Boosting Healthcare's Immune System

Top trends, strategies, and solutions for addressing evolving security & privacy challenges in the healthcare industry

Perhaps more than in any other industry, people, services, and systems are inextricably tied together in the healthcare space. It's why even a single security incident can wreak such havoc, since it impacts everyone equally — from care providers, employees, and contractors to patients and visitors.

Even more concerning is that hacks, breaches, and malware can compromise quality of care, leading not just to a multitude of inconveniences and delays but also resulting in sobering life-or-death implications.

But while cybersecurity tools and technologies continue to evolve at a dizzying speed, so are the threats they're trying to prevent. Malicious traffic from unauthorized users and bad actors now affects more than 70% of healthcare organizations,[1] resulting in a staggering rise in data breaches, theft, and fraud. Recent data found the healthcare industry is now the second-most vulnerable to ransomware attacks, just behind professional services.[2]

As hospitals and healthcare organizations of all sizes struggle to protect their assets, systems, and patient records, the threat of cyber attacks only continues to grow, overwhelming existing budgets and available means of security. This guide will help you better understand the current and future cyber risks in healthcare, and highlight the tools, technologies, and strategies you can leverage to protect yourselves, your partners, and your patients from the clear and present dangers of the Digital Age.

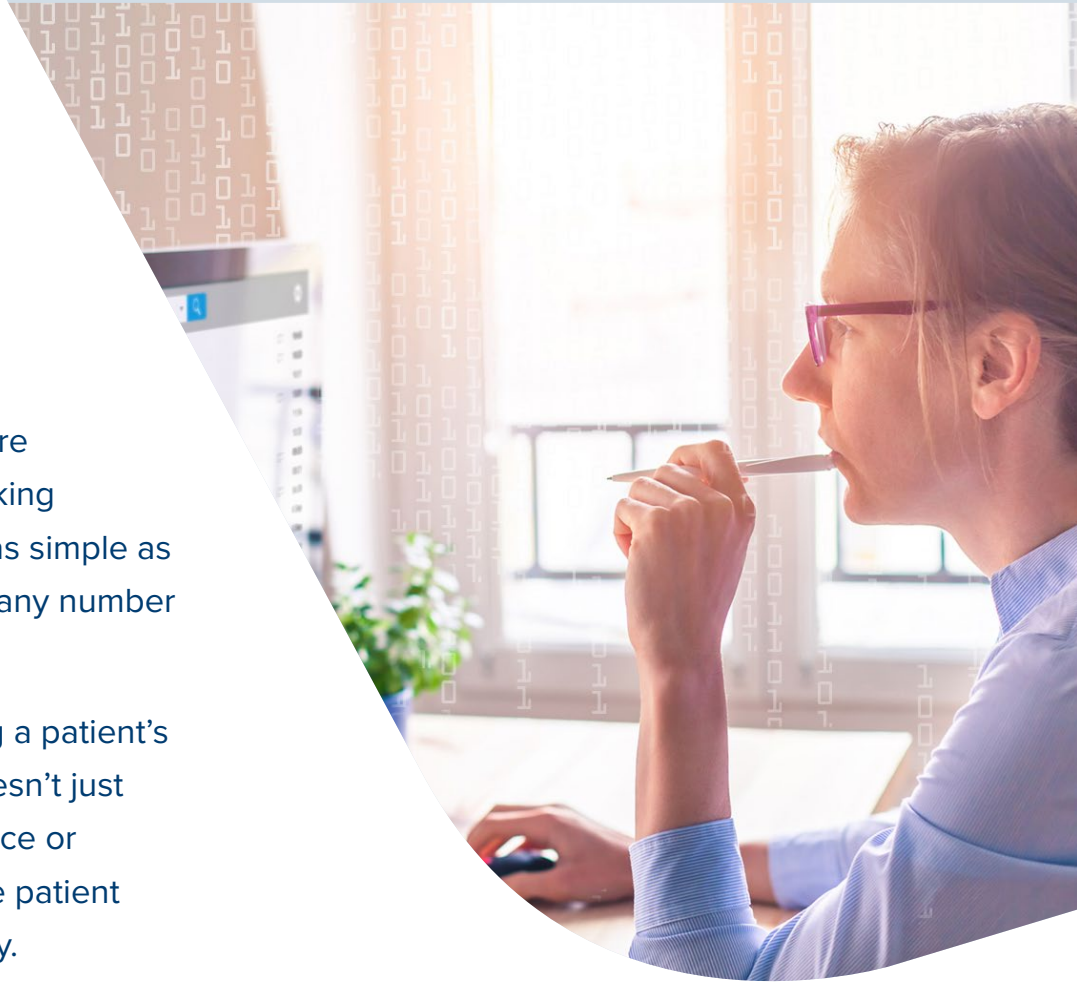
The US healthcare industry is a gold mine for industrial hackers. Commandeering hospital systems has become stable and profitable work for those willing to execute these attacks.[3]

