



RESEARCH ARTICLE

Crisis Leadership in the Aftermath of Healthcare Cyberattacks: Digital Forensics, Organizational Learning, and Patient Safety

Mercy Asaa Asiedu¹, Ernest Kobbie Doe², Jesse Kwaku Doe³

¹ Department of Management, Graduate School of Management, Abidjan, Ivory Coast

² School of Computing, University of Portsmouth, Portsmouth, United Kingdom

³ College of Health Sciences, University of Ghana, Legon, Ghana

ABSTRACT

Healthcare cyberattacks threaten not only digital infrastructure but also organizational continuity and patient safety. Although existing research has examined crisis leadership, digital forensics, organizational learning, and cyber resilience, these areas are often treated separately. This conceptual paper integrates these perspectives to explain how healthcare organizations can convert cyber incidents into opportunities for learning and resilience development. Drawing on literature from crisis leadership, cybersecurity, digital forensics, organizational learning, healthcare resilience, and patient safety, the paper develops a conceptual framework linking crisis leadership, digital forensic effectiveness, organizational learning, cyber resilience, and patient safety. Five propositions are advanced. The framework argues that effective crisis leadership supports digital forensic investigation, that forensic investigation strengthens organizational learning, and that leadership enhances the translation of forensic findings into organizational change. Organizational learning is subsequently proposed to strengthen cyber resilience, while greater resilience reduces cyber-related risks to patient safety. The paper contributes by repositioning digital forensics as a source of organizational knowledge, extending crisis leadership into the post-cyberattack healthcare context, and linking cyber resilience directly with patient safety. The framework provides a basis for future empirical testing and offers practical guidance for healthcare leaders seeking to improve post-incident learning, recovery, and organizational preparedness.

Keywords: Crisis Leadership, Healthcare Cyberattacks, Digital Forensics, Organizational Learning, Cyber Resilience, Patient Safety

1. Introduction and Background

Healthcare delivery is becoming more dependent on interconnected digital infrastructures, including electronic health records, laboratory information systems, diagnostic platforms, medication-management systems, and networked medical devices. This dependence has improved the speed and coordination of care, but it has also increased the consequences of cybersecurity incidents. Ransomware and related attacks can restrict access to clinical information, interrupt diagnostic and treatment workflows, divert patients, and place additional pressure on neighboring facilities. Empirical studies have shown that hospital ransomware incidents can disrupt emergency care, reduce patient volumes at affected hospitals, increase demand at nearby hospitals, and create substantial difficulties for healthcare professionals during recovery (Abouk & Powell, 2024; van Boven et al., 2024). Cybersecurity in

healthcare should therefore be understood not only as an information technology concern but also as an organizational and patient-safety problem.

The response to healthcare cyberattacks extends beyond technical containment. Leaders must make decisions under uncertainty, establish priorities for service continuity, coordinate clinical and technical teams, communicate with internal and external stakeholders, and guide the organization through recovery. Research on healthcare crisis management shows that effective crisis leadership involves both task-oriented and person-oriented behaviors and that leadership and management practices can support organizational resilience and performance during disruptive events (Atkinson et al., 2024; Yang et al., 2024). These responsibilities become particularly important in cyber crises because leaders must balance the restoration of digital systems with the immediate need to maintain safe clinical services.

Digital forensics provides an important link between incident response and organizational recovery. Post-incident investigation can establish what occurred, identify affected systems, determine contributing causes, preserve reliable evidence, and support corrective action. Contemporary cybersecurity guidance increasingly embeds investigation within broader incident-response and recovery processes. The National Institute of Standards and Technology (NIST) Cybersecurity Framework 2.0 emphasizes governance, response, and recovery, while NIST SP 800-61 Rev. 3 integrates incident response throughout organizational cybersecurity risk management and emphasizes effective detection, response, and recovery (Nelson et al., 2025; Pascoe et al., 2024). In healthcare, however, the value of digital forensics should not end with technical remediation or attribution. Evidence generated during an investigation can also provide an important basis for organizational learning.

Organizational learning is critical because recovery without learning may leave the underlying conditions that enabled an incident unchanged. Patterson et al. (2023) found that organizations often struggle to convert cybersecurity incidents into sustained learning. Common weaknesses include superficial causal investigations, limited participation in learning activities, poor implementation of lessons, and insufficient evaluation of whether corrective actions reduce subsequent risk. For healthcare organizations, these limitations have wider implications because recurrent cyber vulnerabilities can threaten service continuity, information integrity, and ultimately patient safety.

Despite growing research on healthcare cyberattacks, crisis leadership, incident response, and organizational learning, these streams remain insufficiently integrated. Existing studies commonly examine the operational consequences of cyberattacks, technical incident-response processes, or leadership during healthcare crises separately. Less attention has been given to how crisis leadership shapes the use of digital forensic evidence, how forensic findings are converted into organizational learning, and how such learning contributes to safer and more resilient healthcare delivery. The increasing recognition that cyber incidents can produce clinical and system-wide disruption strengthens the need for such an integrated perspective (Abouk & Powell, 2024; van Boven et al., 2024).

