



Ransomware: A Public Health Crisis



Executive Summary

Ransomware is no longer just an IT risk. In healthcare, it disrupts care delivery, delays treatment, and directly threatens patient lives. Attacks cascade across entire health systems, overwhelm regional capacity, and impose severe financial and reputational costs. The evidence shows ransomware must be treated as a public health crisis. This paper examines key issues regarding the impact of ransomware in healthcare, including:

Patient Mortality:

Data found in-hospital mortality increased 33 percent during ransomware incidents, equal to 42-67 preventable deaths over five years. Mortality rose from three in 100 Medicare patients to four in 100 under attack conditions.

Clinical Disruption:

Imaging, labs, pharmacy, billing, and communications can fail instantly, leading to canceled appointments, diverted ambulances, delayed surgeries, and handwritten records prone to errors.

Regional Ripple Effects:

Neighboring hospitals absorb diverted patients, resulting in longer waits, more cardiac arrests, and higher stroke activations. In rural areas, a single attack can cut off urgent care for entire communities.

Financial Impact:

Average recovery cost in 2024 was \$2.5 million, with most ransom demands exceeding \$1 million. Prolonged outages have forced small hospitals offline permanently, threatening local healthcare access.

PHI Theft and Extortion:

Nearly two-thirds of incidents involve data theft, with attackers using double or triple extortion to pressure victims and expose sensitive patient information.

Policy Momentum:

Bipartisan legislation and the first proposed HIPAA Security Rule update in a decade reflect growing recognition that healthcare cybersecurity is essential to public safety.

Healthcare cannot defend against ransomware alone. Protecting patient lives and ensuring care continuity requires a whole of society response that unites providers, government, vendors, and communities in shared defense. Without coordinated action, ransomware will continue to erode patient safety, public trust, and the stability of modern healthcare.

33% 

increase in mortality rate during an attack

\$2.5M 

average recovery cost in 2024

2/3rds 

of incidents involve PHI + org data theft



Ransomware Hits Healthcare Putting Lives at Risk

Ransomware attacks against healthcare organizations threaten lives, delay critical care, shut down vital networks, and throw entire health systems into chaos. These impacts extend far beyond IT. As the [United Nations](#) highlighted last November, “ransomware and other cyberattacks on hospitals and other health facilities are not just issues of security and confidentiality; they can be issues of life and death.”

Critical systems like imaging, labs, other diagnostics, pharmacy, billing, and communications can go dark in an instant. And when they do, care delivery is stalled, ambulances rerouted, surgeries delayed, and vital diagnostic tests lost. Staff revert to handwritten records, raising the risk of transcription errors, misplaced files, and medication mistakes. In operating rooms, anesthesia checklists disappear; ICU vital signs go unrecorded putting lives at risk; in emergency departments, clinicians may not know a patient's allergies or the last medication administered. Every minute matters.



Ransomware and other cyberattacks on hospitals and other health facilities are not just issues of security and confidentiality; they can be issues of life and death.

– United Nations

The scale of these impacts is also increasing. Over [250 healthcare organizations \(PDF\)](#) experienced ransomware attacks in 2024. That is two and a half times the amount that experienced attacks in 2021 and [over five times](#) the amount from 2015. We must protect against ransomware attacks with a sense of urgency, using a whole-of-society approach. Else, we invite devastating patient outcomes, crippling financial costs, operational impacts that ripple across communities, and losing patient trust in the healthcare system:

- Government first responders and regulators can work together to provide timely assistance in balance with holding industry stakeholders to reasonable account for doing their part. This requires better communication and prioritization of needs within the government, and two-way lines of communication that serve a public safety mission over stove-piped agency mission sets.
- Healthcare IT vendors and cybersecurity firms can provide [Secure-by-Design](#) technical solutions to healthcare industry clients, source hardware and software components from trusted supply chains, and responsibly report cybersecurity vulnerabilities, threats, and trends to other industry partners so they can proactively defend against emerging threats.
- Providers can reimagine their approach to cybersecurity, from enterprise architecture to frontline training, to protect patient lives, institutional reputation, and public trust.
- Other healthcare industry stakeholders globally can incorporate cybersecurity related ethical, market, and legal hazards into their principled approach to decision-making: healthcare executives and boards can account for these risks when making hiring and budget decisions; universities can train future healthcare professionals in how to responsibly take cybersecurity into account in their everyday job roles; patients themselves can be equipped to know their cybersecurity and data rights and risks, to make better informed decisions about their care.