Threats Within, Threats Without

Healthcare is an industry in transition. Many healthcare organizations are eager (and mandated) to toss out legacy and paper-based systems in favor of the latest electronic medical record and mobile health technologies — and they're doing so at a rapid pace. Yet despite these modernization efforts, technology practices in the healthcare space, especially around system integration and data security, haven't caught up to the level required by these robust and complex tools.

As a result, hospitals and healthcare providers now face a range of internal and external threats to their data and operations:

MATRIX42



Data leaks, theft & fraud

Internal infrastructure and hospital information systems (HIS) are vulnerable to employee mistakes and internal bad actors. Leaking information, whether accidental or on purpose, or something as simple as opening a questionable email can expose the organization to any number of threats and exploits.

Then there's the fact that data is worth a lot of money. Stealing a patient's ID, which is commonly used to perpetrate insurance fraud, doesn't just digitally expose the organization, it can result in denial of service or refusal of care for the patient, and create further burdens if the patient chooses to go through the arduous process of record recovery.

Data theft and fraud create a liability nightmare for health systems and hospitals. They can be subject to crippling fines for violating the Personal Health Information Protection Act (PHIPA) or the Health Insurance Profitability and Accountability Act (HIPAA), not to mention a host of other data security and privacy regulations.

In 2018, healthcare data breaches of 500 or more records were reported at a rate of 1 per day. By December 2020, that rate had doubled.[4]

Increased prevalence & use of mobile devices

Bring your own device (BYOD) provisions for full-time staff, contractors, visitors, and patients further increase digital exposure and risk. Before COVID, mobile device use was already high among patients and clinicians alike, and there's no reason to think this will change when the pandemic is over. But every smartphone, smart watch, wearable, tablet, laptop, portable game device, and e-reader increases vulnerability to threats, both for the individual and the organization.

For example, if a patient waiting for an appointment opens her phone close enough to a near field communication (NFC) device, she could be subject to eavesdropping, data modification and corruption, a relay attack, or any number of other serious breaches of her information. That, inevitably, leads to further malfeasance within the hospital's network and EMR systems, putting other sensitive patient data at risk while subjecting the violated individual to potentially years of financial and personal records recovery.

COVID has only exacerbated the risks of digital exposure and put more stress on the system by dramatically increasing network traffic. Physicals, consultations, education, test result reviews, and most other in-person interactions have all moved to video conferencing and telehealth. Not only does this expose sensitive data to hackers as it's transmitted over the networks, the greater traffic and strain on services and communications also results in more data throughput. And the bigger the data set, the bigger the risk.

81%
of adults own a smartphone.[5]

95%
of teens own a smartphone.[5]

80%
of physicians use smartphones and medical apps at work.[6]

AI-based attacks

Improvements to artificial intelligence (AI) and its widespread adoption have "democratized" cyber attacks. Programming is easier to learn and no longer requires the technical mastery previous hacking tools once did.