This paper addresses this gap by developing a conceptual framework linking *crisis leadership, digital forensic investigation, organizational learning, and patient safety* in the aftermath of healthcare cyberattacks. It argues that crisis leaders influence not only immediate response and recovery but also whether forensic knowledge is translated into structural, behavioral, and procedural change. By connecting leadership theory with cybersecurity incident investigation and healthcare safety, the paper seeks to explain how healthcare organizations can move beyond simply restoring disrupted systems towards learning from cyber incidents in ways that strengthen organizational resilience and protect patients.

2. Literature Review and Proposition Development

2.1 Crisis Leadership in Healthcare Organizations

Crisis leadership refers to the actions through which leaders prepare for, respond to, and learn from events that threaten organizational functioning. Crises differ from routine managerial problems because they combine urgency, uncertainty, resource pressure, and potentially severe consequences (Riggio & Newstead, 2023; Wu et al., 2021). In such settings, leaders must provide direction while coordinating multiple professional groups and adjusting decisions as new information becomes available. Recent work emphasizes that crisis leadership is not limited to the attributes of a single senior executive. It is also collective, contextual, and dynamic, requiring coordinated leadership across organizational levels (Nesse et al., 2024). In healthcare, this complexity is intensified because leadership decisions can directly affect continuity of care and patient outcomes.

Evidence from healthcare settings indicates that both task-oriented and person-oriented leadership behaviors are important during disruption. Yang et al. (2024) found that crisis leadership behaviors were positively associated with staff performance evaluation and commitment to sustaining change. Atkinson et al. (2024) similarly identified leadership and management practices that support resilience and organizational performance during crises. Communication, coordination, role clarity, psychological safety, and learning are therefore mechanisms through which organizations maintain functioning under pressure.

Cyberattacks create a particular leadership challenge because clinical, technical, legal, communication, and operational decisions must often be made simultaneously. Leaders must establish service priorities, coordinate cybersecurity and clinical teams, authorize contingency measures, and support recovery without compromising an investigation. Crisis leadership is therefore expected to influence the conditions under which digital forensic investigation can be conducted effectively. We therefore make the following proposition:

Proposition 1: *Effective crisis leadership positively influences the effectiveness of digital forensic investigation after healthcare cyberattacks.*

2.2 Healthcare Cyberattacks as Organizational Crises

Healthcare cyberattacks should not be treated solely as information technology failures. Digital systems are embedded in clinical work, medication management, diagnostics, scheduling, communication, and access to patient records. Ewoh & Vartiainen (2024) describe healthcare cybersecurity as a sociotechnical problem involving technology, people, and organizational processes. This perspective is important because disruption to one digital component can propagate across clinical and administrative functions. Empirical evidence shows that ransomware attacks can alter healthcare delivery beyond the compromised network. Van Boven et al. (2024) documented major operational difficulties during hospital ransomware incidents. Abouk & Powell (2024) found decreases in emergency department visits and inpatient admissions in attacked hospitals, alongside temporary increases in emergency department activity at nearby hospitals. Cyberattacks therefore display the characteristics of organizational crises because they generate uncertainty, time pressure, disrupted routines, and potential harm.

Recognizing cyberattacks as organizational crises expands responsibility beyond technical specialists. Senior and clinical leaders become responsible for continuity of care, escalation, communication, resource allocation, and restoration priorities. The quality of these decisions may shape both the effectiveness of the investigation and the organization's capacity to learn from the event.

2.3 Digital Forensics and Post-Incident Investigation

Digital forensics provides the processes through which digital evidence is identified, preserved, examined, and interpreted following an incident. In healthcare, forensic investigation can help reconstruct attack pathways, establish affected systems and data, identify weaknesses in controls, and support legal, regulatory, and organizational responses. Forensic readiness is especially important because evidence may be lost if appropriate logging, preservation, access controls, and procedures are not established before an incident. Chernyshev et al. (2019) argued that healthcare investigations can be constrained by insufficient forensic readiness, while Elyas et al. (2015) showed that readiness depends on coordinated organizational, procedural, and technical capabilities.

Current cybersecurity guidance also situates investigation within wider risk management. NIST SP 800-61 Revision 3 emphasizes that incident response should be integrated across cybersecurity risk-management activities and not treated as an isolated technical function (Nelson et al., 2025). This approach supports the argument that forensic findings have value beyond attribution. They can expose weaknesses in processes, decision structures, technology, training, and organizational controls.

However, forensic evidence does not automatically produce organizational improvement. Technical findings must be interpreted, communicated, and translated into decisions. Leadership therefore becomes important at the boundary between investigation and organizational action.

2.4 Organizational Learning from Cybersecurity Incidents

Organizational learning refers to processes through which experience is converted into knowledge and embedded in organizational practices. Crossan et al. (1999) conceptualized learning as a multilevel process involving intuiting, interpreting, integrating, and institutionalizing. This is relevant after cyber incidents because lessons initially identified by investigators or individual staff must become shared practices, procedures, and capabilities if the organization is to change.

