Held Hostage: The Invasion of Ransomware Hits Medical Practices

by SVMIC Information Services Department

It's a modern-day twist on an age old crime - holding hostage something of value until a ransom is paid. Cunning cybercriminals have developed a low cost, highly effective method of extortion. And beyond the cost of the ransom payment itself, it is a scheme which puts critical health information assets at risk, potentially brings healthcare delivery and supporting operations to a grinding halt, and creates new liability issues for your organization.

The FBI reports that victims paid about $24M in ransom payments in 2015, and those numbers are expected to increase in 2016. While no industry or sector is immune from these targeted attacks, the sensitivity of protected health information (PHI) and healthcare services' dependence upon electronic access to that data create an attractive, profitable target for the cyber sleuth. This is evidenced by the numerous recent news stories relating to ransomware attacks upon healthcare centers across the United States and Canada. Adding to its appeal as the current crime-of-choice by cybercriminals, ransomware is easily distributed and virtually impossible to trace to its origin.

Ransomware works by electronically "taking hostage" of its victim's critical systems and data, such as the medical practice's EHR or billing solution. The perpetrator uses a combination of alluring social tactics and malicious software to gain network access and compromise computer systems. The most common method of entry is through well-crafted phishing e-mails, which often appear to come from someone the recipient knows, such as a commonly utilized online retailer, a business partner, or a coworker. The phishing email message typically creates a sense of urgency and threatens a negative outcome if the recipient doesn't take action. Some variations include attachments, such as fictitious invoices mandating payment to avoid legal ramifications, while other communications include enticing links to a seemingly valid and reputable website offering a relevant service or useful information. As the unsuspecting victim opens the attached document or navigates to the link, embedded, malicious code is immediately executed. The victim's systems and servers are now compromised and encrypted, rendering them inaccessible by their owner and users. The cybercriminal follows with an online demand for payment by Bitcoin, an untraceable digital currency used on the Internet. Once the ransom is paid, a decryption key is released to the victim.

Delivering a ransom payment seems appalling; however, some organizations have determined that making such a payment is the most efficient way of resuming delivery of critical care to their patients and other routine business operations. Others refuse to pay ransoms and, instead, restore the systems from backups - a process which can take several days and cause significant disruption of operations.

Fortunately, as an SVMIC-insured, your policy includes limited Cyber Security Insurance coverage to assist in recovering some of the expenses related to such a cyber-attack. That said, we realize any event which causes a significant disruption in patient care has the potential to generate costs well beyond a monetary ransom payment or technical systems recovery costs. The commonly held truth of sound healthcare that says "an ounce of prevention is worth a pound of cure" is also appropriate to your organization's data security practices. There are some common steps all medical practices can take to avoid becoming the next victim of a cybercrime.

Remember, we identified two areas of weakness cybercriminals typically exploit: social and technical. To effectively address and prevent the threat of a security breach of any type, you need to implement both technologic and human safeguards. To that end, we recommend taking proactive steps in protecting your practice's information systems.

Ensure that IT staff or service providers address these areas:

1. Implement routine, scheduled software patches which incorporate latest security-related updates and reduce vulnerabilities to ransomware and other security attacks.
2. Deploy proper implementation of preventive software controls on laptops, desktop computers, and network servers.
3. Install adequate firewalls, and utilize intrusion detection and event-monitoring solutions.
4. Install and maintain antispam and antivirus software on email servers.
5. Deploy web filtering products, to block suspicious web traffic and known, compromised websites.
6. Conduct internal or outsourced phishing tests to evaluate effectiveness and identify gaps relating to employee security awareness and training needs.
7. Maintain appropriate backups, protected from unauthorized access and online attacks.
8. Review and test backup and recovery procedures on a routine and scheduled basis.

Identify and assign appropriate staff to:

1. Develop and lead ongoing training and security awareness programs for all employees, including appropriate Internet use (including, but not limited to, social media portals); recognition of phishing emails; and employee responsibilities in maintaining a cyber-secure workplace. Instruct employees to be wary of links and attachments, particularly Word and Excel documents, which can execute malicious macros upon opening.
2. Maintain a safe environment where employees can openly report potential security incidents or concerns. Consider establishing a hotline or other protocols for reporting suspected malware, ransomware infections, and other suspicious online activity.
3. Develop incident response procedures and protocols that guide IT staff and management teams in the event of a security breach.
4. Periodically evaluate backup schedules and content. Review disaster recovery test results.
5. Review cyber insurance coverage and evaluate policy limits as they relate to your particular practice's needs and objectives.
6. Develop and periodically review your practice's business continuity and disaster recovery procedures to ensure adequacy of operations recovery in the event of a system breach or other potential disaster scenarios.

If your "ounce of prevention" is ultimately unable to prevent a ransomware attack, you may be left with two choices: pay the ransom or restore from backup. If you decide to pay the ransom, don't assume your troubles are over. The malicious code is still lurking within your systems and must be removed; otherwise, cyber criminals can return to wreak further havoc and make additional demands.

Should your practice experience a cyber-related security event, it is prudent to contact SVMIC as soon as practicable to determine if professional assistance is available through your Cyber Security Insurance. Please be aware also, as stated in your Policy, that coverage applies to ransomware payments only when pre-approved by the insurance company.

SVMIC Sentinel May 2016
To subscribe: www.svmic.com