GUIDE

How to stay a step ahead of cybersecurity threats in healthcare

Spectrum ENTERPRISE

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

Patient data needs to be quickly and easily accessible to the right medical professionals, across multiple shared networks and devices, but must remain secure to ensure patient safety and privacy. 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.

of healthcare organizations have experienced a data breach over the past three years.[3]

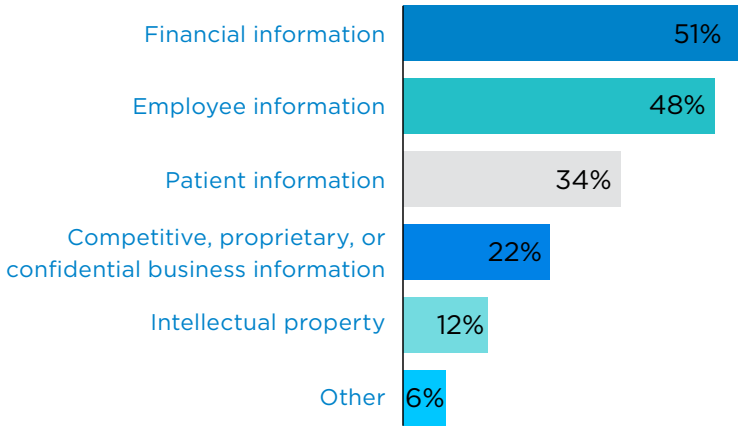
Some 93 percent of healthcare organizations experienced a data breach during the past three years, with 57 percent reporting more than five data breaches during the same timeframe.[1] The healthcare industry experienced a 42 percent jump in the number of hacking incidents between 2020 and 2019, with hacking incidents responsible for 62 percent of all patient data breaches in 2020.[2]

Attackers are drawn to the sector because of its huge amount of protected health information (PHI), which includes valuable personal data. The risk to this confidential patient information is enormous. In 2020 alone, 26.4 million patient records were exposed — significantly higher than the nearly 12 million individuals impacted by healthcare data breaches in 2018.[4]

HIPAA fines incurred because of violations caused by data breaches can range from $100 to $50,000 each,[5] but the potential harm isn't just financial in nature. A recent survey found that healthcare organizations who experienced data breaches also experienced damages to:[6]

- **Effectiveness:** 41 percent suffered an operational outage that affected productivity.
- **Patient care:** 32 percent incurred an operational outage that put physical safety at risk.
- **Reputation:** 32 percent experienced damage to brand awareness.
- **Business information:** 25 percent lost critical data.

Breaches are likely to continue as long as healthcare organizations possess what hackers want. In recent healthcare security incidents, threat actors most often targeted:[7]



Spectrum ENTERPRISE

Tracking evolving threats

Cyberattacks on healthcare organizations are more prevalent, 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.

The top data breach threats in healthcare organizations include:

DDoS: Distributed denial of service (DDoS) attacks have increased in size, duration, sophistication and frequency during the Covid pandemic. There were nearly 5.4 million DDoS attacks worldwide in the first half of 2021 alone, up 11 percent year-over-year. The average attack duration was 50 minutes, up 31 percent.[8] Since 2020 the healthcare sector has suffered some of the largest attacks, with average attack size of more than 60,000 megabits per second; other industries suffered attacks of 10,000 mbps or less.[9]

Ransomware: Today's advanced strains of ransomware encrypt data on a network and often lock users out of their devices. Ransomware was the leading cause of healthcare data breaches in 2020, accounting for nearly 55 percent of incidents.[10]

Business email compromises: Email compromise, a category that includes phishing attacks, was identified as the root cause of 21 percent of healthcare data breaches in 2020. It was the third most-common attack type that year.[11]

Insider threats: An insider threat refers to incidents caused by someone within or close to an organization, such as an employee, a former employee, a contractor or a business partner, who misuses his or her authorized access in a way that negatively impacts the organization. Insider threats accounted for 7 percent of data breaches in the healthcare sector during 2020.[12]

2020 healthcare security incident type breakdown:[13]

Spectrum ENTERPRISE

One-third of healthcare companies report that a data breach resulted in reputation damage and put patient physical safety at risk.[14]

Real-world cyberattacks

Details of healthcare cybercrimes help paint a clear picture of the evolving threat. Read these 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 user names and passwords from email recipients.

