HealthManagement
Promoting Management and Leadership

Cyber vs Disaster Recovery Reshapes Hospital Preparedness

Ransomware has reshaped how hospitals plan for service continuity, exposing gaps between traditional disaster recovery and the realities of cyber incident restoration. When core systems are encrypted or compromised, recovery is rarely a straightforward restoration from backups. Clinical services can be disrupted for weeks while teams operate on temporary workarounds and rebuild environments with forensic assurance. Experience at a large regional health network shows how quickly an infection can cascade across complex infrastructure and how long essential platforms can remain unavailable. Parallel efforts at a major health system demonstrate the value of rehearsed contingencies that assume extended outages rather than short interruptions. Together these insights point to a resilience model that keeps patient care moving under constraint, treats cyber recovery as distinct from physical disaster recovery and plans explicitly for prolonged disruption.

From Disaster Recovery to Cyber Recovery

An attack during the COVID-19 pandemic illustrated the speed and scale of impact that differentiates cyber recovery from traditional disaster recovery. A malicious attachment was opened on a work computer and later connected to the virtual private network. Within a short window, 1,300 servers went offline in around 15 minutes. Traditional disaster recovery plans assume rapid restoration from trusted backups after tangible events. Cyber incidents introduce uncertainty about system integrity, possible data exfiltration and the need for forensic validation before bringing services back.

This difference set the trajectory for response. The electronic health record was unavailable for four weeks, far exceeding downtime procedures that anticipated hours or a few days. Teams could not rely solely on standard playbooks. Cyber recovery required building and validating systems in stages while maintaining care delivery. It reframed assumptions about visibility, because the indicators of compromise were not obvious in the way physical incidents are. Recovery pace was dictated by the need to understand what happened, clean the environment and re-establish trust in every component that supported clinical operations.

Sustaining Care During Prolonged Outages

Extended outages brought into focus which services could adapt and which could not. Routine charting, ambulatory activity and emergency care continued with modified processes, but radiation oncology could not proceed safely without the technology that supports treatment. To avoid unacceptable gaps in care, the organisation built an isolated interim environment dedicated to sustaining cancer services while forensic work and restoration continued elsewhere. In parallel, an offline version of the electronic health record was connected to selected desktop computers and printers to generate patient data printouts for clinicians. This approach provided essential information at the point of care without reconnecting to untrusted systems.

Must Read:** **Defending Against Interlock Ransomware

Recovery also required large-scale remediation. The hospital replaced 5,500 compromised endpoints and introduced new security tooling during the incident. Measures included deploying an endpoint detection and response platform, moving to immutable backups and using cloud-based visibility to compensate when on-premises tools were ineffective. These steps aimed to reduce the likelihood of a repeat event and shorten recovery time if one occurred. The experience prompted wider changes to downtime planning, shifting from short interruptions to multiweek contingencies with practical mechanisms for delivering essential data, segmenting temporary environments and prioritising services that cannot safely revert to paper.

The operational lesson was clear. Organisations need pathways that allow critical services to continue with safe technical enablers when primary systems are unavailable. That means designing interim environments that are isolated, establishing trusted data flows that do not rely on the

compromised network and preparing clinical teams to work with reliable printouts or offline tools for as long as necessary.

Exercising Resilience and Understanding Threats

Preparedness improves when scenarios are tested under realistic constraints. Since 2018 a large health system has run ransomware exercises that bring together executive leaders and clinical operations to assess how services would be maintained if key systems were unavailable for an extended period. The focus is on concrete impacts such as the loss of printing or scanning, and how teams would adjust workflows to sustain care. This moved planning from theoretical documents to operational readiness grounded in the specifics of how clinical and support functions actually work.

To support this, the organisation mapped critical processes across departments over two years, determining what each area would need to continue operating for 30 days rather than a few hours. This mapping clarified dependencies, manual fallbacks and the minimum technical capabilities to keep patient care moving. Technical readiness was further tested through red team and blue team exercises with third parties, probing monitoring and response capabilities. Outcomes showed where existing tools could be used more effectively and where new capabilities were required to support resilience after an attack.

The threat landscape underlines the need for such preparation. Insider threats remain significant because trusted physical or virtual access can lead to harm through negligence or malice. Ransomware continues to evolve and shows no sign of slowing. Denial-of-service attacks can knock systems offline in any production environment, which is especially challenging when technology underpins much of patient care. Social engineering remains a common entry point, and the rise of convincing deepfakes challenges traditional verification. These dynamics reinforce a posture that treats prevention, detection and recovery as complementary capabilities, with cyber recovery recognised as a distinct discipline that enables safe continuity of care during extended disruption.

Hospitals are recalibrating resilience for incidents that can disable critical systems at speed and keep them offline for weeks. Experience with rapid server outages, a four-week electronic health record interruption and large-scale endpoint remediation shows that recovery depends on interim technical environments, reliable offline data delivery and methodical rebuilding. Programmes that rehearse extended outages, map 30-day continuity needs and test monitoring through adversarial exercises strengthen operational readiness. The central lesson is consistent across contexts: plan for prolonged disruption, maintain essential clinical services with safe temporary solutions and build cyber recovery alongside traditional disaster recovery so that patient care continues even when the unexpected occurs.

Source: HealthTech

Image Credit: iStock

Published on : Mon, 29 Sep 2025