Ransomware: The New Reality of Cybercrime

White Paper

Coker GROUP
Business Advisors for the Healthcare Industry

TERRY J. WILK, MBA, FCHIME, CJMC
Senior Vice President

KYLE CHANG
Senior Manager/Chief Technology Officer

April 2016

CONTACT
For further information about Coker Group and how we could be of assistance, call 800-345-5829 x2021.

TABLE OF CONTENTS

Cybercrime, a form of online *terrorism,* is now threatening the very safety and well-being of our nation's healthcare system. No hospital, physician, or other healthcare provider is immune to the operational chaos, harrowing events, and potential financial ruin that can result from sudden cybercrime attacks. Safety nets and other safeguards are available to minimize these risks, but many providers do not know how vulnerable their IT systems and networks are until it is too late.

This paper defines today's most devastating form of cybercrime – ransomware – and outlines concrete methods for mitigating this risk. Providers must take prudent steps to identify and address their IT security weaknesses to protect more thoroughly their invaluable data and financial assets from ransomware and other dangerous exposures now and in the future. Their very futures depends on it.

KEY WORDS: **Ransomware; Digital Mugging; Trojan Horse; CryptoLocker; Bitcoin; Tox; Zero Day Viruses or Zero Day Malware; Cerber; Nuclear Exploit Kit; Security Hygiene; Patches; Whitelist; Permissions; Holes**

INTRODUCTION

Cybercrime is terrorizing healthcare in a big way. Almost daily, we read about new security breaches in small, medium, and large healthcare organizations (i.e., providers) that often affect hundreds, thousands, or even millions of people and their private health and other personal information.

Cybercrime is an intentional attack against a provider's proprietary data assets. It describes any illegal activity in which a computer is used as a means to commit a crime against another individual's or provider's computer, network, or database. Cybercriminals are incredibly intelligent people who try to break into an IT infrastructure to snoop around; to inject electronic viruses and other malware; to expose, steal, or destroy data; and now to hold data and systems hostage for payment. This latter event is referred to today as *ransomware*. Ransomware is a form of *digital mugging* that has extreme ramifications for the healthcare industry.

This paper explores the emerging threat of ransomware and outlines what providers can do to prevent ransomware and other forms of malware from occurring in their organizations.

THE EMERGING BUSINESS OF RANSOMWARE

Unfortunately, ransomware attacks are no longer random events. Cybercriminals are becoming more organized, and they are establishing professional businesses as they try to

make money on this type of cyberattack. They now are attacking healthcare on an increasing basis. Once these criminals exploit a security vulnerability and encrypt data, they begin the ransom process, which is almost impossible to stop. Some of these cybercriminal organizations are now publishing "frequently-asked questions" and "payment instructions" during a ransomware attack.

A Peak Under the Hood of Ransomware

Using the age old method of extortion and hostage tactics, married with the latest in deceptive electronic information, ransomware authors have attacked major global institutions to extort money by secretly installing a *Trojan Horse* (i.e., a malicious computer program) to encrypt user files on individual PCs or servers. Many of these PCs were compromised because they were not protected from these threats and through user naiveté through social engineering tactics used against them to gain unauthorized access to their systems and data files. (Note: Social engineering is a type of psychological manipulation of people to have them take actions or devulge confidential information, such as login IDs and passwords.) Once they gain access, cybercriminals find and take advantage of software vulnerabilities within an operating system or a software application.

On July 5, 1993, a cartoonist by the name of Peter Steiner created a cartoon featuring two dogs that published in the *New Yorker* magazine. One dog sat in front of a PC with a monitor while the other sat on the floor looking at the dog sitting in front of the PC. The caption of the cartoon read, "On the Internet, nobody knows you're a dog." The cartoon was not only funny and exaggerated the possibilities of the Internet, but it also made a very poignant statement that any individual around the world that has access to the Internet could purport to be anyone. In 1993, the Internet became more prolific, and accessibility was no longer limited to military, academia, or large conglomerates. As a new, unchecked, powerful communications medium, the Internet became subject to illegal activity. Fast forward to 2016. While there have been significant strides in IT security technologies, such as firewalls, anti-virus, anti-malware, anti-adware, anti-root kit, web-filtering, spam filtering, etc., there has not been significant progress in educating computer users on the dangers of security breaches and, now, ransomware.

