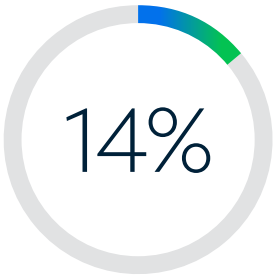
GUIDE

Stay a step ahead of cybersecurity threats in healthcare

Healthcare organizations (HCOs) face an imperative to deliver patient care effectively and keep personal data secure.



of healthcare IT leaders say their IT security teams are fully staffed.[3]

Patient data needs to remain secure yet easily accessible to the right medical professionals across multiple shared networks and devices. The far-reaching potential impact of a data security breach — in an era of ever-increasing incidence and severity of attacks — makes healthcare network security uniquely challenging.

More than 90% of HCOs experienced a cyberattack in 2024, and of those, nearly 70% experienced disruptions in patient care as a result.[1] Attackers are drawn to the sector because of its huge amount of protected health information (PHI), which includes valuable personal data, such as medical records, demographic details and insurance and payment information. In 2024, 25.6 million healthcare industry records were affected by ransomware attacks alone.[2]

HIPAA fines incurred due to data breaches range from around $140 to over $70,000 per violation.[4] Data breaches can also harm productivity and patient care. As a result, IT leaders are investing in a range of measures to protect their networks. Among HCOs that have experienced a ransomware attack:[5]

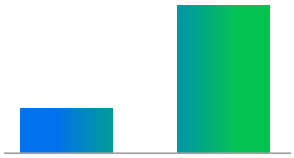
- **62%** implemented new security tools.
- **57%** put new security policies in place.
- **49%** enhanced security awareness training programs.
- **43%** upgraded legacy technology.
- **30%** increased cybersecurity staff.

Spectrum BUSINESS®

Tracking evolving threats

Cyberattacks on HCOs are more prevalent than ever, and the profile of threats is constantly changing. Protect your organization from a wide range of attack vectors by understanding current and emerging types of threats.

Proportion of an organization's sensitive data affected during a typical breach:[6]



6% All industries

20% Healthcare

$7.42M

Average cost of a data breach in the healthcare industry.[9]

Social engineering

This technique is used by cybercriminals to exploit human psychology and trick people into revealing confidential information or performing actions that compromise security. Phishing is one common method, with attackers often impersonating legitimate entities to steal sensitive data or plant malware through malicious files or downloads.

AI-powered cyberthreats

These emerging methods leverage AI to create more convincing and automated attacks, making them harder to detect and potentially more effective. One example includes using AI to develop deepfakes, which are realistic fake videos, audio or images employed to trick individuals into granting access to systems or data. AI can also help generate highly personalized phishing emails, power chatbot phishing efforts and attack AI systems by corrupting training data or finding vulnerabilities in the models. More than 90% of security experts expect a significant rise in AI-driven threats in the next few years.[7]

Ransomware and other malware

Malware is broadly defined as any malicious software designed to harm or exploit computer systems. Ransomware is a type of malware attackers use to restrict access to a computer system or files and then demand payment for their release. Healthcare is the second most targeted industry for ransomware behind manufacturing, accounting for 10% of all publicly reported ransomware victims in 2024.[8] Downloaders are another common malware type, distributed through malicious or compromised websites, typically via fake software updates. New malware variations appear each year, underscoring the need for organizations to remain up to date and vigilant.

Distributed denial of service (DDoS) attacks

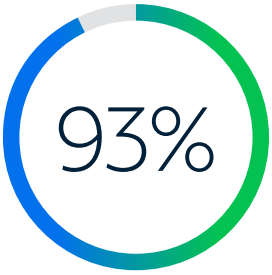
These brute-force attacks are throwing more traffic at networks than ever before, combining volumetric, session-exhaustion and application-layer attack vectors. In session-exhaustion attacks, the firewall is essentially turned inside out, becoming a tool for attackers instead of a network defense. Application-layer attacks target the code that runs the website or application. The average cost of an application-layer DDoS attack is $6,130 per minute.[10]

Data breaches

The unauthorized access, disclosure or loss of sensitive, confidential or protected information continues to be a risk faced by HCOs large and small. The theft can involve personally identifiable information (PII), such as Social Security numbers, bank account details and PHI, as well as corporate data like customer records and financial information. In some cases, attackers prefer to corrupt rather than steal from databases: deleting tables, changing records or erasing entire databases.

15,000

Number of medical devices at a typical 1,000-bed hospital.[11]



of HCOs are running insecurely connected medical devices that are vulnerable to known public exploits.[12]

How cyberattacks can be prevented

Breaking down the details of healthcare cybercrimes helps paint a clear picture of the evolving threat. Read these hypothetical examples and see how organizations might have been better protected against an attack.

Phishing attacks expose data

Type of breach: The employee email network of a health system was hit by three potential data breaches in less than six months.

