

Cyber resilience in public health: a narrative case study of the Aurum Institute ransomware attack

Jacqueline Paterson¹, Cristian Pieterse², Khangwelo Mulaudzi³, David A Clark^{4,5}

¹ Data Operations, Aurum Institute,

² ICT, Aurum Institute,

³ Administration, Aurum Institute,

⁴ CEO, Aurum Institute,

⁵ Public Health, Vanderbilt University Medical Center

<https://doi.org/10.61473/001c.170686>

South African Health Review

Vol. 28, 2025

Aim

Ransomware has become a decisive risk for public health organisations, halting programme delivery, compromising sensitive data, and eroding trust. This case study shares the experiences of a South African non-profit organisation, the Aurum Institute, which was the victim of a ransomware attack in February 2024. The case study details the incident and response, and discusses lessons learnt in terms of preparedness, containment, and recovery.

Method

Adopting a descriptive case study approach, this paper provides a detailed narrative to reconstruct the ransomware attack on the Aurum Institute, describing the context in which the incident occurred, what happened during the attack, and the impacts that followed. The analysis is constructed around the themes of preparedness, containment, and subsequent operational recovery.

Findings

Aurum's resilience depended not on any single control, but on a combination of implementing a dynamic business recovery plan, cloud segregation of core services, disciplined leadership, external forensic support, and recoverable backups. These strengths enabled the organisation to preserve critical business functions and prepare for structured restoration, while the incident also exposed important weaknesses in monitoring, credential governance, vendor oversight, and data inventories.

The case demonstrates that recoverable backups, segmented cloud-based services, disciplined crisis leadership, and specialist forensic support were central to restoring continuity after the attack.

Conclusion

Cybersecurity is now inseparable from public health mission continuity. As such, health NPOs should treat cybersecurity as enterprise governance, prioritise investments according to risk and affordability, strengthen identity and detection capabilities, improve segmentation and recoverability, and engage donors, stakeholders, and insurers in more realistic conversations about the costs and trade-offs of resilience.

Introduction

Public health practice increasingly depends on digital systems such as laboratory informatics, data warehouses, electronic data capture, study management systems, donor reporting, and collaboration platforms. Most modern organisations also rely on digital platforms for fi-

nance, human resources, operations, administration, and communications. Yet many non-profit organisations (NPOs) operate these systems with constrained budgets, outsourced and fragmented vendor arrangements, legacy workloads, and uneven security maturity.

Recent South African incidents illustrate that cyber-attacks are no longer exceptional events: Transnet expe-

experienced a major ransomware-related disruption in 2021; the National Health Laboratory Service reported a ransomware attack in 2024 that made key laboratory systems inaccessible; and, in 2026, the Centre for High Performance Computing at the Council for Scientific and Industrial Research reported a cybersecurity breach affecting the Lengau computing cluster. Taken together, these cases reinforce the conclusion that cyber-attacks have become a matter of ‘when’, not ‘if’.

This paper offers a narrative analysis intended for senior public health executives, board members, donors, and programme leaders. The focus is organisational: how organisations prepare for risk; how crises are led and contained; how communications sustain trust; and how recovery preserves mission continuity. Technical elements are included where they help explain the incident and lessons learnt are presented.

Case description

The Aurum Institute (Aurum) is a South African public health and research NPO that works at a local level and with a footprint in several African countries as well as globally. Aurum works across health programmes, research, and corporate support functions and therefore depends heavily on digital infrastructure to sustain service delivery, reporting, compliance, and internal operations. In February 2024, a LockBit 3.0 affiliate exploited these realities at Aurum.

Initial compromise and attacker activity

On 4 February 2024, attackers obtained access to Aurum’s on-premise systems via poorly configured back-office firewall-administrator credentials. In this case, the firewall service vendor had left a weak default password on a key firewall portal that was subjected to a common-password or brute-force attack. The attackers then created new local firewall user accounts, deleted the compromised user account, adjusted rules to enable remote pathways, implemented software to mask their presence, and began reconnaissance.¹ Over eight days, they harvested privileges using Mimikatz, scanned servers, and exfiltrated approximately 15 gigabytes of internal documents, human resources (HR) data, and operational files using FileZilla.

