitchell, 2000). Thus, building empathy between the two groups and fostering a collaborative cybersecurity culture focused on preventing future data breaches (Sharma, 2025). The process also ensures that the risk mitigation plan is built by those expected to adopt the practices, which will decrease resistance or reversion to old practices (Bridges & Mitchell, 2000). Organizations that successfully adopt improved processes will establish trust within the community and begin to restore their reputation (Decker & Galer, 2013). Therefore, by addressing the emotional and psychological factors that cause change resistance, OHS can ensure its risk mitigation plan yields lasting organizational resilience and stronger protections against cyber threats.

Build and Sustain a Preventative Culture

Finally, OHS leaders must establish cultural norms that adhere to regulated cybersecurity practices to foster a shared responsibility for protecting PHI. The nudge theory can directly impact the sustainability of OHS's processes by aligning all individuals towards a shared set of cybersecurity values. This method emphasizes the importance of everyone working in the same direction and with the same goals in mind (Sharma et al., 2021). By targeting autonomous decision-making, leaders can help staff execute the hospital's cybersecurity vision (Sharma et al., 2010). Those with a toolset can make informed decisions that sustain practices and spend less time doubting their judgment (Mersinas & Bada, 2024). Applying the Nudge Theory will orient individuals towards the central goals: upholding OHS's policies and protecting patient data (Mersinas & Bada, 2024). OHS needs to create a community of cyber-aware individuals who can withstand cybersecurity attacks, educate one another on emerging threats, and prevent data breaches of patient PHI. Without everyone centralizing efforts towards preventive measures and fully adopting organizational security practices, OHS will continue to experience data breaches (Sharma et al., 2021). This could result in the loss of funding, a decline in reputation, and ultimately, the hospital's closure. The persistence of sustainable cybersecurity practices fosters trust, enhances resilience, and safeguards patient information in the long term.

Conclusion

OHS has faced three major data breaches resulting in millions of PHI records being exposed. Clinical leadership must develop a strategic cybersecurity strategy to prevent future incidents, promote organizational resilience, and rebuild trust between the hospital and the community. An immediate-term goal exists to rebuild trust with the OHS staff and the community. This can be achieved by admitting to wrongdoing, offering transparency around the data breach, and investigating the extent of the breach. These strategic short-term actions will provide empathy and help stop the immediate threats. Thus, it enables OHS to focus on its long-term strategic goal of building a risk-preventative culture.

To achieve long-term strategic goals, leaders must consider problem-solving models, such as SWOT analysis, to understand existing threats. This will enable proper prioritization based on the likelihood and severity of occurrence. Leaders can then appropriately assign personnel, enhance training, and influence the development of a comprehensive risk mitigation plan.

Next, leaders will need to gather data from the SWOT analysis, employees' lived experiences, and analysis of the breaches to form a risk mitigation plan. The plan should factor in change management techniques such as Bridges Transition Model to promote empathy with staff and help decrease resistance to cybersecurity-related process change. Considering the emotional and psychological impacts of staff will help increase adoption of the changes, promote confidence to fend off future cyberattacks, and give opportunities for OHS to build a cybersecurity program that fits its needs.

Finally, after successfully adopting new practices aimed at preventing future data breaches from phishing attacks, the entire OHS staff must sustain the cultural changes. To prevent a return to the insecure practices that introduced the original vulnerabilities, all staff at OHS must continually work towards a common vision. Using techniques such as the Nudge Theory, leaders can champion a culture where every individual remains vigilant and raises awareness of insecure data practices. This practice not only sustains a proactive risk-aware culture but will also allow for the maturity of practices in the face of new threats.

Overall, OHS must respond strategically to the series of phishing-related data breaches. They have faced a significant impact on their employees, operations, and stakeholders. Leaders must balance short-term and long-term goals to provide a holistic risk management solution that will reestablish trust, mitigate remaining threats, and establish a risk management plan. Thereafter, OHS can initiate strategic, long-term initiatives to foster a proactive culture that is prepared to address existing and emerging cybersecurity threats.

