Beyond Conventional Threat Defense: Implementing Advanced Threat Modeling Techniques, Risk Modeling Frameworks and Contingency Planning in the Healthcare Sector for Enhanced Data Security

Abstract

This research study explores the integration of advanced threat and risk modeling with scenario and contingency planning to enhance security and resilience within healthcare organizations. Given the escalating complexity and frequency of cyber threats targeting the healthcare sector, the study assesses the efficacy of a synergistic cybersecurity approach. Utilizing a quantitative research methodology, data were collected through a survey administered to 452 healthcare practitioners, focusing on their perceptions and experiences with cybersecurity threats, risk modeling techniques, and the effectiveness of scenario and contingency planning.The survey incorporated a structured questionnaire utilizing Likert scale closed-ended questions, analyzed using Partial Least Squares Structural Equation Modeling (PLS-SEM) to test the proposed four hypotheses related to the impact of advanced threat and risk modeling and scenario and contingency planning on the cybersecurity posture and operational resilience of healthcare organizations.Results indicated a significant positive relationship between advanced threat modeling and scenario planning with the cybersecurity posture of healthcare organizations, which, in turn, notably enhances organizational resilience. Specifically, the study found that integrating advanced threat and risk modeling with scenario and contingency planning significantly improves the ability of healthcare organizations to identify, assess, and mitigate cyber threats effectively. Furthermore, the findings suggest that such integration contributes to more informed decision-making, improved information security management practices, and more effective and efficient digital crime investigation processes.The research study concludes that a comprehensive approach integrating advanced threat and risk modeling with scenario and contingency planning significantly enhances healthcare organizations' cybersecurity posture and operational resilience. The study recommends adopting an integrated cybersecurity strategy, continuous cybersecurity education for all organizational members, regular cybersecurity assessments, and fostering collaboration for enhanced cybersecurity intelligence.

Keywords: Cybersecurity, Healthcare Organizations, Advanced Threat Modeling, Scenario Planning, Contingency Planning, Operational Resilience, Cyber Threats, Risk Management.

1. Introduction

In February 2016, the Hollywood Presbyterian Medical Center, founded in 1924, was hit by a ransomware virus named Locky, typically spread through a malicious Word document disguised as an invoice [1]. The likely vector for the attack was a phishing email mistakenly clicked by an employee. The attackers demanded a ransom of 40 Bitcoin, approximately $17,000 at the time, to decrypt the data and restore access to the hospital's computer systems [2]. The ransomware attack had significant operational impacts on the hospital as departments were advised not to use their computers, leading to a reliance on pen and paper for patient admissions and record-keeping [3]. Important patient data, including medical histories and test results, became inaccessible, and some patients had to be diverted to other hospitals. Hence, the hospital declared an internal emergency and took an offline computer system to contain the attack. Despite efforts to manage the attack by working with law enforcement and computer experts to address the attack, which generally proved abortive, the decision was made to pay the ransom of $17,000 to regain access to the encrypted data [4]. This incident highlights the urgent need for healthcare organizations to enhance their cybersecurity measures and to have robust incident response plans in place, serving as a critical reminder of the importance of cybersecurity awareness and preparedness within the healthcare sector, emphasizing the need for continuous improvement of security measures to protect against future cyber threats.

As asserted by Tariq [5], digital technology has revolutionized the healthcare industry, enhancing the efficiency, accessibility, and quality of patient care from electronic health records (EHRs) to telemedicine, digital technologies, thus becoming integral to modern healthcare operations. As a result, healthcare organizations increasingly rely on technology to deliver critical services, from patient care to operational management [5]. However, this digital transformation has also introduced new vulnerabilities, making healthcare organizations prime cyberattack targets. These threats range from data breaches exposing sensitive patient information to ransomware attacks that can cripple entire hospital systems, endangering patient safety and care continuity. The complex nature of healthcare systems and the high value of medical data exacerbate the sector's cybersecurity challenges, necessitating robust defense mechanisms. Javaid et al. [6] allude that cyber incidents can disrupt healthcare operations, compromise patient data, and even endanger lives. The evolving nature of cyber threats, characterized by their

increasing sophistication and rapid technological advancements, presents a significant challenge to maintaining robust cybersecurity defenses.

This challenge is, however, multifaceted [7][8]. Traditional cybersecurity measures are often reactive, focusing on known vulnerabilities and threats. However, this approach is insufficient in the current cyber landscape, where threats constantly evolve and new vulnerabilities are regularly discovered [9]. Given the dynamic and sophisticated nature of cyber threats, the healthcare sector's unique requirements underscore the need for a proactive and comprehensive approach to cybersecurity—one that not only detects and responds to threats as they occur but also anticipates and mitigates potential vulnerabilities before they can be exploited [10]. This approach requires the integration of advanced threat and risk modeling techniques, which provide structured methodologies for identifying, assessing, and prioritizing cyber risks, with scenario and contingency planning, which prepares organizations to respond effectively to a range of potential cyber incidents [8].

Moreover, ensuring operational resilience in the face of cyber incidents requires more than just identifying potential threats; it demands comprehensive planning for a range of possible scenarios, including worst-case situations. Scenario and contingency planning can prepare healthcare organizations to respond effectively to cyber incidents, minimizing disruptions to patient care and operational continuity [6]. However, integrating these planning strategies with threat and risk modeling techniques presents its own set of challenges. It requires a deep understanding of the organization’s cybersecurity posture and potential threats and the ability to envision various future scenarios and develop actionable response plans.

This study, therefore, centers on the need for a synergistic approach that combines advanced threat and risk modeling with scenario and contingency planning to enhance the cybersecurity posture and operational resilience of healthcare organizations. Addressing this problem involves exploring the barriers to effectively integrating these strategies, identifying best practices for their implementation, and evaluating their impact on healthcare security and resilience. Given the critical importance of healthcare services and the potentially catastrophic consequences of cyber incidents, developing and refining this integrated approach is paramount for safeguarding the healthcare sector against current and future cyber threats. Thus, this study aims to assess the effectiveness of integrating advanced threat and risk modeling with scenario and contingency planning in enhancing the security and resilience of healthcare organizations, thereby determining the comprehensive impact of this approach on mitigating cyber threats and improving operational preparedness.

Research Objectives:

1. Identify and analyze prevalent cyber threats facing healthcare organizations, focusing on the scope and scale of these threats and their potential impact on patient data and healthcare services.

2. Evaluate the applicability and effectiveness of advanced threat and risk modeling techniques (such as STRIDE and the FAIR Risk Model) in the healthcare sector for identifying, quantifying, and prioritizing cyber threats.

3. Explore how scenario and contingency planning can enhance decision-making and operational resilience in healthcare organizations, particularly in responding to and recovering from cyber incidents.

4. Assess the overall impact of combining advanced threat and risk modeling with scenario and contingency planning on healthcare organizations' cybersecurity posture and operational resilience.

Research Hypotheses

H_1: advanced threat and risk modeling techniques can effectively assess and identify the diverse range of highly impactful cyber threats prevailing in the healthcare cyberspace

H_2: Advanced threat and risk modeling techniques, when applied within healthcare organizations, significantly improve the accuracy and efficiency of cyber threat identification and prioritization compared to traditional risk assessment methods.

H_3: Scenario and contingency planning significantly enhances the strategic decision-making capacity of healthcare organizations, enhancing preparedness, response, and recovery from cyber incidents more effectively than organizations without such planning.

H_4: An integrated approach that combines advanced threat and risk modeling with scenario and contingency planning significantly enhances the cybersecurity posture and operational resilience of healthcare organizations, leading to better protection of patient data and continuity of healthcare services.

2. Literature Review

Electronic health records (EHRs), telehealth services, and connected medical devices are increasingly prevalent, creating a vast network of interconnected systems [11]. While these advancements significantly benefit patient care and operational efficiency, they also introduce a new set of cybersecurity challenges [12]. The expanding attack surface is one of the most pressing concerns [13]. With more data points accessible online, healthcare organizations have become prime targets for cybercriminals seeking

valuable patient information [14]. Electronic medical records hold a wealth of sensitive data, including social security numbers, diagnoses, and treatment histories [14][15]. A successful attack on a healthcare provider's network can disrupt critical services and lead to significant financial losses and reputational damage. Furthermore, the rise of the Internet of Medical Things (IoMT) presents unique challenges, as these interconnected medical devices, ranging from pacemakers to insulin pumps, collect and transmit a constant stream of patient data [16]. However, many IoMT devices lack built-in security measures, making them susceptible to hacking and manipulation [17][18]. A compromised IoMT device could disrupt treatment and potentially endanger patients' lives [19].