Research suggests that this transition is often incomplete. Patterson et al. (2023), in a systematic review of learning from cybersecurity incidents, found weaknesses in participation, causal analysis, implementation of lessons, and evaluation of whether corrective actions reduce future incidents. Their subsequent qualitative study found that defensiveness, superficial reviews, and failure to address systemic causes can obstruct effective learning (Patterson et al., 2024). The existence of forensic evidence is therefore insufficient. Organizations require structures and leadership practices that enable evidence to be discussed and converted into corrective action.

Digital forensic investigation can strengthen organizational learning by supplying evidence about what occurred, how controls failed, and where organizational assumptions were inaccurate. More complete evidence should improve post-incident analysis and reduce dependence on speculation. We therefore make the following proposition:

Proposition 2: *Effective digital forensic investigation positively influences organizational learning following healthcare cyberattacks.*

Leadership is also likely to influence this relationship. Leaders determine who participates in post-incident review, whether difficult findings are acknowledged, whether blame suppresses disclosure, and whether resources are committed to implementing lessons. We therefore make the following proposition:

Proposition 3: *The positive relationship between digital forensic investigation and organizational learning is stronger when crisis leadership is effective.*

2.5 Organizational Learning and Cyber Resilience

Organizational resilience refers broadly to the capacity to prepare for, absorb, adapt to, recover from, and learn from disruption. Healthcare resilience literature shows that resilience is not simply a return to the pre-crisis state. It also involves adaptation and capability development that improve responses to future shocks (Carbonara et al., 2024). Learning is therefore central to resilience because organizations that identify causes but fail to change remain vulnerable to recurrence.

Post-cyberattack learning may strengthen resilience through revised incident-response plans, improved technical controls, better forensic readiness, clearer leadership responsibilities, staff training, stronger backup arrangements, and improved communication protocols. Patterson et al. (2023, 2024) similarly emphasize the need to address underlying causes and evaluate whether corrective actions improve future security. We therefore make the following proposition:

Proposition 4: *Organizational learning following healthcare cyberattacks positively influences organizational cyber resilience.*

2.6 Cyber Resilience and Patient Safety

Patient safety provides the final outcome of the proposed framework. Healthcare cyber resilience matters because failures of digital systems can affect access to records, communication, diagnostics, treatment workflows, and coordination of care. Ewoh & Vartiainen (2024) identify patient safety as a central concern in healthcare cybersecurity, while van Boven et al. (2024) show that ransomware incidents can substantially disrupt acute-care processes. Abouk & Powell (2024) further demonstrate that disruption can extend to nearby hospitals through shifts in patient demand.

A resilient healthcare organization should be better able to preserve essential clinical functions, activate workable contingencies, restore systems safely, and incorporate lessons that reduce the impact of future incidents. Resilience should therefore be viewed not only as a cybersecurity outcome but also as a patient-safety capability. We therefore make the following proposition:

Proposition 5: *Greater organizational cyber resilience positively influences patient safety in healthcare organizations.*

2.7 Integration of the Constructs

The reviewed literature suggests a sequential but interconnected process. Crisis leadership shapes the environment in which digital forensic investigation occurs. Forensic investigation generates evidence that supports explanation and learning. Leadership influences whether that evidence is interpreted and converted into organizational change. Organizational learning strengthens cyber resilience, while resilience improves the capacity to maintain safe care during future disruption. The proposed model in **Figure 1** therefore connects leadership, technical investigation, learning, resilience, and patient safety within a single post-cyberattack process. This integration addresses an important gap because these domains have largely developed in parallel despite their practical interdependence in healthcare organizations.

