June 2021
TodaysMedicalDevelopments.com

TODAY'S MEDICAL DEVELOPMENTS

Your Source for the Design and Manufacture of Medical Devices and Equipment

Cybersecurity for Healthcare Systems, Medical Devices More Critical Than Ever

Rise in ransomware attacks forcing hospitals to harden cybersecurity

SHANE KEATING AND STEPHANIE VAN NESS
Integrated Computer Solutions

Cybercriminals have stepped up their game during the pandemic, launching ransomware attacks at an alarming pace. In 2020, more than 90 U.S. healthcare organizations reported **ransomware attacks**, which affected over 600 separate clinics, hospitals and organizations and 18 million-plus patient records.

© ICS | https://www.ics.com

Ransomware attacks typically happen when hackers gain access to secure systems and encrypt files using malware to lock out the rightful owner. Access can be obtained using something as simple as an innocent-looking link in an email or by leaving a password in the wrong place. The cybercriminals will demand money to decrypt the files and also to prevent publication of sensitive data.

Hospitals that lose access to their databases will find themselves in a bind. They might have to turn away patients needing care, or delay treatment. If hospitals lose access to lifesaving devices like ventilators and dialysis machines, particularly while in use, the consequences can be deadly.

Businesses without adequate disaster recovery and backup plans are effectively forced to pay the ransom.

The threat to the healthcare and public health sector is so great that in October 2020, the Federal Bureau of Investigation, the Cybersecurity and Infrastructure Security Agency, and the Department of Health and Human Services (HHS) jointly released an advisory describing the "tactics, techniques, and procedures" cybercriminals use against targets in this sector to infect systems with ransomware for financial gain.[1]

The FDA has taken notice also, appointing an acting director of cybersecurity to enhance supervision of approvals for medical devices – essential as modern medical devices running complex software can be used as entry points into hospital networks. As other ways to infiltrate systems close down, cybercriminals look for easier ways to gain access.

Hospitals are appealing targets

Though ransomware attacks have been a threat to businesses and government agencies for many years, prior to 2016 healthcare organizations were not considered primary targets.[2] But that has certainly changed. Attacks targeting healthcare systems escalated during the pandemic because hospitals in particular have become easy targets. One key reason relates to hospitals' rapid adoption of information technology. That would seem like a positive – better technology can improve care. But, most healthcare organizations have expanded their reliance on IT without also expanding their IT support staff.

(This expansion happened largely in response to Meaningful Use program incentives, which encouraged healthcare organizations to use EHR, or electronic health records. In 2008, EHR utilization was just 9.4%. By 2016 it was 96.9%.)[3]

What can healthcare organizations do to protect EHR Data and safeguard patients?

Train people

Focus on educating your entire workforce about the risks. Any email from an unknown source, promising financial windfalls or warning the user about negative consequences needs to trigger a warning signal for your employees. Never click on a link unless you can see where that link goes. Never download and run software from a link unless you know exactly what it does and where it came from. Many organizations use fake spam emails to test people's willingness to click on suspect links.

Limit access

Hospitals require many people and systems to operate, all of whom need some degree of access to its network. Still, you can ensure that everyone who needs to enter your network has a level of access that is appropriate. A very common tactic used by attackers is privilege escalation whereby they obtain access to one user's data and then figure out how to leverage this data to get access to a higher privilege level.

Update software

Not only must you update EHR system software, you also need to update and maintain the software controlling every MRI machine, insulin pump, cardiopulmonary bypass machine and all the other

medical devices used to treat patients. This can be difficult because not only must you regularly install updates and security patches, you first need to ensure that the updates are compatible with older equipment, or risk rendering those machines useless. More than half of rural hospitals fail to regularly patch their networks, leading to the influx in cyberattacks that are now specifically targeting them.

Older software such as Windows 7 may be difficult to remove entirely due to compatibility issues with legacy devices and systems. However, steps can be taken to isolate older systems and ensure that they cannot be used as entry points into the core network.[4]