If only one member of society attempts to shoulder the community's cybersecurity burdens, they become a single point of failure. Together, we can create a future where ransomware actors will have to beat every member of the healthcare ecosystem before they can impact one.

For this reason, the Halcyon Ransomware Research Center (RRC) is making protecting the healthcare sector from ransomware attacks one of its flagship priorities. This paper provides a public baseline of current ransomware threats and their impact on the sector, and initial recommendations for healthcare organizations to build resilience. The RRC intends to build on this baseline with data-driven intelligence and policy reports conducted in coordination with RRC partners.



Limited cybersecurity investment forces providers to focus on personnel gaps instead of building robust technical defense layers.

Healthcare is a High-Value, High-Risk Target

Healthcare organizations have little tolerance for downtime and safeguard highly sensitive personal health information (PHI), making them lucrative targets for ransomware operators. Yet these organizations are often under-resourced and unable to contend with today's sophisticated attacks.

Many manage technical debt—e.g., legacy IT systems whose patching lifecycle has ended, fractured network architectures, and outdated security solutions—and other risks that make them vulnerable to threat actors. This risk is understandable, because healthcare systems typically operate on thin budgets and choose to prioritize clinical care over cyber defense. Limited cybersecurity investment forces providers to focus on personnel gaps instead of building robust technical defense layers.

Yet this is a false choice, because investing in cyber defense is the same as investing in clinical care. Ransomware actors' sophisticated tools and understanding of specific healthcare systems arms them to easily exploit those systems when they are left unprotected. They can breach defenses, disable backups, and launch encryption campaigns within hours. Criminals are then free to do harm, risking patient care.

Even when endpoint protection (EPP) and endpoint detection and response (EDR) tools are in place, attackers are successful at an alarming rate. They can circumvent traditional tools in minutes using trusted system processes, by exploiting vulnerable drivers, or by back-doored installers.

Without sufficient funding and goals established at the executive level, organizations likely cannot avoid making this false choice of prioritizing immediate healthcare provider needs over protection of the very digital infrastructure that providers use. Nor can they maintain around-the-clock monitoring, behavioral insights, or dedicated ransomware prevention solutions at the tactical level. The result is that hospitals are exposed to fast-moving cyber campaigns.

Devastating Patient Outcomes and Confirmed Fatalities

Ransomware delays diagnosis, interrupts treatment, and in worst case scenarios impacts patient mortality. A University of Minnesota analysis of Medicare data found that in-hospital mortality rates for hospitalized Medicare patients increased by 33 percent at hospitals victimized by ransomware, translating to an estimated 42 to 67 additional deaths across a five-year period. In practical terms, mortality rose from roughly three in 100 hospitalized Medicare patients to four in 100 during ransomware attack periods. These findings demonstrate that even short-term care disruptions from ransomware can directly translate into preventable patient deaths.



Ransomware delays diagnosis, interrupts treatment, and in worst case scenarios impacts patient mortality.

Other research found that in the first week of a ransomware attack, hospitals turned away patients, leading to a 20 percent drop in admissions and a 40 percent decrease in emergency cases, and limiting diagnostic testing for those treated. These providers have described “operating blind,” with handwritten notes supplanting electronic health records (EHRs) and decisions made without lab or imaging confirmation. For conditions like stroke or sepsis, even a short delay can determine survival.

Across affected hospital trusts, NHS officials documented 170 separate incidents of patient harm ranging from delayed cancer screenings and transfusions to postponed maternal care. In 2024, following a ransomware attack on a London pathology provider, there was a confirmed patient fatality linked to delayed blood test results.