The payload executed during the night of 12 February 2024. By dawn, 21 servers, including bespoke HR support systems, laboratory quality control (QC) systems, data warehouses, domain controllers, site servers, and legacy SharePoint servers, were encrypted, and ransom notes and data exposure threats appeared. Anxiety spiked among staff and partners and leaders faced complex decisions about containment, communication, data exposure, and ransom demands.

Incident response and recovery actions

Aurum’s independently segmented, cloud-hosted authentication systems, enterprise resource planning system, financial databases, payroll, SharePoint Online, project management business systems, email, and collaboration systems remained unaffected and fully operational, preventing total organisation system collapse. All endpoint devices had been proactively protected against ransomware, so no user devices were infected. At 06:00 on 13 February, the information and communications technology (ICT) team escalated to leadership, and incident command convened.

Containment

Within four hours, containment measures were authorised: compromised servers were shut down; affected segments were isolated; foreign internet protocol (IP) ranges were geofenced on the firewall; organisation-wide password resets were forced, and additional endpoint protection was deployed. A disaster was declared under the business recovery plan, the Information Regulator was notified, and data inventories of the affected servers were compiled so that operational impacts could be determined for each dataset and system.

After consultation with the lead ICT vendor, management secured the services of an expert digital forensic and cybersecurity consultant to guide the response and conduct an independent investigation. Leadership considered whether to engage the attackers to clarify the nature of the exfiltrated data in view of the ransom demands. The decision was to work through the forensic expert to obtain proof of exfiltration and to advise the attackers of the organisation’s non-profit, public health role. The attackers remained dispassionate and intransigent, and Aurum ultimately chose not to pursue further negotiation, anchored in growing confidence that immutable offsite backups would enable full restoration of systems and data, although the public data exposure threat remained.²

Recovery

Clean-room recovery began: each workload was rebuilt and verified in isolation before return to production to prevent reinfection. Full operations were restored over 12 days, and all core on-premise systems were rebuilt within 16 days of the initial encryption. Aurum avoided catastrophic data loss and prolonged operational collapse. The direct costs of securing the independent digital forensic service, ICT staff overtime, and rebuilding compromised infrastructure amounted to approximately R1.8 million, while indirect costs, fatigue, and reputational work were not quantifiable but were estimated to be significant (see [Table 1](#)).

In a fortunate parallel development, a major global law-enforcement operation disrupted the LockBit 3.0 criminal enterprise in the two weeks after this attack commenced,³ rendering further decisions on managing

Table 1. Total cost components of a ransomware incident

Category	Examples
Direct	Forensics and investigations; rebuild tooling; additional protection software; overtime; potential ransom payments; darknet surveillance
Indirect	Productivity loss; reporting delays; reputational management; regulatory risk
Insurance	Premium increases; deductibles; sub-limits; incident services

Table 2. SWOT summary

Category	Description
Strengths	Immutable offsite backups; executive support; cloud platforms insulated core functions
Weaknesses	Limited SIEM/SOC; vendor alerting gaps; staff awareness; asset/data inventory gaps
Opportunities	Co-managed SOC; donor advocacy for cyber budgets; segmentation; quarterly simulations
Threats	Insurance costs; re-attack risk; privacy exposure (POPIA/GDPR); supply-chain issues
Implications	Outsource execution, not accountability; Board sets RTO/RPO targets and cyber-resilience risk tolerance and ensures funding for risk mitigation

potential data-exfiltration exposure and ransom payment moot. As a precaution, Aurum implemented six months of dark web monitoring for any exfiltrated data, but none materialised.

Independent forensic audit

Following Aurum's cyber-attack, an independent forensic investigation was undertaken, and a multidisciplinary review was undertaken to identify ongoing threats, opportunities, strengths, and weaknesses. The resulting SWOT summary (Table 2) is useful not as a substitute for strategy, but as a way of making the organisation's post-incident choices explicit and accountable.

