Cybersecurity Transformation in Healthcare

3 Priorities for 2023 and Beyond

An Industry Under Pressure

The global healthcare industry is undergoing an incredible transformation driven by a wide range of rapid changes, such as innovations in medical technology, the emergence of new care delivery methods, and the relentless pursuit of positive patient outcomes. These changes are pushing healthcare organizations to rethink how care is delivered—and enable them to provide more efficient and effective care at scale.

But these changes also introduce a new challenge: **more opportunities for cyberattackers**. For example, the growing use of IoMT technology creates unprecedented levels of data—more than 19 terabytes of clinical data alone,[1] while other research indicates that 30% of the world's data is generated by the healthcare industry.[2] This data poses a serious risk that, if not properly secured, can result in irreparable damage.

Coupled with emerging threats such as sophisticated phishing campaigns and attacks using generative AI and machine learning, healthcare organizations are under tremendous pressure to stay ahead. Chief information security officers and their teams face a critical question:

How can healthcare leaders stay ahead of the latest threats? And more importantly, how can they continue to deliver the exceptional care that their patients deserve?

3 Key Cybersecurity Trends in Healthcare

Several trends strongly impact cybersecurity in the healthcare industry today:

- **The rise of remote care** opens up new attack vectors against personal devices and cloud services.
- A surge in medical and nonmedical **connected devices**.
- The increasing **complexity of healthcare organizations' overall IT environment** combined with resource constraints.

Let's examine these more closely.

1. The Rise of Remote Care

Remote care delivery, such as telehealth and remote patient monitoring (RPM), is making monumental progress. The past three years accelerated this trend as patients and practitioners preferred telehealth for increased flexibility, especially as they grappled with the pandemic. As a result, care delivery is now virtual, at home, or wherever patients are.

At the same time, remote care widens the industry's attack surface. For example, patients at home often lack the strict safeguards present in hospital networks, and a wide range of personal and healthcare devices go underprotected. Attackers can exploit these gaps and infiltrate a health system—as healthcare organizations saw with the recent Apache Log4j vulnerability.

2. Connected Healthcare Devices Continue to Evolve

Heart monitors. Infusion pumps. Dialysis machines. These are just a few examples of the numerous connected devices that help hospitals and health services deliver better patient outcomes.

While these smart medical devices offer a substantial upside to health outcomes, they also introduce countless new endpoints into the cybersecurity landscape. Manufacturers built in a base level of security for IoMT devices, but new threats constantly surface to specifically target IoMT devices.

Medical practices often try to extend the life of devices running end-of-life software that still deliver care value, creating a complex maze of systems to manage and monitor. A 2020 report from Palo Alto Networks Unit 42 pointed out that over 83% of healthcare systems were running on outdated software.[3]

It's also more than just the countless number of smart medical devices that expand the attack surface. Other types of smart connected devices add to the cybersecurity complexity. These include tools like digital wall boards, kiosks, and video screens that streamline self-service information to patients and support admission, discharge, and transfers (ADT).

1. Sundar Krishnan and Narasimha Shashidhar, "eDiscovery Challenges in Healthcare," *International Journal of Information Security Science*, Vol. 8, No. 2, August 2019.
2. "Episode 5: The Rise of Telehealth," RBC Capital Markets, last visited August 18, 2023.
3. *Unit 42 IoT Threat Report*, Palo Alto Networks, June 10, 2020.

3. Complex IT Environments and Resource Constraints

The healthcare industry faces technical complexities unlike any other. Organizations constantly deploy new medical tools, applications, and services at scale, hosted within data centers or cloud providers, within the care location networks, or delivered by SaaS providers. IT teams must manage the IT infrastructure amidst the tool sprawl and maintain connectivity between hospitals and their distributed care efforts. This requires significant technical resources that many organizations (and IT teams) simply do not have.

Adding to this network complexity is the tendency of hospitals and health systems that bolt on siloed point solutions to address each security challenge. Oftentimes, this collage of nonintegrated point security solutions generates more alerts and noise than increased protection of care operations that reduce security risks. These solutions lack the synchronization and integration needed to respond to today's sophisticated threats.

The massive volume of data generated by healthcare and the value of the data to cybercriminals adds more pressure on healthcare organizations to safeguard their data, protecting patient privacy and confidentiality along with the integrity of the data to deliver patient care.

Why Cyberthieves Specifically Target Healthcare

1. Healthcare data is highly sensitive

The information—for both patients and healthcare employees—is highly personal and easily identifiable by matching records with countless public databases. As a result, numerous analyses indicate the economic value of a stolen healthcare record is substantially greater than that of a stolen Social Security number, and even higher still compared to a typical credit card number.

