Protecting data in the hospital of the future

Why cybersecurity is a critical piece of Enterprise Intelligence

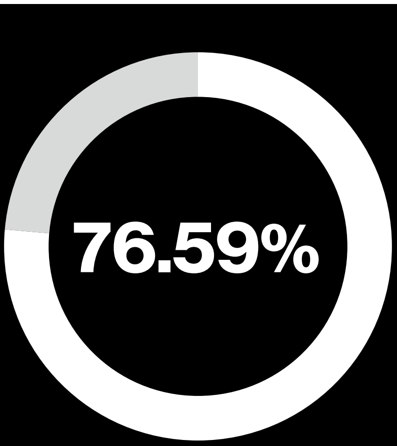
verizon

From SmartBrief

The large hospitals and health systems of the future are advancing care quality and resource management with faster, better data. This is made possible by greater connectivity between devices, but these potential access points must be secured to protect patient health information, payment data and other personal details.

Failure to do so puts both the hospital and patient at risk – and the dangers are increasing. Healthcare data breaches have become more frequent over the past 14 years (with the exception of 2022), and the main causes are hacking/IT incidents.[1]

In 2021, 715 healthcare data breaches were reported -- more than any other year since the HHS Office for Civil Rights began publishing records.[1] That year saw the protected health information of almost 50 million Americans breached.[2] In 2022, there were 571 incidents with confirmed data disclosure.[3]



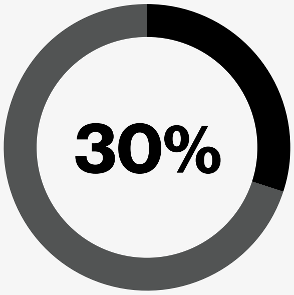
Between 2015 and 2019, 76.59% of recorded data breaches were in the healthcare sector.[1]

The healthcare industry is a popular target for cyberattacks. This is, in part, because healthcare organizations often have larger databases that are tempting for hackers.[1] Additionally, more than half of the most frequently used internet-enabled hospital devices are at risk for cyberattacks.[2]

The 2022 Data Breach Investigations Report from Verizon found that threat actors are usually external (61%) and usually have financial motives (95%), followed by espionage (4%), convenience (1%) and grudge (1%).[3]

The economic downturn has created an especially “ripe environment” for hackers, Merritt Maxim, vice president and research director for Forrester, said on a recent webinar.[4] An increase in online employee interactions, coupled with large numbers of people leaving companies, means more vulnerabilities. “Hackers are continuing to probe for weaknesses and will continue to do that in the year ahead,” Maxim said.

Hospitals make up 30% of large data breaches.[2]



Challenges in healthcare cybersecurity

IT professionals and leaders of large hospitals and health systems face a variety of challenges in protecting their networks, databases and connected devices. The biggest vulnerabilities are:

Data breaches, which can go undetected for weeks or even months when health systems don’t have a real-time view into their network. This might lead to organizations owing financial penalties to the Office for Civil Rights if they fail to report a data breach within the mandated window. Basic web application attacks, miscellaneous errors and system intrusion represent 76% of breaches.[3]

Ransomware attacks, which were at an all-time high last year for healthcare with an almost 13% increase – a rise as big as the past five years combined.[3] When hackers hold healthcare data hostage, care providers sometimes can't get to the information they need to serve patients. At least one patient death was reported last year as a result of a ransomware attack.[5]

A critical shortage of security experts, which makes it difficult to support frequent protocol updates and patching.[6]

Security of the supply chain, which is a significant vulnerability and was responsible for 62% of system intrusion incidents in 2022.[3]

Layered within these challenges is the move toward Enterprise Intelligence. Healthcare organizations need to think about where they are vulnerable today as they build the infrastructure of the future, and cybersecurity must be a top priority in these transformations.

The consequences of falling short

Failure to protect data can bring significant consequences for healthcare organizations, such as reputational harm; financial effects, including breach penalties; impact on business continuity; and compromised care.

The motive for most hackers is money, and ransom payments can be costly for healthcare organizations. The average cost of a healthcare breach was more than $9 million in 2021.[7] Interruptions bring additional costs: For midsize hospitals, a cyberattack causes an average shutdown time of 10 hours and costs $45,700 per hour on average.[2]

The average cost of a healthcare breach was more than $9 million in 2021.[7]

For midsize hospitals, a cyberattack costs about $45,700 per hour.[2]

Organizations can also face multimillion-dollar Health Insurance Portability and Accountability Act fines for failure to report breaches in the mandated timeframe. In 2018, the largest financial penalty for HIPAA violations, $16 million, was paid by a health insurance provider after the investigation of a data breach in 2015.[1]

Even more serious is the impact on patient care. Breaches can lead to rescheduled appointments, diverted ambulances and delayed procedures.[8] Almost half of healthcare IT professionals said their organization has experienced a ransomware attack in the past two years, and of those, 45% said they led to patient complications.[9]

Top cybersecurity innovations

These incidents show that the perimeter around data is porous, and "hackers are absolutely taking advantage of that," Merritt warned. "It's not a question of if you get compromised, it's when," and rapid detection is vital.

There are four key paths that hackers can take to get to an organization's data: credentials, phishing, exploiting vulnerabilities and botnets. No organization is safe without a plan to handle them all.[3]

To address today's cybersecurity challenges and prevent these consequences, healthcare organizations should invest in cutting-edge technologies to protect their data.

