QIX & HTAA Presents

RANSOMWARE

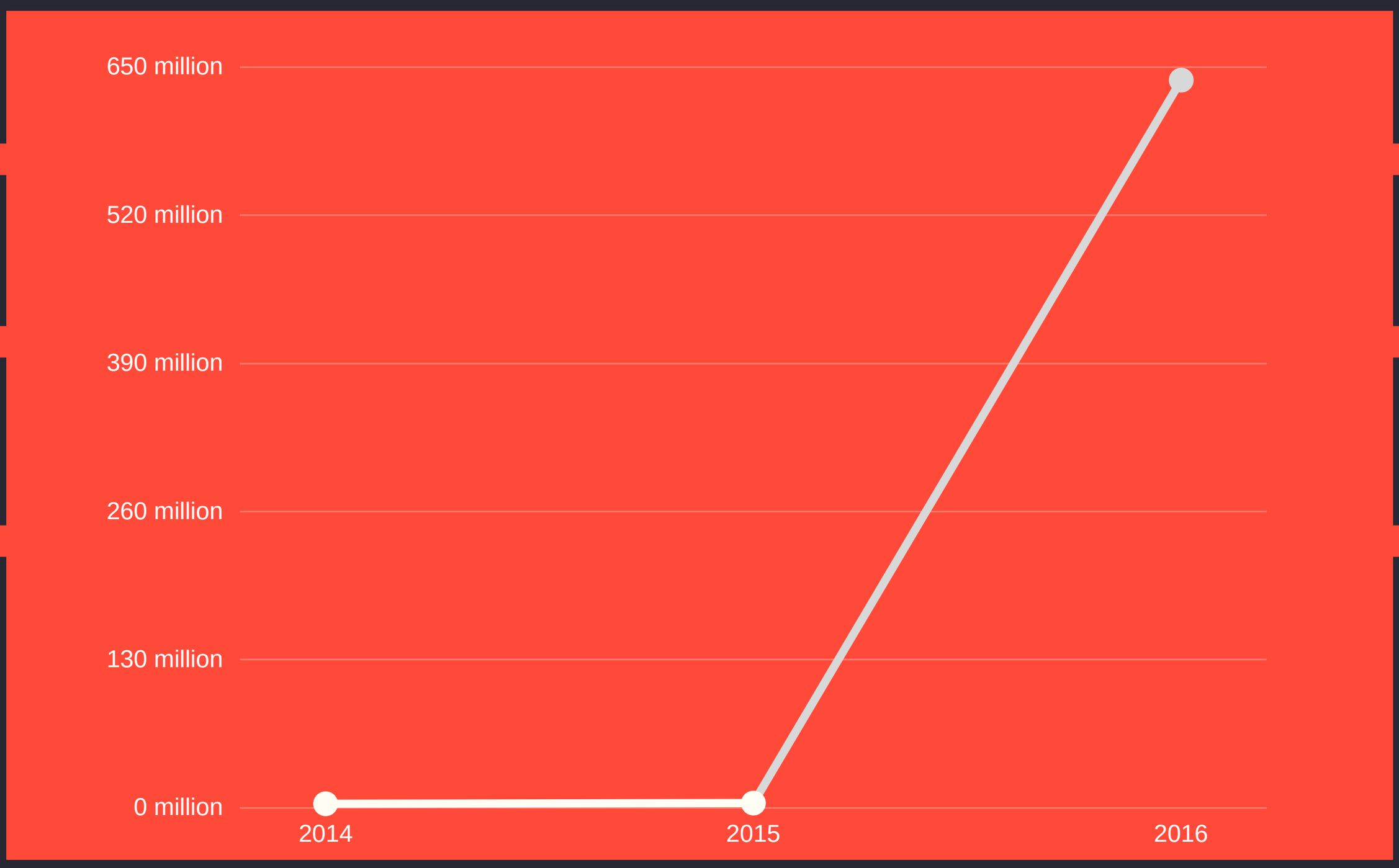
Everything you need to know about one of the most common and dangerous cyber threat for healthcare organizations.

SUMMARY

The threat from “ransomware” to healthcare institutions has grown over the past few years to the point where the news media and public are taking notice. All indications are that this trend will continue. The reasons for this are many, including,

- Growing involvement of Organized Crime in
- Cyberattacks;
- Increasing sophistication and availability of attack
- software packages;
- Botnets used for Spam and Denial of Service attacks;
- Relatively low ransom demands;
- Increasing availability of untraceable cyber-currency
- payments;
- International barriers to prosecution; and,
- Slow implementation of security in healthcare.