Discussion

Three dynamics shape the current cyber threat environment. First, health data carries enduring value on illicit marketplaces, from patient identifiers and clinical records to cohort datasets and trial metadata. Unlike payment tokens, these records cannot be easily invalidated.^{4,5} Second, rapid digitalisation, which accelerated during the COVID-19 pandemic, often outpaces cyber-architecture hardening, leaving flat networks, weak end-point telemetry, and legacy servers that underpin critical programme and organisational functions.⁶ Third, ransomware-as-a-service has industrialised cybercrime: groups like LockBit 3.0 supply affiliates with builders, tooling, automation, counter-security, and 'customer support', lowering barriers and increasing attack volume against all targets, including healthcare organisations.¹ Cybercriminals now also use artificial intelligence and machine learning to make their attacks faster, more scalable, and harder to detect by automating key parts of the cyberattack process.⁷ There are no moral restraints on cybercrime groups: money and profit are their un-

abashed drivers of activity and all organisations, including healthcare and humanitarian organisations, are considered 'fair game' targets in the pursuit of illicit profit.^{8,9}

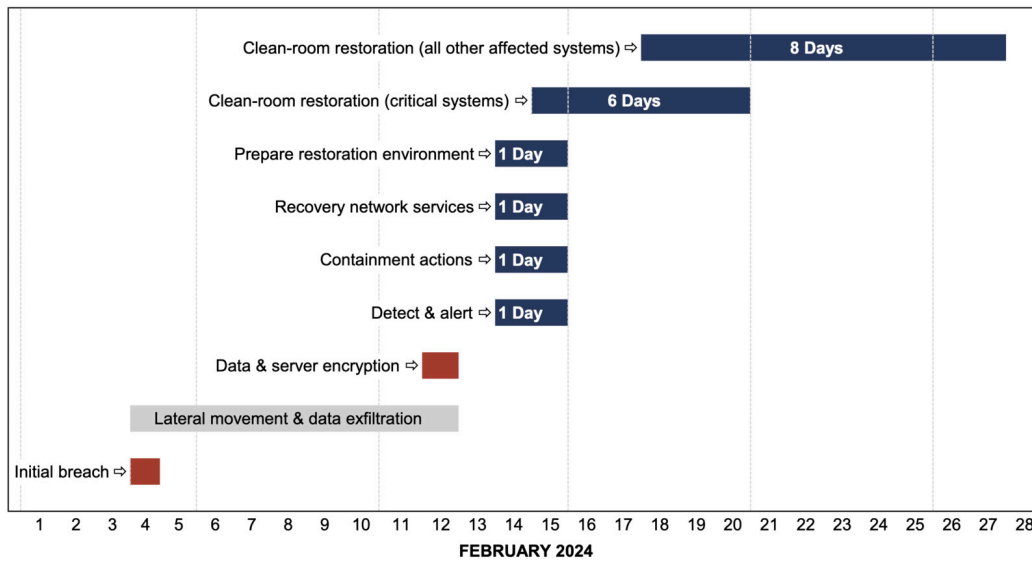
Sector intelligence underscores the trend: the healthcare sector reports among the highest attack rates and recovery costs; backup compromise attempts are common; and recovery often exceeds a month for severe incidents.^{1,8} Standards bodies and agencies increasingly emphasise governance, monitoring, identity hardening, segmentation, and tested recoverability as essential capabilities.⁸

Impact

The incident's effects extended well beyond information ICT. Donor data management compliance standards e.g., Protection of Personal Information Act (POPIA), Health Insurance Portability and Accountability Act, and the General Data Protection Regulation (GDPR) and reporting cadences were threatened; epidemiologic and workflow dashboards became unavailable; laboratory QC workflows reverted to paper; potential HR and payroll delays created workforce anxiety, and government, partners, and other stakeholders required repeated briefings.^{10,11} These disruptions map directly onto public health outcomes: slower detection of programme issues, delayed grant deliverables, and potential interruptions in care-support activities.^{12,13}

To anchor continuity, the Aurum team defined recovery time objectives (RTO) and recovery point objectives (RPO) for critical services and instituted fallback standard operating procedures such as manual aggregation, offline registries, and interim HR support-system processing. Proactive alignment of clinical and programme teams with ICT recovery plans reduced friction and established priorities that sped up restoration of essential reporting.

