Hospitals and health systems in the crosshairs

verizon

Ransomware attacks threaten healthcare, but effective cybersecurity can mitigate the risk

The healthcare cyberattack landscape

The healthcare industry has been hit hard during the COVID-19 pandemic, and not just by health-related challenges. Cybersecurity attacks also have increased, with bad actors taking advantage of the uncertain environment, increased remote work and spiking care needs, and creating expensive and logistically difficult problems for hospitals and health systems.

Healthcare breaches totaled 599 in 2020, an increase of 55.1%[1] from the prior year, and they topped 550 again in 2021 as bad actors took advantage of employee distractions, such as working from home while caring for children and concerns about job security, says David Grady, chief cybersecurity evangelist with Verizon Business Group. These factors made people more vulnerable to clicking on unsafe links, and healthcare industry attacks in 2020 were nearly on par with other industries, such as the financial sector.

Ransomware attacks, where cyberattackers demand a ransom to restore access to files or networks, are increasing as well — a trend that is likely to continue this year.[2] In 2020, 560 healthcare organizations fell victim to ransomware attacks,[3] and a 2021 worldwide survey of healthcare and public health organizations found 34% were hit by ransomware in the past year.[4]

More recently, a new dimension to ransomware attacks has emerged, with hackers not only encrypting data and making it impossible to access, but also stealing it. They demand an initial ransom to unlock the data, so the healthcare organization can use it, and then demand a second ransom in exchange for not publicizing or selling it on the dark web.

There has also been an increase in demand for payment to avoid a distributed denial of service attack, which is when a bad actor overwhelms an organization's IT systems and servers with a tidal wave of requests that can knock it offline.

It may seem surprising that cybercriminals would target hospitals and other healthcare entities, and this belief can lead to a false sense of security. As a result, many organizations are inadequately protected against ransomware, which typically infects machines via:[5]

- Phishing emails with a malicious attachment.
- A user clicking on a malicious link.
- A user viewing an advertisement containing malware.

Healthcare organizations may think they will be spared from these types of attacks because they do meaningful and compassionate work, but that is wishful thinking, Grady says, noting, "The bad guys are heartless and see healthcare organizations as an easy target." They focus on organizations they view as vulnerable, or as very likely to pay a ransom because it is essential to resume operations as quickly as possible. In addition, health data has a high value in black markets online.[6]

Financial impact

Healthcare organizations can face significant financial consequences after an attack. The average ransomware payment for healthcare and public health sectors is $131,000. When including the costs of downtime, worker hours, device costs, networks and lost opportunity, the total expenditure can reach up to $1.27 million.[4]

Ransomware attacks specifically cost healthcare organizations $20.8 billion in downtime in 2020,3 and 10% of data breaches over the past 12 months started with ransomware and led to extortion and operational downtime.[7]

In October 2020, a ransomware attack on one university health network delayed patient care and cost the health system more than $63 million in lost revenue and resulting increased expenses, even though the network chose not to pay the ransom. The attack affected computers and patient medical records in six hospitals, and patients, including those with cancer, experienced delays in treatment.[8]

Disruption to care

Care disruptions are common with ransomware as well as other cyberattacks and can result from:[9]

- Stolen, leaked or encrypted medical records or other data needed for normal operations.[10]
- Damage or loss of service to medical devices or other critical systems.
- Closure of departments and entire hospitals.
- Diversion of patients to other hospitals.[6]
- Delay or cancellation of critical primary care and treatment.
- Effects on secondary care, such as obtaining medical results.

These disruptions could lead to dire consequences. In a survey of 597 health delivery organizations,[11] 71% of respondents said a successful cyberattack resulted in longer lengths of stay for patients, and about the same percentage said ransomware attacks created delays in medical procedures and tests that resulted in poor outcomes for patients.

Meanwhile, 36% of respondents saw an increase in complications from medical procedures following a ransomware attack, and about a fifth said cyberattacks had increased patients' mortality rate.

Disruption of care can also leave organizations exposed to longer-term repercussions, including lawsuits. In Alabama, a lawsuit has been brought against a hospital, alleging that care shortfalls linked to a ransomware attack led to a severe brain injury and subsequent death of a newborn.[12]

Protecting your organization

Attacks on healthcare systems continue to make headlines, but there is often a disconnect between concerns about cyberattack risks and the commitment to invest in protective measures.

An April 2021 HIMSS survey of IT leaders in US healthcare found nearly half identified cybersecurity, hackers and malware as their top technology concerns.[13] Meanwhile, just 9% were completely comfortable with their current Wi-Fi infrastructure. But despite these concerns, recent research from CyberMDX and Philips shows most hospitals fail to identify cybersecurity as an investment priority.[10]

Annual IT budgets for midsize hospitals averaged $3.5 million, and for large hospitals the average was $3.1 million.[10] But annual internet of things and medical device cybersecurity spending averaged $293,000 for midsize hospitals and $329,000 for large hospitals.[10]

Hospitals and health systems that recognize the risk of ransomware and want to defend themselves should create a cybersecurity program with some of the best practices that will better protect them.[14]

Risk identification: Healthcare organizations should make use of publicly available intelligence, such as cyberthreat intelligence feeds, to learn about device vulnerabilities and early indications that a ransomware or malware attack might be imminent. Advanced analytics and user and entity behavior patterns can also help uncover unknown threats. It's important to perform recurring cybersecurity assessments and penetration testing, and to fix any vulnerabilities identified.

