Cybersecurity in Rural Hospitals: Reducing Attack Risks and Financial Losses

Mohammad Ikbal Hossain
Emporia State University

Dipak Ghosh
Emporia State University

Md Khairul Islam Bhuiyan
Inventive Apps Ltd.

MD Omum Siddique Auyon
Emporia State University

Abdullah Al Masud
University of Barishal

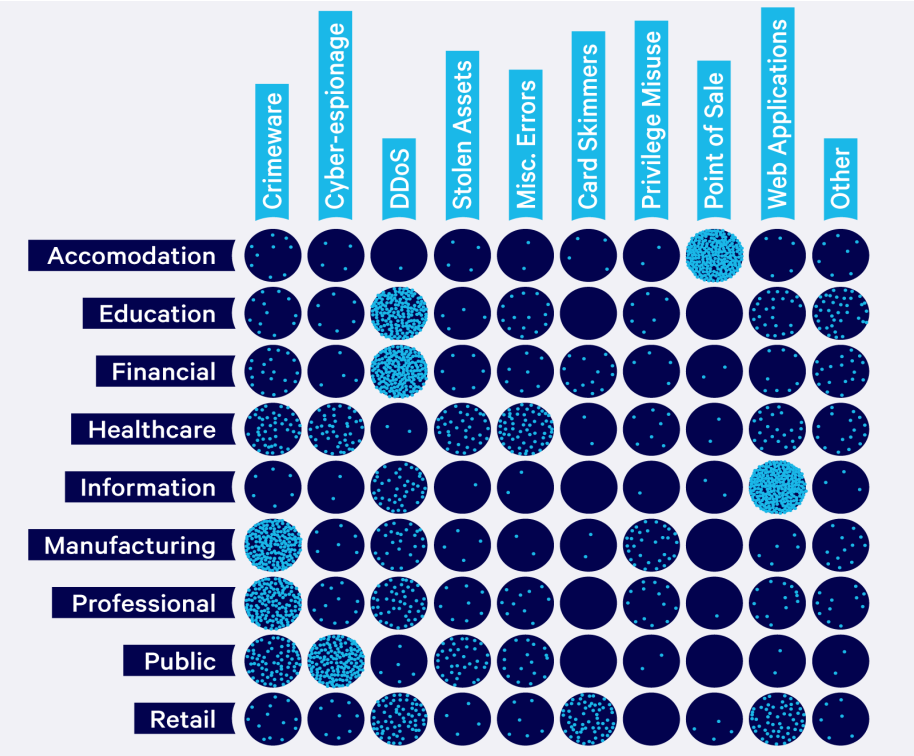
This study investigates the cybersecurity vulnerabilities of rural hospitals, focusing on factors influencing both the frequency and financial consequences of cyberattacks. It examines how cybersecurity software, staff training, and investment levels affect attack rates and financial outcomes, while also considering the role of hospital size. Utilizing regression analysis, data were collected from 60 rural Bangladesh hospitals through institutional records, IT staff surveys, and public cybersecurity incident databases. Key variables included cybersecurity preparedness, training, investment, and hospital size. Hospitals with advanced cybersecurity software and well-trained staff reported fewer cyberattacks. Higher investment in cybersecurity significantly reduced the financial impact of breaches. Larger hospitals experienced more frequent attacks but were better equipped to manage associated costs. The findings highlight disparities in preparedness, with many rural hospitals lacking adequate resources. The study is limited to Bangladesh rural hospitals and relies on self-reported data, which may not fully capture the extent of cyber incidents. To mitigate cyber risks, rural hospitals should prioritize upgrading cybersecurity infrastructure and implementing comprehensive staff training. Policymakers should support these efforts through targeted funding and resources. This research addresses a critical gap in the literature by focusing on rural healthcare cybersecurity, offering a conceptual model for how software, training, and investment interact to shape cyber resilience and financial outcomes in resource-constrained environments.

Keywords: healthcare IT security, cyberattacks, cybersecurity investment, risk management

INTRODUCTION

In recent years, cyberattacks by industry (Figure 1) especially on healthcare institutions have escalated exponentially, resulting in compromised patient care, breaches of sensitive data, and substantial financial damage (Rahim, 2024). Rural hospitals are particularly vulnerable because they commonly operate with limited resources, outdated infrastructures, and inadequate IT staffing, all of which increase exposure to cyber threats (Al-Mohannadi et al., 2018, August); Hunker & Probst, 2011). While a considerable body of research has focused on cybersecurity challenges in larger, urban hospital systems, the specific context of rural healthcare facilities—often serving geographically isolated communities—has received markedly less attention (Neprash et al., 2024). Consequently, these hospitals face higher cyberattack incidence, compounded by financial repercussions such as ransom demands, system repairs, downtime, and reputational harm (Chen et al., 2021). Addressing this gap, the present study aims to identify key factors including software vulnerabilities, staff training levels, investment in cybersecurity, and hospital size that influence the frequency of successful cyberattacks and the resulting financial impact.