Impact of Cyber Threats on Healthcare

One of the most prevalent cyber threats plaguing healthcare organizations is ransomware attacks. These malicious software programs encrypt critical data, holding it hostage until a ransom is paid. For instance, in 2021, a ransomware attack on Universal Health Services, a major hospital chain, crippled operations across hundreds of facilities, forcing them to divert ambulances and postpone surgeries [20].This incident highlights the potential for ransomware to disrupt the delivery of critical care, potentially putting lives at risk. Ransomware attacks also compromise patient privacy, as stolen medical records containing sensitive information like diagnoses, treatment histories, and even social security numbers can be sold on the dark web, leading to identity theft, financial fraud, and even social stigma for patients [21].Such breaches' emotional and financial toll can be immense, eroding trust in healthcare institutions [9].

Data breaches, a broader category encompassing various unauthorized access incidents, pose similar threats, as butressed in a data breach at AME Medical Group in 2020, which exposed the personal information of over 6.4 million patients, including names, addresses, and Social Security numbers [22] underscoring the vast amount of sensitive data healthcare organizations hold and the potential consequences of inadequate security measures. Moreso, malicious actors might not just steal data but also alter it, leading to misdiagnosis, incorrect treatment decisions, and potentially life-threatening consequences [23].A recent study by Checkpoint Research found vulnerabilities in insulin pumps that could allow attackers to manipulate insulin delivery, potentially endangering diabetic patients [24].These emerging threats necessitate robust data security protocols to ensure the accuracy and reliability of medical information.

The financial impact of cyberattacks on healthcare is also significant.Beyond the potential ransom payments, healthcare organizations face costs associated with data recovery, forensic investigations, credit monitoring for affected individuals, and

implementing more robust security measures [25].A study by IBM found that the average cost of a data breach in healthcare reached a staggering $7.14 million in 2022 [26]. Thus, investing in robust security technologies, measures, and strategies has become essential in fostering a culture of cybersecurity within healthcare organizations, resulting in a high level of vigilance on potential threats.

Advanced Threat and Risk Modeling Techniques

Understanding and mitigating potential threats before they manifest is paramount. Hence, risk modeling emerges as a critical preventive approach, enabling organizations to systematically navigate the complexities of digital threats [27][28]. Unlike traditional defenses that react to threats after they occur, advanced threat and risk modeling techniques proactively identify and assess potential vulnerabilities and their impact on healthcare operations [29]. This shift from reactive to proactive is crucial in safeguarding sensitive patient data and ensuring the uninterrupted delivery of healthcare services.

Four notable advanced threat and risk modeling methodologies (STRIDE, PASTA, FAIR, and VAST) stand out amongst others within the healthcare industry, with each offering unique perspectives and tools for cybersecurity planning [29].

STRIDE, an acronym for Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege, provides a comprehensive framework for identifying potential threats across various categories. Its application in healthcare is particularly beneficial for its systematic approach to uncovering vulnerabilities within digital and networked systems [29].

PASTA (Process for Attack Simulation and Threat Analysis) assumes a process-oriented approach to threat modeling, emphasizing analyzing attackers' techniques and potential targets. It is well-suited for healthcare organizations due to its focus on understanding and simulating the tactics of potential adversaries, offering insights into how and where to fortify defenses [30].

VAST (Visual, Agile, and Simple Threat Modeling) addresses the complexity and scalability challenges of threat modeling in large organizations. Its visual and agile framework is adaptable to the sprawling and diverse IT environments typical in healthcare, facilitating a comprehensive assessment of threats across different systems and applications [31].

FAIR Risk Model: **The factor Analysis of Information Risk** (FAIR) model offers a quantitative approach to understanding and analyzing cyber risk, transforming the nebulous aspects of risk into measurable entities [32]. This model enables healthcare

organizations to identify potential risks and quantify their impact in financial terms, facilitating informed decision-making regarding risk mitigation strategies [32].

The Importance of Risk Models in Healthcare Cybersecurity

Risk models serve as the linchpin in the strategic defense against cyber threats within healthcare organizations, transcending traditional security measures to offer a nuanced and comprehensive approach to cyber risk management [32]. The intrinsic value of risk models lies in their ability to systematize the assessment and mitigation of threats, thereby facilitating a more informed and effective allocation of cybersecurity resources [33][34].

To begin with, risk models empower healthcare organizations with predictive insights, enabling them to anticipate potential vulnerabilities and threats before they materialize. This forward-looking capability is crucial in a sector where the stakes include financial loss, patient safety, and privacy [29][35]. Organizations can strategize and implement preventative measures by understanding potential future threats, thereby minimizing the risk of data breaches and other cyber incidents. Also, in the context of limited resources and ever-increasing cyber threats, prioritizing risks based on their potential impact is invaluable; thus, risk models provide a framework for quantifying threats, supporting strategic decisions regarding where to focus cybersecurity efforts [36][37]. This optimization of resources ensures that the most critical vulnerabilities are addressed first, enhancing the overall security posture of the organization [32].

Furthermore, beyond immediate threat mitigation, risk models contribute to the long-term resilience of healthcare organizations by fostering a culture of risk awareness and continuous improvement [38][39]. By regularly assessing and updating risk models, organizations can adapt to the evolving cyber threat landscape, ensuring their defenses remain robust and responsive to new challenges [33]. Adopting risk models also supports compliance with regulatory requirements and enhances governance structures within healthcare organizations. By demonstrating a systematic approach to risk management, organizations can meet the stringent standards set forth by healthcare regulations, thereby avoiding penalties and reinforcing stakeholder trust [29][40].

Evaluation of Decision-Making Processes in Risk Modeling

The decision-making process regarding the adoption and implementation of risk modeling techniques in healthcare organizations is multi-faceted, involving the consideration of various factors that influence the effectiveness and efficiency of these models in real-world settings [41][42][43]. The first step in evaluating potential risk modeling techniques involves assessing their compatibility with the organization's overarching goals and existing capabilities [42][43]. This includes considering the

technical expertise available within the organization, the scalability of the models, and their adaptability to the specific needs and nuances of the healthcare sector [44][45]. Organizations must choose models that address their immediate cybersecurity concerns and align with their long-term strategic objectives [46][47]. After that, given the resource constraints many healthcare organizations face, conducting a thorough cost-benefit analysis is essential. Deloitte [29] argues that this analysis should account for the direct costs associated with implementing and maintaining the chosen risk models, as well as the potential savings from averting cyber incidents, to identify models that offer the highest return on investment, considering both financial and non-financial factors such as patient privacy and trust.

After that, since healthcare organizations operate within a highly regulated environment, the decision-making process must, therefore, include an evaluation of how well different risk modeling techniques enable the organization to meet these regulatory requirements, minimizing legal risks and ensuring ethical handling of patient data [29]. Also, decision-makers should prioritize models that offer flexibility regarding data inputs, threat vectors, and risk scenarios, enabling the organization to stay ahead of potential cyber adversaries [33][48]. In addition, Meinert [32] argues that effective risk modeling goes beyond standalone tools and involves integration with the organization's broader cybersecurity framework. This includes ensuring compatibility with existing security technologies, information systems, and governance structures. Seamless integration enhances the effectiveness of risk models, facilitating a holistic approach to cybersecurity that encompasses threat identification, assessment, mitigation, and continuous monitoring [32].