Growth in Ransomware Attacks



The first three of these are benefits to criminals and are driven by income. Opportunities for making illegal money cannot be expected to go unrealized unless there is significant fear of prosecution. The next three are risk factors for the criminal. Unfortunately, low ransom demands across thousands of victims and international barriers make prosecution the exception, not the rule. And except for the last one, these are all factors that are out of the hands of the industry or its professionals. The healthcare industry is an obvious target due to its acute reliance on patient data and its immaturity in cybersecurity. Together, they represent a perfect storm for creating a cybercrime threat to the entire healthcare system.

In this eBook, we explain the nature of ransomware and identify key factors that can minimize the risk that a ransomware attack will be successful in healthcare organizations.

Ransomware poses one more threat to securing PHI and the solution to it is similar what is needed to prevent many other threats that are faced by our industry. As in all risk management, implementing an industry standard security and controls framework, like NIST Computer Security Framework, and its sustained governance and risk management process are the cornerstone of every organization’s ransomware strategy.

When a hack can freeze an entire system’s access to patient data, medical centers turn to a

WHAT IS RANSOMWARE?

Ransomware is any software that can be used to threaten an organization with damage to one of the InfoSec Triad (Confidentiality, Integrity, and Availability) in return for payment of a ransom. In order to work,

- The threat must be credible;
- Ransom must be less than the loss from the threatened damage;
- An untraceable (or at least not prosecutable) mechanism for
- payment of the ransom must be offered to the victim; and
- Relief from the damage given when the ransom payment is made.

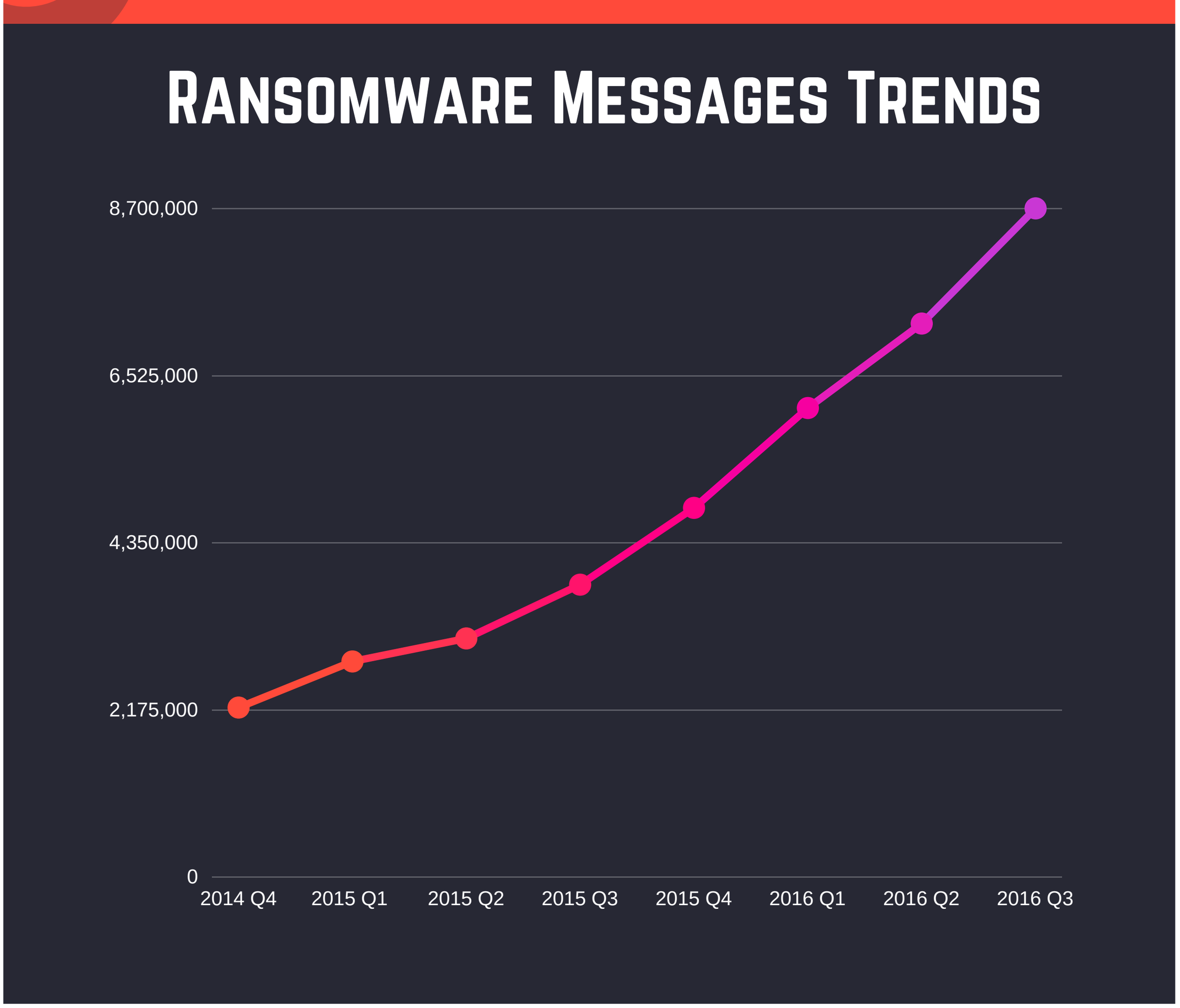
The underlying criminal activity is extortion. The problem with laws surrounding extortion is that they were never designed to address either digital extortion or the transnational nature of cybercrime. Unfortunately, in the current world order, we cannot expect punishment of foreign-based organized cybercrime entities.

