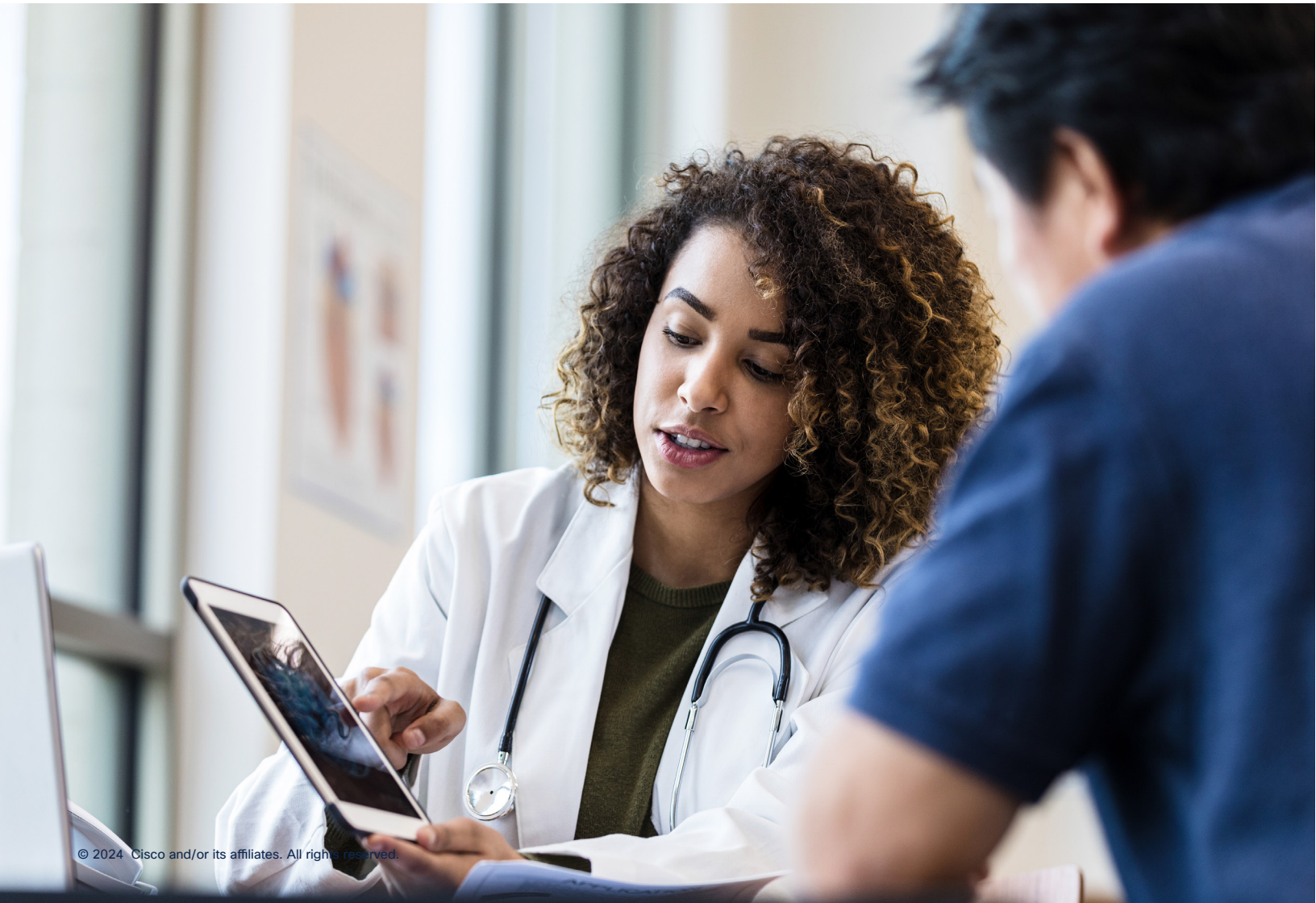
Cybersecurity Threats Top of Mind for Healthcare



Contents

The cybersecurity landscape

Healthcare is evolving into a new era where nearly everything is connected through digital technologies that improve the way care is delivered to patients. The future of healthcare is being driven by innovation and digital transformation, with a heightened focus on open standard interoperability and distributed ecosystems.

While the acceleration of digital technologies, medical device utilization, AI and cloud-based services, and telehealth have been beneficial in driving more informed care delivery and greater access to care, the introduction of more devices on the network creates increased risk across the threat landscape. The U.S. Department of Health and Human Services' (HHS) Office of Civil Rights reported a staggering 264% increase in healthcare ransomware attacks and a 256% increase in breaches involving hacking over the past five years.[1]

Cybersecurity remains top of mind for healthcare, as it is the most targeted industry, incurring the highest average cost per breach for 14 consecutive years; the current average cost of a breach is $9.77 million.[2]

Keeping up with cybersecurity threats has always been a challenge, but today the speed at which new threats are introduced is astounding. The sophistication of threats and the use of advanced tools like artificial intelligence, machine learning, and other technologies are making ransomware, phishing, and other known forms of attacks more prevalent.