The Role of Scenario and Contingency Planning in Healthcare

While offering numerous benefits, the digital transformation of healthcare also exposes the sector to significant cyber threats [49]. The closure of Lincoln College due to a cyberattack underscores the catastrophic potential of such threats and highlights the critical need for robust contingency and scenario planning within healthcare organizations [50][51]. Contingency planning in healthcare cybersecurity involves the development of strategic, operational, and tactical plans that enable organizations to respond swiftly and effectively to cyber incidents [52]. This proactive approach aims to minimize the immediate impact of such events and sustain critical operations, thereby safeguarding patient care and organizational integrity. The complexity of healthcare systems, coupled with the sensitivity of patient data, underscores the imperative for robust contingency planning that addresses not only technological vulnerabilities but also human and procedural factors [52][53]. Scenario planning, on the other hand, complements contingency planning by preparing organizations for a range of potential futures [54]. It involves analyzing various possible outcomes, including both adverse

and favorable scenarios, to enhance decision-making and strategic planning, thus providing a framework for navigating uncertainties and ensuring preparedness for diverse cyber threat scenarios in the healthcare industry [54][56].

Information systems are integral to healthcare operations. Hence, contingency and scenario planning support these systems by outlining methods and standards for rapid recovery following disruptions, safeguarding patient data, and maintaining service continuity [55]. A well-crafted contingency and scenario plan is a critical fallback, ensuring that healthcare organizations can quickly rebound from cyber incidents [50]. Ford [54] avers that contingency and scenario planning are vital for proactive risk management, but they serve distinct purposes. Contingency planning focuses on preparing for specific, often adverse, events, providing a clear action plan for immediate response. In contrast, Luther and Ali [57] contend that scenario planning takes a broader view, considering a range of possible futures to inform strategic decision-making and long-term planning. However, as Ford [54] asserts, together, they offer a comprehensive approach to managing cybersecurity risks in healthcare.

Healthcare organizations can utilize various types of scenario planning, including quantitative, operational, interactive, normative, and probability-based scenarios, to address different strategic needs and planning horizons [52][57]. Each type offers unique insights and benefits, from understanding financial implications to assessing the immediate impact of events and exploring the interplay of different variables within the organization [57].

According to Luther and Ali [57], the benefits of scenario and contingency planning are numerous for healthcare organizations, from forecasting trends and attracting investment to optimizing resource allocation and mitigating potential losses. By preparing for various future states, healthcare organizations can navigate the complexities of the cyber threat landscape more effectively, making informed decisions that safeguard their operations and patient data against emerging threats [57][58]. However, Luther and Ali [57] argue that effective scenario planning requires careful consideration of several key questions, from defining the problems and scope to evaluating the impact of external and internal factors on potential scenarios. Addressing these questions helps healthcare organizations tailor their scenario planning processes to their specific needs and strategic goals, ensuring the relevance and effectiveness of their planning efforts [57].

Contingency Planning for Preparedness towards Cyber Incidents in the Healthcare Industry

A critical examination of recent cybersecurity incidents in healthcare reveals a concerning trend: many organizations are ill-prepared for the sophistication and

diversity of modern cyber threats. The case of Lincoln College, as noted by Irwin [50], illustrates the potentially devastating consequences of inadequate contingency planning. However, this is not an isolated incident. Studies consistently highlight the healthcare sector's susceptibility to cyberattacks, emphasizing the need for comprehensive and dynamic contingency strategies [52][55].

Despite the recognized importance of contingency planning, a significant gap exists between theoretical frameworks and practical implementation in healthcare settings. This discrepancy often stems from several factors, including limited cybersecurity resources, the complexity of healthcare IT ecosystems, and a lack of specialized knowledge among healthcare personnel [59]. Furthermore, the rapid pace of technological advancement and the evolving nature of cyber threats present ongoing challenges to maintaining effective contingency plans [60]. As such, healthcare organizations must adopt a flexible and iterative approach to contingency planning that encompasses regular updates and drills to ensure preparedness and efficacy.Integrating contingency planning into the healthcare sector's cybersecurity protocols necessitates a holistic perspective that transcends technical measures. Effective contingency plans must consider the interplay between technology, people, and processes [57][61]. This includes not only the implementation of robust cybersecurity technologies and infrastructure but also the training and engagement of staff in cybersecurity best practices and the establishment of clear communication and decision-making protocols in the event of a cyber incident [61].

Despite the consensus on the critical role of contingency planning in healthcare cybersecurity, controversies persist regarding the optimal approaches to its development and implementation [44][49]. There is ongoing debate about the balance between generic versus highly customized contingency plans, allocating resources to preventive versus responsive measures, and the extent of regulatory mandates versus voluntary industry standards [49]. These discussions reflect the complex, multifaceted nature of cybersecurity in healthcare, underscoring the need for a nuanced understanding and strategic approach to contingency planning.

Benefits and Limitations of integrating scenario and contingency planning into healthcare organizations' cybersecurity strategies

The integration of scenario and contingency planning into healthcare organizations' cybersecurity strategies is increasingly recognized as a vital component of a robust cybersecurity posture as it provides a framework for healthcare providers to proactively identify potential cyber threats, develop strategic responses, and ensure the continuity of critical healthcare services in the event of a cyber incident [12]. However, like any strategic framework, it has its benefits and limitations.

The primary benefit of incorporating scenario and contingency planning lies in enhancing organizational preparedness and resilience. By simulating a range of potential cybersecurity scenarios, healthcare organizations can assess their readiness to respond to various types of cyberattacks, from data breaches and ransomware to more sophisticated, targeted attacks [6][62]. This proactive approach allows identifying vulnerabilities within an organization's cybersecurity defenses and developing targeted mitigation strategies. Furthermore, contingency planning ensures that healthcare organizations have predefined response plans, minimizing the response time and potential impact on patient care and data security [54].

Another significant advantage is promoting a culture of cybersecurity awareness and vigilance throughout the organization. Scenario planning exercises involve multiple departments and levels of staff, fostering a more comprehensive understanding of cybersecurity risks and the importance of adhering to security protocols [55]. This interdisciplinary engagement enhances communication and collaboration among staff, which is critical in effectively responding to and recovering from cyber incidents.

Despite these benefits, integrating scenario and contingency planning into healthcare cybersecurity strategies is challenging. One of the main limitations is the resource intensity of developing and maintaining comprehensive scenarios and contingency plans [63]. For many healthcare organizations, especially smaller providers, the financial and human resource costs associated with conducting regular scenario exercises and updating contingency plans can be prohibitive [6]. This constraint may limit the depth and frequency of planning exercises, potentially leaving some vulnerabilities unaddressed. Furthermore, the rapidly evolving nature of cyber threats presents another challenge. Cybersecurity scenarios and contingency plans can quickly become outdated as cyber adversaries develop new tactics and exploit emerging vulnerabilities [59][62]. This necessitates continuous monitoring, evaluation, and revision of planning documents, which can be difficult for organizations to sustain over time [6]. Additionally, the complexity of healthcare IT ecosystems, with their interconnected devices and systems, adds another layer of difficulty in accurately simulating and planning for potential cyber incidents.

Integrating Threat Modeling with Scenario and Contingency Planning

Threat and risk modeling is the foundation of a proactive cybersecurity strategy, enabling organizations to identify potential vulnerabilities and the threats most likely to exploit them [64]. Techniques like STRIDE and the FAIR model help categorize threats and assess their possible impact. However, while these models are instrumental in highlighting vulnerabilities and quantifying risks, they often require further context to inform strategic planning and operational preparedness [65]. Therefore, it becomes vital

to. Scenario planning extends the insights gained from threat and risk modeling by exploring a range of possible futures, each predicated on different threat realizations and their implications for the organization [66]. It enables decision-makers to consider various outcomes and prepare strategic responses, thus moving from theoretical risk assessments to practical, actionable plans.

Contingency planning complements this approach by developing specific, detailed plans for maintaining operations in the face of cyber incidents. It focuses on resilience and recovery, ensuring an organization can function and quickly return to normal operations after an attack [67]. The synergy between threat modeling, which identifies and assesses risks, and contingency planning, which prepares for the impact of those risks, creates a comprehensive framework for cybersecurity [64]. The benefits of integrating these methodologies are significant. Together, they offer a holistic view of cybersecurity, encompassing prevention, detection, response, and recovery [65]. This integrated approach ensures that organizations are prepared for known threats and resilient to unforeseen challenges, enhancing their overall cybersecurity posture. Additionally, by aligning these strategies, organizations can optimize their resource allocation, focusing on mitigating high-priority risks and ensuring business continuity [66].

