ARMIS®

WHITE PAPER

Protecting Healthcare Organizations from the Devastating Impacts of Ransomware

Introduction

Healthcare Delivery Organizations (HDOs) are the largest and most lucrative target for ransomware attacks in the world. Owing to the sensitive nature of the devices healthcare delivery organizations rely on, and the proximity to patient care of those devices, malicious actors have targeted HDOs for being more likely to pay ransomware demands to ensure continuity of patient care. Securing the healthcare environment from cyberattacks is more important than ever.

A complicating factor for cybersecurity efforts is the massive uptick in connectivity in healthcare environments. Due in part to accelerated digital transformation efforts in the wake of the COVID-19 pandemic, more of the healthcare environment is connected than ever before, from the computers used for intake to medical carts to smartphones and laptops, even the HVAC system or building management systems.

This white paper will delve into the true impact of cyberwarfare in healthcare, navigating the ever-growing threat of ransomware attacks, and provide a guide for building a better, safer, and more proactive approach to cybersecurity to protect your organization and patients.

The Cost of a Data Breach in Healthcare

The digital healthcare landscape is growing and changing rapidly, expanding the attack surface at a rate that leaves organizations struggling to keep pace and ultimately, leaving them vulnerable to attacks. What's more, is the lack of cybersecurity resources and funding within healthcare organizations, forcing them to make ends meet with limited resources and personnel. Many organizations end up falling back into old ways without knowing how to improve or where to begin. This means following mostly manual processes, spending hours combing through data and coming up with ad hoc action plans, and needing to make countless decisions about which areas to prioritize based on incomplete information.

The stakes of poor visibility and cybersecurity posture are higher than ever. The average **cost of a healthcare data breach in 2023** was approximately $11 million – the costliest of any sector. According to Armis Labs, 37% of medical, healthcare, and pharmaceutical organizations reported over two breaches in the past year. And it's likely much worse than many professionals are even aware of, given that organizations are often blind to their own vulnerabilities. In a healthcare context, the vulnerabilities are often found in specialized devices that are difficult to upgrade (if an upgrade is even possible or enabled) due to their importance and patient usage, and expensive to replace. In an environment that is constantly aiming to provide the best quality of care with increasingly stringent budgets, cybersecurity is often operating on a less-than-ideal level. Unfortunately, without proper visibility of the attack surface, the threat of an attack is always looming.

$11M

The average cost of a healthcare data breach in 2023

37%

Of healthcare organizations have suffered 2+ attacks

53%

Of medical devices have known vulnerabilities that are exploited

35%

Feel their organization has insufficient cybersecurity budget

Spotlight on Ransomware Attacks

57% of healthcare organizations impacted by cyberattacks reported poor patient outcomes as a result

While attacks in the healthcare industry prove costly to the business, the greater impact is felt by patients, their safety, and their access to timely and effective care. **Health-ISAC's Q4 report** for last year highlighted that ransomware attacks against the healthcare sector rose steadily throughout 2023. Patients are significantly at risk in the event of a ransomware attack, with a **28% increase in mortality rate** in affected healthcare organizations in 2023.

In 2024 alone, the healthcare sector witnessed three of the most significant security breaches arising from ransomware attacks. In June, Synnovis, a pathology service provider for the National Health Service (NHS) in England, was targeted in a ransomware attack forcing major hospitals to declare emergency status. Affected hospitals were unable to match patients' blood types at their normal frequency. Patients were diverted and hundreds of urgent cancer operations and treatments were canceled due to the inability to guarantee blood transfusions.

Ascension – one of the largest healthcare entities in the United States with over 140 hospitals and over 40 care facilities – was a major victim, with its operations massively disrupted due to a ransomware attack on its comprehensive network of facilities. The attack severely impacted its ability to provide care, as various crucial clinical systems such as the electronic health records (EHR) were compromised. The infrastructure and communication systems were also impacted, making electronic assistance impossible, and forcing staff to revert to manual processes. Some facilities even had to divert emergency care. Ascension took stringent measures, advising business partners to disconnect systems to curtail the attack's spread and involving third-party cybersecurity firms for investigation and system restoration.

