WHY HEALTHCARE AND SENIOR HOUSING PROVIDERS ARE VULNERABLE AND STEPS FOR PROTECTING YOUR ORGANIZATION

Ransomware has become big business for cybercriminals and a top global threat to individuals and organizations. The healthcare industry has been hit especially hard with a growing number of high-profile attacks that have shut down hospitals or seriously disrupted operations and patient care.
WHY HEALTHCARE ORGANIZATIONS ARE VULNERABLE

While every industry is at risk, hospitals, senior housing and other healthcare organizations have become highly attractive targets. In fact, they’re predicted to be the number one target for cyberattacks in 2017.¹

Healthcare organizations should be aware of what puts them at risk and take steps to protect their sensitive data and assets. Some of the leading reasons for their vulnerability are:

• Healthcare organizations tend to be slower at updating certain information technology (IT) systems with the latest security patches, in part because of the disruption updates bring to patient-related equipment and databases and the complexity of systems.²

• Digitizing health records increases the cost and complexity of IT systems. Supporting and protecting electronic health records along with existing systems is a challenge, especially in smaller organizations.³

3 out of 4 hospitals don’t have a designated security person.

• There is a lack of qualified security professionals on staff to improve cybersecurity defenses. In fact, three out of four hospitals don’t have a designated security person.⁴

• Many healthcare organizations prioritize compliance over security. But HIPAA (Health Insurance Portability and Accountability Act) and HITECH (Health Information Technology for Economic and Clinical Health) regulations only provide a framework for protecting patient data and systems, while cybercriminals are developing new methods daily.

• Healthcare data is highly valuable on the black market. Patient records contain names, addresses, social security numbers, insurance payment information and medical histories that cybercriminals can use for medical and tax fraud.⁵

In addition to the downtime and security costs associated with responding to a cyberattack, there are significant financial repercussions. Healthcare organizations may face fines, legal bills and other penalties for exposing customer information or violating HIPAA regulations.

Most healthcare organizations spend less than 6% of their overall IT budget on cybersecurity.⁶ Yet, they are predicted to be the number 1 target for cyberattacks in 2017.
RANSOMWARE—EARLY ROOTS IN HEALTHCARE

The first instance of ransomware occurred more than two decades ago. It was distributed on a floppy disk to AIDS researchers who thought it was a survey exploring patients’ risk of contracting AIDS. That was in 1989, and ransomware has been evolving ever since. It is now the fastest-growing type of malware.

Ransomware accounts for 72% of all malware incidents in healthcare.

Recently, a virulent strain of ransomware called WannaCry infected hundreds of thousands of computers worldwide as part of a large-scale global attack. Within a matter of hours, parts of the United Kingdom’s National Health Service were shut down, impairing patient services across more than a dozen hospitals.

While most of the impacted organizations were outside of the United States, WannaCry showed how easily ransomware can spread, infecting computers through a vulnerability in Microsoft Windows. Hospitals that didn’t update their systems with the latest Microsoft security patch were left open to attack.

WannaCry was perhaps the largest global attack of its kind, but other types of ransomware are spreading across the country and disrupting hospital systems and services. A healthcare facility in New York recently shut down its computer network due to an attack. The hospital reverted to paper-based charts while staff worked to restore systems—a process that took weeks.

PROTECTING YOUR ORGANIZATION

Staying ahead of the next threat can feel like a cat and mouse game, but there are steps you can take to avoid or minimize the impact of an attack. Below is a brief checklist for you to consider when reviewing the security of your IT environment.

- Practice good cyber hygiene, such as updating computers with the latest security patches, maintaining strong passwords, and using antivirus/anti-spam software.
- Put a comprehensive backup and recovery plan in place. The healthcare facility mentioned earlier had access to backup tapes to restore hospital files and chose not to pay the ransom.
- Educate staff on security best practices and regularly communicate the latest tactics cybercriminals are using to lure people into downloading ransomware.
- Limit access to the internet and, where possible, isolate machines like medical equipment or computers used for communicating with banking partners.
- Consider cybersecurity and privacy as well as crime insurance policies as part of your risk management strategy. Each of these is designed to insure you against specific threats and, collectively, their coverage can be customized to your needs.

What is ransomware?

- Malicious software (also known as malware) that encrypts files, so they can no longer be accessed. Users are instructed to pay a ransom, usually in the form of a cryptocurrency called bitcoin, to recover their files or risk losing them entirely.

How does it spread?

- Social engineering tactics, including phishing emails that entice users to click on malicious links or attachments.
- Websites or ads (malvertising) that appear to be legitimate but contain malware.
- Outdated systems or computers that don’t have the latest security patches installed.

Should you pay the ransom?

- While it is an individual decision, many experts advise not paying the ransom, as there is no guarantee you will get your files back. It could also make you a target for future attacks.

What is ransomware?

- Malicious software (also known as malware) that encrypts files, so they can no longer be accessed. Users are instructed to pay a ransom, usually in the form of a cryptocurrency called bitcoin, to recover their files or risk losing them entirely.

How does it spread?

- Social engineering tactics, including phishing emails that entice users to click on malicious links or attachments.
- Websites or ads (malvertising) that appear to be legitimate but contain malware.
- Outdated systems or computers that don’t have the latest security patches installed.

Should you pay the ransom?

- While it is an individual decision, many experts advise not paying the ransom, as there is no guarantee you will get your files back. It could also make you a target for future attacks.
YOUR PARTNER IN MANAGING RISK

For more information on ransomware preventive measures, download the US-CERT ransomware overview.

M&T Bank has over 30 years of experience delivering innovative lending and banking solutions to healthcare organizations. With a $6 billion healthcare portfolio and a dedicated Healthcare Specialty lending group that supports more than 400 Commercial Bank healthcare clients across 21 states, our professionals have deep industry expertise that can help you grow your business, while meeting today’s increasingly complex regulatory environment.

M&T Insurance Agency, Inc. (MTIA) can provide comprehensive cyber security and privacy as well as crime insurance policies to help you effectively manage risk and protect your assets in the event of a cyber event.

Find out how we can work together to help keep your organization financially healthy and secure. Call Christopher Callaghan at 410-244-4041.

You can also send us an email, contact your M&T Bank Relationship Manager, or visit your local M&T Bank branch.

Insurance products are offered by M&T Insurance Agency, Inc., not by M&T Bank. Insurance Products offered are: Not FDIC insured • Not a deposit in, obligation of, nor insured by any federal government agency • Not guaranteed or underwritten by the bank • Not a condition to the provisions or terms of any banking service or activity.


All products and services are subject to eligibility and restrictions may apply.
All trademarks, service marks and trade names referenced in this material are the property of their respective owners.
Unless otherwise specified, all advertised offers and terms and conditions of accounts and services are subject to change at any time without notice. After an account is opened or service begins, it is subject to its features, conditions, and terms, which are subject to change at any time in accordance with applicable laws and agreements. Please contact an M&T representative for full details.