Operational and Financial Impact

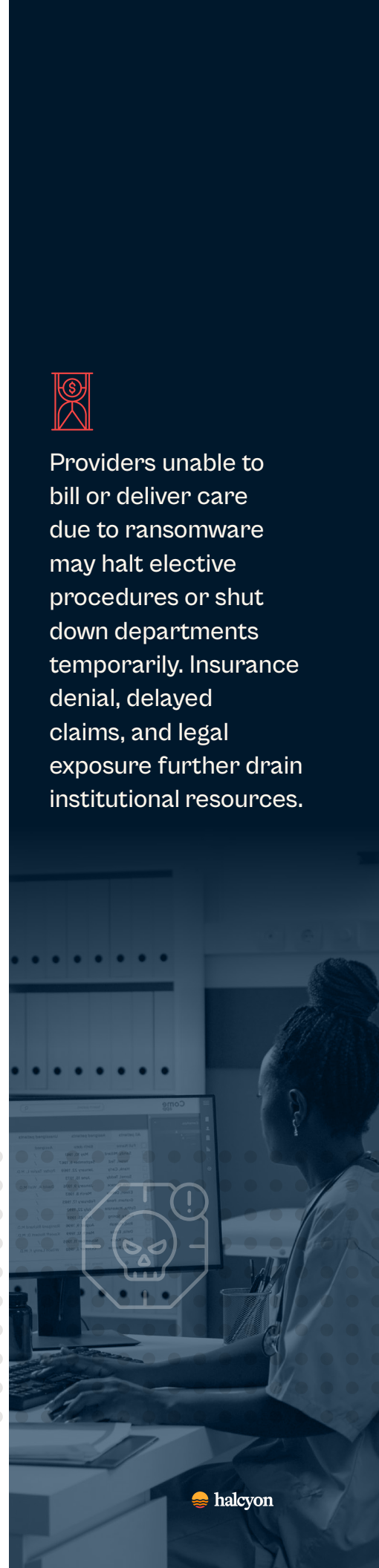
Ransomware attacks also inflict staggering financial damage. Beyond paying a potential ransom, hospital and other healthcare facility victims face additional costs associated with recovery, legal fees, lost revenue from downtime, patient notifications, and reputational damage. In 2024, the average cost to recover from a healthcare ransomware attack was over \$2.5 million, with nearly two-thirds of ransom demands exceeding \$1 million.

Impacts often extend beyond the healthcare organizations attacked. Providers unable to bill or deliver care due to ransomware may halt elective procedures or shut down departments temporarily. Insurance denial, delayed claims, and legal exposure further drain institutional resources.

Small and rural hospitals face the greatest financial risk. And rural hospital closures—temporary and permanent—can be catastrophic for healthcare access across entire regions. Short outages can cause weekly losses of \$1.5 to \$2.5 million, which can threaten the long-term financial viability of providers operating on thin margins. For example, a rural Illinois hospital shut down after 14 weeks offline, as billing and staffing losses pushed cashflow into crisis.



Providers unable to bill or deliver care due to ransomware may halt elective procedures or shut down departments temporarily. Insurance denial, delayed claims, and legal exposure further drain institutional resources.



Regional Ripple Effects: The Blast Radius

When a hospital or clinic goes offline, nearby providers are strained. They are forced to absorb influxes of diverted patients, stretching existing resources. A JAMA Network Open report documented that during a 2021 ransomware attack on four hospitals, two adjacent hospitals experienced a surge in emergency department patient volume, longer waiting times, and increased stroke code activations.

Another study highlighted a dramatic rise in time-sensitive emergencies. In hospitals that were not directly hit by ransomware, emergency department arrivals went up by 15 percent, wait room time by 48 percent, cardiac arrests by 81 percent, and suspected strokes surged by 75 percent during attacks at nearby facilities. Survival rates for cardiac arrests also fell sharply, reflecting delays in emergency response caused by network-wide disruptions.

The more regional stakeholders do their part, the safer a region's patient needs are from the effects of ransomware. When there is no other hospital nearby during an attack against a rural hospital, the risk of additional patient mortality or adverse outcomes significantly increases.