In some cases, AI training models can be purchased off the shelf, making it more accessible to a wider audience and substantially reducing the amount of time required to launch several attacks in rapid succession that overwhelm a hospital's defenses. Now, a malware attack, from conception to execution, only needs weeks instead of months to play out, and infection and deployment takes just minutes.

Malicious algorithms infused with AI methodology can be planted inside any unsuspecting — and unprepared — organization. For example, malware that tracks access, passwords, and traffic can easily be deployed as a piece of seemingly harmless code, undetectable at first. But as the AI model unfolds and builds itself within the network, it can start harvesting the organization's data long before any vulnerability tools will recognize a data outflow from certain ports.

By the time someone finds out, the AI model has been running for months, sending hospital systems into reactive mode and forcing them to undertake costly damage control.

The average ransomeware payment is now

$111,605[7]

Global ransomware damage could reach

$20 billion in 2021[8]

The perils of patient-centered care

Improvements to artificial intelligence (AI) and its widespread The healthcare industry's emphasis on patient-centered care is a good thing on the surface, but it requires balancing an optimal patient experience with heightened data protection. Patients expect each member of their care team to know the details of their condition, diagnosis, and treatment plan without having to start from scratch each time. To do this effectively, hospitals and healthcare providers need integrated systems and a seamless flow of information.

The problem is, to protect that flow of information and safeguard patient records, organizations need to find and hire the right resources and experts who can oversee the technologies and processes. But that's a tall order these days as organizations grapple with budgetary limits and have difficulty hiring enough skilled people into full-time roles. Without knowledgeable team members or managers at the helm, organizations are at the mercy of gaps in processes, outdated tools and security practices, and worse.

Healthcare has ... lagged behind other industries in investment and innovation in information technology. Now they are scrambling to catch up, and hospitals and health systems are facing a tight supply of skilled IT managers and executives."[9]

Threats Neutralized: Tools that Meet the Security Needs of Modern Healthcare

Healthcare, like many other industries, is facing a technology reckoning. On the one hand, digital tools and technologies open up much needed avenues of efficiency and information sharing that's making the delivery of healthcare easier and more responsive to patient needs. On the other hand, those same technologies pose a unique set of threats to the industry that if not well understood or managed can have a severe impact on patient data and privacy, quality of care, finances, compliance, and other aspects.

To respond to these threats and challenges effectively, your organization needs to adopt the right tools and processes that include:

Data governance & compliance

Healthcare information systems (HIS) are not designed for data privacy and protection. As such, you need to empower end users while also reducing exposure. To do so requires a two-pronged approach:

First, create and enforce strong data governance policies and guidelines for your employees, such as best practices for handling and sharing information, identifying phishing scams, and recognizing easy access points to the network. The same initiatives must also extend to your IT team to standardize policies around existing infrastructure.

Second, update and upgrade all firmware, operating systems, application configurations, and zero-day policies in accordance with compliance standards.

Operationalizing data security with automation

With better guidelines and standards in place, securing your data is really about operationalizing those plans. Automating license renewals and access controls, deploying and enhancing identity and access management like two-factor authentication, for example, and funneling all user actions and activities through a few select, trusted apps and platforms allows you to assert better control over and secure your organization's data.

Inventory management

Knowing where your assets are and when new ones come online can be achieved through persistent searching and discovery tools that help establish a real-time baseline of existing assets and provide vigilance over new or rogue assets. Most healthcare organizations use vulnerability advisory tools to run scheduled or ad-hoc security scans, leaving huge amounts of time when systems are unmonitored and ripe for a breach.

A more proactive solution scans continuously across every public and private connection and conducts root cause analysis to identify any problems and resolve them upfront, rather than guessing and waiting for a bigger problem to arise.

Remote work management & support of digital workspaces

As the number of remote workers and digital workspaces increases, so does the demand for secure access and transactions. Supporting and protecting your remote workforce can be done through virtual configuration management database (CMDB) management using automated visibility tools. For telehealth or remote project teams, you can plan for database access beyond the clinic or campus by creating rules for different users and groups and then automating deployment and implementation of those rules in a centralized system like a CMDB.