What was lost: Emails with malicious links were sent to a wide range of internal and external accounts without authorization as the hacker attempted to obtain usernames and passwords from email recipients.

What might have mitigated or thwarted the attack: The use of anti-malware protection and a next-generation firewall may have prevented the attack. Encrypted data, both in transit and at rest, would have rendered all the health system's emails and other records unreadable. Use of multi-factor authentication (MFA), updated software and expert training for employees about current phishing methods could have deterred the attackers' efforts.

Ransomware attack strikes health system

Type of breach: A ransomware attack shut down the computer network of a health system with seventeen hospitals for two days.

What was lost: The health system paid an undisclosed amount in ransom to stop the attack, which forced hospitals to reschedule non-emergency surgeries and left providers with no access to electronic health records.

What might have mitigated or thwarted the attack: The use of antivirus software and a next-generation firewall, as well as content scanning and filtering to detect threats in advance, could have prevented the intrusion. MFA and segmented security zones within the network could have hindered bad actors from moving laterally if they gained access to one device, while endpoint security solutions could help protect individual devices connected to the network.

Hospital hit by DDoS attack

Type of breach: A hacker launched a DDoS attack against a leading children's hospital, disabling parts of its network.

What was lost: In addition to disrupted admissions and recordkeeping that put young patients' lives at risk, the hospital's donations page and multiple business applications went offline. It took several days to bring the hospital back to normal operations.

What might have mitigated or thwarted the attack: DDoS protection services could have blocked the offending IP address and prevented secondary attacks. Machine learning and AI might have identified anomalies in traffic flows, triggering targeted IP address cleansing. With the address blocked, clean traffic would be allowed to pass, which would have enabled sites and applications to continue operations. In addition, access to a cloud-based portal may have provided the real-time traffic visibility, insights, analytics and in-depth reporting needed to help avert the attack or limit its impact.

Finding the right protection

Continuously keeping ahead of cybersecurity threats to your network requires comprehensive and coordinated coverage. A unified security approach integrated with your internet and network connectivity can help you eliminate vulnerabilities and expedite issue resolution. The approach should include firewalls, unified threat management (UTM) and DDoS protection. The support of a network services provider is also vital, including for cloud-based security services such as secure web gateways, cloud access security brokers, identity management and zero trust network access.

When it's time to evaluate a provider and its services, ask the following questions to help you find the best protection possible:

- How can you protect us from malware, phishing and other common cyberattacks?
- How do you identify and mitigate network threats? Can you scan our network for attacks and drain suspicious traffic?
- What protection do you provide against volumetric DDoS attacks?
- Do you have a means for enabling us to continue to work productively on unaffected parts of the network after a DDoS attack?
- Do you provide UTM? What protection does that provide?
- Can your firewall protect traffic across our various sites?
- Is a next-generation firewall part of what you offer? What does it provide?
- Do you have an integrated solution that includes firewall, UTM and internet service to simplify protection?
- Does your solution provide complete visibility across network components to make potential vulnerabilities easier to identify?
- Can you help implement a zero-trust network architecture with MFA, access management and cloud security for staff working on-site and remotely?
- How are you prepared to support our organization as our network needs change and cyberthreats evolve?
- How can you help offload day-to-day administration work from our IT team during and after implementation?
- What types of teams and experts will we have access to for support? Are they available 24/7/365?
- How will you ensure all of our WiFi sites are protected?

Comprehensive coverage and support

Widespread, coordinated network protection can keep you one step ahead of evolving healthcare network threats. You can balance the needs for complexity in coverage and simplicity in operation by choosing managed security services. With the right partner, you're supported from design through implementation and provided with ongoing support. See how Spectrum Business® is uniquely qualified to protect your healthcare network.

Learn more

1. "2024 Ponemon Healthcare Cybersecurity Report," Proofpoint, 2024.
2. Rebecca Moody, "Ransomware Roundup: 2024 End-of-Year Report," Comparitech, January 9, 2025.
3. Jordan Scott, "New CDW Research Report: Shortages Impact Healthcare Cybersecurity Strategies," June 10, 2024.
4. "HIPAA Violation Fines," The HIPAA Journal, August 10, 2024.
5. "2024 HIMSS Healthcare Cybersecurity Survey," HIMSS, 2025.
6. "The State of Data Security: Measuring Your Data's Risk," Rubrik Zero Labs, 2024.
7. "Cybercrime Trends 2025," SoSafe, 2025.
8. "The State of Cyber Security 2025," Check Point Research, 2025.
9. "Cost of a Data Breach Report 2025: The AI Oversight Gap," Ponemon Institute and IBM Security, July 2025.
10. "Application Security in a Multi-Cloud World 2023," Radware, November 8, 2023.
11. Steve Alder, "63% of Known Exploited Vulnerabilities Can be Found in Hospital Networks," The HIPAA Journal, March 12, 2024.
12. "State of CPS Security: Healthcare Exposures 2025," Claroty, 2025.

Spectrum BUSINESS®