Global Information Assurance Certification Paper

“Is there a Yelp for Ransomware?” Incident response planning that does not rely on Plan B

GIAC (GSLC) Gold Certification

Author: Matt Freeman, matt.freeman@hawaiiantel.com
Advisor: Manuel Humberto Santander Peláez
Submitted: July 18th, 2016

Abstract

What if there was a service that could classify the impact of each variant of ransomware. A system to help IT decision makers determine if they could decrypt their data or proceed to system restore. How about an app for rating your hijacker’s customer service? Did they provide easy to follow instructions to transfer the bitcoin ransom? Do they have a history of quickly releasing files or just take the money and run? If your organization is depending on a 4-star rating from your data’s kidnapper, it might be time to re-evaluate your incident response planning. Businesses of all types are under constant attack by ransomware and healthcare providers are no exception. Reliance on older operating systems and a non-technical workforce provides an opening for ransomware and can result in delayed patient care or loss of patient data. Proper implementation of specific critical security controls will ensure your IT staff does not have to resort to googling your attacker’s reputation after receiving their ransom demands.

1. Introduction – Plan A or Plan B for Ransomware Incident Response

According to the FBI's Internet Crime Complaint Center, ransomware attacks have increased 74% between 2014 and 2015 in the United States (FBI, 2016). The first half of 2016 has seen half a dozen successful ransomware attacks on US hospitals (Gammons, 2016). Hospitals are particularly vulnerable as their IT systems often rely on older software while system administrators focus on converting to newer electronic records systems (Zetter, 2016). One recent example of a successful ransomware attack on a US hospital occurred in March 2016 at Kentucky's Methodist Hospital (Krebs, 2016). The successful ransomware attack at this hospital illustrates the importance of having a plan in place before a security incident occurs.

Every business needs to have someone responsible for the protection of electronic assets against threats such as ransomware. The manager of an information technology team tasked with improving network security, information security or cybersecurity can implement basic controls to help protect their business. This guide will assist the manager in identifying challenges and creating solutions using the 'Plan A' and 'Plan B' method.

Plan A is the documented process and procedure for responding to a cyber-threat that aligns with corporate security policy. Plan A is based on industry best practices such as the SANS Critical Security Controls and is intended to provide the manager with a playbook to use during cybersecurity incidents. Plan A should be in place before an incident occurs and aims at preventing it or mitigating the impact. Plan B is a set of recommendations to consider if Plan A has failed. Plan B is more reactive but still allows the manager to respond to a security incident.

Using the example of a recent ransomware attack at Methodist Hospital managers can develop their own Plan A and gain insight into how Plan B can still be valuable.

2. Increasing Sophistication of Ransomware

Ransomware is evolving faster than some businesses can adapt. Despite having a variety of expensive tools to detect and prevent malware, ransomware continues to disrupt businesses and stress users. UTM firewalls and endpoint anti-virus can fail to prevent ransomware attacks.

Detection systems for ransomware can prove redundant, as the signs of infection are direct and immediate as opposed to stealthier C2 malware variants. To prepare an effective defense against ransomware, it is important to understand how ransomware works and identify its goals.

Ransomware is a term for malware designed to prevent access to your electronic resources. There are two general branches of ransomware. Crypto based malware attempts to encrypt files on the compromised host, such as Word documents, .pdf files, Excel spreadsheets, images, and databases. The second type, locking, attempts to prevent access to the host itself. The end goal of each variety is to deny access while demanding ransom in exchange for releasing access back to the user. More aggressive variants will begin encryption of local assets while attempting to explore for shared network resources to propagate itself across the network (Savage, 2015).

Computer viruses, worms, and trojans (summarized as malware) have been a threat to computers for decades (Snyder, 2010). As the complexity of malware has evolved over the years so has the function. Early viruses were often destructive in nature, attempting to crash computers or delete resources in a very visible way. In the last decade, malware has become stealthier. Less focused on destroying your assets and more interested in hijacking them to use for other purposes. Over the last several years, the threats evolved into ransomware as cyber criminals look to monetize their efforts more directly.

While there are thousands of ransomware variants, two particular ransomware variants have become the most active in the first half of 2016: Locky and Teslacrypt (Symantec, 2016). The Locky variant of ransomware reaches targets via Word document attachments (TrendMicro, 2016). Upon opening the attachment on a vulnerable system, the ransomware attempts to use macros that will download an executable. The executable proceeds to search for then encrypt targeted file types. Additionally, the Locky variant will explore for mapped network drives and attempt to replicate the encryption to those resources. Another variant, Teslacrypt uses indirect download through website advertisements. Dubbed malvertising, these variants typically exploit vulnerable JavaScript versions to download and execute the payload while users are browsing websites.