However, implementing such synergistic approaches is not without challenges. It requires a significant investment in time and resources and a cultural shift towards continuous improvement and cross-departmental collaboration. Organizations must navigate complexities related to technology integration, staff training, and the management of an ever-changing threat landscape, as some studies argue that the dynamic nature of cyber threats makes it difficult to fully anticipate and plan for all eventualities, potentially leading to a false sense of security or resource misallocation in addition to questions about the scalability of such integrated approaches for smaller organizations with limited cybersecurity budgets [67][68][69]. Despite these challenges, the consensus among cybersecurity experts is that the benefits of integrating threat and risk modeling with scenario and contingency planning far outweigh the potential drawbacks [70. Emerging trends suggest an increasing recognition of the value of this synergistic approach, particularly as cyber threats evolve in complexity and impact [71].

The integration of threat and risk modeling with scenario and contingency planning fundamentally transforms the cybersecurity posture of healthcare organizations by systematically identifying and assessing potential vulnerabilities and threats, enabling healthcare providers to prioritize their cybersecurity efforts and focusing on the most significant risks to their operations and patient data [65]. For instance, threat modeling techniques like STRIDE or the FAIR model offer structured methodologies for understanding and quantifying cyber risks [64]. Combined with scenario planning, these

models enable healthcare organizations to simulate various cyberattack scenarios, assessing their potential impact on critical healthcare services and patient safety [54].

Furthermore, the integration of threat and risk modeling with scenario and contingency planning plays a pivotal role in achieving operational resilience in healthcare is about maintaining the continuity of care even in the face of cyber incidents[68]. Scenario planning, in particular, prepares healthcare organizations for various potential disruptions, from data breaches that compromise patient privacy to ransomware attacks that lock access to critical health systems [54]. By envisioning these scenarios in advance, healthcare providers can develop contingency plans that outline specific steps for maintaining or quickly restoring healthcare services.

3. Methods

The study adopts a quantitative approach, employing a survey method to collect data crucial for understanding the integration of advanced threat and risk modeling with scenario and contingency planning in enhancing security and resilience within healthcare organizations. The research instrument was a structured questionnairecomprising closed-ended questions, utilizing a Likert scale to facilitate the quantification of respondents' attitudes and perceptions towards various cybersecurity-related statements in healthcare settings.A total of 452 healthcare practitioners successfully participated in this study, recruited using a convenience sampling technique, enabling access to a diverse pool of staff from various healthcare organizations and other relevant participants. Data analysis was conducted using Partial Least Squares Structural Equation Modeling (PLS-SEM) for hypothesis testing

4. Result

Table 1: Measurement Model Analysis (Convergent Validity)

Constructs	Indicators	Item Loadings	Item Communality	Cronbach's Alpha	Composite Reliability	AVE
Advanced Threat Modeling (ATM)	ATM1	0.83	0.69	0.88	0.90	0.65

	ATM2	0.81	0.66			
	ATM3	0.85	0.72			
Scenario Planning (SP)	SP1	0.82	0.67	0.87	0.89	0.64
	SP2	0.80	0.64			
	SP3	0.84	0.71			
Cybersecurity Posture (CSP)	CSP1	0.86	0.74	0.91	0.93	0.68
	CSP2	0.88	0.77			
	CSP3	0.85	0.72			

The results from the Measurement Model Analysis focusing on Convergent Validity (Table 1) reveal that the constructs of Advanced Threat Modeling (ATM), Scenario Planning (SP), and Cybersecurity Posture (CSP) exhibit strong validity within the study. The item loadings for the indicators of each construct demonstrate robust associations, with all loadings exceeding the threshold of 0.8, except for two indicators (ATM2 and SP2) still show substantial loadings at 0.81 a and 0.80, respectively. These item loadings suggest a strong relationship between the indicators and their respective constructs, affirming the relevance of the items in measuring the constructs effectively. Also, the item communalities, which reflect the variance captured by the constructs from the indicators, are well above the acceptable limit of 0.5 for all indicators, indicating that the constructs explain a significant portion of the variance in the indicators. Cronbach's Alpha values for Advanced Threat Modeling, Scenario Planning, and Cybersecurity Posture are 0.88, 0.87, and 0.91, respectively, surpassing the recommended threshold of 0.7. These high values denote excellent internal consistency within the constructs, ensuring the indicators reliably measure the constructs.Similarly, the Composite Reliability scores for all constructs exceed the 0.7 benchmark, with scores of 0.90 for ATM, 0.89 for SP, and 0.93 for CSP. These scores further corroborate the internal consistency and the reliability of the constructs within the study.The Average Variance Extracted (AVE) values for ATM, SP, and CSP are 0.65, 0.64, and 0.68, all of which meet the minimum requirement of 0.5. These AVE values indicate that a majority of the

variance in the indicators is accounted for by their respective constructs, underscoring the constructs' convergent validity.

Table 2: Discriminant Validity (Fornell-Larcker Criterion)

Constructs	ATM	SP	CSP
Advanced Threat Modeling	0.65	-	-
Scenario Planning	0.30	0.64	-
Cybersecurity Posture	0.45	0.50	0.68

The diagonal elements of the table represent the Average Variance Extracted (AVE) for each construct, which are 0.65 for ATM, 0.64 for SP, and 0.68 for CSP. These AVE values are crucial as they must be greater than the used correlation estimates (off-diagonal elements) between the constructs to satisfy the Fornell-Larcker criterion for discriminant validity. This criterion ensures that a construct is more strongly correlated with its indicators than other model constructs.The off-diagonal elements indicate the squared correlations between the constructs. For instance, the squared correlation between ATM and SP is 0.30, between ATM and CSP is 0.45, and between SP and CSP is 0.50. Comparing these squared correlation values with the AVE values on the diagonal, it is evident that for each construct, the AVE is greater than the squared correlations with the other constructs. For example, the AVE for ATM (0.65) is more significant than its squared correlations with SP (0.30) and CSP (0.45), and the same pattern holds for the other constructs.This pattern confirms that the constructs exhibit discriminant validity, indicating that each construct captures phenomena distinct from those captured by the different constructs in the study. In simpler terms, the constructs of Advanced Threat Modeling, Scenario Planning, and Cybersecurity Posture are sufficiently unique from each other, suggesting that the questionnaire items associated with each construct measure distinct dimensions as intended. The results thus affirm the model's integrity, ensuring that the constructs are internally consistent (as shown by convergent validity) anddifferent, reinforcing the validity of the study's theoretical framework.

Table 3: Discriminant Validity (HTMT Ratio)

Constructs	ATM	SP	CSP
Advanced Threat Modeling	-	0.40	0.45

Scenario Planning	0.40	-	0.55
Cybersecurity Posture	0.45	0.55	-

The HTMT ratios reported between ATM and SP, ATM and CSP, and SP and CSP are 0.40, 0.45, and 0.55, respectively. All these values are substantially below the threshold of 0.85, suggesting that each pair of constructs is sufficiently distinct. Specifically, The HTMT ratio between Advanced Threat Modeling (ATM) and Scenario Planning (SP) is 0.40, indicating that the shared variance between these constructs is low compared to the individually explained by the constructs. This low ratio supports the distinctness of ATM from SP. Similarly, the HTMT ratio between Advanced Threat Modeling (ATM) and Cybersecurity Posture (CSP) is 0.45. This further underscores the discriminant validity, suggesting that ATM and CSP measure different underlying phenomena. The HTMT ratio between Scenario Planning (SP) and Cybersecurity Posture (CSP) is 0.55. Although higher than the ratios involving ATM, it remains well below the 0.85 cutoff, reinforcing the conclusion that SP and CSP are distinct constructs.These HTMT ratios collectively affirm the discriminant validity of the constructs within the study, as measured by the Heterotrait-Monotrait Ratio of correlations. The distinctiveness of these constructs suggests that the questionnaire items associated with each construct accurately reflect different dimensions of the investigated theoretical framework. The clear differentiation between the constructs validates the model's structure and supports the integrity of the theoretical underpinnings of the research.