How is it growing?

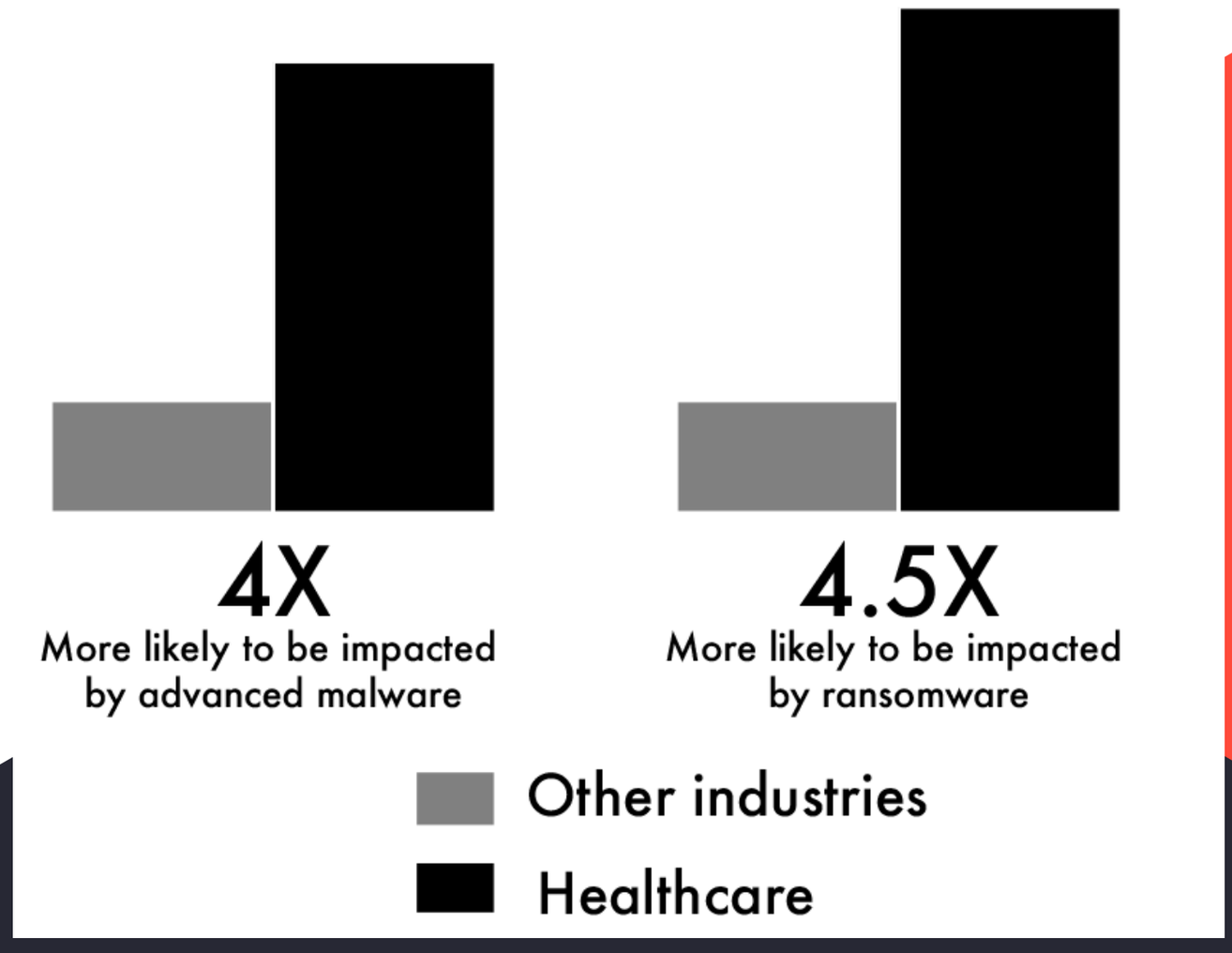
Criminal exploitation of ransomware began in the middle of the last decade as a natural extension of “Denial of Service” (DoS) attacks. Although it grew during the next 8 years, it did not really take off as a major threat until three trends converged. First, the use of encryption made the consequences of a successful attack much more serious. Second, commercialization of botnets as a delivery vehicle matured, permitting an attacker to attack thousands of systems at a time. And third, the rise of cryptocurrency, such as Bitcoin, made the tracking and prosecution of the criminals much more difficult.