Figure 1. Incident timeline to full operational recovery



Recovery speed also shaped impact. Survey data from Veeam, a global software company specialising in data protection and software recovery, suggest that average dwell time of cyber-criminals in hacked systems has fallen sharply, with some organisations now facing encryption or exfiltration within 24 hours of the initial breach,^{14,15} while recovery duration depends on the extent of infection, the availability and quality of backups, the ransomware variant implicated, the organisation's preparedness, and the sensitivity of the compromised data.^{14,15} In Aurum's case, the existence of immutable backups, ICT expertise, early external forensic support, and an incident response plan inclusive of a robust communications strategy contributed to restoration over twelve days (see [Figure 1](#)), which was shorter than the 21-day industry average reported by CIGENT in March 2024.^{14,16}

Once the incident had been managed, some of the longer-term implications prompted assessment of future impacts on the organisation: donor confidence increasingly hinges on credible cyber-risk management,^{14,17} while cyber-insurance for South African NPOs remains difficult to secure and can be prohibitively expensive, particularly where insurers require security controls that smaller organisations may struggle to fund.¹⁶

The disaster team held daily meetings to assess, record, and monitor the status of the threat and recovery. Input by the digital forensics consultant was carefully noted and a 'rolling' plan developed to address immediate issues and plan for longer-term interventions. Included in this 'rolling' plan was a communications strategy for staff and stakeholders to be kept informed as appropriate. Weekly senior staff townhall-type meetings were held to address key issues of concern. Senior management held separate briefing and update sessions with funders. Recordings of the daily and weekly meetings were summarised and included in the business recovery plan for use in the event of future incidents.

This routine did more than coordinate recovery. It created a practical learning cycle during the incident itself, in which information from ICT recovery activities, forensic findings, leadership decisions, stakeholder communications, and programme impact assessments was repeatedly reviewed against immediate recovery needs and longer-term continuity obligations. Emerging lessons were therefore tested against operational realities as the response unfolded, allowing Aurum to distinguish between controls that materially aided recovery, such as immutable backups, cloud-based service segregation, and disciplined communications, and weaknesses requiring future remediation, including credential governance, vendor oversight, real-time monitoring, and data inventory completeness.

Analysis of the event

What the attack looked like

The kill-chain resembled a typical ransomware attack pattern: compromised credential-based initial access; firewall rule manipulation; privilege escalation and lateral movement; data staging and exfiltration, and rapid encryption.^{1,18} Detecting the compromise lagged substantially owing to limited real-time threat detection capability, over-dependence on vendor monitoring, insufficient centralised logging, and the discovery that available firewall tools had not been properly configured for advanced attacks. These findings indicated that the organisation's preventive and detective controls were uneven rather than absent.

Ransom demands

One unusual feature of this case was that the ransom-payment debate was overtaken by the global law-enforcement action against the LockBit 3.0 criminal enterprise. Even so, the issue warrants discussion. For NPOs

under pressure, paying a ransom may appear to offer a rapid route to data recovery and continuity, but it carries major risks: attackers may not provide a working decryption key; they may demand additional payments, and they may treat payment as evidence that the organisation is a viable future target.^{17,19} There are also legal, ethical, and strategic concerns, particularly where payment could support criminal enterprises or conflict with regulatory obligations.^{17,20} The implication is not that every case can be resolved identically, but that organisations should decide their principles in advance, strengthen recovery options, and minimise the chance that crisis conditions force a hurried decision.

Factors that aided recovery

At the same time, recoverability was strong. Previously implemented immutable backups using WORM (write once, read many) technology²¹ provided tamper-proof clean restore points; cloud platforms insulated core office, communications, HR, and finance functions; and incident command enforced disciplined execution. A particularly important architectural result of Aurum's system segmentation between on-premise and cloud-based systems was that financial, payroll, and communications services were preserved. This allowed the organisation to continue functioning and enabled leadership to communicate internally and externally without resorting to parallel and potentially insecure channels.

Organisational governance enablers

The incident also revealed important governance features.²² Incident command integrated executive leadership with expert forensic, ICT, compliance/legal, communications, HR, finance, and programme staff. Decision rights were explicit, daily situation-management meetings maintained shared situational awareness, and the board's role shifted from oversight at a distance to active risk stewardship through emergency procurement and support for remediation. Communications were calibrated to sustain trust: internal advisories explained actions and expectations; donor updates outlined mitigation and timelines, and partners received factual, timely reports consistent with regulatory obligations. By contrast, vendor-management weaknesses were exposed in alert thresholds, escalation protocols, and verification of security operations centre (SOC) capability.