These findings underscore that ransomware is not just a technical or financial risk, it is a direct threat to patient safety across entire regions. Attacks on one hospital ripple outward, overwhelming neighboring facilities and amplifying the risk of preventable deaths. In rural areas with no backup capacity, the consequences are even starker, potentially leaving entire communities without access to emergency care. Cybersecurity gaps in healthcare therefore translate directly into delayed treatment, worsened outcomes, and lives lost, making proactive defense a matter of public health, not just IT security.

PHI Theft and Data Extortion

Nearly two-thirds of ransomware incidents involve data theft, and more than half include additional extortion demands after PHI is exfiltrated. Before locking systems, attackers often exfiltrate patient data, especially PHI. They usually perform double extortion, demanding payment first for decryption keys to retrieve locked data, and again to prevent public exposure or sale of the stolen data.

For example, during the 2024 Change Healthcare attack, the BlackCat/ALPHV ransomware gang exfiltrated over six TB of billing and PHI before encrypting and incapacitating significant portions of Change Healthcare's functionality. Change Healthcare paid \$22 million in response to the gang's demands. This prevented the release of the stolen data, but unfortunately the extortionists did not restore Change Healthcare's data.



Nearly two-thirds of ransomware incidents involve data theft, and more than half include additional extortion demands after PHI is exfiltrated.



Hospitals face operational paralysis, the inability to access EHRs, lab systems, or diagnostic imaging, while also confronting patient privacy breaches.



Across many industries, ransomware actors have also conducted what is termed 'triple extortion,' wherein gangs extend ransom demands beyond the victim organization to include affected third parties, such as patients, customers, or business partners. For example, the [Hive ransomware group](#), which frequently targeted healthcare providers, attempted to extort money not only from hospitals but also from the individuals whose data was exposed during attacks.

Nearly two-thirds of ransomware attacks against healthcare providers simultaneously encrypted and exfiltrated data. Also, attackers routinely target backups in two-thirds of healthcare ransomware cases, knowing the inability to restore systems from backups means a higher probability of payment. While some attackers skip the encryption step and demand ransom solely for releasing stolen data, the healthcare sector still sees full-scale encryption in most attacks.

This double and triple extortion model magnifies the harm. Hospitals face operational paralysis, the inability to access EHRs, lab systems, or diagnostic imaging, while also confronting patient privacy breaches. Sensitive PHI such as test results, diagnoses, and treatment histories can be leaked, sold, or used for targeted blackmail.



Nearly two-thirds of ransomware attacks against healthcare providers simultaneously encrypted and exfiltrated data.

Even with successful system decryption, the data breach triggers breach notification obligations, possible HIPAA enforcement actions, class-action lawsuits, credit monitoring expenses, and patient counseling. Individual patients may suffer emotional harm from fear that their most sensitive medical histories have been weaponized against them, and delays in care can erode trust between them and their provider.

This threat model signifies a fundamental assault on the confidentiality, trust, and integrity of the healthcare ecosystem. When healthcare leaders shift from reactive data recovery to proactive data protection and threat deterrence, they ensure patient support and trust.

Growing Consensus for Healthcare Cybersecurity Policy Mandates

US policymakers recognize ransomware attacks on healthcare as a significant threat to national security and public health, and their appetite to assign roles and responsibilities for mitigating this threat is growing. For example:



US policymakers recognize ransomware attacks on healthcare as a significant threat to national security and public health.

- The bipartisan draft Healthcare Cybersecurity Act of 2025 directs the Cybersecurity and Infrastructure Security Agency (CISA) and the Department of Health and Human Services (HHS) to collaborate more closely and provide cybersecurity training to healthcare providers.
- The bipartisan draft Health Care Cybersecurity and Resiliency Act similarly mandate the provision of cybersecurity training for owners and operators of healthcare and public health digital infrastructure. It also authorizes HHS to provide cybersecurity grants to eligible healthcare entities.
- HHS has proposed the first update to the HIPAA Security Rule in over a decade focused on cybersecurity. The related Notice of Proposed Rulemaking, which was authored and published during the end of the Biden Administration and beginning of the Trump Administration, respectively, revises existing standards to better protect digital PHI, shifting accountability and cost (estimated at \$9 billion the first year and \$6 billion for immediate subsequent years) for safeguarding digital PHI to regulated entities and health plan sponsors.
- These proposed policies reflect a powerful shift: growing bipartisan support for assigning legal accountability and liability for healthcare sector cybersecurity roles and responsibilities. Healthcare organizations that fail to invest in cybersecurity now may be unprepared to comply with such new laws and policies if they are formally adopted. This may risk legal penalties, grant restrictions, rising insurance costs, and loss of operational accreditation.