Unlike virus or worm creators of the past who might have just been after internet infamy, ransomware authors want to get paid. Once their malware has successfully locked up your files they turn on their 'customer' service charms. The primary objective is to make the ransom payment as easy as possible while remaining hard to trace by authorities. Ransomware criminals use electronic currency such as bitcoin to transfer funds. Ransomware includes step by step instructions on how to purchase and transfer bitcoin to their anonymous brokerage account. The more detailed and customer friendly their ransom demands, the easier it is for the 'customer' to recover their files. After confirmation of payment, the ransomware will send the decryption key that restores user access to their data.

As in non-technical hijacking situations, the FBI does not recommend paying the ransom (FBI, 2016). If an organization did not have the necessary plans in place to mitigate a ransomware outbreak, they may face a difficult choice between paying the ransom and losing data.

2.1. Impact of Ransomware on Businesses with focus on Healthcare

Consider a targeted attack scenario from the perspective of a cyber-criminal. Your objectives are to (a) make some money, (b) minimize your efforts, and (c) not get caught. When looking at targets, you want to focus on a business that generates revenue and may have vulnerable IT systems. Possible targets could be a bank, a retail chain, or a hospital. A bank or retail chain typically prioritize their revenue generating systems while the hospital is likely putting the core of their IT investment into patient care technology, including electronic health records. As a ransomware attacker, your goal is to prevent access to the most critical data possible to ensure a quick payout from the target. It is no doubt that financial institutions will feel the sting of lost revenue but attacking a hospital's file systems can put lives at risk.

Now consider your method of attack. Robbing a bank is dangerous and requires a fast getaway. Using a targeted spear-phishing attack aimed at an employee in the accounting department that you looked up on Linkedin is low risk and anonymous. A quick email titled "June 2016 Invoice" with an attached Word document containing malicious macros has a decent

chance of allowing your ransomware package of choice to deploy. Low risk, low effort, high reward.

The FBI estimates that businesses have lost $24 million in 2015 to ransomware attacks (FBI, 2016). While cyber criminals operate in a world without rules, the manager has to contend with budgets, bosses, projects, vulnerable but critical software, and strict compliance regulations. Healthcare providers have an expectation under HIPAA guidelines to implement and maintain technical and administrative controls to protect patient privacy. The HITECH expansion directs healthcare providers towards electronic records (Charles, 2015). These regulatory guidelines developed in 1996 and expanded in 2009 focus on maintaining privacy while enhancing ease of access to records. This challenge for the manager presents many issues to prioritize and solve.

Every business should have a cybersecurity program that protects its digital assets. Before you can build an effective cybersecurity program, it is important to understand the business's objectives. Consider one of Methodist Hospital's vision statements: "To effectively manage resources through the continuous development of systems, care processes and staff" (Methodist Hospital, 2016). This strong but simple declaration sufficiently empowers the manager to prioritize processes that will focus on investment of IT security resources. A manager should consider their organization's mission statement when creating their objectives for the security program. The objectives of the security program should be aligned to help meet the needs of the business. An effective manager will also take the time to measure the current resources available to the cybersecurity program to establish a baseline of capabilities. Compare the current capabilities of the program to the long-term security objectives to develop a plan on how to improve. Meanwhile, remain vigilant to changes in the landscape – whether political, financial, or regulatory. A successful manager will adjust the objectives of the security program to align with new information about business priorities. With an understanding of the threats facing them and the needs of the business, the manager can begin to create and implement their 'Plan A'.

Matt Freeman, matt.freeman@hawaiiantel.com

2.2. Building a security program

Once the manager has analyzed the requirements of their business, it is time to begin forming the cybersecurity program. One of the early roadblocks encountered when starting up a new group is how to justify the existence of and funding for the cybersecurity program. Educating executives and non-security focused IT staff will require the manager to prepare stats and metrics to illustrate the negative consequences of not having an information security program. Selling the decision makers on the idea will help to gain the necessary levels of support before implementing new policies and procedures. Creating a mission statement for the cybersecurity program that aligns the business priorities with the security program objectives is a good way to bridge political disagreements.