The case supports a cyber-resilience perspective in which attacks are treated as highly likely rather than exceptional. In that framing, the objective is not prevention alone but the ability to withstand, recover from, and adapt to disruption while maintaining operations.³ Aurum's experience suggests that resilience depends on layers of protection and preparation spanning technology, processes, people, and sound governance.

Lessons learnt

Although the cyber-attack heightened organisational anxiety and operational pressure, it also created an important opportunity for structured organisational learning. The lessons that follow were not derived from retrospective reflection alone. They emerged from daily incident documentation, multidisciplinary review meetings, forensic investigation findings, recovery planning sessions, and a subsequent independent post-incident assessment. The consistent recording of decisions, actions, challenges, and outcomes throughout the crisis enabled Aurum to identify strengths and weaknesses in its preparedness, containment, and recovery capabilities, and to translate these into practical implications for future resilience.

The depth of the formal investigation and the comprehensive documentation of the incident further led to the conclusion that both the event itself and the lessons arising from it should be shared through a symposium as well as the scientific and professional literature. In this way, the learning generated by the incident could extend beyond Aurum and assist leaders of other non-profit and public health organisations to strengthen their own resilience against increasingly sophisticated cyber-crime threats.

The main lessons emerging from this case are therefore commonly applicable and relevant to organisations like Aurum, but they also require careful qualification because resilience measures must be prioritised in relation to risk, affordability, operational dependence, and organisational maturity.

Preparedness

Preparedness strongly influences recovery success and timelines, but not all organisations can implement the same controls at the same pace or at the same investment levels. For example, immutable backups, clean-room procedures, and segmentation materially improve resilience, yet they compete with other organisational mission demands and are expensive, thus they should be prioritised through a risk-based process rather than presented as universally non-negotiable.

Likewise, migration to cloud services with their typically greater security infrastructures can improve resilience when it is architected and governed well, but cloud adoption is also expensive and as a stand-alone does not guarantee secure outcomes because of human behavioural risks.

The same is true of cyber-awareness training: it is important, but its value depends on content, delivery, repetition, and whether it changes behaviour rather than merely satisfying a compliance requirement. Such training should be monitored and measured against improved breach reporting, frequency of minor breaches, and competency evaluations post training.

Containment

Swift authorisation and implementation of containment measures allowed further intrusion and compromise of data to be prevented. These included the isolation of affected segments, geofencing of foreign IP ranges on the firewall, forced organisation-wide password resets and deployment of additional endpoint protection.²³

Although Aurum had never previously encountered a ransomware attack, it was addressed in the business recovery plan through which the disaster was declared. The value of which became evident throughout the recovery process.

The value of having up-to-date data inventories for every server became evident when the process of operational impacts was being determined for each dataset and system.

Securing the services of an expert digital forensic and cybersecurity consultant to guide the response and conduct an independent investigation proved invaluable. This assisted in decisions on whether or not to engage the attackers and in obtaining proof of exfiltrated data. It is obviously funding dependent but an item for consideration to be included in any contingency budget.

Recovery

Structured and transparent communication with both staff and stakeholders was a vital factor in maintaining donor confidence and allaying staff anxiety. Regular townhall sessions were held with management to provide updates on recovery progress and address any critical issues. Consistent and ongoing capture of the response process, recovery progress, and emerging challenges allowed Aurum to enrich its business recovery and continuity plans and to refine policies relevant to procurement, vendor management, outsourced accountability, and cybersecurity standard operating procedures. This conversion of incident experience into updated organisational artefacts was an important part of the learning process, because it moved lessons from observation into future preparedness.

Conclusion

Aurum's ransomware incident illustrates the organisational nature of cyber risk. More than just an ICT failure, it was a leadership challenge, a governance test, and a public health continuity crisis. The organisation recovered because several conditions aligned: leadership activated incident command early; communications were handled with discipline; segmented, cloud-hosted core business systems reduced the risk of total collapse; ex-

ternal forensic expertise was brought in quickly, and immutable backups supported clean-room restoration. At the same time, the incident exposed weaknesses in monitoring, credential governance, vendor oversight, and data visibility which are likely to be familiar to many resource-constrained organisations.