Coordinated Defense: A Public-Private Imperative

We need a whole-of-society approach to defending hospitals and other healthcare providers from ransomware attacks and other malicious cyber activity. We cannot defend against the speed and scale of such attacks with siloed defenses. It requires cohesive public-private preparation, incident response, intelligence sharing, and resilience, where healthcare providers and vendors, government agencies, the cybersecurity industry, the Health-ISAC, and other stakeholders work together in real time.

Collaborative models like the Joint Cyber Defense Collaborative (JCDC) at CISA, the HHS 405(d) Program, and voluntary reporting frameworks shared by trusted parties enable actionable intelligence sharing, broader situational awareness, and a rightsizing of organizational strategies, roles, responsibilities, and resource allocations across all stakeholders.

Healthcare organizations cannot spend or hire their way out of the ransomware crisis alone. But a whole-of-society approach could elevate baseline security for the entire ecosystem and make it harder for threat actors to succeed.



We need a whole-of-society approach to defending hospitals and other healthcare providers from ransomware attacks and other malicious cyber activity.



A Leadership-Centered Framework for Resilience

Ransomware should continue to be elevated to a strategic executive and board-level concern. Effective mitigation demands a cohesive and system-wide strategy, centered on organizational resilience.

This includes integrating cyber risk into enterprise governance and policy, embedding secure infrastructure and monitoring in everyday operations, fostering a culture of vigilance and preparedness, and ensuring partnerships extend beyond internal walls to include regional collaboration.

The following recommendations offer practical steps to accomplish these goals at the board and executive leadership level, including but not limited to CISOs, at the strategic level:



Board-Level Cybersecurity Accountability:

Ensure cybersecurity budgetary and staffing requirements are standing agenda items in board meetings, addressed not only during CISO updates but also within Legal, Compliance, and Accounting discussions to embed cyber risk into core governance and financial oversight.



Engagement and Expectation Setting with Incident Response Stakeholders:

Sound incident response often requires timely and effective communication and coordination between internal and external parties. Establishing good relations and setting expectations of roles and responsibilities between your organization's incident response team and external partners in advance of an incident is a best practice. Some external partners include, but are not limited to, third party incident response firms and general counsel; regional leaders responsible for FBI, CISA, and HHS cyber incident response; and Health-ISAC leadership, who may offer connections to other ISAC members who have experienced similar incidents.



Participation in Incident Response

Planning: CISOs and their teams often – and rightly – take a leadership role in developing organizations' cyber incident response policies and plans. It is critically important that the wider workforce is trained in these plans. Similarly, an organization's board and executives would benefit from incident response training tailored to the special roles they will be expected to play during a crisis. This training is good preparation, and it can inspire constructive feedback and accountability from an organization's top level before an attack occurs.

The following recommendations offer practical steps for CISOs and their teams to accomplish resilience at the organizational planning level:



Develop and Practice Incident Response

Plans: Cyber incident response policies and plans, and periodic preparedness drills, should include clinical, operational, legal, communications, supply chain, and patient advocacy teams to simulate real-world incidents and coordinate an effective crisis response. In addition to internal coordination, these plans should account for coordination with external partners, including but not limited to third party incident response firms and general counsel; local FBI, CISA, and HHS incident response personnel; and other local, state, and federal government entities who may offer assistance or request information based on sector- or region-specific laws, policies, and regulations.



Staff Training and Cultural Engagement:

Phishing simulation training alone is ineffective, so prioritize phishing-resistant MFA and technical safeguards. Reinforce these with embedded, scenario-based exercises like tabletop drills for clinical and administrative staff, supported by cultural initiatives and leadership engagement that make security awareness part of daily operations.