This alarming ransomware attack occurred on the heels of the Change Healthcare attack, which the American Hospital Association called "the most significant cyberattack on the U.S. health care system." Intruders made use of stolen credentials to gain access through an external-facing platform that lacked multi-factor authentication. This incident has created a staggering financial fallout, with immediate costs related directly to the cyber incident and system restoration already exceeding $600 million. The incurred revenue loss, inclusive of an undisclosed sum as a ransom payment, exceeded $250 million. Early predictions suggest that these costs rise beyond $1 billion. The Black Basta ransomware variant, suspected to be involved in the Ascension attack, has led the FBI, CISA, HHS, and MS-ISAC to release the technical details of the exploit and suggest preventive measures to safeguard other organizations from similar threats.

With the significant impact on patient outcomes, bolstering security has become absolutely life-critical

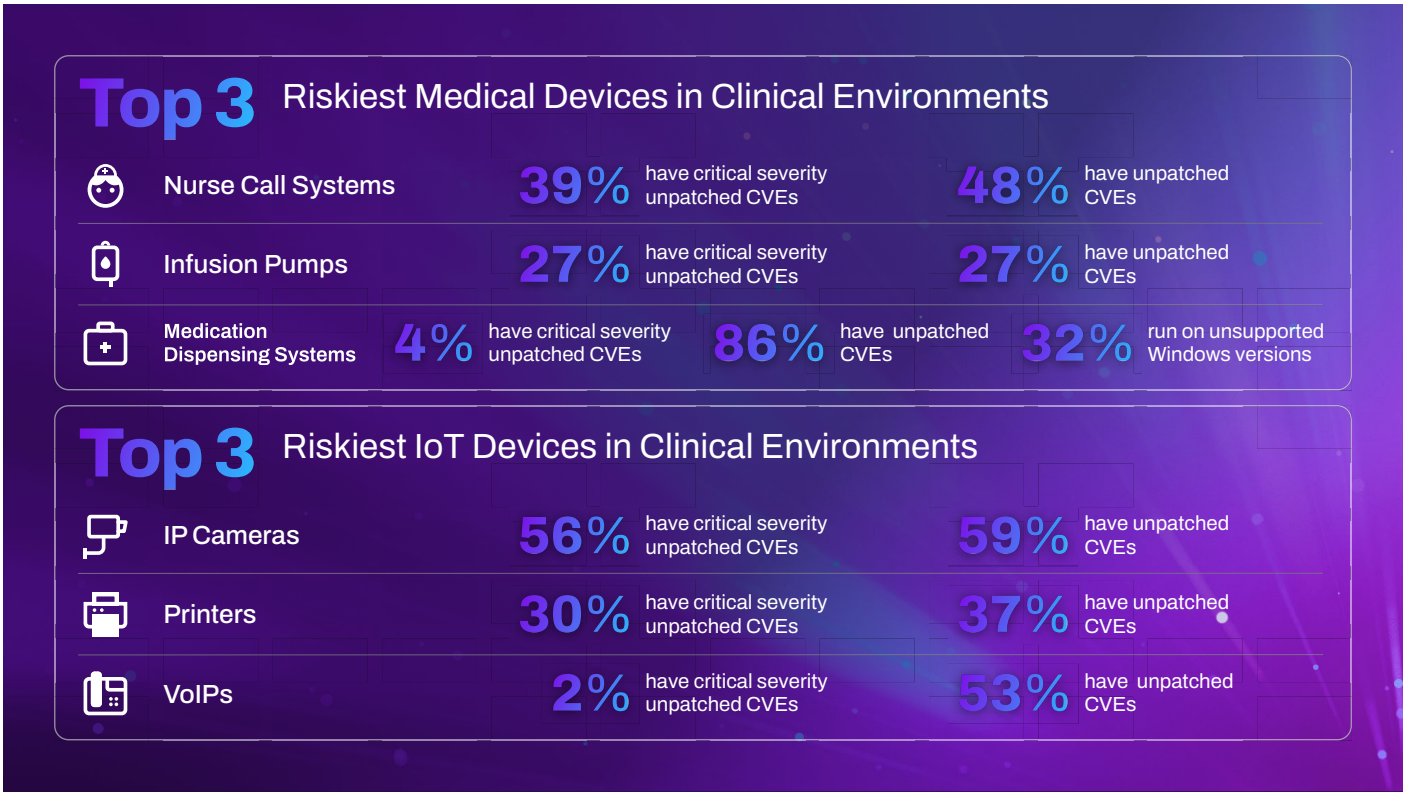
Unfortunately, there is a high likelihood that compromised devices and assets may be directly involved in patient care and are crucial for the daily operations of the facility. The pressures that attacks place on HDOs are substantial, as organizations will seek to immediately resolve the situation and eliminate any delays to patient care. This pressure and responsibility for providing a standard of care increases the likelihood that ransoms will be paid. As a result, healthcare and pharmaceuticals are consistently in the top two industries that are impacted by cyberattacks. For every healthcare organization that is impacted by cyberattacks, 57% reported poor patient outcomes as a result, and increased complications from medical procedures for nearly half of them, according to a **Ponemon Institute study**. In previous years, data security was the primary cybersecurity focus in healthcare, but with the significant impact on patient outcomes, even deaths indirectly attributed to ransomware attacks, bolstering security has become absolutely life-critical.