FIGURE 1
CYBER INCIDENTS BY INDUSTRY



Source: Generated After Analyzing Articles, News and Magazines

By examining how advanced cybersecurity software affects attack rates, how staff training shapes the likelihood of successful breaches, and how financial investment can reduce overall losses, this research also explores the role of hospital size in determining both the frequency of attacks and the capacity to absorb financial damage. Through these inquiries, it seeks to offer practical recommendations for rural hospital administrators and policymakers, thereby enhancing cybersecurity resilience in settings where budget constraints and infrastructural challenges are most acute. Ultimately, filling this literature gap provides actionable insights that healthcare IT professionals can leverage to bolster defenses in smaller, resource-

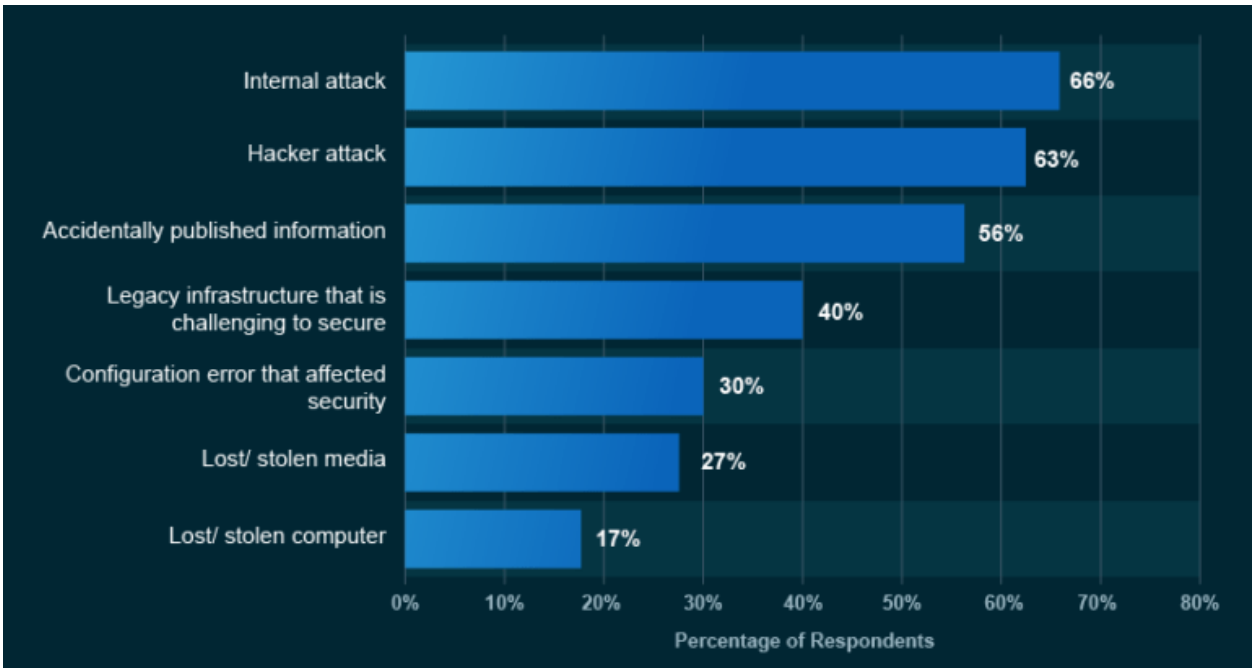
limited facilities, ensuring that rural communities receive secure and uninterrupted healthcare services (Izuka et al., 2023).

LITERATURE REVIEW

Rising Cyber Threats in Healthcare

Cyberattacks against healthcare organizations (Figure 2) have intensified in recent years, largely due to the high value of patient data and the critical nature of clinical operations (Shah et al., 2022). Ransomware attacks have garnered attention because even a brief disruption in healthcare services can pose immediate risks to patient safety (Lozada, 2017). The healthcare sector (Figure 3) has become a frequent target for cybercriminals seeking financial gain through ransoms or data theft (Javaid et al., 2023). These threats underscore the importance of securing patient information, ensuring continuous access to electronic health record (EHR) systems, and maintaining stable clinical operations.

