EMERGENCY SECURITY CARE: HOSPITALS, HEALTH FACILITIES AND RANSOMWARE

Ransomware attacks are proliferating at an alarming rate. In the US healthcare sector, they increased by 71% during the month of October. On October 28th, the US FBI and two federal agencies announced an "increased and imminent cybercrime threat" and stated that attackers aimed for "data theft and disruption of healthcare services."[1,2]

Amidst the coronavirus pandemic, these threats are more somber and sobering than ever before. Says INTERPOL Secretary General Jürgen Stock, "Locking hospitals out of their critical systems will not only delay the swift medical response required during these unprecedented times, it could directly lead to deaths."[3]

Sharpen your cyber security awareness with these short-term strategies

Join An Intelligence Sharing Organization	Healthcare oriented cyber intelligence sharing organizations can expediently provide critical information. Organizations to join include the Health Information Sharing Analysis Center (H-ISAC), and the Information Sharing and Analysis Organization (ISAO).
Malicious Link Awareness	Inform your teams not to click on links. And it's not just email links that pose a threat. It's also links that are presented to users over Zoom and other seemingly trustworthy platforms.
Up-To-Date Systems	Simple but an easy slip: Ensure that your systems are up-to-date and that patches are installed where necessary.
Network Settings	Where feasible, update your network settings as to filter out active links and to remove attachments from emails.
Scan Backups	Malware can operate on a delayed-release model. Scan your backups to ensure that they are malware-free.

[1] Check Point Software, Hospitals Targeted in Rising Wave of Ryuk Ransomware Threats, 29 October, 2020
https://blog.checkpoint.com/2020/10/29/hospitals-targeted-in-rising-wave-of-ryuk-ransomware-attacks/

[2] FBI Warns Ransomware Assault Threatens US Health Care System, Associate Press, Frank Bajak, 29 October, 2020
https://apnews.com/article/fbi-ransomware-healthcare-system-7531ca8d2742d855cd374213d111821c

[3] Cybercriminals Targeting Critical Healthcare Institutions with Ransomware, Interpol, 4 April, 2020
https://www.interpol.int/en/News-and-Events/News/2020/Cybercriminals-targeting-critical-healthcare-institutions-with-ransomware

Fortify your cyber security strategy and infrastructure with these longer-term initiatives

Partner with CISA, the FBI and HHS	To communicate issues quickly and to coordinate responses, consider developing partnerships with key federal organizations that can assist in the event of a cyber attack.
Rapid Response	Train a team to rapidly respond to unsavory cyber scenarios. Get them ready to execute a plan at lightning speed.
Micro-Segmentation	Micro-segmentation can prevent malware from spreading. Don't leave room for hackers to maneuver.
Zero Trust	Policy management and identity access can stop a criminal from entering your network. In healthcare settings with multiple facilities, this can be complex and time-consuming. Yet, with cyber security vendor assistance it is often possible.
Application Whitelisting	Implementing application whitelisting ensures that only approved programs are able to operate on your network.
Multi-Factor Authentication	While hospital and healthcare systems often resist implementing multi-factor authentication due to the need for physicians and nurses to immediately access systems, review your healthcare environment to see where this might be feasible. Cyber security vendors can assist.
Penetration Testing	Invite your IT team to hack your own system. Or hire an external expert to test your system for you. This type of system evaluation will help ensure that your organization cannot easily be hacked.
Data Backup	Adhere to the 1-2-3 rule when it comes to data backups. Ensure that you have three copies of data that are stored on at least two different types of media, and ensure that one of those copies is not digital. Your backup systems need to be good enough to get everything going seamlessly. Make sure that you're able to easily port backup data to your systems and applications.
IT Lockdown Plan	If your IT system is disrupted, how will you quarantine the issue and quickly communicate it to others? Your rapid response team can take the lead, but be sure to have a wider strategy in place.
Ransomware Response Checklist	CISA and MS-ISAC have produced a checklist that can serve as an acceptable appendix to an incident response plan. Get the checklist here.
Continuity and Incident Response Plan	For when your systems are down, ensure that you have multiple printed copies of this plan. For further guidance on the latest healthcare focused incident response methodologies, visit the US Cyber Security and Infrastructure Security Agency's website, here.

Following these steps not only protects against ransomware, but can also reduce costs, result in improved data management and lead to a better allocation of resources both in and around a cyber breach.

Should you simply skip the planning and just pay the hackers?

Ransomware continues to exist because organizations willingly pay the fees. If you can avoid paying, you can help put hackers out of business.

In addition, paying ransomware fees does not guarantee the safe return of your data. In past incidents, hackers have collected the Bitcoin payments and then dumped data on the dark web or worse.

Says Check Point Software's ransomware expert Lotem Finkelsteen, "Many hospitals have the security mechanisms in place to detect ransomware as it begins to infiltrate systems. In these cases, it may be possible for organizations to remove the ransomware quickly and to rebuild affected systems." Paying ransomware fees isn't always worth consideration, especially if you have alternative options.

Why ransomware in healthcare, rather than other malware?

Although healthcare organizations are seeing many types of cyber attacks, ransomware is a criminal favorite because the money often comes in quickly. At the end of the day, cyber criminals aim to make a quick buck (or a few hundred thousand).

The buzz in the building

Across 2020, nearly 60 US healthcare organizations have seen ransomware attacks, and 510 buildings have been affected. In recent weeks, at least five US hospitals have suffered from ransomware attacks.[4]

A physician in one of the affected hospitals shared that her biggest fear is a preventable death that occurs due to lack of access to computers. "All of our computers are off and we are running entirely on paper charting, using fax machines to communicate between different parts of the hospital," the doctor said.[5]

The recent ransomware attack in Germany, in which one patient died, should serve as a wakeup call to hospital and health facility leaders. Taking immediate action on hospital and healthcare cyber security is imperative.

For a comprehensive guide to ransomware prevention in hospital and healthcare settings, visit the US Cyber Security and Incident Security Agency's website.

---

[4] Wave of Ransomware Attacks Hobble 5 US Hospitals as COVID-10 Cases Surge: FBI, New York Post, Associated Press, 29 October, 2020 https://nypost.com/2020/10/29/fbi-warns-of-imminent-ransomware-attacks-on-various-hospitals/

[5] Russia-Based Hackers Plan New Wave of Attacks Against U.S. Hospitals: Security Firm, Insurance Journal, 2 November, 2020 https://www.insurancejournal.com/news/national/2020/11/02/589183.htm