Prevention is Better Than a Cure – Moving to a Proactive Cybersecurity Approach

Despite the ever-growing risk of ransomware and other cyber attacks in healthcare, it seems responses are still lagging behind.

A concerning **12% of the industry still relies on End-of-Support (EoS) Operating Systems** because often no new security patches are issued, leaving the devices susceptible to attacks. Imaging workstations and nurse call systems remain among the riskiest devices in clinical environments.

Cybersecurity attacks can spread within an organization like cancer. Early detection is key for effective treatment and loss prevention. Regular pre-screening methods avoid catastrophic impacts on organizations and patients alike.



Comprehensive asset visibility and continuous security are essential for protecting healthcare organizations. With many HDOs lacking up-to-date asset inventories and understanding of their attack surfaces, the risk of exploitation increases. In order to not only respond effectively in the event of an attack, but also move toward a more proactive, preventive stance, healthcare security teams, and indeed the operations and management teams at large, must undertake a full panel of tests, measures, and reinforcements to stay ahead of the attackers.

Cybersecurity Health Checks

Guidance for Building an Effective Security Program

1. **Ensure Your Policies are Updated** - Ensuring that information security policies are regularly reviewed and updated is a fundamental element to good cybersecurity posture. Set the tone at the top of the organization and ensure policies are always sufficient to address the reality of the current attack landscape.

2. **Conduct a 'Full Physical'** - A comprehensive and holistic asset inventory is the cornerstone of any security program. A view of all enterprise, IoT, medical/IoMT, OT, cloud, remote, and virtual assets ranging from MRI scanners to HVAC systems or Building Management Systems, is key to knowing where an attack could manifest. Knowing the clinical context of every asset helps prioritize security efforts effectively to address the biggest potential impacts on patient care first and foremost.

3. **Check for Any Abnormal Findings** - Vulnerability and security issue assessments require a combination of active scanning, passive analysis for sensitive equipment, prioritization mechanisms, threat intelligence, and process management to ensure optimal risk reduction and efficient remediation. Ensure your security assessment scope encompasses every asset in the environment.

4. **Triage, Assess, and Treat** - Ensure that the greatest clinical impact is addressed first and prioritize efforts around the true operational or clinical context and patient risk implications of every asset. Focus efforts on the areas with the highest risk and impact first. Deduplicate findings to create an accurate list of threats, prioritize accordingly, and assign remediation tasks to the appropriate lead to drastically reduce the time from initial notification to remediation.