Vendor and Regional Collaboration: Smaller providers should leverage available federal grant programs, such as HRSA cooperative agreements and the [CISA/FEMA State & Local Cybersecurity Grant Program](#), which provided approximately \$280 million in Fiscal Year 2024 to fund cybersecurity upgrades, shared services, and training. Regional partnerships and consortiums offer cost-effective, scalable solutions that extend resilience beyond large health systems.

The following recommendations offer practical steps for CISOs and their teams to accomplish resilience at the tactical level:



Tamper-Resistant Endpoint and Detection

Controls: No endpoint protection or detection tool can fully resist modern attackers—they routinely disable or bypass them. To address this, deploy a dedicated anti-ransomware solution that actively protects EPP and EDR systems from being unhooked or terminated by attackers, while monitoring behavior in real time to detect ransomware activity before encryption occurs.



Data Exfiltration Protection and Early

Warning: Attackers now often steal patient data before encryption, then demand additional ransom payments. Implement data loss prevention and network monitoring tools to detect unusual outbound data activity, enabling early alerts and faster incident response.



Segmented Backups: Follow the 3-2-1 principle; maintain three copies of patient data across two media types, with one copy isolated or offline. Conduct monthly recovery tests that simulate real-world disaster scenarios to verify data integrity and ensure fast restoration capabilities.



Network Micro-Segmentation: Partition your network by function such as EHR, lab, pharmacy, billing, and administration to restrict lateral movement in the event of a breach and protect critical systems from rapid spread.



Identity and Access Governance: Enforce phishing-resistant multi-factor authentication across all user accounts.

Monitor administrative-level access and revoke permissions promptly when staff roles change, or personnel depart to prevent misuse or abuse.

This layered approach ensures ransomware defenses are not limited to perimeter protections but integrated across the organization to protect critical systems and support sound incident response.

The Halcyon Ransomware Research Center (RRC) looks forward to generating more data-driven organizational best practices and policy recommendations as it builds on this baseline paper. Its goal is to expand these recommendations to include solutions that can be adopted beyond individual healthcare organizations, towards a truly whole-of-society approach.

In Summary: Ransomware is a Public Health Emergency

Ransomware in healthcare has become a public health crisis with damaging effects. When digital systems fail, hospitals lose access to labs, imaging, pharmacy, billing, and communications. That collapse causes care delays, missed treatments, outpatient backlogs, and emergency diversions. Ambulances are rerouted, surgeries are delayed, and clinicians revert to handwritten orders, prone to errors.

Every minute counts in an emergency. Waiting for lab results can delay life-saving treatment for strokes, heart attacks, or sepsis. Real-world incidents have led to thousands of canceled appointments, confirmed patient deaths, and spikes in mortality during breach periods. These attacks spread across entire health systems. Emergency waiting times increase, and acute cases surge. In rural regions, a single ransomware event can cut off urgent care for an entire community.

This is not just a financial crime. It is a direct attack on patient care. When digital systems fail, clinical workflows, emergency response, and overall healthcare integrity unravel. Ransomware must be treated with the same urgency as infectious outbreaks or mass casualty events. Response and planning must include clinical leadership, emergency management, legal counsel, operational staff, and community partners to ensure resilience across the care continuum.

The stakes extend beyond hospitals. A single attack cascades through supply chains, public safety, and local economies, threatening the well-being of entire regions. Protecting healthcare from ransomware is therefore a whole-of-society responsibility, one that requires coordination between government, private industry, and communities to safeguard patient lives and preserve trust in critical infrastructure.

Halcyon, the leading anti-ransomware solution provider, is purpose-built to defeat ransomware attacks. Our technology takes an end-to-end approach to proactively disrupt threats at every stage of the attack lifecycle, from pre-execution to data exfiltration and encryption. With a 24/7 expert team that does the heavy lifting for you, and a robust ransomware warranty, Halcyon eliminates the need for ransom payments, ensures operational continuity, and protects businesses from data extortion. **Learn more at halcyon.ai.**



This is not just a financial crime. It is a direct attack on patient care. When digital systems fail, clinical workflows, emergency response, and overall healthcare integrity unravel.