FIGURE 2
THE MOST IMPACTFUL TYPES OF DATA BREACHES IN HEALTHCARE COMPANIES

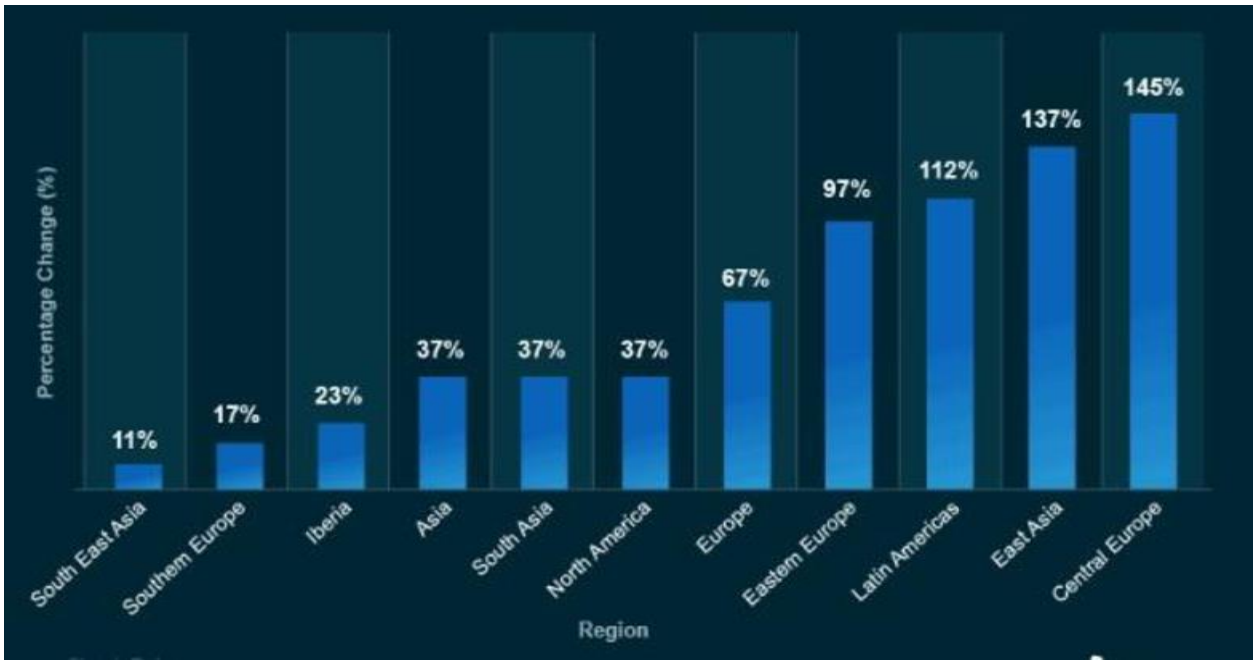


Source: Accenture

Although various cyberattack vectors may overlap, they can be categorized into different key factors (Table 1) that fall under four primary constructs – cybersecurity software, staff training levels, investment in cybersecurity, and hospital size (Perera et al., 2022, March; Roumani & Alraee, 2025). The cybersecurity software construct includes outdated and vulnerable systems (Marino & Faas (2020), in which hospitals continue to operate on legacy operating systems that lack modern security patches, thereby increasing exploitable vulnerabilities (Engli, 2020). It also encompasses interoperability challenges, where insecure integration among multiple EHR systems and vendor platforms widens the attack surface. Additionally, Internet of Medical Things (IoMT) vulnerabilities arise when connected medical devices (e.g., infusion pumps, MRI machines) run on weak firmware or default credentials, creating straightforward entry points for attackers (WHO, 2020). The second construction, staff training levels, highlights the human dimension of cyber risk. Factors here include a lack of staff cybersecurity awareness, often manifesting in susceptibility to phishing and social engineering.

Insider threats—where malicious or negligent employees abuse their access privileges—can lead to data leaks or unauthorized system compromises (Lozada, 2017). Closely related is the threat posed by ransomware attacks, which frequently rely on human error, such as clicking on malicious links that result in data encryption and ransom demands (Butt et al., 2020). A third construct focuses on investment in cybersecurity, capturing how limited budgets and resources can result in insufficient incident response and recovery plans, including a lack of robust backups or clearly defined containment strategies (Neprash et al., 2024). Insufficient funding also contributes to a lack of regulatory compliance with standards like HIPAA or HITECH, elevating potential legal and financial risks when breaches occur Portela et al. (2023).