2. Potentially exorbitant payouts

Many organizations choose to incur the costs of a cyber incident such as ransomware to resume patient care and restore normal operations. In fact, the average ransom demand for the healthcare industry is $1.4[4] million, and healthcare is more likely to pay out ransoms than other industries.

3. An increase in the number of legacy, undersecured systems

Healthcare organizations are often careful with modernizing systems and security tools, causing them to run many critical workloads using legacy cybersecurity systems that are easily compromised by hackers. This is made even more problematic by the increased use of public cloud services and unsecured personal networks to access critical data, such as patient records, images, and test results.

4. Limited resources

The cybersecurity skills gap is felt acutely in the healthcare field, where business and technical leaders make difficult decisions on where to use their finite budgets. Recruiting and retaining qualified cybersecurity staff is a huge challenge, and positions often stay unfilled. This means risk exposure can be extremely high, causing slow reactions to fast-moving attacks or delaying the time to spot a threat that has already nested in the network.

4. *Unit 42 Incident Report*, Palo Alto Networks, July 26, 2022.

Factors Driving the Expanding Attack Surface

The revolution in healthcare delivery represents a quantum leap forward for patient outcomes—greater efficiency for practitioners and staff, easier access to healthcare for patients, and better diagnostics and analytics for treatment and prevention. The problem is these advancements also generate enticing new opportunities for cyberattackers.

Cyberattack tools are surreptitiously, easily, and inexpensively obtained by potential data thieves on the dark web, and the economic value of healthcare records is substantial. Protected health information, payment data, personally identifiable information, intellectual property—this treasure trove of accessible digital data motivates attackers to target healthcare.

The cost of inaction is substantial. Research indicates that the average cost for a healthcare industry data breach is more than **$10 million**—higher than that of any other industry.[5] Adding to that direct financial loss are the costs of regulatory penalties and legal judgments due to improper protection of patient data.

Cyberattacks not only strike at IoMT systems that directly monitor and manage patient health, but they also impact organizations' far-flung critical infrastructure, such as power, heating/cooling, and technology-driven business operations.

These outages can result in patients being diverted to other facilities, cancellation of nonemergency procedures, and an inability to access electronic health records.

The New Fundamentals of Securing Healthcare

As care delivery continues to transform, you need a cybersecurity approach built on cyber resilience—one that prevents threats before they occur, reduces mean time to detect and respond, protects devices and users, and ensures effective care continuity. This means a cybersecurity strategy beyond the traditional approaches.

We recommend prioritizing these key areas:

- Reduce IT complexity.
- Automate security.
- Safeguard patient data.

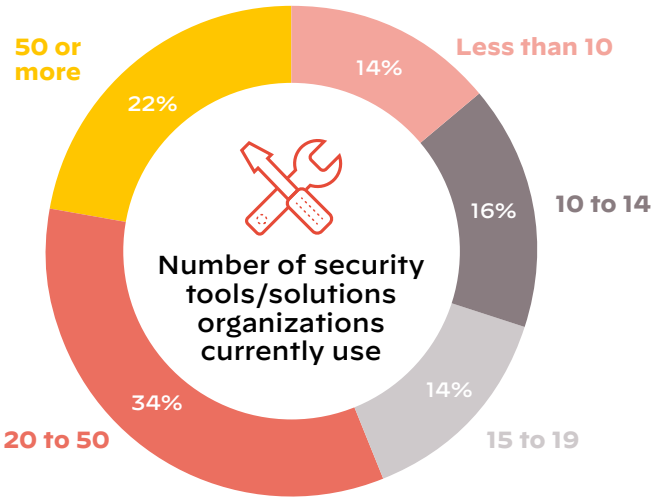
Reduce IT Complexity

Your organization should focus on reducing IT complexity and simplifying your tech stack. For example, security platforms offer best-of-breed tools and services along with unified management across centralized systems, remote care locations, IoMT devices, and cloud services.

Security platforms allow healthcare organizations to use cyber tools such as next-generation firewall, intrusion detection, IoT security, and data loss prevention across the full range of devices, applications, networks, and cloud services. These tools operate and interact under a single, unified platform for security teams to manage more efficiently and effectively.

Platforms also reduce complexity by using a single management console to provide a real-time, comprehensive view of all network traffic and application behavior. Having dozens or more distinct cybersecurity tools and services on a platform developed and deployed by a single vendor simplifies a health delivery organization's IT stack, particularly when its operations are distributed and remote.

