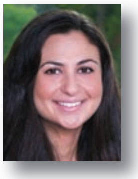
BY DESIREE KHOURY

Ransomware: 3 Strategies to Minimize the Threat

Another pandemic morning: you've got your new favorite mug—the one that says "You're on mute"—full of coffee, you're wearing your work-appropriate shirt and a pair of sweatpants, and you're all set for the first video call of the day. You type in your credentials and search your shared drive to find the right material for your meeting . . . but the folder isn't there. Other folders are missing, too; then they start disappearing in front of your eyes. Soon, all that remains on your screen is a terrifying graphic, the headline "<expletive> happens!" and now all your files are encrypted! There are some instructions about paying a ransom in Bitcoin.



***Desiree Khoury** is Vice President of Marketing and Business Development, Cyber & Professional Lines Group, Tokio Marine.*

Ransomware attacks have been on the rise for a few years, but when COVID-19 triggered a near-universal pivot to remote work, a whole new world of vulnerabilities opened to the criminals behind them: workers using home computers and connections, falling back on weak passwords, relying on widely available communication applications, and the general sense of panic.

While HIPAA may have relaxed rules and regulations to ease the transition and lower the burden on healthcare providers during the pandemic, that doesn't mean that criminals have dialed back their activities. In fact, healthcare entities may have become the most susceptible of all.[1] Why are healthcare organizations so vulnerable? Exactly what is ransomware? What are the strategies you can employ to maximize your security and minimize your susceptibility to this threat?

The ABCs of ransomware

Ransomware is a type of malicious software, otherwise known as malware, that denies legitimate users access to a computer system and/or computer data until ransom is paid to the perpetrators, according to the U.S. Cybersecurity and Infrastructure Security Agency.[2] In most ransomware attacks, an internal user mistakenly clicks on a link in a phishing email or visits an infected website, allowing the criminal hacker to hijack a computer system and/or computer data.

Across all industries worldwide, ransomware attacks increased by 40% to 199.7 million cases in the third quarter of 2020.[3]

The healthcare industry is particularly susceptible to ransomware attacks, which have increased as the pandemic has spread. There are clear reasons for these vulnerabilities:

- **Overall stress—**Healthcare providers work in a high-stress environment under normal circumstances. The pandemic has multiplied that stress, which creates vulnerabilities and errors cybercriminals seek to exploit.
- **Weak security and unprotected endpoints—**Bad actors look for targets with nonexistent or weak security measures and controls. The rapid

adoption of telemedicine/telehealth brought many more unprotected devices and connection points into the healthcare ecosystem: Cell phones, personal laptops, public Wi-Fi networks, even medical devices that rely on wireless connectivity can be a risk.[4]

- **High level of interconnectedness—** Networked applications that make possible just-in-time deliveries of needed supplies, service requests to partners, shared lab results, etc., also expose healthcare organizations to each other's technical and process weaknesses. A cybercriminal may enter and "hide" in one company's system for months in order to exploit connections to a partner organization with deeper pockets or a higher risk profile. Ransomware perpetrators seek to exploit what they can, knowing that each door they open leads to another.

U.S. healthcare providers warned

On October 28, 2020, the U.S. Cybersecurity and Infrastructure Security Agency issued a warning specifically to U.S. hospitals and healthcare providers about an "increased and credible cybercrime threat" using Trickbot, BazarLoader, and BazarBackdoor to infect victim networks.[5] "Trickbot provides its operators a full suite of tools to conduct a myriad of illegal cyber activities," the warning states, including "credential harvesting, mail exfiltration, cryptomining, point-of-sale data exfiltration, and the deployment of ransomware, such as Ryuk and Conti."

Trickbot is a "trojan" virus, meaning it typically goes undetected in your network, spreading quickly through emails with malicious attachments and disguised links. Ultimately, Trickbot triggers a ransomware variant called Ryuk, which, according to Tokio Marine HCC's Cyber & Professional Lines Group claims data, starts its ransom demands at seven figures. That doesn't include the cost of the associated downtime.

Based on Ryuk cases investigated in a variety of sectors including healthcare by Arete Incident Response, one of Tokio Marine's forensic vendors, the average duration of business downtime is estimated to be about 9.47 days, and the average ransom demand paid is $621,064.05 (USD).[6]

So, when your cyber insurance provider asks what steps you have taken to address a ransomware attack, they are not being alarmist. You wouldn't leave your car door open, your key in the ignition, and your wallet in the center console of your vehicle. Your network and data are worth a lot more to your practice than any one vehicle, aren't they?

3 proactive ransomware prevention strategies

Fortunately, there are several approaches that healthcare entities can implement to lessen

Improving the safety, quality, and cost-effectiveness of care across all settings
Patient Safety
Evidence-based Medicine
Technology Decision Support
ECRI
The Most Trusted Voice in Healthcare
ecri.org

exposure and minimize costly downtime in the event of a ransomware attack.

Strategy #1: Upgrade legacy antivirus software to what's called "next generation" virus protection, which uses artificial intelligence and pattern recognition to pinpoint vulnerabilities and recognize early indications of a threat before it takes hold. Such antivirus software is a much more effective approach than relying on updates to keep abreast of new virus definitions.

Strategy #2: Move to a multi-factor authentication sign-in process for end-point reinforcement. This method validates the identity of each user by two different methods—usually a password or phrase and a unique, one-time identifier sent to a second device such as a phone or fob—whenever data or confidential information is accessed.

Strategy #3: Contract with a vendor to provide business continuity and disaster recovery services. This means moving data storage to the cloud, where it can be safeguarded and retrieved in case of a breach.

Organizations that employ these countermeasures are much less likely to be attacked and, if attacked, are much less likely to experience irrecoverable losses. That's why these three approaches are essential weapons in the fight against ransomware. To protect entities against ransomware attacks, these should be as ubiquitous in every healthcare organization as the seat belts are in your car and the smoke detectors are in your home. CrowdStrike, Duo, and Datto are examples of vendors that offer these services at a variety of tiers, making them easier to access and employ.

A final word

Ransomware isn't going away any time soon and attending meetings from your kitchen table probably isn't either. Just as we've learned to mind our backgrounds and keep an eye on that little microphone icon, it's time for every healthcare provider to take action regarding their data vulnerabilities. MPL

References

1. Datto's Global State of the Channel Ransomware Report, Datto.com, Nov. 17, 2020, www.datto.com/blog/new-research-dattos-2020-global-state-of-the-channel-ransomware-report.
2. "Ransomware Guidance and Resources," U.S. Cybersecurity & Infrastructure Security Agency, https://www.cisa.gov/ransomware.
3. "40% Increase in Ransomware Attacks in Q3 2020," SecurityBoulevard.com, Nov. 16, 2020, https://security-boulevard.com/2020/11/40-increase-in-ransomware-attacks-in-q3-2020/.
4. "National Cybersecurity Awareness Month," U.S. Food & Drug Administration, October 2020, www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity#guidance.
5. "Alert: Ransomware Activity Targeting the Healthcare and Public Health Sector," U.S. Cybersecurity & Infrastructure Security Agency, Nov. 2, 2020, https://us-cert.cisa.gov/ncas/alerts/aa20-302a.
6. "US Government Alerts of Imminent Attacks Against the Healthcare Sector by Trickbot Group," November 2020, https://areteir.com/wp-content/uploads/2020/11/Arete_Insight_US-Government-Alerts-of-Imminent-Attacks-Against-the-Healthcare-Sector-by-Trickbot-Group_November2020-1.pdf.

For related information, see www.tmhcc.com.