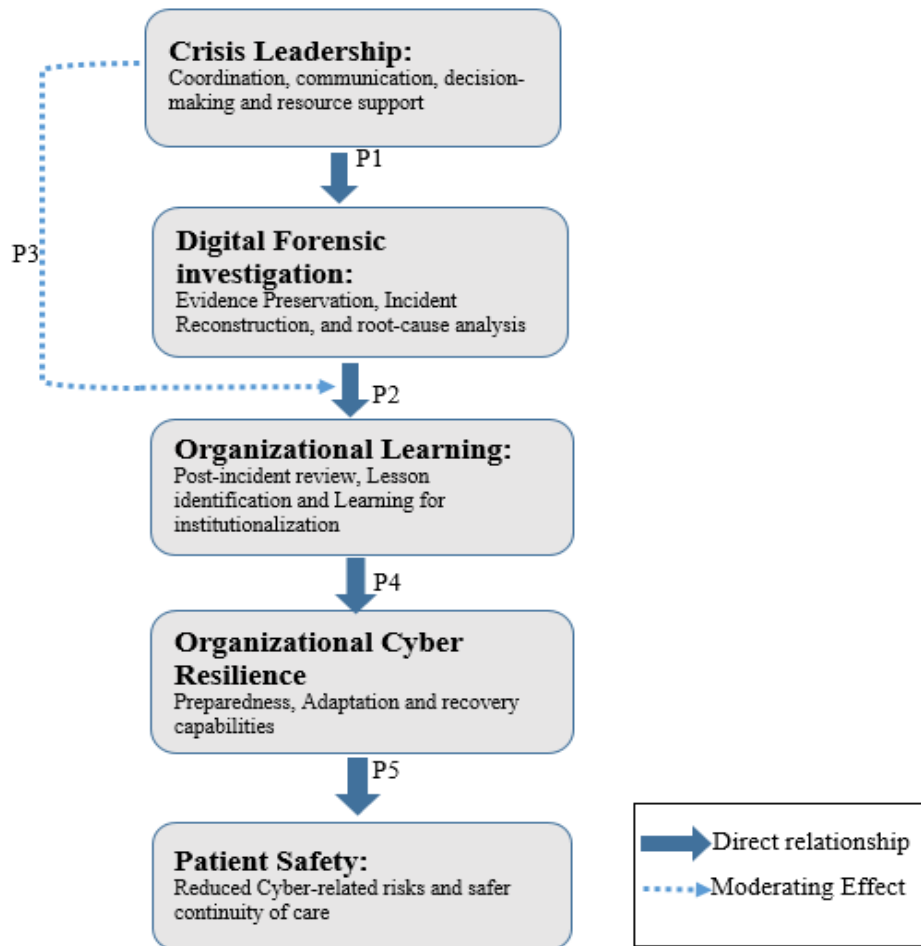


Figure 1: Conceptual Framework showing the sequential but interconnected process of Crisis Leadership in the Aftermath of Healthcare Cyberattacks.

3. Methodological Approach

This paper adopts a conceptual research design based on structured integration of literature from several related but largely separate research domains. Conceptual research is appropriate where the objective is to connect existing theoretical perspectives, clarify relationships among constructs, and develop a framework that extends understanding beyond individual disciplinary boundaries (Jaakkola, 2020). The approach used in this study combines theory synthesis with conceptual model development. Rather than testing relationships empirically, the paper integrates existing knowledge to explain how crisis leadership, digital forensic investigation, organizational learning, cyber resilience, and patient safety may interact following healthcare cyberattacks.

The literature synthesis was guided by established approaches to integrative and conceptual reviews (Snyder, 2019; Torraco, 2016). Relevant literature was organized around four principal domains: crisis leadership and healthcare crisis management; cybersecurity incidents and digital forensics; organizational learning and resilience; and patient safety within digitally dependent healthcare environments. Searches focused on combinations of terms including “*crisis leadership*”, “*healthcare*”,

“cyberattack”, “ransomware”, “digital forensics”, “forensic readiness”, “cybersecurity”, “incident learning”, “organizational learning”, “cyber resilience” and “patient safety”. Because the research problem crosses disciplinary boundaries, literature addressing transferable organizational and cybersecurity theories outside healthcare was also considered where it contributed directly to development of the proposed relationships.

Priority was given to peer-reviewed journal articles and authoritative cybersecurity guidance. Recent publications were emphasized to reflect developments in healthcare cybersecurity and organizational responses to digital disruption. Earlier studies were retained where they provided established theoretical foundations, particularly for organizational learning and digital forensic readiness. Sources concerned exclusively with technical attack execution, without relevance to leadership, investigation, organizational learning, resilience, or healthcare consequences, were not central to the synthesis.

Analysis proceeded through an iterative comparison of constructs, mechanisms, and outcomes across the identified literature. Particular attention was given to recurring relationships between leadership behavior and crisis response, forensic investigation and knowledge generation, organizational learning and capability development, and resilience and continuity of safe healthcare delivery. Areas in which these literatures converged were subsequently used to establish theoretically defensible links among the constructs. Table 1 shows the Key papers that were used in this paper.

Table 1: Key Literature for the Study

Author	Theme	Contribution to this paper
Atkinson et al., 2024	Healthcare crisis leadership and resilience	Supports the role of leadership behaviors and management practices and resilience in crisis situations.
Yang et al., 2024	Crisis leadership behavior in healthcare	Shows that crisis leadership improves staff outcomes and coordinated response during disruption.
Ewoh & Vartiainen, 2024	Healthcare cybersecurity as a sociotechnical issue	Frames cyberattacks as organizational, people, and process problems with patient-safety implications.
Van Boven et al., 2024	Health care impacts of ransomware attacks	Demonstrates operational and clinical disruption caused by hospital ransomware incidents.
Abouk & Powell, 2024	Ransomware and hospital service disruption	Provides evidence that attacks reduce emergency department visits and admissions and shift demand to nearby hospitals.
Chernyshev et al., 2019	Digital forensic readiness in healthcare	Highlights the importance of forensic readiness for post-incident investigation.
Nelson et al., 2025	Incident response and cybersecurity risk management	Grounds digital forensics and incident response within broader cybersecurity risk management.