As a result, ransomware attacks are growing at an alarming rate from a baseline that is already large.

As new exploitation opportunities arise the malware designers rapidly invest resources in creating new and more dangerous ransomware packages. As an example, the Wanna Cryptor (WCry) package is a highly sophisticated tool that leverages an exploit stolen from the NSA and released by the Shadow Brokers. Although not technically a Zero-day attack (there were patches available a month before release), it illustrates a whole class of threats that include zero-day attacks. It also illustrates some of the ways in which exploits fail to achieve their potential. Any exploit is most effective when it is fresh. Where money is the objective, the newer the attack the more return on investment. Once released, countermeasures are quickly developed and the profit declines. The return on investment from WCry could easily have been more than $1 Billion. Current estimates indicate that the income generated by WCry are a tiny fraction of that. Due to its notoriety, that income will very soon be reduced to a trickle. Phishing attacks, by comparison, collect large amounts of ransom cash slowly over a much longer period of time, flying under the radar of victims and law enforcement.



Healthcare industry vs average industry



Like all exploits, there is a lifecycle of a ransomware attack. Although there are variations to the time frame, it is useful to look at each stage and see what can be done to detect the attack, prevent it from being successful and improve the outcome.

INSTALLATION AND INFECTION

PROPAGATION

COMMAND AND CONTROL

MALICIOUS ENCRYPTION

RANSOM DEMAND

DECRYPTION

PAY

Step One: Installation

Generally, ransomware is a malicious payload. That means it is more or less independent of the mechanism that installs it on a system. We can assume that any malware delivery system can and will be used to install the ransomware. As ransomware becomes more sophisticated, the delivery systems are becoming more complex. Many varieties use multiple delivery systems to attack different vulnerabilities in the hope that one of them may be successful. Compound delivery systems may incorporate a second stage that acts like a worm, replicating to connected nearby systems.

It is useful to point out that the most prevalent attack vectors all involve some action by a user. The two most common vectors are phishing emails and compromised Internet web servers. Another vector is the introduction of malware, such as a Trojan or Internet worm, from another infected system that is granted access or privileges within a protected network. Most of these attacks are opportunistic from a largely random selection of targets. Occasionally, IT infrastructure is directly attacked, but targeted phishing or social engineering is far more likely to succeed than an attack on the external defenses of a network. As in all cybersecurity, these general observations are likely to change as we do a better job of defending our systems and as new attack tools and methods are invented.