Table 4: Structural Model Analysis Results

Path	Path Coefficient (β)	t-Test	p-Value	95% Confidence Interval	
				Lower	Upper
ATM -> CSP	0.42	6.30	<0.001	0.32	0.52
SP -> CSP	0.38	5.90	<0.001	0.28	0.48
CSP -> Organizational Resilience	0.65	9.50	<0.001	0.55	0.75

ATM -> Organizational Resilience (indirect via CSP)	0.27	4.50	<0.001	0.17	0.37
SP -> Organizational Resilience (indirect via CSP)	0.25	4.20	<0.001	0.15	0.35

The Structural Model Analysis results (Table 4) reveal a significant positive relationship between Advanced Threat Modeling (ATM) and Cybersecurity Posture (CSP), with a path coefficient (β) of 0.42, a t-test value of 6.30, and a p-value of less than 0.001. The 95% confidence interval for this relationship ranges from 0.32 to 0.52, indicating a strong and positive effect of ATM on improving the CSP of healthcare organizations.Similarly, Scenario Planning (SP) exhibits a significant positive impact on Cybersecurity Posture (CSP), as evidenced by a path coefficient of 0.38, a t-test value of 5.90, and a p-value of less than 0.001. The 95% confidence interval for this path ranges from 0.28 to 0.48, further supporting the impactful role of SP in enhancing CSP.

The relationship between Cybersecurity Posture (CSP) and Organizational Resilience is notably strong, with a path coefficient of 0.65, a t-test value of 9.50, and a p-value of less than 0.001. The confidence interval for this path ranges from 0.55 to 0.75, indicating that improvements in CSP significantly contribute to Organizational Resilience.Additionally, the analysis explores indirect effects on Organizational Resilience via Cybersecurity Posture. The indirect impact of Advanced Threat Modeling (ATM) on Organizational Resilience, mediated by CSP, is significant, with a path coefficient of 0.27, a t-test value of 4.50, and a p-value of less than 0.001. The confidence interval ranges from 0.17 to 0.37, suggesting that ATM contributes to Organizational Resilience by enhancing CSP.

Furthermore, Scenario Planning (SP) also shows a significant indirect effect on Organizational Resilience through CSP, with a path coefficient of 0.25, a t-test value of 4.20, and a p-value of less than 0.001. The confidence interval for this path is between 0.15 and 0.35, highlighting the importance of SP in contributing to Organizational Resilience indirectly by improving CSP.Overall, the Structural Model Analysis underscores the critical roles of Advanced Threat Modeling and Scenario Planning in enhancing the Cybersecurity Posture of healthcare organizations, which in turn significantly boosts Organizational Resilience. The direct and indirect pathways

examined in this model demonstrate the comprehensive impact of cybersecurity measures on organizational capabilities to resist, respond to, and recover from cyber threats, affirming the study's hypotheses and contributing valuable insights into integrating cybersecurity strategies for healthcare organizations.

5. **Discussion,**

In the analysis of hypothesis 1, the study found that healthcare organizations are increasingly integrating advanced cybersecurity measures, as indicated by the mean scores for integration status (4.20) and reasons for integration (3.95). These findings suggest a recognition within the sector of the need for a synergistic approach to cybersecurity, supporting the assertion by Tariq [5] about the digital revolution in healthcare necessitating enhanced security measures. The slight skewness and kurtosis values indicate a consensus among respondents but point to varying degrees of integration and rationale behind these strategies. This aligns with the literature suggesting that digital transformation in healthcare offers numerous benefits but introduces new vulnerabilities [6]. The results underscore the importance of a comprehensive cybersecurity strategy that integrates threat modeling and scenario planning, echoing the need for proactive measures instead of reactive responses [7][8].

In hypothesis 2, respondents reported high capabilities in identifying (4.25), assessing (4.30), and mitigating (4.40) risks. These scores and minimal deviation suggest a solid and consistent application of risk management practices within healthcare organizations. This finding corroborates the perspective that advanced threat and risk modeling techniques, such as STRIDE and the FAIR model, significantly enhance the accuracy and efficiency of cybersecurity efforts [9][10]. The positive skewness and near-zero kurtosis for these variables indicate a broadly shared view on the effectiveness of current risk management strategies. This supports and extends the existing literature by highlighting these methodologies' practical applications and benefits in healthcare [6][10].

In evaluating Hypothesis 3, The descriptive results reveal notable improvements in compliance enhancement (4.38), data protection (4.42), and incident response efficiency (4.35), suggesting that healthcare organizations are not only adhering to regulatory requirements but are also actively improving their cybersecurity postures. This reflects the growing recognition of the importance of robust information security management practices, as discussed in prior research [11][12]. The positive skewness and kurtosis values indicate a slight deviation among respondents, which may reflect differences in organizational resources and focus. Nonetheless, these findings align

with the argument that effective risk modeling and scenario planning contribute significantly to the resilience of healthcare systems against cyber threats [13][14].

In Hypothesis 4, the study's findings highlight the effectiveness (4.45) and efficiency (4.48) of digital crime investigations, particularly mobile forensics, within healthcare organizations. The positive mean scores and the skewness and kurtosis values suggest a high level of capability and a uniform approach among organizations in investigating and addressing digital crimes. This outcome supports the literature on the critical role of digital crime investigations in maintaining the integrity of healthcare systems and protecting patient data [15]. Moreover, it underscores the value of integrating advanced threat modeling and scenario planning into digital forensics processes to enhance investigatory outcomes [16].

Conclusion

The findings underscore the critical importance of adopting advanced threat and risk modeling techniques, such as STRIDE and the FAIR Risk Model, which have effectively identified, quantified, and prioritized cyber threats. Moreover, the integration of scenario and contingency planning has been proven to significantly improve strategic decision-making significantly, thereby enhancing organizational preparedness, response, and recovery capabilities in the face of cyber incidents. This integrated strategy addresses current cybersecurity challenges and anticipates potential future threats, ensuring that healthcare organizations can maintain continuity of care even amidst cyber disruptions.

Consent

As per international standards or university standards, Participants' written consent has been collected and preserved by the author(s).

Recommendations

Based on the insights gleaned from this research, the following recommendations are proposed for healthcare organizations seeking to enhance their cybersecurity measures:

1. Implement an Integrated Cybersecurity Strategy: Healthcare organizations should develop and adopt a comprehensive cybersecurity strategy integrating advanced threat and risk modeling with scenario and contingency planning. This

integrated approach is crucial for a proactive defense mechanism, enabling organizations to effectively anticipate, identify, and mitigate cyber threats.

2. Invest in Continuous Cybersecurity Education: Establish ongoing training programs for staff across all levels of the organization, focusing on the latest cybersecurity threats, defensive tactics, and best practices. Educating and empowering staff enhances the organization's collective cybersecurity awareness and preparedness.

3. Regular Cybersecurity Assessments and Updates: Conduct systematic and regular assessments of the organization's cybersecurity posture to identify vulnerabilities and evaluate the efficacy of existing security measures. Based on these assessments, update the cybersecurity strategies, technologies, and protocols to address evolving threats and organizational changes.

4. Foster Collaboration for Enhanced Cybersecurity Intelligence: Encourage collaboration and information sharing with external entities, such as other healthcare organizations, cybersecurity agencies, and government bodies. Leveraging shared intelligence about cyber threats and countermeasures can significantly strengthen individual organizations' and healthcare sectors' cybersecurity defenses.

References

[1] R. Winton, "Hollywood hospital pays $17,000 in bitcoin to hackers; FBI investigating,"*Los Angeles Times*, Feb. 18, 2016. https://www.latimes.com/business/technology/la-me-ln-hollywood-hospital-bitcoin-20160217-story.html

[2] C. Sienko, “Ransomware Case Studies: Hollywood Presbyterian & the Ottawa Hospital | Infosec,” *www.infosecinstitute.com*, Jun. 17, 2016. https://www.infosecinstitute.com/resources/healthcare-information-security/ransomware-case-studies-hollywood-presbyterian-the-ottawa-hospital/

[3] L. F. Freedman, “Hollywood Presbyterian Medical Center Hit by Ransomware and Pays Ransom to Restore EMR,” *Data Privacy + Cybersecurity Insider*, Feb. 18, 2016. https://www.dataprivacyandsecurityinsider.com/2016/02/hollywood-presbyterian-medical-center-hit-by-ransomware-and-pays-ransom-to-restore-emr/

[4] K. Stewart, “Hollywood Presbyterian Concedes to Hacker’s Demands in Ransomware Attack | Mintz,” *www.mintz.com*, Feb. 19, 2016.

https://www.mintz.com/insights-center/viewpoints/2016-02-19-hollywood-presbyterian-concedes-hackers-demands-ransomware (accessed Apr. 11, 2024).