Additionally, the platform model helps healthcare organizations improve their overall cybersecurity posture. Using a natively integrated foundation substantially alleviates the technical burden of



Source: *What's Next in Cyber*. Survey of 1,300 C-level executives worldwide.

Figure 1: Security tool sprawl in today's enterprise organizations

5. *Cost of a Data Breach Report*, IBM, July 27, 2022.

security tool integration and optimization by shifting the responsibility from the healthcare provider to an experienced, proven cybersecurity technology partner.

Automate Security

Today's cybersecurity threats overwhelm healthcare SOCs that have to manually investigate hundreds or even thousands of alerts per day. Steps like automated triage and alerts work, but many earlier-generation alert systems lack the sophistication, context, and nuance necessary to avoid alert fatigue.

Research from Enterprise Strategy Group notes that 34% of organizations say the volume of alerts has increased over the past two years, and that 38% consider "filtering the noise out of alerts so we can focus on the right signals" to be a top challenge.[6] Instead, "intelligent automation" should be the goal, helping healthcare organizations to fully leverage automation at every step—prevention, detection, and response.

When enhanced with artificial intelligence and machine language technologies, automation tools within cybersecurity platforms can analyze huge data volumes to prevent zero-day and other emerging threats. Knowledge gained from each thwarted attempt is then reused to prevent future attacks, reducing the time and effort spent on security operations.

Safeguard Patient Data

Protected health information (PHI) and personally identifiable information (PII) are tempting targets for malicious actors. At the same time, regulations such as HIPAA, GDPR, and HITECH place strict measures on patient data privacy. That's why your cybersecurity approach should prioritize securing patient information and meeting regulatory compliance requirements.

First, look for vendors that recognize unique patient privacy requirements and offer tailored solutions for every organization. For example, hospitals with a large collection of networks, clouds, devices, and users need an end-to-end security solution that secures their entire environment—network, cloud, endpoints, IoT—and enhances security operations. These tools and services from a single vendor can work together to orchestrate your defense and prevent data breaches before they occur.

Second, elevate security posture and compliance and reduce risks by addressing these common areas of vulnerability:

- Risk analyses and management
- Security and access controls

Risk Analyses

Your organization should conduct ongoing risk analyses and identify vulnerabilities to systems and services holding PHI and electronic protected health information (ePHI). These should be conducted continuously and at a minimum following any material change to policies and procedures or changes in technology within your environment.

Risk Management

Once risks and vulnerabilities are identified, your team should undergo remediation efforts and prioritize risks most susceptible to compromise. This includes working with other vendors and business associates to address their security gaps.

Security Controls

Regularly subject the security tools in your environment to security scrutiny and assessments. Make sure they were implemented properly, operating as intended, successfully protecting patient data, and keeping your organization compliant and online.

Access Controls

Excessive permissions and human errors are major causes of successful breaches in healthcare. Access controls should be based on Zero Trust and least-privileged access, where only authorized staff can access sensitive data.

Of course, your vendors should also have a proven track record of regulatory compliance and experience in the healthcare industry. They should be well-regarded among other healthcare providers and thoroughly understand the regulatory environment in your region.

6. Joan Goodchild, "SOC Teams Burdened by Alert Fatigue Explore XDR," Dark Reading, May 14, 2021.

The Best Security for Your Patients

Healthcare organizations must keep up with the rapid and widespread change in the business, technical, regulatory, cybersecurity, and risk landscape. The rate of change is dizzying, but it must be addressed in order to achieve the most important goal: **improving patient outcomes**.

Central to that goal is healthcare organizations' ability to plan, build, deploy, and manage the most secure digital environment possible. The increasingly digital nature of healthcare makes cybersecurity vulnerabilities a huge problem to acknowledge and overcome. Cybersecurity attacks threaten the reliable, consistent delivery of healthcare throughout the entire healthcare lifecycle, and service interruptions and data theft pose potentially damaging consequences.

At the heart of solving the healthcare cybersecurity risk equation is the ability of organizations to (A) come to grips with the sources of those risks, (B) allocate sufficient financial and human resources to address the problem, and (C) adopt a cyber resilience mindset to healthcare. With a platform approach to cybersecurity, your security team has the tools it needs to build that cyber resilience and stay ahead of today's emerging threats.

Visit us at www.paloaltonetworks.com/healthcare to learn more about how Palo Alto Networks secures healthcare organizations around the world.

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com