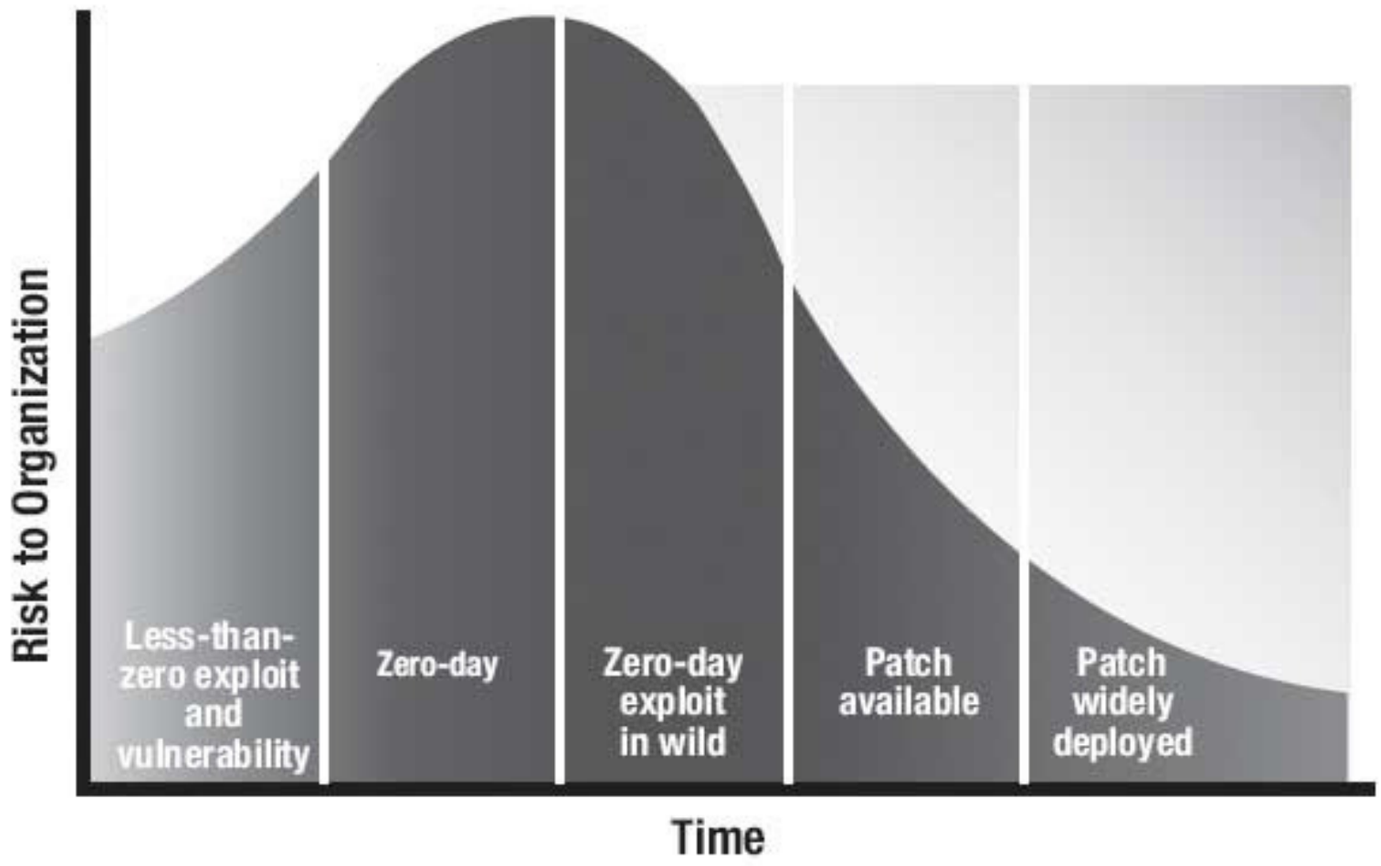
Botnets, a network of private computers infected with malicious software are an important factor in the prevalence of ransomware. They provide an easy way for a criminal to “hire” a mercenary army of infected systems needed to attack thousands of targets at a time. Botnets are used to distribute Spam emails that have malicious file attachments or entice the user to visit a malicious website that can attack vulnerabilities in the victim’s system. In both cases, policy and user training can minimize the threat of these attacks.

Did you Know?

43 percent of cyber attacks are aimed at small businesses.