5. **Do Regular Checkups** - Many attackers are able to proliferate through the network due to blindspots in traffic movement and patterns. Monitoring policies should not only be for known threats but include zero-day exploits and anomalous behaviors – spikes in data access and exfiltration, lateral movement between unrelated zones, or authentication behaviors never before seen. Leveraging artificial intelligence and effective threat detection methods regularly can preempt an attack before it is exploited by bad actors.

6. **Manage Third Party Risks** - Ensure all vendor-managed assets are cataloged, assess vendor credentials, site-to-site tunnels, and remote access software. Utilize vendor-provided security hardening documents and procedures. Foster collaboration between security teams and other organizational teams, including clinical engineers, facilities management, and physical security, for a successful cybersecurity program.

7. **Isolate the Problem** - Implement network segmentation through asset inventory, communication mapping, policy creation, and enforcement automation to proactively reduce risks and prevent ransomware. Enforce complex passwords, expiring passwords, and review unencrypted credentials and default IoT device credentials, and apply Role-Based Access Control (RBAC).

Cybersecurity Health Checks

8 **Protect Your Eyes and Ears** - Human errorr emains a major threat, accounting foro ver 80% of cyber incidents. Equipping your teams to identify and mitigate threats is key to rebuilding patient trust in the face of evolving dangers. Enhance email security controls to combat phishing, the top vector for cyberattacks, and apply additional security measures as they become available. Enable MFA across all external-facing systems, and internal critical applications, making it a standard security control requirement.

9 **Do a Stress Test** - Dynamic and real-time risk assessments are key to a continuous security improvement model. By staying on top of your changing environment, teams can quickly address weaknesses and zero-day exploits. Conduct penetration tests for much deeper visibility into threat paths than a standard vulnerability scan. Understand the entire attack surface by evaluating every asset, from the ground to the cloud. Prepare for cyberattacks by ensuring and testing backups and conducting simulations and tabletop exercises to maintain organizational preparedness and continuity.

10 **Send for a Referral** - Regular reporting to executives and the board are important to support the cybersecurity initiatives. Security posture reporting should be broken down into multiple categories and corresponding scores for better transparency and focus. For example, endpoint security, IoT security, medical device security, cloud security, IAM security all feed into the overall security posture of the organization.

11 **Preventive Care** - Leverage automation through connected platforms to reduce response times and prevent malware attacks. Ensure your cybersecurity tools are able to accurately assess the current attack landscape, what may impact you next, what trends are occurring in recent attacks, and build up your security posture in advance of an attack even taking place.

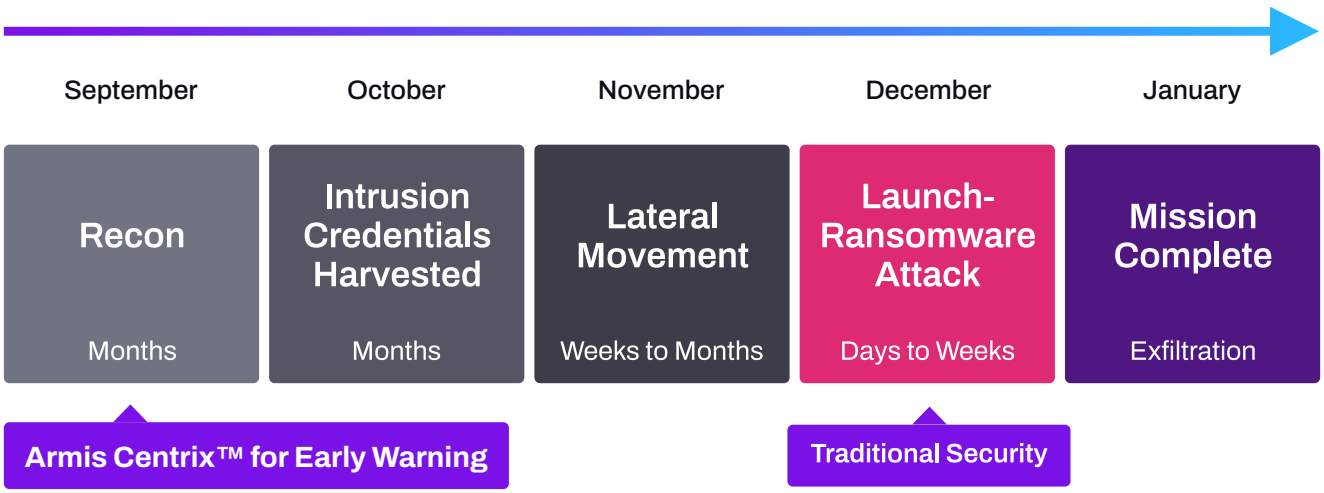
Anticipate Threats and Resolve Vulnerabilities and Other Security Concerns Before They are Exploited