Cybersecurity technologies

- **Private networks**. Healthcare is largely Wi-Fi dependent, but healthcare IT leaders lack confidence in the security of their Wi-Fi networks, and many are planning to move to 5G and private networks.
- **Zero-trust frameworks** that verify every person and device every time, regardless of where they originate or whether they are already behind the corporate firewall.
- **Network detection and response**, which can flag intrusions sooner to help address delays in breach reporting that can result in HIPAA fees.
- **IOT security and mobile device security**, such as credentialing, that prevent devices from being used by hackers as an access point.

The ideal solution is a broad, end-to-end security portfolio that protects the network and mobile devices. This should include secure, private networks and a real-time view of potential intrusion activity both externally and internally so that breaches are flagged as soon as possible – sometimes while the intrusion is in progress.

How cybersecurity supports Enterprise Intelligence

The benefits of cybersecurity go beyond avoiding breaches. Tomorrow's successes will be achieved by healthcare organizations that prioritize digital innovation to build smarter, more efficient and more agile enterprises. Transformation starts by bringing together disconnected systems to create powerful, modular and intelligent solutions that can enable new functionality, smarter insights and faster decision-making. The result is Enterprise Intelligence.

Organizations building Enterprise Intelligence will leverage the embedded security of private networks and cloud near-edge computing with high speed and low latency to enable rapid, secure use of real-time insights. For example, artificial intelligence-enabled video, diagnostic scopes and computer vision can flag anomalies and recommend a biopsy during a procedure when identification and assessment is most critical. Real-time asset tracking can help determine the location and condition of medical-grade equipment based on inference data.

Meanwhile, AI is increasingly being used in cyber programs to identify vulnerabilities and threats, predict attacks on data, and provide alerts and recommendations for response. An organization that is operating with Enterprise Intelligence can leverage AI to identify and respond to threats in "real time."

While funding for advanced cybersecurity technologies was robust during the pandemic, recent economic challenges have made organizations more concerned about maximizing return on investment from their cybersecurity investments, Maxim said.

Chris Novak, managing director for Verizon Cyber Security Consulting, noted that organizations are increasingly addressing cybersecurity amid budget or headcount cuts, leading them to take a different approach.[4] "Historically, we saw lots of organizations focus on trying to do it all themselves and now ... a lot of them are starting to say, 'We need the same level of security, but maybe doing it ourselves isn't always the answer.'"

Managed services, such as those offered by Verizon, can play an important role for organizations that lack the capabilities or personnel to implement certain technologies. Maxim pointed to a resurgence of managed services that offer more value-add beyond standard monitoring, including more active detection.

Getting started

Hospitals and health systems that want to tighten cybersecurity and make the most of the rich data available to them can begin with a few simple steps:

- Start with a security program health check to assess data vulnerability.
- Follow up by assessing current programs and tech stacks for vulnerabilities.
- Consult with a trusted partner like Verizon to create a roadmap for streamlining the security portfolio and programs.
- Leverage services including ransomware attack simulations; network detection and response capabilities; private networks; remediation, resolution and recovery services; and fully managed security services.

Healthcare organizations need secure data at their fingertips and a real-time view across every access point in the network. Those that prioritize cybersecurity will be able to put their information, technology and resources to the right use: providing next-level care as quickly as possible.

Learn more at verizon.com

References

1. Healthcare Data Breach Statistics. The HIPAA Journal. https://www.hipaajournal.com/healthcare-data-breach-statistics/
2. Adams, K. Healthcare data breaches by the numbers: 9 stats. Becker's Health IT. March 23, 2022. https://www.beckershospitalreview.com/cybersecurity/healthcare-data-breaches-by-the-numbers-9-stats.html
3. 2022 Data Breach Investigations Report. Verizon. https://www.verizon.com/business/resources/reports/dbir/
4. Maintaining strong cybersecurity in turbulent economic times. Verizon/Forrester. Jan. 26, 2023. https://www.brighttalk.com/webcast/15099/570308
5. Balasubramanian, S. Cybersecurity must become a top priority In healthcare. Forbes. Oct. 24, 2022. https://www.forbes.com/sites/saibala/2022/10/24/cybersecurity-must-become-a-top-priority-in-healthcare/
6. Poremba, S. The cybersecurity talent shortage: The outlook for 2023. Cybersecurity Dive. Jan. 5, 2023. https://www.cybersecuritydive.com/news/cybersecurity-talent-gap-worker-shortage/639724/
7. Southwick, R., Ransomware attacks on hospitals are rising. Chief Healthcare Executive. July 20, 2022. https://www.chiefhealthcareexecutive.com/view/ransomware-attacks-on-hospitals-are-rising
8. Starks, T. An 'unprecedented' hospital system hack disrupts health-care services. Washington Post. Oct. 6, 2022. https://www.washingtonpost.com/politics/2022/10/06/an-unprecedented-hospital-system-hack-disrupts-health-care-services/
9. Southwick, R. Ransomware attacks continue to rise, and they're hurting patients: Survey. Chief Healthcare Executive. Jan. 24, 2023. https://www.chiefhealthcareexecutive.com/view/ransomware-attacks-continue-to-rise-and-they-re-hurting-patients-survey

verizon

From SmartBrief