Step Two: Infection

Once the delivery tool has found a victim, it must install the ransomware payload. This process can range from very straight forward to highly sophisticated. To be successful, the payload must be installed, given adequate permission to access the target files, infect the system and /or network with malicious code, and remain undetected. If the exploit only gives limited access, a second exploit is launched to escalate the privilege of the attacker to perform encryption on the files. If the exploit is detected during infection the chance of payout to the attacker is much less. The payload is usually obfuscated or encrypted and must be unpacked. “Zero-day” exploits are preferred because they do not have patches and are less likely to be detected by security monitoring tools.



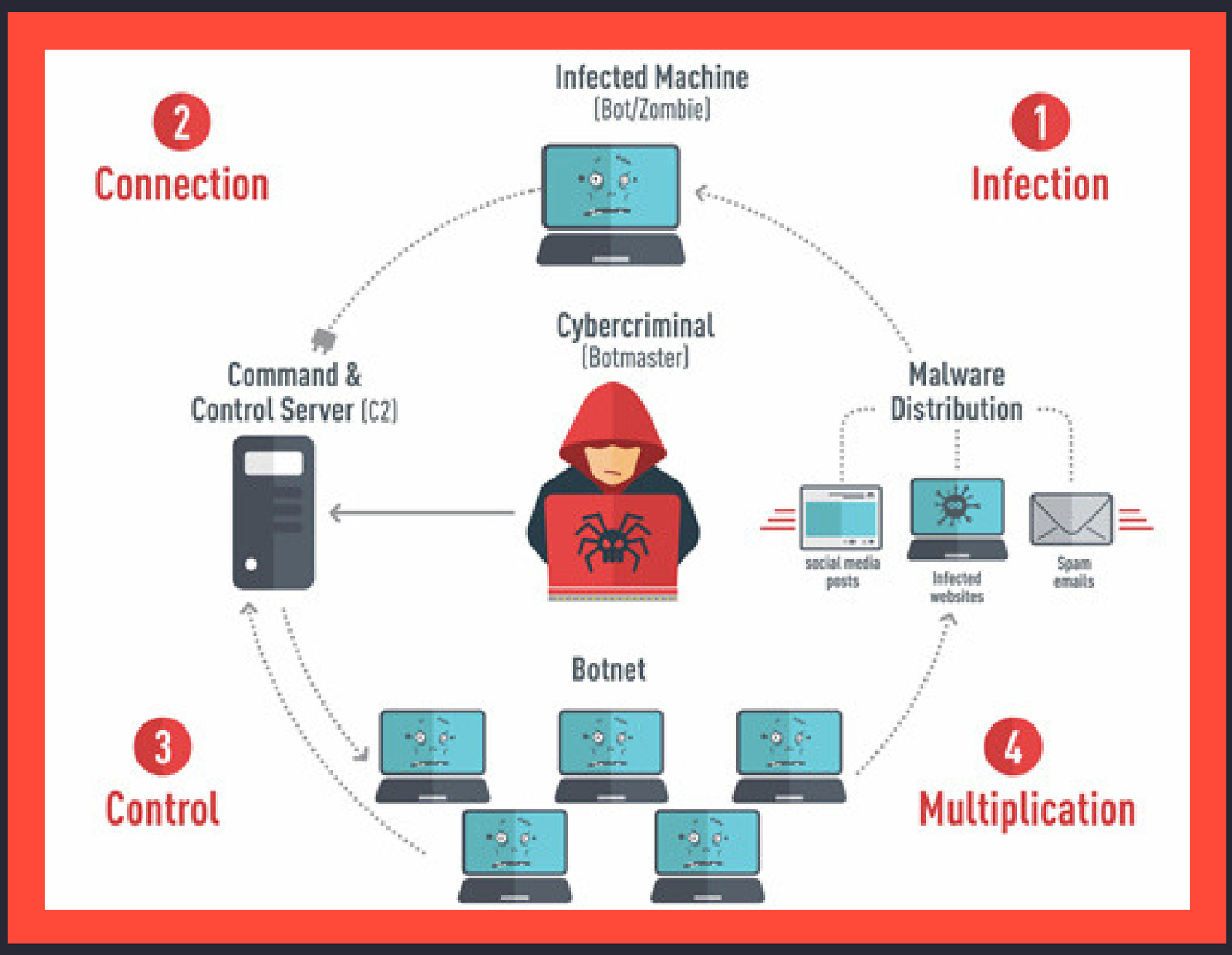
The less-than-zero threat is the period of time before a vulnerability is publicly announced. While the zero-day threat poses a severe level of risk, the less-than-zero threat can pose a serious danger as well.