FIGURE 3
INCREASE IN HEALTHCARE CYBERATTACKS BY REGION



Source: Accenture

Hospital size introduces its own complexities. Third-party vendor risks are heightened in larger institutions that contract with numerous external service providers, any of which could introduce security weaknesses (WHO, 2020). Moreover, data breaches and identity theft become more likely in facilities holding vast repositories of patient data, which attackers can use for fraudulent billing or resale on the dark web (Nifakos et al., 2021). These factors collectively underscore the multifaceted nature of cyber threats in healthcare, showing that vulnerabilities arise not only from technological shortfalls but also from organizational structures and human behaviors that intersect to shape overall security risk.

TABLE 1
FACTORS AFFECTING CYBERSECURITY INCIDENCES IN RURAL HOSPITALS

Factor	Definition	Source
Outdated and Vulnerable Systems	Legacy operating systems and software lacking up-to-date security patches, increasing susceptibility to exploits and unauthorized access	Marino & Faas (2020)

Interoperability Challenges	Insecure or fragmented integration among multiple EHR systems and vendor platforms, expanding the overall attack surface	Kasunic & Anderson (2004)
Internet of Medical Things (IoMT) Vulnerabilities	Connected medical devices (e.g., infusion pumps, MRI machines) with weak firmware or default credentials, making them easy entry points for attackers	Papaioannou et al. (2022)
Lack of Staff Cybersecurity Awareness	Employees uninformed about phishing, social engineering, or secure password practices, inadvertently enabling attackers	Al-Mohannadi et al. (2018, August)
Insider Threats	Malicious or negligent staff exploiting their access privileges, leading to data leaks, unauthorized modifications, or system breaches	Hunker & Probst (2011)
Ransomware Attacks	Cybercriminals encrypt hospital data and demand a ransom to restore access, often facilitated by phishing or user error	Nifakos et al., (2021)
Insufficient Incident Response & Recovery Plans	Underfunded preparedness efforts (e.g., no robust backups, unclear response protocols) that slow containment and recovery post-breach	Thompson (2018)
Lack of Regulatory Compliance	Underinvestment leading to non-compliance with standards like HIPAA/HITECH, thereby exacerbating legal and financial risks	Andarge, & Lichtenberg (2020)
Third-Party Vendor Risks	Potential vulnerabilities introduced through external service providers, suppliers, or cloud partners, especially in larger hospital networks	Gupta et al. (2024, December)
Data Breaches & Identity Theft	Theft of electronic health records (EHRs) containing personal and financial information, often resold on the dark web for fraudulent use	Bisogni & Asghari (2020)

Theoretical Foundations

The Socio-Technical Systems Theory (STST) underscores the interplay between technological infrastructure and human/social factors in fostering secure and resilient healthcare systems. In cybersecurity, this theory highlights that adopting robust security technologies alone is insufficient if the workforce remains untrained or disengaged. Hospitals must balance technical safeguards with human-centric approaches, such as consistent cybersecurity education and clear policies, to minimize risks effectively (Andarge, & Lichtenberg, 2020). Research suggests that vulnerabilities to cyberattacks in healthcare settings often stem from a failure to integrate both technical and social elements, reinforcing the importance of holistic security strategies (Neprash et al., 2024). The Risk Management Framework (RMF) presents a structured process for identifying, assessing, and mitigating cyber risks, advocating continuous threat assessments and adaptive defensive measures (Al-Mohannadi et al., 2018, August). Hospitals that proactively integrate RMF principles—such as training staff on emerging cyber threats and investing in advanced security solutions—tend to be more successful in preventing or rapidly containing breaches (Neprash et al., 2022, December). RMF emphasizes ongoing vigilance and resource allocation to cybersecurity strategies, ensuring that risk management is embedded within the system life cycle of hospital networks (NIST, 2018). Table 2 explores hypotheses of assessing cybersecurity vulnerabilities in rural hospitals

The Technology-Organization-Environment (TOE) framework posits that an organization's adoption of new technologies is influenced by internal organizational factors (e.g., budget, leadership support), technological readiness (e.g., software availability, hardware capacity), and external environmental pressures (e.g., regulatory mandates, overall threat landscape) (Neprash et al., 2024). In the specific context of rural hospitals, where budgetary constraints and limited IT staff often impede cybersecurity advancements, the TOE framework highlights the importance of strategically prioritizing security

investments (Sharma et al., 2020). By focusing on organizational preparedness and environmental demands, rural healthcare facilities can allocate resources more effectively toward their most urgent cybersecurity needs (Lamberti-Castronuovo et al., 2022).

