deepwatch™

SOLUTIONS BRIEF

Cyber Skills Gaps Leave Healthcare Vulnerable to Ransomware

Accelerate Cyber Resilience in Hospitals, Clinics, and Pharmacies

HOW DO HEALTHCARE ORGANIZATIONS ADDRESS THE CYBER SKILLS SHORTAGE?

Ransomware attacks have become a common and critical business risk for healthcare providers. The US Department of Health and Human Services reported over 450 successful ransomware attacks in 2023.[1] These attacks are no longer merely about financial gain and patient data, they disrupt critical healthcare services, delay treatment, and can even lose lives.

Unfortunately, the cybersecurity talent shortage mirrors that of the healthcare industry. Skilled security professionals are essential to anticipate, withstand and recover from ransomware attacks.

1. HHS.gov, HHS Cybersecurity Report 2023

THE CHALLENGE OF HEALTHCARE SECURITY STAFFING

There are a variety of challenges in staffing a cybersecurity effort at healthcare organizations. You must recruit, hire, and retain talent that is in short supply and high demand. There are a variety of different security roles and skill sets, from analysts to engineers, that must be considered. While many budgets fail to consider active threat hunters, they are essential to stopping ransomware from impacting patients.

CYBERSECURITY SKILLS GAP FACTS

1. Estimates suggest there are over 3.5 million unfilled cybersecurity jobs in 2024.[1]
2. By every measure, cybersecurity threats targeting healthcare victims have increased, suggesting the growing need for cybersecurity professionals.
3. High salaries, competition with remote opportunities, and lean budgets contribute to the hiring challenges.
4. On average, it takes 100+ days to fill healthcare security positions, almost three times the national average for other industries.
5. Lack of experienced security staff keeps many organizations from realizing the full capabilities of advanced security tools or sufficiently improving security team performance.

1. Cybersecurity Ventures, "Top 10 Cybersecurity Predictions and Statistics for 2024"

deepwatch™

TOP CYBER CONCERNS FOR HEALTHCARE

1. Due to a lack of skilled cybersecurity personnel, healthcare organizations often struggle to maintain robust defenses, making them more susceptible to ransomware and phishing attacks.

   1. CyberTalk.org,: How to Boost Healthcare Cybersecurity in 2023

2. The cyber skills gap can lead to outdated software and unpatched systems, creating easy entry points for attackers.

   2. ASIS International, "The Cyber Workforce Shortage Hinders Healthcare Supply Chain Security"

3. Limited security staff can lead to delayed responses that allow attackers to remain undetected longer.

4. Reduced security staff can lead to frustration and burnout, already a problem among security professionals, and result in mistakes or misconfigurations.

HEALTHCARE SECURITY PROGRAM NEEDS

A cyber resilient healthcare security program anticipates threats, builds and executes ransomware recovery plans, ensures business continuity, and continuously adapts the security effort to meet new challenges. Deepwatch can help accelerate cyber resilience by providing the talent, the technology, and processes to protect your environment and your patients.

WHY DEEPWATCH

The cybersecurity skills gap puts healthcare organizations at risk of ransomware attacks. Hospitals and pharmacy groups are naturally focused on patient care, while Information Technology is focused on the many connected devices and monitors essential to meet patient needs. They have less time to anticipate the changing tactics and techniques of ransomware threats.

Deepwatch helps healthcare organizations optimize security budgets with continuous coverage along with technical and vertical expertise for a range of best of breed security tools including SIEM, Hyperautomation, Firewalls, Endpoint Detection & Response tooling, and Vulnerability Management solutions. We recruit, hire, and continuously develop industry-leading analysts and engineers. We work with your security team to build a cyber resilient program that can detect, respond, and improve against inevitable attacks, and we're there to make those bad days a whole lot better.

CYBER RESILIENCE CAN SAVE LIVES

Healthcare organizations must build resilience to maintain patient care. They must anticipate data breaches, withstand and recover from ransomware attacks, and adapt programs to avoid reinfection. Without the right security professionals on staff, every incident needs triage.

While you focus on patient care, let Deepwatch experts help you detect and respond to cyber threats, build more resilient programs, and get more from your security tool investments.

deepwatch™

DEEPWATCH ENTERPRISE BASED CYBER RESILIENCE FOR HEALTHCARE

Skilled Support for Your Security Operations

- 24/7/365 coverage with industry experts
- Reduced alert overload and fatigue
- Faster, seamless technology integration

Build Resilient Programs

- Fast, risk aware, precision response to attacks
- Improved visibility across networks and devices
- Security program maturity and improvement

Reduce Staffing Costs and Complexity

- Reduce staffing costs
- Minimize complexity in technical hiring
- Improve staff work/life balance

Support Patient Care

- Ensure business continuity, focus on patient care
- Guarantee scalability during surges in care
- Show program maturity with better narratives to stakeholders

GO BEYOND DETECTION.

BECOME CYBER RESILIENT.

deepwatch™

ABOUT DEEPWATCH

Deepwatch is the leading managed security platform for the cyber resilient enterprise. Our platform combines comprehensive threat management capabilities, expert practitioners, and precise automated actions. Embrace preventative actions to improve your security posture and enhance your speed of response. Join leading global brands relying on Deepwatch for cyber resiliency and security peace of mind.

CONTACT US

GET STARTED

4030 W Boy Scout Blvd. Suite 550
Tampa, FL 33607

www.deepwatch.com