Words to know: Propagation

Although some attackers use phishing, compromised webservers, or social engineering to get the user to click on the link, this type of attack can only expect a few systems to be infected at a time. Some ransomware builds in a propagation module that seeks other potential targets known to the victim. Once infected, the victim becomes a delivery path to infect other nearby systems.

Step 3: Command and Control

A ransomware attack involves connection from the victim to a Command and Control (C&C) server. C&C is a standard feature of most malware. It provides the ability for the attacker to trigger the encryption, verify ransom payment and provide the decryption key. It also permits a compromised device to be controlled later if a rootkit is part of the attack. There are often multiple C&C servers. The C&C server may provide updates to the code from the server either to keep the initial attack small or to maintain a presence on the device for future exploits.



Step 4: Malicious Encryption

Ransomware often involves encryption of critical files using a key that is known only to the attacker. This key may be embedded in the code or provided by the C&C server. Some past versions didn’t use a unique encryption key for each system, but most recent ransomware does. Also, most ransomware uses Public Key Cryptography, so that the decryption key is not embedded and must be sent to the victim. Depending on the sophistication of the ransomware, the Master Boot Record, selected files, or the entire file system may be encrypted. There is also the potential for the attack code to attempt to identify backup media and encrypt that as well.

Step 5: Ransom Demand

The demand for ransom will be posted on the system's screen giving an amount and a ransom due date. There are many variations on the ransom note, but it is important to understand that the amount of ransom may increase and there is potential for second or more rounds of ransom.

Ransomware attacks rose 250% in 2017

Step 6: Decryption

There are some cases where the ransoms paid have not resulted in successful restoration of files. Sometimes a key is never sent or it will be withheld to extort more ransom. However, if the ransom payment is relatively small and the ransomware software is efficient, the attacker will be more interested in getting payment and less likely to use time demanding more money.

Ransom Payment

The growth of ransomware is related to the cyber currency, Bitcoin. This is because it provides a level of isolation and anonymity that frustrates law enforcement. Bitcoin ransom payments are made to a bitcoin address and require the purchase of the cyber currency. Bitcoin is becoming more prevalent but is not universally supported in the banking industry.

Protection

The best protection against a ransomware attack is a fully developed security program based on a Risk Management framework such as NIST's Cybersecurity Framework. These programs provide a holistic and dynamic security governance structure to ensure that all controls are working together to decrease risk. They use continuous monitoring and risk assessment of critical security controls, focusing on those that are especially important to address changes in the current threat environment. The following controls in a security program that implements Risk Management can reduce the likelihood of success and impact of the loss of a successful ransomware attack.

Controls that affect Likelihood

- Build a security program with robust and active governance to assess evolving threats and place them in context of the organization's critical business requirements and the threats from all sources. It must engage all IT users and have the support of senior management to take action and control risk.

- Deploy patching and security updates quickly upon release. Have a program to ensure that all applicable security updates are identified and implemented. The timing of patches can be critical when new exploits are developed.

- Provide comprehensive user security training. It should be focused on helping users spot suspicious Internet and email content, dangerous behaviors such as the download of files or macro execution and social engineering attacks such as phony helpdesk calls. An anti-phishing campaign to educate and test your staff on their preparedness for a phishing attack is advisable.

- Keep current Anti-Virus/Anti-malware solution installed on each workstation and server. Host Intrusion Detection (HIDS) is also very desirable where feasible. These systems are best when they are centrally managed and can provide notification to a Security Operations Center or a SEIM.

- Deploy a Web Content Filter. This can apply reputation blacklists and identify certain malicious content.

- Deploy a Network Intrusion Detection or Protection System (NIDS/NIPS). Signature or behavior-based, they identify attacks or unusual network traffic. Ransomware in an enterprise setting will exhibit certain detectable behaviors or may use known exploit code.

Words to know: NIDS/NIPS

A network intrusion protection system (NIPS) is an umbrella term for a combination of hardware and software systems that protect computer networks from unauthorized access and malicious activity.

Controls that affect Likelihood of a successful ransomware event

- A Security Event/Incident Management (SEIM) organizes event data to present a sophisticated view of enterprise activity. It also consolidates alerts from various other systems to keep relevant events from being overlooked.