One recent ransomware threat that received media attention is *CryptoLocker.* This new variant surfaced within the last two to three years and encrypts (makes unreadable) company files using private security keys that only a hacker has. The hacker uses these keys to unlock data files after a ransom is paid. The ransom is paid in *Bitcoin*, which is an untraceable digital currency that has real value.

Hollywood Presbyterian Hospital in California regained access to their files after paying a $17,000 ransom. The incident encrypted all of Hollywood Presbyterian's computer systems, including lab work, pharmaceutical orders, and even emergency room files. Although the $17,000 may not seem significant, Symantec, a pioneer in anti-virus technologies, recently reported that the dollar amount of ransomware payouts topped $5 million per year.

Ransomware attacks are not random. Cybercriminals do their homework and usually take their time targeting vulnerable individuals and organizations. These people know quite well that most providers have significant weaknesses in their IT infrastructures and that they are not prepared for cyberattacks.

Another reality is that, as technology has evolved over the last decade, cybercriminals have had ample opportunity to learn how to compromise the technology. It's a form of Murphy's Law: while smart people develop technology to help humanity, other smart people find ways to exploit this same technology for personal gain. Technology has become faster and easier to build. For example, look at how rapidly smartphones have developed over the last ten years, the most recent five years, and then over the last six months. Comparatively, the tools of the cybercriminal have been developing at an exponential rate, as well, because they have for the most part been left unchecked. These "digital crime lords" can develop commercial-grade software programs that are smart enough to infiltrate the most advanced firewalls and anti-virus systems and, then, develop a customer service desk to receive payment.

Most recently, *Tox* has surfaced and is now readily available on the Internet. Tox is a ransomware development kit available to those individuals who want to enter the ransomware business. Tox was discovered by Intel Security labs, and it is a ransomware service that not only includes software to develop a ransomware Trojan Horse, but also a ransomware Bitcoin collection service. Tox also offers a secured site to host malware operations like ransomware for a nominal fee of 20% of all collected Bitcoin. This action is a cyber shakedown by very well-organized digital mafia without a face. We do not know how to identify "which dog has their paw on the pulse of cybercrime!"

Ransomware Takes Advantage of the Human Need for Instant Gratification

Cybercriminals know that, by nature, most people are lazy, they don't pay attention, and they want things now. For example, about 90% of the time, CryptoLocker was introduced into organizations by way of an email attachment. People assume that if they receive an attachment in an email from someone they know, that everything must be okay. Also, many people continue to use email as a way to transfer data files when it was built to be only a

messaging system. Cybercriminals take advantage of the inherent security weaknesses of email.

For example, consider this typical scenario: someone is working on a project with several co-workers, and a document needs to be created and edited by team members. One person starts the document, sends it to the other team members, and the game of document ping pong begins. Perhaps one of these individuals is working on their home computer that may be infected with an undetected virus. The virus then attaches itself to the document that the team is sharing and delivers the CryptoLocker payload, which launches a ransomware attack (email attachment Trojan Horse). Another example might be that because an individual is a common recipient of infected PCs emails, this person is sent another email attachment from a coworker. Because he recognizes the coworker, he assumes that this is a legitimate email, opens the attachment, and infects his computer.

At this point, one may ask, "Where does my anti-virus software or anti-malware software come into play?" "Where is the protection that my vendor or CIO promised?" Unfortunately, thanks to new ransomware development kits like Tox, cybercriminals use what is known is *Zero Day Viruses* or *Zero Day Malware* to deliver the CryptoLocker or ransomware payload. These toxic viruses are previously unknown viruses that take advantage of both known and unknown software weaknesses. Applying updates to Windows, Adobe, Java, Internet Explorer, Google Chrome, and other anti-virus and security software can help, but, unfortunately, software manufacturers may not yet have a cure for these new viruses that can infect a PC and deliver the CryptoLocker or ransomware payload. Once the PC is infected, data files stored on both the PC and its mapped network drives are encrypted with secret keys and can be held for ransom.