When it comes to security in healthcare, it's clear that uncertainty has become the new normal. Many organizations are not sure how to identify and manage digital risks in the ever-changing threat landscape, and their current risk management strategies just can't keep up.

Cybersecurity breaches for healthcare organizations have a negative impact on more than just an organization's financial and reputational standing. Breaches can involve the theft of Protected Health Information (PHI) and Personal Identifiable Information (PII), and can also result in longer patient stays, delays in procedures, and diversions to other facilities.

Medical device security is also a concern for healthcare providers, as bad actors take aim at vulnerable unpatched systems and improperly configured devices. We know that connected medical devices can represent a large percentage of the devices on a Healthcare Delivery Organization's (HDO) network, and 53% of connected medical and other IoT devices in hospitals have a known critical vulnerability.[3]

The proliferation of smart and connected medical devices will only continue as we shift from acute and post-acute care sites (emergency rooms and assisted care facilities) to less secure locations and home-based services.

To complicate the landscape further, healthcare organizations must also consider standards and regulatory requirements such as those found with the Health Insurance Portability and Accountability Act (HIPAA), the International Organization for Standardization (ISO), the National Institute of Standards and Technology (NIST), the General Data Protection Regulation (GDPR), and the Payment Card Industry Data Security Standard (PCI DSS).

[1] HHS Press Office, February 2024

[2] Cost of a Data Breach Report 2024, Ponemon and IBM

[3] The State of Healthcare IoT Device Security 2022, Cynerio

Focusing on a strategy of security resilience

Today's digital footprint in healthcare extends beyond the traditional technology borders that create complexity. With this extended enterprise business model, most business functions exist outside of the confines of the HDO's infrastructure. The digital platforms connecting these business functions can be regional, national, or global.

And when everything is open, distributed, and connected, security and business resilience requires more than what previous cybersecurity approaches have offered. Healthcare organizations must transition to a new security strategy of security resilience that focuses on detection, response, and recovery. A plan that considers what is connected, and in what context.

As we become more connected, visibility and actionable insights across networks, clouds, endpoints, and applications are becoming ever more critical to align the digital needs of the business with the desired security posture of the organization.

New digital business models are also driving a need for converged services, such as networking and security, to be delivered in the cloud, to reduce complexity, and to improve speed and agility. Ultimately, these security tools provide healthcare organizations the ability to pivot easily to the new needs of business, for example, scaling access to large data sets in the cloud or securing remote workers.

To protect critical patient data and clinical systems, many healthcare IT leaders have adopted the zero trust security framework to bolster cybersecurity defenses. Cisco defines zero trust as a comprehensive approach to securing all access across an organization's applications and environment, from any user, device, and location. It protects the workforce, workloads, and workplace.

While zero trust is both a strategy and an architectural model, organizations need to recognize that it is also a journey that incorporates the organization's risk management goals and business needs. (See the journey of one large U.S.-based pediatric children's hospital's toward zero trust.)

The overarching mission for Chief Information Security Officers (CISOs) and their security teams is to protect their institutions amid unpredictable change, while maintaining business continuity and driving security resilience and readiness.

Assessing your cyber-readiness

As you set cyber goals for your organization and assess cyber-readiness, here are some points of consideration for leadership:

1. Are you creating a culture of cybersecurity?
2. Is your organization secure, or do you feel that your organization is too complex to secure, thanks to business partners, recent mergers and acquisition activity, vertical integration, or other complicated scenarios?
3. Are you securing your organization against the most important risks to the business? In other words, is your cyber strategy aligned with your business strategy?
4. Do you have real-time visibility into devices, applications, and users accessing your healthcare network and data?
5. Are you prepared for accelerated digitization in the next three to five years? And more specifically, are you looking far enough forward to understand how today's technology investments will have cybersecurity implications in the future?[4]

As you discuss these critical questions with your stakeholders, we welcome the opportunity to collaborate with you as you create a strategy to address your organization's specific security needs.

Cisco's 40-year heritage of successfully guiding customers through tech and business inflection points, and our investments of more than $10 billion in advanced security technologies, are helping organizations like yours achieve security resilience. And, with over 80% of the world's internet traffic running on Cisco® networks, we have an unparalleled vantage point for protecting the integrity of your business.

Cisco offers an advanced and integrated enterprise security portfolio of products and advisory and implementation services to ensure healthcare leaders like you can act with confidence and thrive in the ever-evolving world of healthcare.

[4] Cybersecurity trends: Looking over the horizon, McKinsey, March 2022

For more information

Explore Cisco's healthcare portfolio explorer and get more insight around cybersecurity.

C11-3578324-01 09/24