References

Abrahams, T. O., Farayola, O. A., Amoo, O. O., Ayinla, B. S., Osasona, F., & Atadoga, A. (2024). Continuous improvement in information security: A review of lessons from superannuation cybersecurity uplift programs. *International Journal of Science and Research Archive*, *11*(1), 1327–1337. https://doi.org/10.30574/ijsra.2024.11.1.0219

Adamu, M. A., Niemimaa, M. I., & Spagnoletti, P. (2025). Towards a Three-Tiered Framework for Fostering Organizational Cybersecurity Culture. In M. Themistocleous, N. Bakas, G. Kokosalakis, & M. Papadaki (Eds.), *Information Systems* (pp. 313–324). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-81325-2_22

Afriyie, H. (2025). Exploring Cybersecurity Asset Management Strategies for Medical Device Safety and Security in Hospitals. *Walden University*.

Al Kinoon, M. (2024). A Comprehensive and Comparative Examination of Healthcare Data Breaches: Assessing Security, Privacy, and Performance. *University of Central Florida*, 110. https://stars.library.ucf.edu/etd2023/110/

Alder, S. (2025, August 25). *July 2025 Healthcare Data Breach Report*. The HIPAA Journal. https://www.hipaajournal.com/july-2025-healthcare-data-breach-report/

Alduraibi, M. (2023). *Investigating the Impact of Lean Six Sigma Principles on Establishing and Maintaining Data Governance Systems in Smes: An Exploratory Study Using Grounded Theory and Ism Approach* [Thesis, Purdue University Graduate School]. https://doi.org/10.25394/PGS.22684780.v1

Balzano, M., & Marzi, G. (2025). At the Cybersecurity Frontier: Key Strategies and Persistent Challenges for Business Leaders. *Strategic Change*, *34*(2), 181–192. https://doi.org/10.1002/jsc.2622

Bisogni, F., Asghari, H., & van Eeten, M. (2017). Estimating the size of the iceberg from its tip: 16th Annual Workshop on the Economics of Information Security. *Proceedings of 16th Annual Workshop on the Economics of Information Security 2017*. http://resolver.tudelft.nl/uuid:6c5c52d6-42a3-48c6-8c95-c539146b6d2a

Božić, V. (2025). *Disaster Recovery and Business Continuity Planning in hospital*. https://doi.org/10.13140/RG.2.2.19818.43200

Bridges, W., & Mitchell, S. (2000). Leading Transition: A New Model for Change. *Leader to Leader*, *16*(3), 30–36.

Choi, J., Robinson, S., Ruddle, T., & Fister, A. (2025). Restoring Public Trust After a Data Breach Crisis: Reputational Response Strategies for Government, For-Profit, and Nonprofit Organizations. *Risk, Hazards & Crisis in Public Policy*, *16*(3), e70026. https://doi.org/10.1002/rhc3.70026

Choi, S. J., & Johnson, M. E. (2019). *Do Hospital Data Breaches Reduce Patient Care Quality?* arXiv. https://doi.org/10.48550/ARXIV.1904.02058

Choi, S. J., & Johnson, M. E. (2021). The relationship between cybersecurity ratings and the risk of hospital data breaches. *Journal of the American Medical Informatics Association*, *28*(10), 2085–2092. https://doi.org/10.1093/jamia/ocab142

Choi, S. J., Johnson, M. E., & Lehmann, C. U. (2019). Data breach remediation efforts and their implications for hospital quality. *Health Services Research*, *54*(5), 971–980. https://doi.org/10.1111/1475-6773.13203

Ciuperca, E. M., Cîrnu, C. E., Stanciu, A., & Cristescu, I. (2022). *Leveraging Socio-Cultural Dimension in Cyber Security Training*. 5242–5248. https://doi.org/10.21125/edulearn.2022.1239

Clement, N. (2023). M&A Effect on Data Breaches in Hospitals: 2010-2022. *Proceedings of the 22nd Workshop on the Economics of Information Security*, 5–8.

Daman, R., Madhava Tripathi, M., & Kanta Mishra, S. (2016). *Cloud Computing for Medical Applications & Healthcare Delivery: Technology, Application, Security and Swot Analysis*. https://www.academia.edu/122332106/Cloud_Computing_for_Medical_Applications_and_Healthcare_Delivery_Technology_Application_Security_and_Swot_Analysis

Farahbod, K., Shayo, C., & Varzandeh, J. (2022). Six Sigma and Lean Operations in Cybersecurity Management. *Journal of Business and Behavior Sciences*, *34*(1), 99–109.