To ensure the long-term success of the program, empower a group to guide the decision-making going forward. This Information Security governance team will be able to adopt a framework that best suits the business need. Using the healthcare example, designate HIPAA compliance as the target. For businesses that do not have industry-specific regulations for protecting electronic data, consider adopting the National Institute of Standards and Technology's Cyber Security Framework (NIST, 2014). With a decision-making entity in place, examine other critical roles to maintaining a secure IT environment: assessment, planning, maintenance, threat intelligence, event analysis, and incident response. Depending on the resources available these roles can be centralized or separated, but it is important that the governance group sets the expectation and primary stakeholder for each of the core functions. Use the selected framework to develop operational objectives and processes that fit the requirements of the business. Be realistic in setting the expectations. A small information security team may not have the ability to deliver an overly complicated program right away, but aim high and create a timeline and roadmap to achieve the desired goals. To determine what the right starting point for your business is, use a maturity assessment system.

Security program maturity is a method to establish a baseline for existing capability. One assessment model is the Cybersecurity Capability Maturity Model (C2M2) produced by the US Department of Energy. The C2M2 model establishes four maturity levels across ten security domains. Maturity level 0 indicates a program without process and procedure. Maturity level 3

shows a program that documents, trains, and reviews processes and procedures (Christopher, 2014). The domains include risk management, change management, and incident response. Using the cybersecurity framework dictated by the InfoSec governance team, evaluate the team's ability to deliver repeatable processes in a variety of scenarios. C2M2 recommends performing an evaluation of current capability against the target domain then analyzing the results. Using the cyber framework goal that the security program aspires to, create plans to improve. Prioritize the initiatives to be consistent with the needs of the business and begin implementation.

The SANS Institute provides a list of 20 recommendations free to the security community and is a trusted resource to use when building an incident response plan for ransomware. The Critical Security Controls are effective, industry standard processes that will have a direct impact on the overall security of a network. In the next section, we will discuss specific controls that help defend against ransomware attacks citing the March 2016 event at Kentucky's Methodist Hospital. To help programs of all maturity levels the review will provide a best case, industry standard expectation (Plan A) and where possible, a viable next best thing (Plan B).

3. Critical Security Control Implementation Options

3.1. Plan A: Critical Security Control #3 secure configurations

Secure configurations for all IT assets may have prevented the ransomware damage at Kentucky's Methodist Hospital. Unpatched OS and third party software is a primary vector for a successful ransomware attack. One example is the popular exploit kit, Angler, which targets vulnerabilities in unpatched Adobe Flash Player software to launch a malicious payload that often includes ransomware (S3, 2015). The manager will ensure that there is a designated process for identifying software assets and creating a standardized management program. Core components of the program must include an expectation of frequency for updates, method of testing and approving updates and remediation plans for failed updates.

This program should include a classification system that identifies business-critical systems and what type of software users can install. Use the organization's acceptable use policy for corporate assets to define access controls for users. Create the inventory of devices and define

expectations for update policy before implementing the operational process. Large organizations will need to simplify and automate where possible. Microsoft provides a centralized management system, Windows Server Update Services (WSUS) to streamline approval and distribution of software updates across the enterprise. Administrators can also apply group policy objects to devices connected to the domain that will enforce regular software updates using pre-approved patches on a defined schedule. This type of system for management of the core operating system is an important part of IT operations but does not account for non-OS software, often referred to as third party software.

Referencing the acceptable use policy, the manager will consider whether an application belongs on the corporate asset. In some cases, productivity software is essential to business success but may have inconsistent levels of vendor support regarding updates. Third party software that enhances user experience, such as Java or Adobe Flash, may not be essential to business operations. If these programs are on corporate assets, a method for updating them is necessary. IT organizations that permit unapproved, end-user installed software will have a difficult time preventing ransomware attacks. Implementing access control is one option although there are ways to allow third party software to remain centrally managed. Remote monitoring and management software (RMM) often includes third party management tools and can detect and patch out of date software installations.

3.2. Plan B: No patching?

Legacy equipment exists in most IT environments. Examples of legacy equipment could be a Windows XP machine is required to run reporting software or a vendor procurement website that only works with Internet Explorer 7.0. Some business owners demand a certain way of doing things, despite the potential risks it may present. Sometimes budgets do not allow for infrastructure upgrades resulting in equipment used longer than it should be. The day to day reality of IT operations is a challenge for the manager. How do you reconcile the business's need for expediency with the policies that dictate strict security?