The broader implication is that cyber resilience is not created by technical controls alone, nor by reflection after a single event. It depends on the ability to capture information during disruption, review it through multidisciplinary governance structures, test assumptions against technical and operational evidence, and convert the resulting insight into improved plans, controls, accountabilities, and simulations for future crises.

Acknowledgements

To protect confidentiality and uphold ethical and security standards, all donor and other personal information has been removed or withheld. All authors are employees of Aurum and three of the authors were part of the emergency response team and therefore had access to the process as it unfolded. Approval for the case study was obtained from the CEO of the Aurum Group.

Abbreviations

Abbreviation	Description
COVID-19	coronavirus-19
GDPR	General Data Protection Regulation
HR	human resources
ICT	information and communications technology
IP	internet protocol
NPO	non-profit organisation
POPIA	Protection of Personal Information Act
QC	quality control
RPO	recovery point objective
RTO	recovery time objective
SIEM	security information and event management
SOC	security operations centre
SWOT	strengths, weaknesses, opportunities, threats
WORM	write once, read many

Published: October 26, 2026 CAT.



This is an open-access article distributed under the terms of the Creative Commons Attribution-NonCommercial 4.0 International License (CCBY-NC-4.0). View this license's legal deed at <https://creativecommons.org/licenses/by-nc/4.0> and legal code at <https://creativecommons.org/licenses/by-nc/4.0/legalcode> for more information.

References

1. Kirubavathi G, Regis Anne W, Sridevi UK. A recent review of ransomware attacks on healthcare industries. *Int J Syst Assur Eng Manag*. 2024;15(11):5078-5096. doi:[10.1007/s13198-024-02496-4](https://doi.org/10.1007/s13198-024-02496-4)
2. National Institute of Standards and Technology. *NIST Cybersecurity Framework 2.0*. NIST; 2024. doi:[10.6028/NIST.SP.1300](https://doi.org/10.6028/NIST.SP.1300)
3. Europol. *Law enforcement disrupts world's biggest ransomware operation*. Europol. February 20, 2024. Accessed January 15, 2026. <https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-disrupt-worlds-biggest-ransomware-operation>
4. Kruse CS, Frederick B, Jacobson T, Monticone DK. Cybersecurity in healthcare: a systematic review of modern threats and trends. *Technol Health Care*. 2017;25:1-10. doi:[10.3233/THC-161263](https://doi.org/10.3233/THC-161263)
5. Shahzadi A, Ishaq K, Dogar AB, et al. Safeguarding the healthcare sector from ransomware attacks: insights from a literature review. *Peer J Comput Sci*. 2025;11:e3073. doi:[10.7717/peerj-cs.3073](https://doi.org/10.7717/peerj-cs.3073)
6. Jiang JX, Ross JS, Bai G. Ransomware attacks and data breaches in US health care systems. *JAMA Netw Open*. 2025;8(5):e2510180. doi:[10.1001/jamanetworkopen.2025.10180](https://doi.org/10.1001/jamanetworkopen.2025.10180)
7. McGlave CC, Nikpay SS, Henning-Smith C, Rydberg K, Neprash HT. Characteristics of short-term acute care hospitals that experienced a ransomware attack from 2016 to 2021. *Health Aff Sch*. 2023;1(3):qxad037. doi:[10.1093/haschl/qxad037](https://doi.org/10.1093/haschl/qxad037)
8. Fišter K, Belani H. Cybersecurity preparedness and resilience in health care: a narrative review. *Int J Health Gov*. 2026;31(1):38-49. doi:[10.1108/IJHG-07-2025-0108](https://doi.org/10.1108/IJHG-07-2025-0108)
9. Neprash H, McGlave C, Nikpay S. Hacked to pieces? The effects of ransomware attacks on hospitals and patients. *Am Econ J Econ Policy*. 2026;18(1):256-281. doi:[10.1257/pol.20240594](https://doi.org/10.1257/pol.20240594)
10. Davids A, Fataar A, Zama A, et al. Clinicians' perspectives on the impact of a ransomware attack on a chemical pathology laboratory at a tertiary hospital in South Africa. *EJIFCC*. 2026;37(2):268-280. Accessed January 15, 2026. https://www.researchgate.net/publication/403380802_Clinicians'_Perspectives_on_the_Impact_of_a_Ransomware_Attack_on_a_Chemical_Pathology_Laboratory_at_a_Tertiary_Hospital_in_South_Africa
11. Dameff C, Tully J, Chan TC, et al. Ransomware attack associated with disruptions at adjacent emergency departments in the US. *JAMA Netw Open*. 2023;6(5):e2312270. doi:[10.1001/jamanetworkopen.2023.12270](https://doi.org/10.1001/jamanetworkopen.2023.12270)
12. Pham TT, Loo TM, Malhotra A, et al. Ransomware cyberattack associated with cardiac arrest incidence and outcomes at untargeted, adjacent hospitals. *Crit Care Explor*. 2024;6(4):e1079. doi:[10.1097/CCE.0000000000001079](https://doi.org/10.1097/CCE.0000000000001079)
13. Belloni G, Monod S, Poroës C, Bühler N, Avendano M, Wernli D. Health systems governance, shocks and resilience: a scoping review of key concepts and theories. *BMJ Glob Health*. 2025;10(6):e017358. doi:[10.1136/bmjgh-2024-017358](https://doi.org/10.1136/bmjgh-2024-017358)
14. Veeam Software. *From risk to resilience: 2025 ransomware trends and proactive strategies*. Veeam. April 2025. Accessed January 15, 2026. <https://www.veeam.com/blog/ransomware-trends.html>
15. Cybersecurity and Infrastructure Security Agency. *Shields up guidance: implementing cybersecurity measures now to protect against critical threats*. CISA. March 2022. Accessed January 15, 2026. https://www.cisa.gov/sites/default/files/publications/Shields%20Up%20Guidance%20-%20Implementing%20Cybersecurity%20Measures%20Now%20to%20Protect%20Against%20Critical%20Threats_April%202023.pdf
16. CIGENT. *Ransomware and recovery time: what you should expect*. CIGENT. March 2024. Accessed January 15, 2026. <https://www.cigent.com/blog/ransomware-and-recovery-time-what-you-should-expect/>
17. van Boven LS, Kusters RWJ, Tin D, et al. Hacking acute care: a qualitative study on the health care impacts of ransomware attacks against hospitals. *Ann Emerg Med*. 2024;83(1):46-56. doi:[10.1016/j.annemergmed.2023.04.025](https://doi.org/10.1016/j.annemergmed.2023.04.025)