Monitor assets

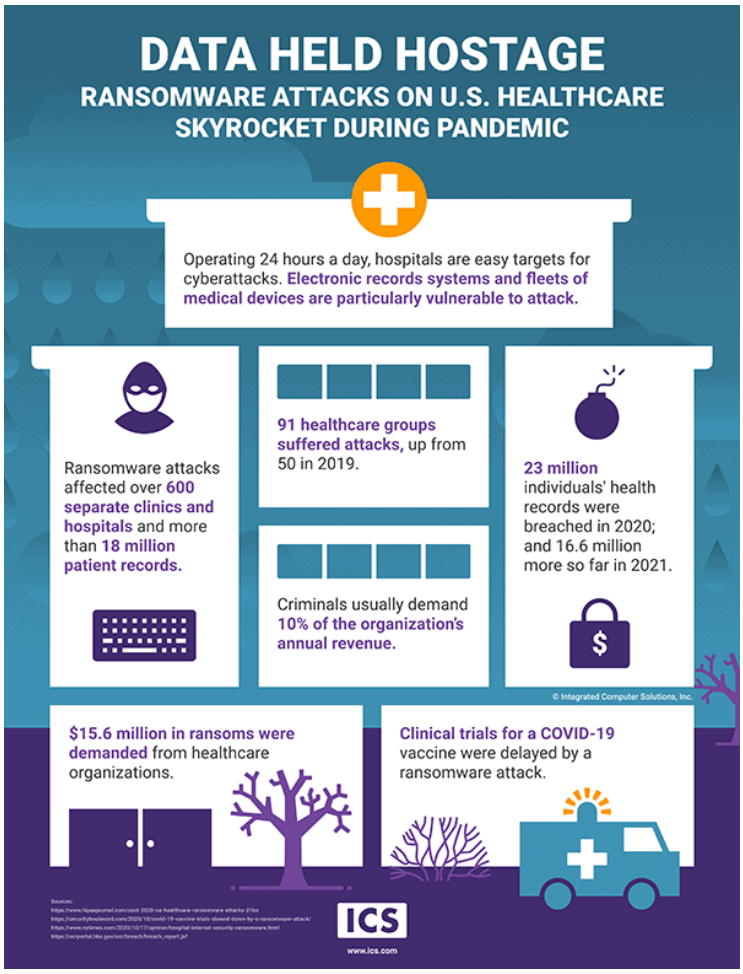
Unusual patterns in usage of your assets should trigger warnings. Many Intrusion Detection Systems (IDS) can provide early warning that general probing of your network could be turning into something more serious. By monitoring who is logging in and when, you may identify something unexpected. Most software-based medical devices will provide a means to understand what is going on with respect to security (e.g. a security log). Actually parsing this and looking for unusual activity can be the difference between catching an attack early and being too late to avoid very expensive remediation.

Update firewall

Firewalls may offer the illusion of protection, but older firewalls are easily hacked and allow hackers to penetrate – and ransom – your entire network. Firewall rules should be constantly updated to ensure that they are covering new threats. Firewalls should be monitored to understand who has access to your network and if there are any unusual patterns in traffic that is coming onto your network.

Back up data often

This is one of the most important things to do. According to the HHS, HIPAA compliance may help hospitals recover from ransomware attacks because HIPAA specifically mandates frequent data backups. If you're hit by a ransomware attack, a recent backup might be all the information you have access to for patient care.



© ICS | https://www.ics.com

Be aware, however, that malware may also infiltrate a backup, compromising and encrypting the backup's data. Consider having different levels of backup ongoing, either by simply storing more backups going further into the past or separating frequency of backup into two streams. One backup job can run on a less-frequent basis and the other can run at higher frequency, providing a way to get a snapshot of the system before infection without significantly adding to storage requirements.

Conduct risk assessment

Identify major risks, such as system outages or data theft, and evaluate how staff can impact those risks. An ongoing plan for minimizing risk is an essential tool in your armory. The field of cybersecurity is continually evolving with new threats being identified all the time. Membership of an ISAO as recommended by the FDA will help you to be aware of developments. Entry points in recent major attacks should be known and understood – even if older unpatched systems are involved (as they often are) - maybe you can isolate/firewall these systems and understand how they can be used as an entry point that could compromise the whole of your network.

It is necessary to explore the level of staff awareness of the measures the institution has implemented to safeguard sensitive records. Hospital staffers work at a frenetic pace and are typically focused on minute-by-minute needs – productivity over long-term planning. If staffers don't truly understand the risks on both a macro and micro level, they will not understand what specific precautions are necessary to keep cybercriminals out of your network – and what role each individual must play.

Audit equipment

Hospitals should regularly audit their medical devices and other machines and segment their networks. This way, the entire network is not compromised if one piece of the network is infected.

Strengthening porous cybersecurity should top your to-do list

The pandemic has accelerated the widespread adoption of telemedicine. Even though society is regaining a sense of normalcy and people are fast returning to in-person activities, remote and online medicine is here to stay. That means, hospitals are more vulnerable than ever to cyberattacks.

To survive, all healthcare systems are urged to immediately (and continuously) address their cyber shortcomings and bolster protections to prevent their services from being interrupted by malware and protect sensitive patient data from being stolen. As the Institute for Security and Technology reminds us, "A cybercriminal only has to be lucky once, while a defender has to be lucky every minute of every day."

About the Authors:

*Shane Keating is cybersecurity engineering and project manager at **Integrated Computer Solutions** (ICS), especially focused on medical device projects. Prior to joining ICS, Shane worked on receiver authentication of GNSS signals for the European Space Agency, and cryptographic acceleration technologies for Intel's Data Center Group in Ireland.*

*Stephanie Van Ness is associate director of marketing at ICS and **Boston UX**. She writes about user experience (UX) design and innovations in technology, from gesture-controlled medical devices to self-driving vehicles.*

Sources:

[1] https://perspectives.ahima.org/ransomwareinhealthcarefacilities/

[2,3] https://www.nytimes.com/2020/10/17/opinion/hospital-internet-security-ransomware.html

[4] https://us-cert.cisa.gov/ncas/alerts/aa20-302a