Increasing Healthcare Organizations' Vigilance and Resilience Amid Rising Cyberattacks

A zero-trust approach coupled with on-demand, clean restore options can help healthcare leaders protect data and patients

Cybercriminals are employing cutting-edge methods to hold healthcare organizations' data hostage, simultaneously causing financial harm and putting patient safety at risk. To defend against these cyberattacks, healthcare organizations must bolster their defenses by implementing high-level strategies that can help protect data and avoid care disruptions. David Houlding, Director, Global Healthcare Security and Compliance Strategy at Microsoft, Rich Krause, Healthcare Specialist at Commvault, and Bill Byron Concevitch, Director, World-Wide Alliances Marketing for Microsoft at Commvault, discussed how to do so during the HIMSS webinar "Cyber Resilience for Uninterrupted Patient Care."

Healthcare faces increasingly intimidating threats

According to a 2024 Microsoft healthcare threat intelligence report:

- Healthcare has witnessed a 300% surge in ransomware attacks since 2015
- 67% of healthcare organizations experienced a ransomware attack in the last year
- 53% of affected organizations admitted to paying ransoms
- The average admitted ransom payment was $4.4 million[1]

"[Ransomware is] lucrative for cybercriminals. We want to help organizations get into a position where it's feasible to not pay the ransom."

DAVID HOULDING | Director, Global Healthcare Security and Compliance Strategy | Microsoft

While more than half of the surveyed affected organizations admit to paying the ransom, others meet the bad actors' demands but keep the transaction confidential. "It's a very lucrative business for cybercriminals. Unfortunately, many [organizations] are not in a position to not pay the ransom. We want to help organizations get into a position where it's feasible to not pay the ransom," Houlding said.

Paying a ransom is just one possible troubling consequence of cyberattacks. Disruptions in care can also occur, as these assaults can shut healthcare organizations down for weeks, according to Houlding.

What's more, ransomware attacks can produce a ripple effect in neighboring facilities. A study showed that when four hospitals were attacked, two neighboring facilities experienced increases of 35.2% in emergency medical services arrivals, 15.1% in patient volume, 47.6% in waiting room time, 74.6% in stroke code activations, 113.6% in confirmed strokes and 81% in cardiac arrest cases.[2]

Care disruptions may be even more dire in rural areas, where hospitals are often isolated. "That can be a patient safety or a life-or-death issue, if your facility is out of operation because of ransomware and there isn't somewhere [nearby] to send that patient," Houlding said.

The path to effective cyber resilience for healthcare organizations

Healthcare providers must have a plan in place to protect themselves and the patients they serve, according to Peter Hands, British Medical Association (BMA) CISO, whose comments from Commvault's recent SHIFT event in London were included in the webinar. He described how the BMA was attacked at about the same time as another well-known British institution. However, because the BMA had data security mechanisms in place and maintained visibility across its estate, it was able to detect the bad actors early enough to limit the attack's damage.

To combat cybercriminals and minimize damage from cyberattacks, healthcare organizations should consider adopting a zero-trust approach based on verifying every request for data access. Zero trust seeks to prevent unauthorized access to sensitive information by allowing staff only the minimal privileges needed for their roles and leveraging multi-factor authentication. Limiting users' privileges across the network means that, even if a cybercriminal can log in with compromised credentials, the potential harm they can cause is contained.

Because organizations must be ready for anything, leaders need constant visibility across what is typically a complex end-to-end healthcare IT environment. This visibility enables organizations to detect threats, then respond, contain and remediate them before damage can be done to the network. "When that [bad actor's] click occurs, you've got to detect it quickly and shut it down," Houlding said.

Early detection: Key to success

Early detection tools are also essential to a holistic cyber resilience approach. These tools "touch all your data every day, so [they] know what normal is. And when [they] detect abnormal [activity, they can] fire up a note and stop things as soon as possible, because the sooner you know [attackers] are in there, the faster the road to recovery starts," Krause said.