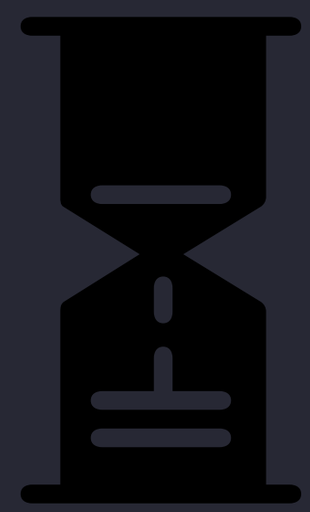
- Vulnerability Scanning/Management tools identify missing patches and misconfiguration of system and application software. There are several types of scanners and all have relevance.

- Implement a continuous Technology Refresh/Legacy System Replacement process. Old software and hardware represent a major risk factor for healthcare organizations. Organizations must be aware of end-of-life and end-of-support dates for computers, software, networked medical devices and all other networked gear.

Don't Wait Until It's Too Late

Controls that Affect Loss and improve remediation timeliness

”During any cyber attack, time is of the essence and practice will make decisions easier and respond quicker.”



- Build a security program with robust and active governance to assess evolving threats and place them in context of the organization’s critical business requirements and the threats from all sources. It must engage all IT users and have the support of senior management to take action and control risk.

- Invest in an adequate backup system. Planning for a ransomware attack should always start with the backup system. What is the maximum acceptable Return to Service interval? This should determine the frequency and completeness of the backup system and media. The system should protect the media as soon as it is written to protect it from damage by the ransomware. If a high availability requirement is met using a Hot failover site, make sure the ransomware cannot damage the failover data. Frequent testing of the Backup media and process should be a regular feature of the security program.

- Segment the network to place barriers and monitoring points within the enterprise. This can isolate a problem allowing portions of the network to remain secure during an attack or at least inhibit propagation. The Access Control Lists between segments should be as restrictive as possible without creating unnecessary operational constraints.

- Test the Continuity Plan. Create a ransomware scenario and test the Contingency Plan against it. During any cyber attack, time is of the essence and practice will make decisions easier and respond quicker.

- Conduct a Business Impact Assessment. Identify what the critical IT assets are for the enterprise. This must include both data and operations. The Return to Operation (RTO) period should be generated as part of this process as well as a complete data Inventory.

- Ensure proper Audit Log Configuration. The Audit logs will help to determine when the initial exploit took place. This is critical since rolling back to a backup may still leave a system that has been compromised.

Vulnerabilities

The most important high-level vulnerabilities for a security program to address are:

- Untrained Users
- Legacy Systems
- Unpatched Vulnerabilities
- Inadequate Backups

Response

- System Disconnect
- Close Access to C&C
- Halt Backup Process
- Isolate Backup Data
- Identify Initial Incident

Prediction of the Future

Although it is tempting to view ransomware as a unique and dangerous new threat, in reality, it is only a step in the evolving war to protect our IT systems, operations and data. Protecting against ransomware for an organization and thus decreasing the Return on Investment to criminals are both possible using the existing security controls. Building each organization's Security Program is the key success factor for properly deploying these controls and staving off future attacks. However, making ransomware a thing of the past will require we all do our part and support international law enforcement efforts to address the jurisdictional issues that have allowed certain areas of the world to be safe havens for cybercriminals.

Ransomware by the Numbers

Global ransomware damages are predicted to exceed $5 billion in 2017

72 % of infected businesses lost access to data for two days or more

A company is hit with ransomware every 40 seconds

71% of companies targeted with Ransomware have been infected

1 in 5 businesses that paid ransom never got their files back

About QI Express

QI Express provides streamlined Cybersecurity for Small and Medium-sized healthcare.

In a world of complex threats, cyber doesn't have to be difficult or expensive. With a mix of simple management tools, experienced coaches, and cybersecurity experts, we give our customers the tools to manage and provide the expertise to execute a scaled Risk Management Program that fits your capabilities and needs. We help you build security for your future.

QI Express offers easy-to-use, comprehensive software which reduces the level of effort and cost while ensuring security and compliance.

Our end to end solution and methodology includes:

- Risk Assessment
- Remediation
- Emergency Preparedness
- Threat Intelligence
- Training
- Coaching
- Education
- Certification
- Monitoring

Learn more by visiting QIExpress.com
or call 1-800-674-9070