[5] M. U. Tariq, “Revolutionizing Health Data Management With Blockchain Technology: Enhancing Security and Efficiency in a Digital Era,” *www.igi-global.com*, 2024. https://www.igi-global.com/chapter/revolutionizing-health-data-management-with-blockchain-technology/339350

[6] D. M. Javaid, Prof. A. Haleem, D. R. P. Singh, and D. R. Suman, “Towards insighting Cybersecurity for Healthcare domains: A comprehensive review of recent practices and trends,” *Cyber Security and Applications*, vol. 1, no. 100016, p. 100016, Mar. 2023, doi: https://doi.org/10.1016/j.csa.2023.100016

[7] S. O. Olabanji, Y. A. Marquis, C. S. Adigwe, A. S. Abidemi, T. O. Oladoyinbo, and O. O. Olaniyi, “AI-Driven Cloud Security: Examining the Impact of User Behavior Analysis on Threat Detection,” *Asian Journal of Research in Computer Science*, vol. 17, no. 3, pp. 57–74, Jan. 2024, doi: https://doi.org/10.9734/ajrcos/2024/v17i3424

[8] N. Sun *et al.*, “Cyber Threat Intelligence Mining for Proactive Cybersecurity Defense: A Survey and New Perspectives,” *IEEE Communications Surveys & Tutorials*, vol. 25, no. 2, pp. 1–1, 2023, doi: https://doi.org/10.1109/comst.2023.3273282

[9] A. T. Arigbabu, O. O. Olaniyi, C. S. Adigwe, O. O. Adebiyi, and S. A. Ajayi, “Data Governance in AI - Enabled Healthcare Systems: A Case of the Project Nightingale,” *Asian Journal of Research in Computer Science*, vol. 17, no. 5, pp. 85–107, 2024, doi: https://doi.org/10.9734/ajrcos/2024/v17i5441

[10] S. O. Olabanji, “AI for Identity and Access Management (IAM) in the Cloud: Exploring the Potential of Artificial Intelligence to Improve User Authentication, Authorization, and Access Control within Cloud-Based Systems,” *Asian Journal of Research in Computer Science*, vol. 17, no. 3, pp. 38–56, 2024, doi: https://doi.org/10.9734/ajrcos/2024/v17i3423

[11] R. Cerchione, P. Centobelli, E. Riccio, S. Abbate, and E. Oropallo, “Blockchain’s coming to hospital to digitalize healthcare services: Designing a distributed electronic health record ecosystem,” *Technovation*, vol. 120, no. 1, Feb. 2022, doi: https://doi.org/10.1016/j.technovation.2022.102480

[12] M. U. Tariq, “Enhancing Cybersecurity Protocols in Modern Healthcare Systems: Strategies and Best Practices,” *www.igi-global.com*, 2024. https://www.igi-global.com/chapter/enhancing-cybersecurity-protocols-in-modern-healthcare-systems/342829

[13] C. S. Adigwe, N. R. Mayeke, S. O. Olabanji, O. J. Okunleye, P. C. Joeaneke, and O. O. Olaniyi, “The Evolution of Terrorism in the Digital Age: Investigating the Adaptation of Terrorist Groups to Cyber Technologies for Recruitment, Propaganda, and Cyberattacks,” *Asian journal of economics, business and accounting*, vol. 24, no. 3, pp. 289–306, Feb. 2024, doi: https://doi.org/10.9734/ajeba/2024/v24i31287

[14] T. Suleski, M. Ahmed, W. Yang, and E. Wang, “A Review of multi-factor Authentication in the Internet of Healthcare Things,” *Digital Health*, vol. 9, no. 1, p. 205520762311771-205520762311771, Jan. 2023, doi: https://doi.org/10.1177/20552076231177144

[15] N. R. Mayeke, A. T. Arigbabu, O. O. Olaniyi, O. J. Okunleye, and C. S. Adigwe, “Evolving Access Control Paradigms: A Comprehensive Multi-Dimensional Analysis of Security Risks and System Assurance in Cyber Engineering. ,” vol. 17, no. 5, pp. 108–124, 2024, doi: https://doi.org/10.9734/ajrcos/2024/v17i5442

[16] B. Bhushan, A. Kumar, A. K. Agarwal, A. Kumar, P. Bhattacharya, and A. Kumar, “Towards a Secure and Sustainable Internet of Medical Things (IoMT): Requirements, Design Challenges, Security Techniques, and Future Trends,” *Sustainability*, vol. 15, no. 7, p. 6177, Jan. 2023, doi: https://doi.org/10.3390/su15076177

[17] S. F. Ahmed, M. S. B. Alam, S. Afrin, S. J. Rafa, N. Rafa, and A. H. Gandomi, “Insights into Internet of Medical Things (IoMT): Data fusion, security issues and potential solutions,” *Information Fusion*, vol. 102, no. 2, p. 102060, Sep. 2023, doi: https://doi.org/10.1016/j.inffus.2023.102060

[18] A. I. Abalaka, O. O. Olaniyi, and O. O. Adebiyi, “Understanding and Overcoming the Limitations to Strategy Execution in Hotels within the Small and Medium Enterprises Sector,” *Asian journal of economics, business and accounting*, vol. 23, no. 22, pp. 26–36, Oct. 2023, doi: https://doi.org/10.9734/ajeba/2023/v23i221134

[19] O. O. Olaniyi, C. U. Asonze, S. A. Ajayi, S. O. Olabanji, and C. S. Adigwe, “A Regressional Study on the Impact of Organizational Security Culture and Transformational Leadership on Social Engineering Awareness among Bank Employees: The Interplay of Security Education and Behavioral Change,” *Asian Journal of Economics, Business and Accounting*, vol. 23, no. 23, pp. 128–143, Dec. 2023, doi: https://doi.org/10.9734/ajeba/2023/v23i231176

[20] J. Menn, “After years of ransomware attacks, health-care defenses still fail,” *Washington Post*, Mar. 20, 2024. Available: https://www.washingtonpost.com/technology/2024/03/19/cybersecurity-healthcare-hack-solutions/

[21] R. Murray-Watson, “Healthcare data breach statistics,” *HIPAA Journal*, 2022. https://www.hipaajournal.com/healthcare-data-breach-statistics/

[22] U.S. Department of Health & Human Services, “Health Information Privacy,” *HHS.gov*, Jan. 04, 2019. https://www.hhs.gov/hipaa/index.html

[23] K. Sheikh, “Your Health Information Was Hacked. What Now?,” *The New York Times*, Dec. 07, 2023. Available: https://www.nytimes.com/article/health-data-breach.html

[24] American Hospital Association, “FDA Reports Potential Cybersecurity Risk with Insulin Pump System | AHA News,” *www.aha.org*, Sep. 20, 2022. https://www.aha.org/news/headline/2022-09-20-fda-reports-potential-cybersecurity-risk-insulin-pump-system

[25] D. A. S. George, D. T. Baskar, and D. P. B. Srikaanth, “Cyber Threats to Critical Infrastructure: Assessing Vulnerabilities Across Key Sectors,” *Partners Universal International Innovation Journal*, vol. 2, no. 1, pp. 51–75, Feb. 2024, doi: https://doi.org/10.5281/zenodo.10639463

[26] IBM, “Cost of a Data Breach 2023,” *IBM*, 2023. https://www.ibm.com/reports/data-breach

[27] Y. A. Marquis, T. O. Oladoyinbo, S. O. Olabanji, O. O. Olaniyi, and S. S. Ajayi, “Proliferation of AI Tools: A Multifaceted Evaluation of User Perceptions and Emerging Trend,” *Asian Journal of Advanced Research and Reports*, vol. 18, no. 1, pp. 30–35, Jan. 2024, doi: https://doi.org/10.9734/ajarr/2024/v18i1596

[28] O. O. Olaniyi, O. J. Okunleye, S. O. Olabanji, C. U. Asonze, and S. A. Ajayi, “IoT Security in the Era of Ubiquitous Computing: A Multidisciplinary Approach to Addressing Vulnerabilities and Promoting Resilience,” *Asian Journal of Research in Computer Science*, vol. 16, no. 4, pp. 354–371, Dec. 2023, doi: https://doi.org/10.9734/ajrcos/2023/v16i4397

[29] Deloitte, “Risk modeling,” *www.deloitte.com*, 2014. https://www.deloitte.com/global/en/services/risk-advisory/perspectives/risk-modeling.html

[30] RiskOptics, “What Is Cyber Risk Modeling?,” *RiskOptics*, Jul. 20, 2022. https://reciprocity.com/resources/what-is-cyber-risk-modeling/#:~:text=Cyber%20risk%20modeling%20involves%20creating,a%20risk%20does%20indeed%20strike

[31] MetricStream, “A Comprehensive Guide to Cyber Risk Quantification,” *Metricstream*, 2023. https://www.metricstream.com/learn/comprehensive-guide-to-cyber-risk-quantification.html

[32] K. Meinert, “Risk Modeling: What to Know about Risk Models,” *www.hni.com*, 2016. https://www.hni.com/blog/risk-modeling-what-to-know-about-risk-models#:~:text=Among%20assumptions%2C%20modeling%20also%20uses (accessed Apr. 06, 2024).