What might have mitigated or thwarted the attack: A managed firewall service could have blocked and protected confidential information from those not authorized to access the network.

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 (EHRs).

What might have mitigated or thwarted the attack: Use of a next-generation firewall could have helped block the attack and warned the health system's IT team to act sooner.

Hospital hit by DDoS attack

Type of breach: A hacker launched a DDoS attack against a leading children's hospital.

What was lost: In addition to the lives of young patients being put at risk, the hospital's donations page was shut down, resulting in approximately $300,000 in lost revenue and another estimated $300,000 in necessary repairs to the computer system.

What might have mitigated or thwarted the attack: Careful monitoring of Internet traffic could have detected the attack. A DDoS solution could have blocked certain IP addresses, allowing clean traffic to pass and productivity to be maintained or restored.

Spectrum ENTERPRISE

Finding the right protection

Continually keeping ahead of cybersecurity threats to your network requires comprehensive and coordinated coverage. Firewalls, unified threat management (UTM), DDoS protection and the support of a network services provider to deliver a managed service solution can help.

When you're evaluating a provider and their services, here are some questions to ask to help you find the best protection possible:

Widespread, coordinated network protection coverage can help protect against cyber threats.

- What protection do you provide against volumetric DDoS attacks?
- During a DDoS attack, do you have a means of letting us continue to work productively on the parts of the network that are not affected?
- How do you identify and mitigate network threats? Can you scan our network for attacks and drain suspicious traffic?
- How can you protect us from malware, phishing and other common healthcare cyberattacks?
- Do you provide UTM? What protection does that provide?
- Can your firewall protect traffic between our various sites as well?
- Is a next-generation firewall part of what you offer? What protection does it provide?
- Do you have an integrated solution that includes firewall, UTM and internet service to simplify protection?
- What type of support is available on nights, weekends and holidays?
- How can a managed service help us protect our organization?
- What partnerships do you have that will help you increase the protection you provide to our network?
- Threats are evolving, and our network is always changing and growing. Can you support us and our investment as the environment and our needs change?
- Is the team supporting your organization specifically trained in and dedicated to the healthcare industry?

Comprehensive coverage and support

Widespread, coordinated network protection coverage can keep you one step ahead of evolving and growing healthcare network threats. When you choose security as a managed service, you're supported from design through implementation and thereafter. See how Spectrum Enterprise is uniquely qualified to protect your organization's network.

Learn more

1. "The 2020 Healthcare Cybersecurity Report." A Special Report from the Editors at Cybersecurity Ventures Sponsored by Herjavec Group. 2020.
2. "Increased Cyberattacks On Healthcare Institutions Shows The Need For Greater Cybersecurity." Nick Culbertson. Forbes. Jun 7, 2021.
3. "The 2020 Healthcare Cybersecurity Report." A Special Report from the Editors at Cybersecurity Ventures Sponsored by Herjavec Group. 2020.
4. "Healthcare Breach Report 2021: Hacking and IT Incidents on the Rise." Bitglass. February 17, 2021.
5. "HIPAA violations and enforcement," American Medical Association, 2020.
6. "Healthcare Persona Survey," Fortinet, 2020.
7. "2020 HIMSS Cybersecurity Survey." 2020. Healthcare Information and Management Systems Society.
8. "Netscout Threat Intelligence Report. Issue 7: Findings from 1H 2021." 2021.
9. *DDoS Attack Trends for 2021*. David Warburton. May 7, 2021.
10. "Healthcare Security: Ransomware Plays a Prominent Role in COVID-19 Era Breaches." Rody Quinlan. Tenable. March 10, 2021.
11. Ibid.
12. Ibid.
13. "2020 HIMSS Cybersecurity Survey." Healthcare Information and Management Systems Society. 2020.
14. "Healthcare Persona Survey," Fortinet. 2020.

About Spectrum Enterprise

Spectrum Enterprise, a part of Charter Communications, Inc., is a national provider of scalable, fiber technology solutions serving many of America's largest businesses and communications service providers. The broad Spectrum Enterprise portfolio includes networking and managed services solutions: Internet access, Ethernet access and networks, Voice and TV solutions. The Spectrum Enterprise team of experts works closely with clients to achieve greater business success by providing solutions designed to meet their evolving needs. For more information, visit enterprise.spectrum.com.

Spectrum ENTERPRISE