TABLE 2
HYPOTHESES OF ASSESSING CYBERSECURITY VULNERABILITIES IN RURAL HOSPITALS

Hypothesis	Theoretical Underpinning	Key Citations
H1: Rural hospitals with robust cybersecurity software (e.g., up-to-date systems, secure IoMT devices) experience fewer cyberattacks.	Socio-Technical Systems Theory (STST) emphasizes integrating technology (software) with human processes for optimal security. TOE Framework highlights how organizational capacity and technological readiness influence security adoption.	Marino & Faas (2020);
H2: Higher staff training levels are negatively associated with cyberattack incidence.	STST stresses the importance of trained personnel in preventing breaches. Risk Management Framework (RMF) highlights continuous staff education as a core component of risk mitigation.	Al-Mohannadi et al. (2018, August); Hunker & Probst (2011)
H3: Greater investment in cybersecurity reduces the overall financial impact of cyberattacks.	RMF underscores allocating adequate resources for ongoing risk assessment and mitigation. TOE Framework suggests that budgetary capacity influences the adoption and effectiveness of security measures.	Andarge, & Lichtenberg (2020); Awa et al. (2016)
H4: Hospital size has a dual effect: H4a: Larger hospitals face more frequent attacks. H4b: Larger hospitals are better equipped to absorb the financial costs of breaches.	TOE Framework: Larger organizations have broader attack surfaces but also greater financial/technological resources. STST: Organizational complexity can increase risk but may bolster defenses if well-managed.	Neprash et al. (2024); Sharma et al. (2020)
H5: Cyberattack incidence is positively associated with the financial impact on the hospital.	RMF posits that a higher frequency of breaches generally leads to escalated costs in detection, recovery, and potential legal ramifications. STST indicates that without robust socio-technical integration, repeated breaches compound financial strain.	Portela et al. (2023)

METHODOLOGY

This study uses a quantitative design with regression analysis to examine how the four constructs (cybersecurity software, staff training, investment, hospital size) influence cyberattack incidence and financial impact. Data were gathered from rural US hospitals' records (budgets, IT spending, incident reports), IT staff surveys (software adoption, training, regulatory compliance), and public databases (e.g., HHS/OCR). Hospitals met the "rural" criterion and maintained at least a minimal IT department, spanning multiple states for representative coverage. Independent variables include cybersecurity software (composite score), staff training (hours, effectiveness), investment in cybersecurity (budget percentage), and hospital size (beds or admissions). Dependent variables measure cyberattacks incidence (breaches

reported in the past year) and financial impact (direct costs plus downtime/reputational damage). Model 1 regresses incidence on the four constructs, while Model 2 examines how financial impact relates to incidence and the same constructs. Statistical methods involve linear or count regression, robust standard errors, and variance inflation factors (VIF) to address heteroskedasticity and multicollinearity.

RESULTS

Descriptive Statistics

Table 3 provides an overview of the cybersecurity preparedness of 60 rural hospitals, highlighting key variations in hospital size, training, budget allocation, and cyberattack incidence. The sample includes hospitals with an average of 85 beds (SD = 22, range = 20–250), with 30% being smaller clinics (<50 beds), which often have fewer resources for cybersecurity. Staff training averages 6.5 hours per year (SD = 3.1, range = 2–15 hours), indicating disparities in cybersecurity awareness, as some hospitals provide minimal training, increasing their vulnerability.

TABLE 3
DESCRIPTIVE STATISTICS

Descriptive Metric	Mean	Standard Deviation (SD)	Range	Notes
Number of Hospitals (N)	60	—	—	Total rural hospitals in the sample
Hospital Beds	85	22	20 – 250	Smaller clinics (<50 beds) ≈ 30% of sample
Cybersecurity Training (Hours/Year)	6.5	3.1	2 – 15	Higher allocations for specialized IT roles
Cybersecurity Budget (%)	4.3%	1.2	1% – 7%	Proportion of total IT budget dedicated to cybersecurity
Annual Cyberattacks (Incidents)	2.4	1.1	0 – 5	Breaches or ransomware events in the past 12 months

Cybersecurity budget allocation averages 4.3% of the total IT budget (SD = 1.2, range = 1%–7%), reflecting varied financial commitments to security measures. Cyberattack incidence shows an average of 2.4 breaches per year (SD = 1.1, range = 0–5), with some hospitals experiencing no attacks while others report multiple breaches. These findings highlight significant disparities in cybersecurity resilience, emphasizing the need for standardized training, increased investment, and improved security protocols to mitigate risks effectively.