Protection and preparation: Healthcare organizations must prepare for worst-case scenarios. Data should be backed up daily to a secure location. Employee training and simulated attacks are key to ensuring everyone is aware of the danger signals of ransomware, malware and suspicious emails. Meanwhile, organizations should implement multifactor authentication for remote access to OT and IT networks, strong spam filters to block phishing emails, filters for network traffic, regular software updates, and regular network scans by antivirus and anti-malwareprograms.[4] Protection against DDoS threats will also become more important, as this type of attack is expected to increase.

Detection: All devices and system users that connect to the network, as well as their network access methodologies, should be discovered and documented, and organizations should maintain an up-to-date list of all authorized devices. There also has been a recent advance in "deception as a service," which involves setting up a dummy copy of an organization's systems to fool hackers into thinking they are attacking the right target. This gives the security team insight into an attack underway so they can contain it and better protect their systems. Finally, healthcare organizations should be able to detect unauthorized exfiltration or removal of data, which could mean an attack is starting.

A response plan: "You don't want to decide how you're going to respond to a ransomware attack when you're in the middle of one," Grady warns. Organizations should decide what course of action they will take well before an attack happens and should prepare for worst-case scenarios. This includes determining whether they will budget to pay the ransom and developing a plan to recover systems and data by using retrieved backup data storage. They will also need a process for post-incident analysis.

In addition to those four components, CyberMDX and Philips found approximately 3 in 4 have considered wireless router upgrades, and close to half are planning to migrate to 5G service.[13] Along with better data security, they're looking at how they can use the network to enhance the clinical experience, streamline operations and get better data faster.

"You don't want to decide how you're going to respond to a ransomware attack when you're in the middle of one."

David Grady, chief cybersecurity evangelist with Verizon Business Group

Achieving effective cybersecurity

Getting cybersecurity right can be a daunting task for hospitals and health systems, especially now that many organizations have seen a reduction in revenue, as well as staff burnout, due to the pandemic. This often means that security resources and capabilities are reduced or underfunded. Even before the pandemic, more than one-third of healthcare organizations eased their cybersecurity burden by working with partners, and nearly 25% prefer to implement or manage their networks through a fully managed service.[13] Working with a partner that can provide specialized services, threat intelligence, deception as a service, preparation and instant response planning can help an organization get more return on their security investment.

Whether your organization works with a reputable security partner or handles cybersecurity in-house, ensuring you have up-to-date knowledge, software and employee training will help you avoid costly, dangerous interruptions and provide the best, safest and most consistent patient care.

References

1. Mitchell, H. Healthcare data breaches up 55.1% in 2020, report finds. Becker's Hospital Review. Feb. 22, 2021. https://www.beckershospitalreview.com/cybersecurity/healthcare-data-breaches-up-55-1-in-2020-report-finds.html

2. McKeon, J. This year's largest healthcare data breaches. Health IT Security. Nov. 30, 2021. https://healthitsecurity.com/features/this-years-largest-healthcare-data-breaches

3. Mitchell, H. Ransomware attacks cost healthcare orgs $20.8B in 2020. Becker's Hospital Review. July 28, 2021. https://www.beckershospitalreview.com/cybersecurity/ransomware-attacks-cost-healthcare-orgs-20-8b-in-2020.html

4. Ransomware Trends 2021. HHS Cybersecurity Program. June 3, 2021.

5. Ransomware: In the healthcare sector. Center for Internet Security. https://www.cisecurity.org/blog/ransomware-in-the-healthcare-sector

6. McKeon, J. 39 ransomware groups targeted healthcare in the past 18 months. Health IT Security. Dec. 17, 2021. https://healthitsecurity.com/news/39-ransomware-groups-targeted-healthcare-in-the-past-18-months

7. 2021 Verizon Data Breach Investigations Report.

8. Cutler, C. UVM Health Network continues to tally costs of ransomware attack. WCAX. June 17, 2021. https://www.wcax.com/2021/06/17/uvm-health-network-continues-tally-costs-ransomware-attack/

9. Costis, A. Ransomware and targeted attacks in the healthcare sector. Security Boulevard. Sept. 23, 2021. https://securityboulevard.com/2021/09/ransomware-and-targeted-attacks-in-the-healthcare-sector/

10. McKeon, J. 2021's top healthcare cybersecurity threats, what's coming in 2022. Health IT Security. Oct. 19, 2021. https://healthitsecurity.com/features/2021s-top-healthcare-cybersecurity-threats-whats-coming-in-2022

11. Bisson, D. Hospital ransomware attacks go beyond health care data. Security Intelligence. Nov. 24, 2021. https://securityintelligence.com/articles/hospital-ransomware-health-care-data/

12. Collier, K. Baby died because of ransomware attack on hospital, suit says. NBC. Sept. 30, 2021. https://www.nbcnews.com/news/baby-died-due-ransomware-attack-hospital-suit-claims-rcna2465

13. 5G in Healthcare. HIMSS/Verizon. June 2021.

14. The way forward: A guide to help prevent ransomware attacks and strengthen cybersecurity. Verizon.