Author	Theme	Contribution to this paper
Patterson et al., 2023	Organizational learning from cybersecurity incidents	Explains why organizations struggle to learn from cyber incidents and supports the learning-resilience link.
Patterson et al., 2024	Practices and challenges of post-incident learning	Shows barriers to converting incident findings into organizational change and supports the leadership moderation argument.
Carbonara et al., 2024	Hospital resilience resources and capabilities	Supports the link between organizational learning and resilience in healthcare organizations.
Neprash et al., 2026	Effects of ransomware on hospitals and patients	Strengthens the patient-safety rationale by linking attacks to disrupted care and worse patient outcomes.
Crossan et al., 1999	Organizational learning framework	Provides the theoretical basis for turning incident insights into institutionalized learning.

The synthesis moved from identification of these relationships to development of five propositions presented in the preceding literature review. These propositions were then organized into an integrated conceptual framework. Consistent with conceptual model development, the propositions represent theoretically derived relationships that require subsequent empirical examination (Jaakkola, 2020). This methodological approach therefore enables the paper to connect fragmented research streams and provide a coherent explanation of how healthcare organizations may transform evidence generated after cyberattacks into organizational learning, improved cyber resilience, and stronger protection of patient safety.

4. Findings and Discussion: Proposed Conceptual Framework

4.1 Crisis Leadership and Digital Forensic Effectiveness

The conceptual synthesis indicates that crisis leadership should be viewed as an enabling condition for effective digital forensic investigation and not as an activity that begins after technical investigation is complete. Healthcare cyber incidents create simultaneous clinical, operational, technical, legal, and communication demands. Leaders must therefore establish priorities, clarify authority, protect critical services, and create conditions in which investigators can preserve evidence without unnecessarily extending disruption. Research on healthcare crisis leadership shows that coordination, communication, role clarity, and adaptive decision-making are important to organizational performance during crises (Atkinson et al., 2024; Yang et al., 2024). These same behaviors are relevant to cyber incidents because forensic teams depend on timely access to systems, cooperation from staff, reliable escalation channels, and leadership support for evidence preservation.

This relationship also involves an important tension. Pressure to restore systems rapidly may conflict with the need to preserve logs, system images, and other evidence required for investigation. Leadership therefore influences the manner in which recovery is pursued as a purely technical restoration exercise

or as a controlled process that balances continuity of care with investigative integrity. NIST guidance similarly treats incident response as part of wider cybersecurity risk management instead of as an isolated technical activity (Nelson et al., 2025). Proposition 1 consequently positions crisis leadership as a determinant of the organizational conditions under which digital forensic investigation is conducted.

4.2 Digital Forensics as a Foundation for Organizational Learning

The second relationship is about the conversion of incident evidence into organizational knowledge. Digital forensic investigation can reconstruct the sequence of an attack, identify compromised systems, expose control failures, and distinguish immediate technical causes from wider process weaknesses. Its organizational value therefore extends beyond attribution or legal evidence. When forensic findings are incorporated into post-incident review, they provide a factual basis for questioning assumptions about existing controls and identifying where procedures, technologies, or behaviors failed.

This argument is consistent with research showing that learning from cybersecurity incidents is often weakened by superficial causal analysis and limited evaluation of corrective actions (Patterson et al., 2023, 2024). Patterson et al. (2024) further found that organizations can struggle with openness, participation, causal investigation, and implementation when attempting to learn from cyber incidents. Forensic evidence can improve this process by reducing dependence on recollection, speculation, or blame. However, evidence does not constitute learning by itself. Learning occurs when findings are interpreted collectively and converted into revised practices, controls, training, or decision rules. Proposition 2 therefore reflects a knowledge-conversion mechanism: effective digital forensics increases the quality of information available for organizational learning, but organizational processes determine whether that information produces change.

4.3 Leadership as the Mechanism for Translating Forensic Evidence into Change

Proposition 3 extends the framework by arguing that crisis leadership strengthens the relationship between digital forensic investigation and organizational learning. This moderating role is important because the same forensic report can produce very different organizational responses. Leaders may encourage open examination of systemic causes, or they may focus narrowly on individual error. They may allocate resources to implement recommendations, or allow lessons to remain as unimplemented reports. They also influence whether technical findings are communicated to clinical, administrative, governance, and executive audiences in forms that support action.

The organizational learning literature suggests that openness, participation, and willingness to address underlying causes are important to learning from cybersecurity incidents (Patterson et al., 2024). These findings suggest that post-incident learning is partly a leadership problem. Effective crisis leaders can create conditions in which weaknesses can be reported, bring different professional groups into the review process, and ensure that lessons are assigned ownership and follow-up. In healthcare, this is especially important because cyber incidents cross professional boundaries. A failure originating in

information technology can produce consequences in emergency care, diagnostics, medication processes, scheduling, or communication. Leadership therefore performs a translation function between technical evidence and organizational adaptation.