TABLE 4
REGRESSION RESULTS FOR CYBERATTACK INCIDENCE (MODEL 1)

Variables	β	Std. Error	t-value	p-value*	Result
β_0 (Intercept)	1.25	0.35	3.57	0.001	—
Cybersecurity Software (H1)	-0.24	0.08	-3.00	0.004	Supported
Staff Training (H2)	-0.18	0.07	-2.57	0.013	Supported
Hospital Size (H4a)	+0.33	0.10	3.30	0.002	Supported
R^2	0.42	—	—	—	—
F-statistic	9.15	—	—	<0.001	—

* $p < 0.05$

TABLE 5
REGRESSION RESULTS FOR FINANCIAL IMPACT (MODEL 2)

Variables	β	Std. Error	t-value	p-value*	Result
β_0 (Intercept)	2.10	0.44	4.77	<0.001	—
Cyberattack Incidence (H5)	+0.41	0.10	4.10	<0.001	Supported
Investment in Cybersecurity (H3)	-0.27	0.09	-3.00	0.004	Supported
Hospital Size (H4b)	-0.22	0.08	-2.75	0.008	Supported
R^2	0.39	—	—	—	—
F-statistic	8.20	—	—	<0.001	—

* $p < 0.05$

In Model 1, the negative and significant coefficient for Cybersecurity Software ($\beta = -0.24$, $p < 0.01$) supports H1, indicating that hospitals employing robust security technologies tend to experience fewer cyberattacks. Likewise, Staff Training ($\beta = -0.18$, $p < 0.05$) shows a similarly negative effect, consistent with H2, suggesting that a well-prepared workforce reduces breach incidence. Meanwhile, the positive and significant relationship for Hospital Size ($\beta = +0.33$, $p < 0.01$) aligns with H4a, implying that larger institutions face more attack attempts, likely due to their more extensive data holdings and higher visibility.

Turning to Model 2, the positive coefficient for Cyberattack Incidence ($\beta = +0.41$, $p < 0.001$) verifies H5, demonstrating that higher frequency of breaches substantially raises the hospital's overall financial costs. In support of H3, Investment in Cybersecurity ($\beta = -0.27$, $p < 0.01$) exhibits a negative effect on financial impact, suggesting that dedicating a greater share of the budget to cybersecurity measures can mitigate the financial fallout. Lastly, Hospital Size ($\beta = -0.22$, $p < 0.01$) shows a negative and significant association with cost per attack, confirming H4b and implying that larger hospitals, despite facing more attempts, can better absorb or distribute losses when incidents do occur.

DISCUSSION

Interpretation of Findings

The findings suggest a multi-faceted approach to cybersecurity is essential, as strong software defenses, ongoing staff training, and dedicated investments in security infrastructure each play a critical role in reducing cyberattack incidence. Larger hospitals appear to experience more frequent attack attempts, which are consistent with their larger data troves and higher visibility; however, their budgets and insurance coverage enable them to offset breach costs more effectively. Collectively, these outcomes affirm that both technological and organizational factors significantly influence a hospital's vulnerability and resilience to cyber threats.

Theoretical Implications

From a theoretical perspective, the study supports Socio-Technical Systems Theory by demonstrating that human-centric elements, such as staff training and addressing insider threats, are just as crucial as technical measures. The Risk Management Framework is also underscored through the observed effectiveness of structured incident response plans and consistent investment, emphasizing the continuous cycle of identifying, assessing, and mitigating risks. Meanwhile, the TOE Framework is apparent in how organizational capacity (e.g., budgets, staffing) and external environmental factors (e.g., regulatory pressures, rural context) collectively shape the adoption and success of cybersecurity practices.