MATRIX42

A change in mindset from “good enough” to “best-in-class”

Many healthcare organizations make one-off investments in tools and technologies out of immediate necessity, resulting in a hodge-podge of solutions that don’t follow a broader master plan and later raise questions about why a particular tool was purchased in the first place.

A shift in mindset toward a more strategic, “best-in-class” one by investing in technologies that put you on proactive — instead of reactive — footing enables a more sustainable and agile IT future. Integrated platforms and extensible tools allow your organization to mix and match solutions that protect the perimeter and all points inside, both at your physical location and on the network, and quickly adapt them to meet evolving threats as soon as there’s a reason to.

Matrix42: A Suite of Cyber Solutions for Hospitals and Healthcare Providers

Matrix42's suite of solutions is the most comprehensive set of proactive and automated privacy and security technologies available for healthcare organizations that meet today's data and network security needs while easing the day-to-day responsibilities of resource-strapped IT teams.

You can gain real-time visibility and insight into all your organization's IT assets, applications, and dependencies through tools and services that include:

- **Secured unified endpoint management (SUEM)** for secure provisioning of your devices and protection of your endpoints, apps, and data
- **Enterprise service management** using ITIL best practices and built-in security to automate your order, approval, and provisioning processes
- **Digital workspace management** to automate processes and drag-and-drop new services and third-party systems from any browser or device
- **Asset management** to optimize software licenses and contracts and ensure compliance across all platforms, including the cloud
- **Discovery and service mapping** to gain a comprehensive view of your infrastructure by discovering and mapping all apps, devices, and configuration profiles
- **Configuration management databases (CMDB)** for defining, storing, and tracking the configuration profiles of all hardware, software, systems, and facilities
- **Cloud migration and security** to securely transfer business operations into the cloud, including data, apps, and IT processes, and ensure data integrity
- **Network security** to protect the integrity of your network from internal and external threats and shore up any vulnerabilities

Assert Greater Control over Healthcare Security & Privacy

Ransomware, malware, hacks, breaches, and data fraud are rampant in the healthcare space. Sensitive personal data and critical systems are at greater risk than ever before, yet reductions in hospital budgets and limited resources are making it harder to mitigate these risks and respond to imminent threats.

Along with broad data governance policies and a consistent application of best practices, your healthcare organization must protect its vulnerable assets and information with cost-effective, flexible, and compliance-oriented technology solutions that can simplify and automate security management.

With Matrix42, your IT team can gain secure control over IT asset and service management, enabling your organization to reduce cyber risks, safeguard sensitive data, and proactively respond to threats of all types while empowering the delivery of optimal patient care.

For more information, visit **www.matrix42.com** or call +1-657-204-0993 to schedule a free, personalized demo.

MATRIX42

Resources

1 Combs, Veronica. “The 5 biggest cybersecurity threats for the healthcare industry.” TechRepublic. Oct. 28, 2020.

2 “Ransomware Payments Up 33% as Maze and Sodinokibi Proliferate in Q1 2020.” Coveware. April 29, 2020.

3 Becker, Jeff. “Arm Yourselves for Healthcare’s Cybersecurity War.” Forrester. Nov. 9, 2018.

4 Healthcare Data Breach Statistics. HIPAA Journal. Retrieved Feb. 15, 2021.

5 Silver, Laura. “Smartphone Ownership Is Growing Rapidly Around the World, But Not Always Equally.” Pew Research. Feb. 5, 2019.

6 Mobile Health Market Report 2013-1017. Research2Guidance.

7 “Ransomware Payments Up 33% as Maze and Sodinokibi Proliferate in Q1 2020.” Coveware. April 29, 2020.

8 Morgan, Steven. “Global Ransomware Damage Costs Predicted to Reach $20 Billion (USD) by 2021.” Cybercrime Magazine. Oct. 21, 2019.

9 “3 of the Biggest Healthcare IT Staffing Challenges (And How to Solve Them).” V-Soft Consulting.