4.4 Organizational Learning and Cyber Resilience

The framework further proposes that organizational learning strengthens cyber resilience. Resilience is not equivalent to restoring systems to their previous condition. A return to the pre-incident state may simply reproduce the vulnerabilities that made the organization susceptible to disruption. Rather, resilience requires adaptation based on what the organization has learned.

Learning can improve cyber resilience through several mechanisms. Forensic findings may lead to redesigned access controls, improved logging, revised escalation procedures, stronger backup arrangements, more realistic downtime protocols, better staff training, or clearer leadership responsibilities. Patterson et al. (2023, 2024) emphasize that learning becomes meaningful when lessons are implemented and their effectiveness is subsequently evaluated. Recent healthcare research similarly emphasize preparedness, response, recovery, and adaptation as important dimensions of cyber resilience. Proposition 4 therefore links organizational learning with resilience through institutionalization. Knowledge generated after an incident must become embedded in routines, structures, technologies, and behaviors that increase the organization's capacity to manage future disruption. In this sense, learning converts a past incident from an isolated adverse event into an input for future organizational capability.

4.5 Cyber Resilience and Patient Safety

The final relationship connects cyber resilience with patient safety. This is central to the framework because the purpose of healthcare cybersecurity is not merely to protect information assets. Digital disruption can interfere with access to electronic records, diagnostics, medication-related processes, scheduling, referrals, communication, and other clinical activities. Van Boven et al. (2024) documented substantial clinical and operational difficulties during hospital ransomware attacks, while Abouk & Powell (2024) found reduced activity at attacked hospitals and increased emergency department activity at nearby hospitals. Recent evidence strengthens this connection. McGlave et al. (2023), using linked ransomware and Medicare claims data, found substantial reductions in hospital volume during the initial attack period and increased in-hospital mortality among patients who were already admitted when an attack began. These findings show the need for cyber resilience to be considered as a patient-safety capability, and not merely an information-security outcome.

Cyber resilience can reduce such risks by enabling organizations to maintain essential clinical functions during disruption and restore digital services in a controlled manner. Resilient healthcare organizations should have tested downtime procedures, alternative communication channels, reliable backups, defined clinical priorities, and cross-functional incident structures. This interpretation is consistent

with the sociotechnical view that healthcare cybersecurity depends on interactions among technology, people, and organizational processes (Ewoh & Vartiainen, 2024). Proposition 5 therefore positions patient safety as the ultimate organizational consequence of cyber resilience.

4.6 The Integrated Conceptual Framework

The five propositions describe a connected post-cyberattack pathway: Crisis leadership → Digital forensic effectiveness → Organizational learning → Cyber resilience → Patient safety

Within this pathway, crisis leadership also strengthens the conversion of digital forensic findings into organizational learning. The framework contributes to existing research in three important ways.

First, it places leadership at the center of post-cyberattack recovery and not just treating cyber response as predominantly technical. Second, it reframes digital forensics as a source of organizational knowledge, beyond evidence for technical, regulatory, or legal purposes. Third, it connects post-incident learning and cyber resilience to patient safety, thereby explaining why leadership and forensic readiness are relevant to healthcare outcomes.

The framework should not be interpreted as a rigid linear sequence. Feedback relationships are likely. Learning from one incident can improve forensic readiness and leadership preparedness for subsequent incidents, while improved resilience may reduce the severity of future disruptions. The model therefore represents a recurring learning cycle in which healthcare organizations can use cyber incidents as inputs for capability development.

The importance of such an approach is reinforced by the changing scale of healthcare cyber risk. Jiang et al. (2025) reported that the number of patient records affected by healthcare data breaches in the United States increased substantially between 2010 and 2024, with hacking and information technology incidents accounting for most affected records by the end of the study period. Prevention remains necessary, but healthcare organizations must also develop the leadership, forensic, learning, and resilience capabilities required to respond when prevention fails. The proposed framework consequently shifts attention from the isolated management of cyber incidents towards an organizational process through which evidence is transformed into learning, resilience, and safer healthcare delivery.

5. Implications

5.1 Theoretical Implications

The proposed framework contributes to several research streams by connecting concepts that have largely been examined separately. First, it extends crisis leadership research into the specific context of healthcare cyberattacks. Existing healthcare crisis leadership studies have primarily examined broader emergencies and organizational disruption (Atkinson et al., 2024; Yang et al., 2024). The present

framework suggests that cyber crises require leaders to manage not only operational continuity and staff coordination but also the preservation, interpretation, and organizational use of digital evidence. Second, the framework extends the organizational role of digital forensics. Digital forensics is commonly associated with evidence collection, incident reconstruction, attribution, and legal or regulatory investigation. The proposed model positions forensic investigation additionally as a knowledge-generating mechanism. Its value therefore depends partly on whether organizations convert forensic findings into changes in structures, routines, technologies, and behaviors. This perspective connects digital forensics with organizational learning and helps explain why technically successful investigations may not necessarily produce stronger organizational capabilities.