Krause cautioned that attackers may initially target an organization's backup mechanisms "because that's the thing that's going to keep you from paying them in most instances. So, your backup mechanism should not only know when somebody is tampering with it but be able to send alerts…so the people that are responsible can act on them more quickly," he noted.

Since cyberattacks may go unnoticed for some time, Krause also recommended immutable data storage that doesn't allow modification of the data after it's been stored so that backups are free from harmful changes. "[Cybercriminals] are not just coming in with guns blazing right out of the gate anymore. They're kind of trickling in. And sometimes you don't know they're in there," he added.

Providing a verified secure and clean infrastructure for recovered data

Healthcare leaders should be aware that recovering from a cyberattack is not the same as recovering from natural disasters or general outages. To recover after a natural disaster or general outage, organizations can simply restore their data in its original state. For example, a server or data center might go down temporarily, after which leaders can reactivate systems.

> **"[Cybercriminals] are not just coming in with guns blazing right out of the gate anymore. Sometimes you don't know they're in there."**
>
> **RICH KRAUSE** | Healthcare Specialist | Commvault

After a cyberattack, leaders must first ascertain that the organization's data is clean and uncompromised; "otherwise, [they] can make matters worse by recovering it," Hands said. Immutable storage can help keep an organization's backup data clean, but that data will need an equally clean and unaltered space in which to be restored.

Krause said that healthcare organizations must maintain a "clean room," a secure environment in the cloud, so that recovered data is not restored to a location that may still be infected with ransomware or malware. "Cleanroom Recovery is really about dependability of that remediation. With Cleanroom Recovery… we can finally help break this whole cycle of ransoms being paid," Houlding explained.

Integration and simplicity lead to effective cyber resilience

Healthcare IT teams are increasingly burdened by working with many disparate security tools. Without integration of these tools across end-to-end IT environments, potential threats may not be promptly detected. With integrated cybersecurity solutions, IT teams can increase visibility and situational awareness so they can respond quickly when threats are spotted. An integrated security system can "give the security analyst a summary of what's just happened and what should they do about it. So, it's actually giving them guidance in the moment, a teachable moment," Houlding said.

Leveraging Commvault's and Microsoft's integrated solutions can make quick recovery from cyberattacks more financially feasible. "On average, customers that adopted Microsoft's backbone of utilizing Azure combined with Commvault Cloud were able to replace 15 existing tools that they were using for backup, recovery and data protection — and drive a five times lower total cost of ownership," Concevitch pointed out.[3]

With this cost-effective technology in place, it's also possible to frequently test recovery readiness. "If you're not testing [recovery], you have no idea whether or not it's actually going to work…and you don't want to be testing it when the fire alarm goes off," Krause concluded. "Cleanroom Recovery technology and automation and integration with Azure really makes it so [maintaining cyber resilience is] not only cost effective, but it's not time consuming. So, it really gives you no reason to not test it all the time and basically be ready to take that punch."

To learn more about Commvault, visit www.commvault.com/use-cases/healthcare

References

1. Microsoft. 2024. *US healthcare at risk: Strengthening resiliency against ransomware attacks*. https://www.microsoft.com/en-us/security/security-insider/emerging-threats/US-healthcare-at-risk-strengthening-resiliency-against-ransomware-attacks.
2. Microsoft, *US healthcare at risk*.
3. Commvault. 2024. New study: The economics of cyber resilience. https://www.commvault.com/gc/the-economic-benefits-of-cyber-resilience-with-commvault-on-azure.

Commvault

About Commvault

Commvault (NASDAQ: CVLT) is the gold standard in cyber resilience, helping more than 100,000 organizations keep data safe and businesses resilient and moving forward. Today, Commvault offers the only cyber resilience platform that combines the best data security and rapid recovery at enterprise scale across any workload, anywhere—at the lowest TCO.

Microsoft

About Microsoft

Microsoft for Healthcare provides innovative solutions that empower organizations to enhance patient engagement, enable health team collaboration, and improve clinical and operational insights.

Produced by HIMSS