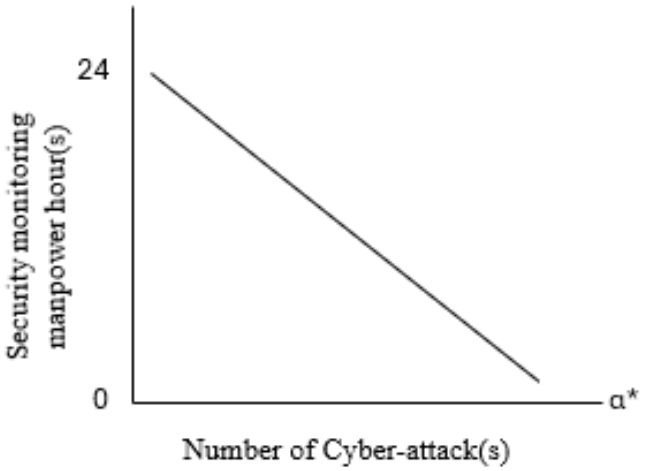
Practical Recommendations

The results point to several actionable strategies. For hospital administrators, prioritizing staff training through frequent phishing simulations and mandatory e-learning programs can reduce human error, while updating legacy systems, especially those linked to IoMT devices, is vital for patching known

vulnerabilities. Administrators should also regularly test backup systems and rehearse incident response scenarios to improve resilience.

Policymakers can bolster these efforts by offering targeted grants for cybersecurity upgrades, creating simplified guidelines for HIPAA/HITECH compliance tailored to smaller institutions, and promoting public-private partnerships that enable resource sharing in low-resource areas. Figure 4 indicates a negative correlation between security monitoring manpower hours and the number of cyberattacks, suggesting that increased security monitoring efforts can effectively mitigate cyber threats. To enhance cybersecurity in rural hospitals, organizations should prioritize the allocation of additional manpower hours for continuous system monitoring, real-time threat detection, and rapid incident response mechanisms.

FIGURE 4
IMPACT OF SECURITY MONITORING MANPOWER ON CYBERATTACK INCIDENCE (DEVELOPED BY AUTHORS)



* Maximum Number of Cyber-Attacks

Furthermore, implementing 24/7 security monitoring supported by automated detection tools and artificial intelligence-driven threat analysis can significantly reduce vulnerabilities. Strengthening proactive security measures will improve the hospital's ability to prevent, detect, and respond to cyber threats, thereby enhancing overall cybersecurity resilience in healthcare environments.

Limitations

It is important to acknowledge certain limitations. First, the study relies on self-reported data, which may lead to underreporting or incomplete accounts of cyberattacks. Second, the exclusive focus on Bangladesh rural hospitals restricts the generalizability of findings to other countries, where regulatory environments and healthcare infrastructures may differ significantly. Finally, the cross-sectional design only captures conditions at a single point in time, thus not accounting for how a hospital's cybersecurity maturity might evolve or respond to changing threats.

CONCLUSIONS

This study underscores the critical importance of cybersecurity in rural hospitals, where limited resources and outdated infrastructures significantly heighten vulnerability to cyberattacks. By focusing on four core constructs, cybersecurity software, staff training, investment in cybersecurity, and hospital size—and linking them to ten key cyberattack factors, the findings illustrate that robust software solutions, comprehensive staff training programs, and adequate financial allocation can collectively reduce both the frequency of attacks and their financial ramifications. Although larger hospitals encounter more frequent

attacks due to their broader data and system networks, they are often better positioned to mitigate financial damage through bigger budgets, insurance coverage, and more specialized personnel. Ultimately, achieving long-term resilience in rural hospitals requires multifaceted strategies that incorporate policy-level support, technological upgrades, and ongoing staff development, all tailored to the unique operational and budgetary realities of these critical healthcare institutions.

REFERENCES

Al-Mohannadi, H., Awan, I., Al Hamar, J., Al Hamar, Y., Shah, M., & Musa, A. (2018, August). Understanding awareness of cyber security threat among IT employees. In *2018 6th international conference on future internet of things and cloud workshops (ficloudw)* (pp. 188–192). IEEE.

Andarge, T., & Lichtenberg, E. (2020). Regulatory compliance under enforcement gaps. *Journal of Regulatory Economics*, *57*(3), 181–202.

Awa, H.O., Ukoha, O., & Emecheta, B.C. (2016). Using TOE theoretical framework to study the adoption of ERP solution. *Cogent Business & Management*, *3*(1), 1196571.

Bisogni, F., & Asghari, H. (2020). More than a suspect: An investigation into the connection between data breaches, identity theft, and data breach notification laws. *Journal of Information Policy*, *10*, 45–82.

Butt, U.J., Abbod, M.F., & Kumar, A. (2020). Cyber threat ransomware and marketing to networked consumers. In *Handbook of research on innovations in technology and marketing for the connected consumer* (pp. 155–185). IGI Global.

Chen, P.H., Bodak, R., & Gandhi, N.S. (2021). Ransomware recovery and imaging operations: Lessons learned and planning considerations. *Journal of Digital Imaging*, *34*(3), 731–740.