Third, the framework contributes to organizational learning and resilience research by proposing a pathway through which learning may emerge after cybersecurity incidents. Patterson et al. (2023, 2024) demonstrate that organizations often experience difficulty translating cyber incidents into sustained learning. The present model suggests that crisis leadership can influence this translation process and that institutionalized learning subsequently contributes to cyber resilience. Finally, positioning patient safety as the ultimate outcome broadens the concept of cyber resilience beyond information-system recovery.

5.2 Managerial and Leadership Implications

The framework has several implications for healthcare managers. Cyber incident preparedness should not be delegated exclusively to information technology or cybersecurity departments. Senior executives, clinical leaders, risk managers, and cybersecurity teams should establish clear decision-making structures before incidents occur. These structures should define responsibilities for clinical continuity, evidence preservation, communication, escalation, and recovery.

Leaders should also treat post-incident review as a learning exercise, and not as a narrow search for individual responsibility. A blame-oriented response may discourage disclosure and limit identification of systemic weaknesses. Instead, forensic findings should be discussed across relevant clinical, technical, and administrative functions and translated into assigned corrective actions. Leadership responsibilities should include ensuring that recommendations are implemented, resourced, and subsequently evaluated.

Healthcare organizations should also strengthen forensic readiness. Appropriate logging, evidence-preservation procedures, documentation standards, and trained personnel can improve the quality of post-incident investigation. Such capabilities should be integrated with business continuity and patient-safety planning instead of being maintained as isolated cybersecurity functions (Nelson et al., 2025).

5.3 Patient Safety and Policy Implications

Cybersecurity preparedness should be more and more considered as part of healthcare safety governance. Evidence that ransomware can disrupt clinical activity and adversely affect patients indicates that cyber incidents can generate consequences comparable to other threats to continuity of care (Abouk & Powell, 2024; McGlave et al., 2023; Van Boven et al., 2024). Healthcare regulators and governing bodies should therefore encourage organizations to integrate cybersecurity resilience, forensic readiness, incident learning, and clinical continuity within institutional risk-management systems.

The framework further suggests that evaluating healthcare cyber resilience should extend beyond technical measures such as recovery time or system availability. Relevant indicators should also consider continuity of critical clinical functions, effectiveness of post-incident learning, implementation of corrective actions, and reduction of risks to patients. Cybersecurity performance can thereby be assessed in terms that reflect more closely the fundamental purpose of healthcare organizations, that is the safe and reliable delivery of care.

6. Suggestions for Future Research

Future research should empirically test the relationships proposed in this framework and examine whether they operate consistently across different healthcare settings. Quantitative studies could develop and validate measures of crisis leadership, digital forensic effectiveness, organizational learning, cyber resilience, and cyber-related patient-safety outcomes. Structural equation modelling would be particularly suitable for testing the sequential relationships proposed in the framework and for assessing the moderating role of crisis leadership in the relationship between digital forensic investigation and organizational learning.

Qualitative research could complement this work by examining how healthcare organizations actually respond to cyber incidents. Interviews with senior executives, clinical leaders, cybersecurity professionals, digital forensic investigators, and patient-safety personnel could provide deeper insight into how forensic findings are interpreted and translated into organizational change. Comparative case studies involving hospitals that experienced ransomware or other major cyber incidents may also help identify leadership behaviors and organizational conditions associated with more effective recovery and learning.

Longitudinal research is especially important because organizational learning and resilience develop over time. Studies could examine how lessons identified immediately after an incident are subsequently implemented, which corrective actions remain in place, and how these changes improve preparedness for later disruptions. This would address an important limitation in current cybersecurity learning

research, which has identified difficulties in evaluating how post-incident actions result in sustained improvement (Patterson et al., 2023, 2024).

Future studies should also investigate contextual factors that may influence the proposed relationships. These may include organizational size, cybersecurity maturity, leadership style, regulatory environment, resource availability, and degree of digital dependence. Cross-country studies could determine whether differences in healthcare infrastructure and cybersecurity regulation alter the effectiveness of post-incident learning.

Finally, research should develop more direct measures of the relationship between cyber resilience and patient safety. Existing studies demonstrate that cyberattacks can disrupt healthcare delivery, but further work is needed to establish how specific resilience capabilities can reduce clinical disruption and patient harm. Empirical validation of these relationships would strengthen the understanding of cybersecurity as both an organizational resilience issue and a core component of modern patient safety.

7. Conclusion

Healthcare cyberattacks are no longer solely technical disruptions. Their consequences can extend across clinical operations, organizational performance, and patient safety. This paper has argued that effective recovery therefore requires more than restoring compromised systems. Healthcare organizations must also understand what occurred, learn from the incident, and translate that learning into stronger capabilities for managing future disruption.

The conceptual framework developed in this paper connects crisis leadership, digital forensic investigation, organizational learning, cyber resilience, and patient safety. Crisis leadership is positioned as an important enabling factor for effective forensic investigation and as a mechanism that strengthens the translation of forensic findings into organizational learning. Digital forensic investigation provides the evidence needed to understand failures and vulnerabilities, while organizational learning determines whether those findings become embedded in revised procedures, technologies, behaviors, and decision structures. Such learning can strengthen cyber resilience and improve the organization's capacity to maintain safe healthcare delivery during future incidents.