18. Harel Y, Carmeli A. A strategic cybersecurity oversight framework: a board's imperative. *J Cybersecur*. 2025;11(1):tyaf021. doi:[10.1093/cybsec/tyaf021](https://doi.org/10.1093/cybsec/tyaf021)
19. Jalali MS, Russell B, Razak S, Gordon WJ. EARS to cyber incidents in health care. *J Am Med Inform Assoc*. 2019;26(1):81-90. doi:[10.1093/jamia/ocy148](https://doi.org/10.1093/jamia/ocy148)
20. Federal Bureau of Investigation, Cybersecurity and Infrastructure Security Agency, Multi-State Information Sharing and Analysis Center. *Stop ransomware: ransomware awareness for institutions of higher education and K-12 schools*. Joint Cybersecurity Advisory. CISA. September 2023. Accessed January 15, 2026. https://www.cisa.gov/sites/default/files/2023-09/aa23-250a-stopransomware-ransomware-awareness-for-ies-and-k-12-schools_5.pdf
21. Strygin A, Escobar M. *What is WORM (write once, read many)?* Veeam. July 2024. Accessed January 13, 2026. <https://www.veeam.com/blog/what-is-worm-storage.html>
22. O'Brien J, Samtani S, Li W. Moving beyond compliance: a maturity model for cyber-resilience investments in high-risk sectors. *Comput Secur*. 2024;138:103686. doi:[10.1016/j.cose.2024.103686](https://doi.org/10.1016/j.cose.2024.103686)
23. Microsoft. *What is endpoint detection and response (EDR)?* Microsoft. Accessed January 15, 2026. <https://www.microsoft.com/en-us/security/business/security-101/what-is-edr-endpoint-detection-response>