Another new form of ransomware is called *Cerber***.** Cerber was built using a ransomware development kit called the *Nuclear Exploit Kit*. Cerber is the latest in the line of designer ransomware CryptoLocker variants and was discovered in March 2016. Besides encrypting local and mapped drives on a PC, Cerber scans, finds, and encrypts other shared folders accessible on that PC. Cerber is so sophisticated that it can encrypt over 10,000 files in under a minute. As an added level of eeriness, Cerber activates the text-to-speech feature on a Windows PC and tells the victim to pay the ransom as follows: "Congratulations, the shared files on your company's PC is now encrypted." The synthesizer voice then tries to extort money from the individual or the company.

The forgoing email attachment scenario is one of the most common ways that malware invades an IT infrastructure. There also have been many instances where computer infections occur via USB flash drives or users visiting websites and downloading viruses.

As a final note, tools such as Google Works (GW) and Microsoft Office 365 (MSO365) help teams collaborate on the web. Whether teams are crafting a document or reviewing numbers on a spreadsheet, both GW and MSO365 can provide a more secure environment to share documents and work together. Using such tools eliminates the need to attach and exchange documents via email while tracking changes and maintaining a document revision history. While using a web collaboration tool like GW or MSO365 cannot guarantee 100% protection from malware, viruses or Ransomware attacks, using one tool like this will help lower the risk of attack. The focus in not just about preventing email attachments or applying antivirus and Windows® updates. Rather, it is about doing everything one can to protect themselves and prevent cyberattacks from occurring. This action is akin to real *security hygiene*.

Preventive Measures

As previously noted, there is no 100% guaranteed way to avoid a ransomware attack from ever occurring. However, there are specific security hygiene measures that providers can take to reduce the risk of such an event from occurring.

1. **Treat Data as an Asset.** First and foremost, providers must recognize and treat data as a valuable asset, just as they treat their finances, buildings, and people. Astute providers take extra care to protect their assets (including data) because they would not be in business without them.
2. **Data Back-Up and Recovery.** Develop plans and practices regarding backing up and recovering data. Many providers are now conducting and testing their data backups multiple times throughout a work day and storing these backups off-line in a secure location. They want to limit the impact of data or system loss while ensuring an expedited data recovery process.
3. **Anti-Virus and Malware Software.** Ensure that all anti-virus and other malware detection software is kept up-to-date. This specialized monitoring and repair software should be running continuously in the background to scan all software, data, and document downloads from the Internet.
4. **Software *Patches*.** Update all computer operating systems, utilities, and application software with the latest patches (e.g., fixes, releases, etc.). Doing so can substantially reduce the exploitable points of entry by a cybercriminal.
5. **Application *Whitelist*.** Publish a list of approved applications (a whitelist) to help prevent unapproved software and programs from running in an IT environment. Enforcing this whitelist will permit only specified programs to run while blocking all other programs, including malicious and unknown software.

6. **Enforce *Permissions*.** Create permissions (i.e., authority levels) to restrict a user's ability to install and run unapproved and unwanted software applications.
7. **Email Attachments and Web Links**. Carefully scan all attachments and flash drives before opening them (see #3, above). Disable the ability to run macros from an email attachment and do not open unsolicited Web Links in emails.
8. **Medical Devices**. Don't forget to include software-enabled and network-connected medical devices such as infusion pumps in cybersecurity planning. Hackers have been known to access and control these devices and change dosing levels with no warning.
9. **Supplier Contracts**. Carefully review each supplier contract to ensure that these suppliers are legally responsible for protecting your data and for understanding how to accomplish this.
10. **Education and Training.** Educate and train each employee that data is an asset and that they must be aware of the data that they need to protect, including personally identifiable information (PII), protected health information (PHI), and how to avoid cyberattacks including phishing and social engineering.

CYBER INSURANCE CONSIDERATIONS

With healthcare cybercrime and ransomware attacks on the rise, providers should evaluate obtaining cyber insurance as part of safeguarding against the potential fallout from these assaults. Following are some of the important factors to consider regarding cyber insurance.