The paper therefore extends existing discussions of healthcare cybersecurity by placing leadership and learning at the center of post-incident recovery. It also broadens the role of digital forensics from technical investigation to organizational knowledge generation and connects cyber resilience directly with patient safety. The proposed relationships remain conceptual and require empirical validation. Nevertheless, the framework provides a basis for examining how healthcare organizations can move beyond restoring systems after cyberattacks towards developing stronger, more adaptive, and safer organizations. In this sense, the aftermath of a cyberattack should be treated not only as a period of recovery but also as an opportunity for structured organizational learning and resilience development.

References

- Abouk, R., & Powell, D. (2024). Ransomware attacks, ED visits and inpatient admissions in targeted and nearby hospitals. *JAMA*, 331(24), 2129–2131.
- Atkinson, M. K., Biddinger, P. D., Chughtai, M.-A., Hayirli, T. C., Hick, J. L., Cagliuso Sr, N. V., & Singer, S. J. (2024). Assessing healthcare leadership and management for resilience and performance during crisis: The HERO-36. *Health Care Management Review*, 49(1), 14.
- Carbonara, N., Pellegrino, R., & De Luca, C. (2024). Resilience of hospitals in an age of disruptions: a systematic literature review on resources and capabilities. *Health Systems*, 13(3), 192–228.
- Chernyshev, M., Zeadally, S., & Baig, Z. (2019). Healthcare data breaches: Implications for digital forensic readiness. *Journal of Medical Systems*, 43(1), 7.
- Crossan, M. M., Lane, H. W., & White, R. E. (1999). An organizational learning framework: From intuition to institution. *Academy of Management Review*, 24(3), 522–537.
- Elyas, M., Ahmad, A., Maynard, S. B., & Lonie, A. (2015). Digital forensic readiness: Expert perspectives on a theoretical framework. *Computers & Security*, 52, 70–89.
- Ewoh, P., & Vartiainen, T. (2024). Vulnerability to cyberattacks and sociotechnical solutions for health care systems: systematic review. *Journal of Medical Internet Research*, 26, e46904.
- Jaakkola, E. (2020). Designing conceptual articles: four approaches. *AMS Review*, 10(1), 18–26.
- Jiang, J. X., Ross, J. S., & Bai, G. (2025). Ransomware attacks and data breaches in US health care systems. *JAMA Network Open*, 8(5), e2510180.
- McGlave, C. C., Neprash, H., & Nikpay, S. (2023). Hacked to pieces? The effects of ransomware attacks on hospitals and patients. *The Effects of Ransomware Attacks on Hospitals and Patients (October 4, 2023)*.
- Nelson, A., Rekhi, S., Souppaya, M., & Scarfone, K. (2025). Incident response recommendations and considerations for cybersecurity risk management. *NIST Special Publication*, 800.
- Nesse, S., Schei, V., & Mitroff, I. (2024). Collective response capacity: Developing crisis leadership in organisations. *Journal of Contingencies and Crisis Management*, 32(3), e12612.
- Pascoe, C., Quinn, S., & Scarfone, K. (2024). *The NIST cybersecurity framework (CSF) 2.0*. Cherilyn Pascoe, Stephen Quinn, Karen Scarfone.
- Patterson, C. M., Nurse, J. R. C., & Franqueira, V. N. L. (2023). Learning from cyber security incidents: A systematic review and future research agenda. *Computers & Security*, 132, 103309.
- Patterson, C. M., Nurse, J. R. C., & Franqueira, V. N. L. (2024). “I don’t think we’re there yet”: The practices and challenges of organisational learning from cyber security incidents. *Computers & Security*, 139, 103699.
- Riggio, R. E., & Newstead, T. (2023). Crisis leadership. *Annual Review of Organizational Psychology and Organizational Behavior*, 10(1), 201–224.

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research*, 104, 333–339.

Torraco, R. J. (2016). Writing integrative literature reviews: Using the past and present to explore the future. *Human Resource Development Review*, 15(4), 404–428.

van Boven, L. S., Kusters, R. W. J., Tin, D., van Osch, F. H. M., De Cauwer, H., Ketelings, L., Rao, M., Dameff, C., & Barten, D. G. (2024). Hacking acute care: a qualitative study on the health care impacts of ransomware attacks against hospitals. *Annals of Emergency Medicine*, 83(1), 46–56.

Wu, Y. L., Shao, B., Newman, A., & Schwarz, G. (2021). Crisis leadership: A review and future research agenda. *The Leadership Quarterly*, 32(6), 101518.

Yang, M., Evans, J. M., Singer, S. J., Gutberg, J., Porter, T. H., & Grudniewicz, A. (2024). Crisis leadership behaviors in healthcare: survey validation and influence on staff outcomes in primary care clinics during the COVID-19 pandemic. *BMC Health Services Research*, 24(1), 590.