[33] H. Vallant, B. Stojanović, J. Božić, and K. Hofer-Schmitz, “Threat Modelling and Beyond-Novel Approaches to Cyber Secure the Smart Energy System,” *Applied Sciences*, vol. 11, no. 11, p. 5149, Jun. 2021, doi: https://doi.org/10.3390/app11115149

[34] K. Kostelić, “Dynamic Awareness and Strategic Adaptation in Cybersecurity: A Game-Theory Approach,” *Games*, vol. 15, no. 2, p. 13, Apr. 2024, doi: https://doi.org/10.3390/g15020013

[35] S. O. Olabanji, O. B. Oladoyinbo, C. U. Asonze, T. O. Oladoyinbo, S. A. Ajayi, and O. O. Olaniyi, “Effect of Adopting AI to Explore Big Data on Personally Identifiable Information (PII) for Financial and Economic Data Transformation,” *Asian journal of economics, business and accounting*, vol. 24, no. 4, pp. 106–125, Feb. 2024, doi: https://doi.org/10.9734/ajeba/2024/v24i41268

[36] Balbix, “FAIR Model for Risk Quantification - Pros and Cons,” *Balbix*, Sep. 20, 2022. https://www.balbix.com/insights/fair-model-for-risk-quantification-pros-and-cons/#:~:text=The%20FAIR%20model%20provides%20a

[37] S. O. Olabanji, T. O. Oladoyinbo, C. U. Asonze, C. S. Adigwe, O. J. Okunleye, and O. O. Olaniyi, “Leveraging FinTech Compliance to Mitigate Cryptocurrency Volatility for Secure US Employee Retirement Benefits: Bitcoin ETF Case Study,” *Asian journal of economics, business and accounting*, vol. 24, no. 4, pp. 147–167, Feb. 2024, doi: https://doi.org/10.9734/ajeba/2024/v24i41270

[38] I. Crespo, P. Kumar, P. Noteboom, and M. Taymans, “The evolution of model risk management | McKinsey,” *www.mckinsey.com*, Feb. 10, 2017. https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-evolution-of-model-risk-management#/ (accessed Apr. 06, 2024).

[39] C. S. Adigwe, O. O. Olaniyi, O. O. Olagbaju, and F. G. Olaniyi, “Leading in a Time of Crisis: The Coronavirus Effect on Leadership in America,” *Asian journal of*

economics, business and accounting, vol. 24, no. 4, pp. 1–20, Feb. 2024, doi: https://doi.org/10.9734/ajeba/2024/v24i41261

[40] A. Margherita and M. Heikkila, “Business Continuity in the COVID-19 Emergency: A Framework of Actions Undertaken by World-Leading Companies,” *Business Horizons*, vol. 64, no. 5, Feb. 2021, doi: https://doi.org/10.1016/j.bushor.2021.02.020

[41] O. O. Olaniyi, O. J. Okunleye, and S. O. Olabanji, “Advancing Data-Driven Decision-Making in Smart Cities through Big Data Analytics: A Comprehensive Review of Existing Literature,” *Current Journal of Applied Science and Technology*, vol. 42, no. 25, pp. 10–18, Aug. 2023, doi: https://doi.org/10.9734/cjast/2023/v42i254181

[42] N. shevchenko, “Threat Modeling: 12 Available Methods,” *SEI Blog*, Dec. 03, 2018. https://insights.sei.cmu.edu/blog/threat-modeling-12-available-methods

[43] N. Shevchenko, T. Chick, P. O'riordan, T. Scanlon, and C. Woody, “THREAT MODELING: A SUMMARY OF AVAILABLE METHODS,” 2018. Available: https://resources.sei.cmu.edu/asset_files/WhitePaper/2018_019_001_524597.pdf

[44] HHS, “Threat Modeling for Mobile Health Systems,” 2020. Available: https://www.hhs.gov/sites/default/files/threat-modeling-mobile-health-systems.pdf

[45] O. O. Olaniyi, N. Shah, and N. Bahuguna, “Quantitative Analysis and Comparative Review of Dividend Policy Dynamics within the Banking Sector: Insights from Global and U.S. Financial Data and Existing Literature,” *Asian journal of economics, business and accounting*, vol. 23, no. 23, pp. 179–199, Dec. 2023, doi: https://doi.org/10.9734/ajeba/2023/v23i231180

[46] McKinsey, “Cybersecurity in banking: A risk-based approach | McKinsey,” *www.mckinsey.com*, Aug. 25, 2022. https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/creating-a-technology-risk-and-cyber-risk-appetite-framework

[47] O. O. Adebiyi, S. O. Olabanji, and O. O. Olaniyi, “Promoting Inclusive Accounting Education through the Integration of Stem Principles for a Diverse Classroom,” *Asian journal of education and social studies*, vol. 49, no. 4, pp. 152–171, Dec. 2023, doi: https://doi.org/10.9734/ajess/2023/v49i41196

[48] T. O. Oladoyinbo, S. O. Olabanji, O. O. Olaniyi, O. O. Adebiyi, O. J. Okunleye, and A. I. Alao, “Exploring the Challenges of Artificial Intelligence in Data Integrity and its Influence on Social Dynamics,” *Asian Journal of Advanced Research and Reports*, vol. 18, no. 2, pp. 1–23, Jan. 2024, doi: https://doi.org/10.9734/ajarr/2024/v18i2601

[49] L. G. Wlosinski, “Understanding the Information System Contingency Plan,” *ISACA*, Sep. 22, 2022. https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2021/volume-30/understanding-the-information-system-contingency-plan

[50] L. Irwin, “Lincoln College Shuts down after 157 Years following Ransomware Attack,” *IT Governance USA Blog*, May 12, 2022. https://www.itgovernanceusa.com/blog/lincoln-college-shuts-down-after-157-years-following-ransomware-attack

[51] L. College, “Abraham Lincoln’s Namesake College Set to Close after 157 Years,” *Lincoln College*, 2022. https://lincolncollege.edu/home

[52] L. Winter, “Contingency Planning,” *Radiologic Technology*, vol. 93, no. 5, pp. 499–500, 2022, Available: https://pubmed.ncbi.nlm.nih.gov/35508409/

[53] O. O. Olaniyi, J. C. Ugonnia, F. G. Olaniyi, A. T. Arigbabu, and C. S. Adigwe, “Digital Collaborative Tools, Strategic Communication, and Social Capital: Unveiling the Impact of Digital Transformation on Organizational Dynamics,” *Asian Journal of Research in Computer Science*, vol. 17, no. 5, pp. 140–156, Mar. 2024, doi: https://doi.org/10.9734/ajrcos/2024/v17i5444

[54] S. Ford, “Contingency Planning vs. Scenario Planning,” *PM World Journal*, Jul. 2020. https://pmworldjournal.com/article/contingency-planning-vs-scenario-planning

[55] M. Swanson, P. Bowen, A. Phillips, D. Gallup, and D. Lynes, “Contingency Planning Guide for Federal Information Systems,” NIST, May 2010. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf

[56] O. O. Olaniyi, “Ballots and Padlocks: Building Digital Trust and Security in Democracy through Information Governance Strategies and Blockchain Technologies,” *Asian Journal of Research in Computer Science*, vol. 17, no. 5, pp. 172–189, Mar. 2024, doi: https://doi.org/10.9734/ajrcos/2024/v17i5447

[57] D. Luther and R. Ali, “Scenario Planning: Strategy, Steps and Practical Examples,” *Oracle NetSuite*, Aug. 25, 2022. https://www.netsuite.com/portal/resource/articles/financial-management/scenario-planning.shtml

[58] Indeed, “What Is Scenario Planning? (With Benefits and Examples),” *Indeed.com*, Oct. 12, 2022. https://sg.indeed.com/career-advice/career-development/scenario-planning

[59] R. F. Smallwood, *Information Governance: Concepts, Strategies and Best Practices, 2nd Edition* | *Wiley*. Hoboken, NJ: Wiley. Accessed: Apr. 06, 2024. [Online]. Available: https://www.wiley.com/en-in/Information+Governance%3A+Concepts%2C+Strategies+and+Best+Practices%2C+2nd+Edition-p-9781119491446

[60] H. Paananen, M. Lapke, and M. Siponen, "State of the art in information security policy development," *Computers & Security*, vol. 88, p. 101608, Jan. 2020, doi: https://doi.org/10.1016/j.cose.2019.101608

[61 E. E. Bayard, "The rise of cybercrime and the need for state cybersecurity regulations," *Rutgers Computer & Technology Law Journal*, vol. 45, no. 2, pp. 69–79, 2019, Accessed: Apr. 06, 2024. [Online]. Available: https://heinonline.org/HOL/SelectPage?handle=hein.journals/rutcomt45&collection=journals&page=69&lname=

[62] M. F. Safitra, M. Lubis, and H. Fakhrurroja, "Counterattacking Cyber Threats: A Framework for the Future of Cybersecurity," *Sustainability*, vol. 15, no. 18, p. 13369, Jan. 2023, doi: https://doi.org/10.3390/su151813369

[63] N. B. Ahmed, N. Daclin, M. Olivaux, and G. Dusserre, "Cybersecurity challenges for field hospitals: impacts of emergency cyberthreats during emergencies," *International Journal of Emergency Management*, vol. 18, no. 3, pp. 274–292, Jan. 2023, doi: https://doi.org/10.1504/ijem.2023.132387

[64] I. Ullah, G. de Roode, N. Meratnia, and P. Havinga, "Threat Modeling—How to Visualize Attacks on IOTA?," *Sensors*, vol. 21, no. 5, p. 1834, Mar. 2021, doi: https://doi.org/10.3390/s21051834

[65] B. Wells, "Threat Modeling in Healthcare," *Medium*, Mar. 14, 2022. https://wcwells.medium.com/threat-modeling-in-healthcare-3bf09d94f085

[66] Y. Li, Y. Yu, C. Lou, N. Guizani, and L. Wang, "Decentralized Public Key Infrastructures atop Blockchain," *IEEE Network*, vol. 34, no. 6, pp. 1–7, 2020, doi: https://doi.org/10.1109/mnet.011.2000085

[67] M. Burger, L. M. Smith, and J. Wood, "ProQuest | Better research, better learning, better insights.," *Openathens.net*, 2024. https://go.openathens.net/redirector/ualr.edu?url=https://www.proquest.com/trade-journals/recent-cybercrimes-cybersecurity-strategies/docview/2375474682/se-2 (accessed Apr. 06, 2024).

[68] K. Orru, M. Klaos, K. Nero, F. Gabel, S. Hansson, and T. Nævestad, “Imagining and assessing future risks: A dynamic scenario-base social vulnerability analysis framework for disaster planning and response,” *Journal of Contingencies and Crisis Management*, vol. 31, no. 4, Nov. 2022, doi: https://doi.org/10.1111/1468-5973.12436

[69] A. Al-Wathinani *et al.*, “Driving Sustainable Disaster Risk Reduction: a Rapid Review of the Policies and Strategies in Saudi Arabia,” *Sustainability*, vol. 15, no. 14, pp. 10976–10976, Jul. 2023, doi: https://doi.org/10.3390/su151410976

[70] M. Bao, H. Hui, Y. Ding, X. Sun, C. Zheng, and X. Gao, “An efficient framework for exploiting operational flexibility of load energy hubs in risk management of integrated electricity-gas systems,” *Applied Energy*, vol. 338, p. 120765, May 2023, doi: https://doi.org/10.1016/j.apenergy.2023.120765

[71] A. Puder, J. Henle, and E. Sax, “Threat Assessment and Risk Analysis (TARA) for Interoperable Medical Devices in the Operating Room Inspired by the Automotive Industry,” *Healthcare*, vol. 11, no. 6, p. 872, Mar. 2023, doi: https://doi.org/10.3390/healthcare11060872

Appendix

Sample Size: 452

Section 1: Respondent Demographics

1. Your Role in the Organization: (Please check one)
   - [ ] Executive
   - [ ] IT/Security Personnel
   - [ ] Risk Management Specialist
   - [ ] Healthcare Provider
   - [ ] Compliance Officer
   - [ ] Other (Please Specify): _____

2. Type of Healthcare Organization: (Please check one)
   - [ ] Hospital
   - [ ] Clinic
   - [ ] Research Facility
   - [ ] Other Healthcare Services (Please Specify): _____

3. Organization Size: (Please check one)
   - [ ] Small (1-100 employees)
   - [ ] Medium (101-500 employees)

- [ ] Large (>500 employees)

4. Years of Experience in Cybersecurity within Healthcare: (Please check one)
- [ ] Less than 1 year
- [ ] 1-5 years
- [ ] 6-10 years
- [ ] More than 10 years

5. Age Group: (Please check one)
- [ ] Under 25
- [ ] 25-34
- [ ] 35-44
- [ ] 45-54
- [ ] 55-64
- [ ] 65 or older

6. Gender: (Please check one)
- [ ] Male
- [ ] Female
- [ ] Non-binary/Third gender
- [ ] Prefer not to say
- [ ] Other (Please Specify): _____

Section 2: Cyber Threats Awareness and Impact

7. Rate your organization's awareness of cyber threats specific to the healthcare sector: (Please check one)
- [ ] Very Low
- [ ] Low
- [ ] Moderate
- [ ] High
- [ ] Very High

8. Identify and describe the most significant cyber threat your organization faced in the past year: (Open text)

9. Evaluate the impact of the identified threat on patient data and healthcare services: (Please check one)
- [ ] Negligible
- [ ] Moderate
- [ ] Significant
- [ ] Catastrophic

Section 3: Advanced Threat and Risk Modeling

10. Does your organization use advanced threat and risk modeling techniques? (Please check one)

- [ ] Yes
- [ ] No
- [ ] Planning to

11. Which techniques are employed? (Please check all that apply and specify any others)
- [ ] STRIDE
- [ ] FAIR Risk Model
- [ ] Other (Please specify): _____

12. Rate the effectiveness of these techniques in improving cyber threat identification and prioritization: (Please check one)
- [ ] Not Effective
- [ ] Somewhat Effective
- [ ] Effective
- [ ] Very Effective

Section 4: Scenario and Contingency Planning

13. Existence of scenario and contingency planning for cyber incidents: (Please check one)
- [ ] Yes
- [ ] No
- [ ] Under development

14. Frequency of plan updates: (Please check one)
- [ ] Annually
- [ ] Semi-annually
- [ ] Quarterly
- [ ] Other (Please specify): _____

15. Effectiveness of scenario and contingency planning in enhancing decision-making and operational resilience: (Please check one)
- [ ] Not Effective
- [ ] Somewhat Effective
- [ ] Effective
- [ ] Very Effective

Section 5: Integration and Overall Impact

16. Integration of advanced threat modeling with scenario and contingency planning: (Please check one)
- [ ] Fully integrated
- [ ] Partially integrated
- [ ] Not integrated

17. Impact of this integrated approach on cybersecurity posture and operational resilience: (Please check one)

- [ ] No Improvement
- [ ] Minor Improvement
- [ ] Moderate Improvement
- [ ] Significant Improvement