1. **Cyber Insurance Options.** As with most insurance, there are many options based on the types of incidents and costs for which Providers seek coverage. Covered events can range from external and internal breaches, data loss, and ransomware payments. Two main costs to consider include first-party costs (the provider's cost) and third-party costs (other's costs that they may try to claim) as a result of the incident.
2. **First- and Third-Party Coverage Features.** First-party coverage features include theft and fraud, forensic investigation, business interruption, extortion, and data loss and restoration. Third-party coverage features include privacy liability, regulatory actions, notification costs, crisis management, call centers, credit/identity monitoring and transmission of viruses and/or malicious code. Each cyber insurance policy will likely be different, and not all policies will have the same first- and third-party characteristics.
3. **Additional Policy Provisions.** Following is a list of other provisions that Providers must carefully consider when evaluating cyber insurance (listed in alphabetical order):

- **Acts and omissions of third parties.** Some cyber insurance policies exclude third parties from coverage. Consequently, the policyholder may not be covered if a third-party vendor it uses to store data suffers a breach.
- **Choice of counsel.** Defense costs may only be covered if the insured selects counsel from a list of law firms specified by the insurer.
- **Coverage for corporations.** A policy may define covered persons but not the corporations or business entities that would be affected by the breach.
- **Coverage for unencrypted devices.** A policy may exclude coverage for devices that are not encrypted by an approved encryption algorithm.
- **Defense trigger.** A policy may require that a lawsuit of written demand be filed as a trigger to activate the insurance provider's defense obligation.
- **Exclusions for acts of terrorism or war.** A policy may provide no coverage if a breach is caused by an act of terrorism or war.
- **Exclusions for omissions.** A policy may limit or exclude coverage for events stemming from security deficiencies including failure to maintain and update security software and features.
- **Location of security failure.** A policy may only cover security incidents such as theft or loss that occur on the policy holder's premises. For example, a device stolen from an employee's home may not be covered.
- **Loss or claim trigger.** A policy may be restrictive in defining what types of events trigger a covered incident.
- **Policy territory.** A policy may limit coverage of loss or theft to just the United States and its territories. Therefore, an employee who loses a device traveling abroad may not be covered.
- **Retroactive coverage.** Most policies specify a retroactive date whereby any losses occurring due to events before that date are not covered.

4. **Cyber Insurance Costs**. Costs will vary by the provider's coverage needs, past and current risks, annual gross revenue, and current security policies and practices. For example, before awarding coverage, providers often will be required to produce various documents and demonstrate compliance in an area including security and risk management plans and techniques, disaster response plans, data access controls, anti-virus and other malware software installed, and frequency of updating security software, firewalls, etc.

CONCLUSIONS

All indications show that ransomware and other cyberattacks are on the increase. Cyber threats are constantly evolving and are becoming more intense and complex. These attacks will disrupt a provider's ability to deliver safe, reliable, and high-quality healthcare services

while causing significant financial ramifications. The healthcare industry will only become more reliant on information technology and the Internet, which, in turn, will increase its vulnerability to cyber risks.

Many providers have invested millions of dollars building massive computing capability, databases, and wired and wireless networks to connect people together to capture and share information. Their goal is to facilitate communication, improve workflows, improve quality, lower costs, satisfy customers, and make a reasonable profit to sustain services. But how much attention have these providers *really* given to protecting these investments from today's and tomorrow's cybercriminals? Apparently, not enough as evidenced by the growing incidents of cybercrime in healthcare, including recent ransomware payment demands. Additionally, we will see an increase in the number government security audits, and five- to seven-figure penalty settlements for security breaches.

Therefore, all providers must ask and answer several fundamental questions about cyber risks including the following:

1. How secure is our IT infrastructure?
2. What known and unknown *holes* (or weaknesses) do we have in this infrastructure?
3. What steps have we taken or should we take to protect our organization?
4. Have we developed, communicated, and executed a formal and proactive IT security plan to prevent, detect, and respond to cybercrime activities and enforce accountability throughout the organization?
5. Who will implement this plan?
6. How informed are we about the current level and business impact of cyber risks to our organization?
7. How does our cyber security program apply industry standards and best practices?
8. How many and what types of cyber incidents do we detect in a typical week?
9. What is the threshold for notifying executive and board leadership of these incidents?
10. How comprehensive is our cyber incident response plan? How often is it tested?
11. Do we have an adequate amount of cyber insurance?

In summary, all providers, regardless of size, must pay attention to the growing issue of cybercrime in general and ransomware, in particular. They must act proactively to understand their risks and take appropriate action to mitigate these risks.