Farrell, M., & Gallagher, R. (2015). The Valuation Implications of Enterprise Risk Management Maturity. *Journal of Risk and Insurance*, *82*(3), 625–657. https://doi.org/10.1111/jori.12035

Gabriel, M. H. (2018). Data Breach Locations, Types, and Associated Characteristics Among US Hospitals. *The American Journal of Managed Care*, *24*(2), 78–84.

Gordon, W. J., Wright, A., Aiyagari, R., Corbo, L., Glynn, R. J., Kadakia, J., Kufahl, J., Mazzone, C., Noga, J., Parkulo, M., Sanford, B., Scheib, P., & Landman, A. B. (2019). Assessment of Employee Susceptibility to Phishing Attacks at US Health Care Institutions. *JAMA Network Open*, *2*(3), e190393. https://doi.org/10.1001/jamanetworkopen.2019.0393

Haider, S. (2009). The organizational knowledge iceberg: An empirical investigation. *Knowledge and Process Management*, *16*(2), 74–84. https://doi.org/10.1002/kpm.326

Heckelman, W. (n.d.). Five Critical Principles to Guide Organizational Changes. *OD Practitioner*, *49*(4), 13–21.

Herisasono, A. (2025). Legal Liability of Health Care Facilities for Leakage of Patient Electronic Medical Records. *Pena Justisia: Media Komunikasi Dan Kajian Hukum*, *24*(1), 44–68.

HIMSS. (2025). *2024 HIMSS Healthcare Cybersecurity Survey*. HIMSS. https://www.himss.org/resources/himss-healthcare-cybersecurity-survey/

Holloway, D. (2025). *Strategies in Cybersecurity for the Protection of Patient Health Information (PHI) - ProQuest*. ProQuest. https://www.proquest.com/docview/3226061104?pq-origsite=gscholar&fromopenview=true&sourcetype=Dissertations%20&%20Theses

K. Pool, J., Akhlaghpour, S., Fatehi, F., & Burton-Jones, A. (2019). Causes and Impacts of Personal Health Information (PHI) Breaches: A Scoping Review and Thematic Analysis. *PACIS 2019 Proceedings*. https://aisel.aisnet.org/pacis2019/71

Kam, H.-J., Mattson, T., & Kim, D. J. (2021). The "Right" recipes for security culture: a competing values model perspective. *Information Technology & People*, *34*(5), 1490–1512. https://doi.org/10.1108/ITP-08-2019-0438

Masuch, K., Greve, M., & Trang, S. (2021). What to do after a data breach? Examining apology and compensation as response strategies for health service providers. *Electronic Markets*, *31*(4), 829–848. https://doi.org/10.1007/s12525-021-00490-3

Mayer, P., Zou, Y., Lowens, B. M., Dyer, H. A., Le, K., Schaub, F., & Aviv, A. J. (2023). Awareness, Intention, (In)Action: Individuals' Reactions to Data Breaches. *ACM Transactions on Computer-Human Interaction*, *30*(5), 1–53. https://doi.org/10.1145/3589958

Mbarek, I. (2024). How Organizations Address Resistance: Understanding Change Management. *International Journal of Applied Business and Management Studies*, *9*(2).

Meisner, M. (2018). Financial Consequences of Cyber Attacks Leading to Data Breaches in Healthcare Sector. *Copernican Journal of Finance & Accounting*, *6*(3), 63. https://doi.org/10.12775/CJFA.2017.017

Mersinas, K., & Bada, M. (2024). Behavior Change Approaches for Cyber Security and the Need for Ethics. In C. Onwubiko, P. Rosati, A. Rege, A. Erola, X. Bellekens, H. Hindy, & M. G. Jaatun (Eds.), *Proceedings of the International Conference on Cybersecurity, Situational Awareness and Social Media* (pp. 107–129). Springer Nature. https://doi.org/10.1007/978-981-99-6974-6_7

Miller, J. (2017). Managing Transitions: Using William Bridges' Transition Model and a Change Style Assessment Instrument to Inform Strategies and Measure Progress in Organizational Change Management. *The 12th International Conference on Performance Measurement in Libraries Proceedings*, 357–364. https://digitalcommons.butler.edu/librarian_papers/74

Moffit, R. E., & Steffen, B. (2017). Health Care Data Breaches: A Changing Landscape. *Maryland Health Care Commission, 1*.