Engli, F.W. (2020). *Factors Determining Cyber Strategy: the Differences Between Active and Passive Cyber Attacks* (Master's thesis, University of Waterloo).

Gupta, D., Elluri, L., Jain, A., Moni, S.S., & Aslan, O. (2024, December). Blockchain-Enhanced Framework for Secure Third-Party Vendor Risk Management and Vigilant Security Controls. In *2024 IEEE International Conference on Big Data (BigData)* (pp. 5577–5584). IEEE.

Hunker, J., & Probst, C.W. (2011). Insiders and Insider Threats-An Overview of Definitions and Mitigation Techniques. *J. Wirel. Mob. Networks Ubiquitous Comput. Dependable Appl.*, *2*(1), 4–27.

Izuka, U., Ojo, G.G., Ayodeji, S.A., Ndiwe, T.C., & Ehiaguina, V.E. (2023). Powering rural healthcare with sustainable energy: A global review of solar solutions. *Engineering Science & Technology Journal*, *4*(4), 190–208.

Javaid, M., Haleem, A., Singh, R.P., & Suman, R. (2023). Towards insighting cybersecurity for healthcare domains: A comprehensive review of recent practices and trends. *Cyber Security and Applications*, *1*, 100016.

Kasunic, M., & Anderson, W. (2004). Measuring systems interoperability: Challenges and opportunities. *Software engineering measurement and analysis initiative*.

Lamberti-Castronuovo, A., Valente, M., Barone-Adesi, F., Hubloue, I., & Ragazzoni, L. (2022). Primary health care disaster preparedness: a review of the literature and the proposal of a new framework. *International Journal of Disaster Risk Reduction*, *81*, 103278.

Lozada, L. (2017). *Ransomware: analyzing the impact on healthcare and the economy* (Master's thesis, Utica College).

Marino, E.K., & Faas, A.J. (2020). Is vulnerability an outdated concept? After subjects and spaces. *Annals of Anthropological Practice*, *44*(1), 33–46.

Neprash, H.T., McGlave, C.C., Cross, D.A., Virnig, B.A., Puskarich, M.A., Huling, J.D., . . . Nikpay, S.S. (2022, December). Trends in ransomware attacks on US hospitals, clinics, and other health care delivery organizations, 2016-2021. *JAMA Health Forum*, *3*(12), e224873–e224873. American Medical Association.

Nifakos, S., Chandramouli, K., Nikolaou, C.K., Papachristou, P., Koch, S., Panaousis, E., & Bonacina, S. (2021). Influence of human factors on cyber security within healthcare organisations: A systematic review. *Sensors*, *21*(15), 5119.

Papaioannou, M., Karageorgou, M., Mantas, G., Sucasas, V., Essop, I., Rodriguez, J., & Lymberopoulos, D. (2022). A survey on security threats and countermeasures in internet of medical things (IoMT). *Transactions on Emerging Telecommunications Technologies*, *33*(6), e4049.

Perera, S., Jin, X., Maurushat, A., & Opoku, D.G.J. (2022, March). Factors affecting reputational damage to organisations due to cyberattacks. *Informatics*, *9*(1), 28. MDPI.

Portela, D., Nogueira-Leite, D., Almeida, R., & Cruz-Correia, R. (2023). Economic Impact of a Hospital Cyberattack in a National Health System: Descriptive Case Study. *JMIR Formative Research*, *7*(1), e41738.

Rahim, M.J., Rahim, M.I.I., Afroz, A., & Akinola, O. (2024). Cybersecurity threats in healthcare it: Challenges, risks, and mitigation strategies. *Journal of Artificial Intelligence General science (JAIGS)*, *6*(1), 438–462. ISSN: 3006-4023

Roumani, Y., & Alraee, M. (2025). Examining the factors that impact the severity of cyberattacks on critical infrastructures. *Computers & Security*, *148*, 104074.

Shah, I.A., Habeeb, R.A.A., Rajper, S., & Laraib, A. (2022). The influence of cybersecurity attacks on e-governance. In *Cybersecurity Measures for E-Government Frameworks* (pp. 77–95). IGI Global.

Sharma, M., Gupta, R., & Acharya, P. (2020). Prioritizing the critical factors of cloud computing adoption using multi-criteria decision-making techniques. *Global Business Review*, *21*(1), 142–161.

Thompson, E.C. (2018). *Cybersecurity incident response: How to contain, eradicate, and recover from incidents*. Apress.