There is never a good time for an attack to happen in the healthcare industry. Every moment can quite literally be a matter of life or death for patients in the system. Therefore, the ability to take a preventive maintenance approach and plan for upgrades or patches is key.

A traditional proactive approach to cybersecurity has simply meant having systems in place and being able to monitor security status on an ongoing basis. However, this often leads to a reactive cycle of only seeing attacks once they pose a real risk to your organization and being caught on the back foot repeatedly.

Healthcare organizations must adopt early warning detection systems to effectively prepare for and mitigate security incidents before they cause significant harm or disruption. To establish a foundational early warning detection system that is timely, accurate, and evidence-based, ensure your cybersecurity practices encompass the following:

- Understand Organizational Assets and Risks: Defending the unknown is impossible. Identify and prioritize critical assets, data, and systems within your healthcare organization. Understand the potential impact of security threats on these assets and the patients that interact with them, and the specific risks your healthcare environment faces.
- Empower with Timely and Accurate Asset Intelligence: AI-powered asset intelligence engines can monitor billions of assets and medical devices worldwide in order to identify cyber risk patterns and behaviors and enrich existing assets.
- Follow the Threat Actors with Early Warning Detection: Employ indicators such as honeypots, intelligence, and research to predict potential threats and make real-time assessments. This type of detection can allow you to plan maintenance around medical device usage and address CVEs before globally accessible knowledge agencies and corporations publish them.
- Stay Informed with Evidence-based Threat Intelligence: Rely on evidence-based threat intelligence feeds and sources to stay informed of emerging threats and the tactics employed by attackers.



Conclusion

The threat of ransomware attacks in healthcare is only increasing and evolving alongside the rapid pace of digital transformation. The stakes are at an all-time high, affecting not just the financial standing and reputation of these organizations, but also the delivery of critical patient care. As we've described, threat detection and early warning systems provide a more proactive approach to cybersecurity, allowing healthcare organizations to provide the best case scenario for their cybersecurity practices. Moving to a proactive and preventive approach is the same standard medical providers employ for the patients they serve — it's time for internal security practices to follow suit.

But it's not enough to simply deploy these systems. Healthcare organizations must also take a holistic approach to cybersecurity, from conducting regular asset inventories and vulnerability assessments to ensuring that security policies are regularly updated to reflect the current attack landscape. It's crucial to factor in the clinical context of every asset when prioritizing cybersecurity efforts, as well as investing in regular penetration testing and continuously assessing risk in the ever-changing healthcare environment.

The path to better cybersecurity in healthcare is not an easy or straightforward one. It involves a constant cycle of monitoring, updating, testing, and adjusting based on new threats and vulnerabilities. However, it is a path worth treading because it ensures the secure delivery of critical care to patients and protects healthcare organizations from the devastating financial and operational impact of ransomware attacks. Our advice to healthcare organizations is clear: Invest in threat detection and early warning systems, embed cybersecurity into the fabric of your culture and operations, and take a preventive, proactive approach to safeguard your organization and your patients against cyber threats.