Nikolaenko, V., & Sidorov, A. (2023). Assessing the Maturity Level of Risk Management in IT Projects. *Sustainability, 15*(17), 12752. https://doi.org/10.3390/su151712752

Pool, J., Akhlaghpour, S., Farhad, F., & Burton-Jones, A. (2019). Causes and Impacts of Personal Health Information (PHI) Breaches: A Scoping Review and Thematic Analysis. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3584865

Prasuna, A., & Rachh, A. (2023). A Study on Challenges of Data Security and Data Privacy in the Healthcare Sector: SWOT Analysis: - 2nd International Healthcare Management Conference 2022: Navigating the New Normal with Focus on Healthcare Accessibility, Innovation and Sustainability. *Asia Pacific Journal of Health Management*. https://doi.org/10.24083/apjhm.v18i1.1675

Priestman, W., Anstis, T., Sebire, I. G., Sridharan, S., & Sebire, N. J. (2019). Phishing in healthcare organisations: threats, mitigation and approaches. *BMJ Health & Care Informatics, 26*(1), e100031. https://doi.org/10.1136/bmjhci-2019-100031

Quinn, S., Ivy, N., Barrett, M., Feldman, L., Witte, G., & Gardner, R. K. (2021). *Identifying and estimating cybersecurity risk for enterprise risk management* (No. NIST IR 8286A; p. NIST IR 8286A). National Institute of Standards and Technology (U.S.). https://doi.org/10.6028/NIST.IR.8286A

Ricci, S., Janout, V., Parker, S., Jerabek, J., Hajny, J., Chatzopoulou, A., & Badonnel, R. (2021). PESTLE Analysis of Cybersecurity Education. *Proceedings of the 16th International Conference on Availability, Reliability and Security*, 1–8. https://doi.org/10.1145/3465481.3469184

Seh, A. H., Zarour, M., Alenezi, M., Sarkar, A. K., Agrawal, A., Kumar, R., & Ahmad Khan, R. (2020). Healthcare Data Breaches: Insights and Implications. *Healthcare, 8*(2), 133. https://doi.org/10.3390/healthcare8020133

Sharma, A. (2025). Managing Resistance in Complex Digital Transformations: A Comparative Study of Change Management Models in Complex Organizational Systems. *International Journal on Science and Technology, 16*(3), 7548. https://doi.org/10.71097/IJSAT.v16.i3.7548

Sharma, K., Zhan, X., Nah, F. F.-H., Siau, K., & Cheng, M. X. (2021). Impact of digital nudging on information security behavior: an experimental study on framing and priming in cybersecurity. *Organizational Cybersecurity Journal: Practice, Process and People, 1*(1), 69–91. https://doi.org/10.1108/OCJ-03-2021-0009

Sharma, N., A. Oriaku, E., & Oriaku, N. (2020). Cost and Effects of Data Breaches, Precautions, and Disclosure Laws. *International Journal of Emerging Trends in Social Sciences, 8*(1), 33–41. https://doi.org/10.20448/2001.81.33.41

Smith, T. T. (2016). Examining Data Privacy Breaches in Healthcare. *Walden University*.

Sufi, F. K. (2024). Open-source cyber intelligence research through PESTEL framework: Present and future impact. *Societal Impacts, 3*, 100047. https://doi.org/10.1016/j.socimp.2024.100047

Triplett, W. (2021). Establishing a Cybersecurity Culture Organization. *Acta Scientific Computer Sciences, 3*(8), 00–00. https://actascientific.com/ASCS/ASCS-03-0153.php

Van Steen, T. (2025). Developing a behavioural cybersecurity strategy: A five-step approach for organisations. *Computer Standards & Interfaces, 92*, 103939. https://doi.org/10.1016/j.csi.2024.103939

Yeng, P. K., Yang, B., & Snekkenes, E. A. (2019). Healthcare Staffs' Information Security Practices Towards Mitigating Data Breaches: A Literature Survey. *Studies in Health Technology and Informatics, 261*, 239–245.