In these situations, consider a two-pronged approach. First, identify and isolate the unsupported software. Use a software inventory tool such as Microsoft's System Center

Configuration Manager (SCCM) to generate a list of all software applications on domain attached workstations and servers. Assess the software for programs that no longer have vendor provided security updates and may be vulnerable to remote exploitation. Classify these systems as business critical legacy devices and isolate within the network. To isolate, create a dedicated VLAN for these systems and implement Access Control Lists (ACLs) on the network switches that limit network traffic from the subnet to other corporate network assets. Allow only sufficient external connectivity to perform whatever function the device needs. If the system must have direct access to the internet, ensure a UTM firewall is inspecting network traffic. Enable event monitoring on these devices to enhance incident detection capabilities. A network IDS such as Suricata can be deployed to monitor network traffic on the legacy VLAN. Install a host-based ID such as OSSEC to monitor for file system changes. By separating and monitoring vulnerable systems, the manager can limit the use of the legacy device as an initial attack vector and potential pivot point.

Secondly, work with decision makers towards a plan to retire or upgrade the problematic systems. If the vendor's website only accepts orders from an older, unsupported web browser have them explain how they will accept the liability of a breach. Have the vendor provide a timeline for upgrading to modern systems or provide alternate means of access. If possible, find a new vendor that takes your security seriously. In this scenario, the business may rely on a rare and critical resource that only this vendor provides, but it will be your job to identify the problem and provide a migration path.

3.3. Plan A: Critical Security Control #5 controlled use of administrative privilege

Interviews with Methodist Hospital staff indicate that the initial compromise of their network began with an infected email attachment that bypassed perimeter defenses and opened by a user (Krebs, 2016). Post event analysis reported that the document prompted the user to enable macros to view an invoice resulting in the download and execution of the Locky ransomware. SANS Critical Security Control #5 calls for the controlled use of administrative privileges and would have eliminated this attack vector. A common theme of information

security is limiting access to necessary and essential use. If the user that opened the Locky Word document did not have sufficient permission to enable macros on the computer, the ransomware would not have been able to detonate and cause an outage for IT systems at the hospital.

More broadly, if an end user does not have sufficient permissions to install third party software to their workstation they will inflict less harm to the network. For users that require non-standard software, implement a change control process to track, manage, and monitor that device. An effective change control process includes a standardized change request method, a review board to determine risk and an inventory system to track changes. Implementation of administrative controls to limit the ability to install software will reduce the chances that malware can execute through macros, PowerShell, or direct install. On a Microsoft Windows domain, implement a group policy that restricts macro execution in Excel and Word by default. End users that need to use macros in these programs will submit a request using the change control process. If the review board confirms the legitimate business need, IT administrators can enable their workstation for macros. Once approved and implemented, the macro-enabled system should be tracked by an inventory management system and classified as higher risk.

3.4. Plan B: Segment the vulnerable systems

Suppose the Methodist Hospital employee that accidently set off the Locky malware by opening a fake invoice was actually in the accounting department. There is a legitimate business need for some employees to be able to utilize macros within applications and they may receive emails with invoices as attachments. The responsible manager will implement access controls across the network and carve out exceptions as necessary for legitimate business use.

For systems that are authorized to operate with higher than normal access levels, implement network segmentation to limit one infected host from compromising the whole network. As described in section 3.2, VLANs and ACLs can limit network traffic between hosts, and limit the spread of malware that seeks to move laterally within the network. Some variants of ransomware such as Locky attempt to identify and encrypt network shares accessible from the first compromised host, including unmapped drives (Abrams, 2016). Placing users of higher risk

workstations into security groups that do not have access to shared network drives can prevent ransomware from spreading.

3.5. Plan A: Critical Security Control #8 malware defenses

Implementing some form of malicious software prevention might seem like a common sense recommendation (and it is), but a mature security program will consider more than defense at the host. Antivirus and antimalware software are almost universally recommended, with the exception of some vendors that claim "antivirus is dead" every few years (McAfee, 2015). Individual prevention systems can fail, so consider using a layered approach to network security. A perimeter defense such as a UTM firewall with IPS will help to filter out inbound malware attacks. Intrusion prevention systems are signature based and will reduce the number of threats, but malware authors are always writing new code or altering existing. The Locky ransomware attack on Methodist Hospital bypassed defenses by presenting as a legitimate email attachment type. Since there was no executable signature to analyze, the host-based antivirus software was not able to detect and prevent the attack. Is antivirus really dead? How did the potential layers of defense fail to protect the network? In this example, the bad guys won this round of malware signature cat and mouse that antivirus signature creators play with malware authors.

Before Locky compromised the host and began to spread across available network shares, there was just a macro embedded in a Word document. The macro would need to establish an external connection to download the executable in an encrypted tunnel, bypassing inspection of the UTM firewall and IPS signatures. Setting up a web proxy is another layer of defense that can help protect the network. In some cases, prevention is just not sufficient. That doesn't mean you should stop trying to prevent attacks. Figure 1 shows the typical attack process of the Locky ransomware variant and how it can bypass network defenses.

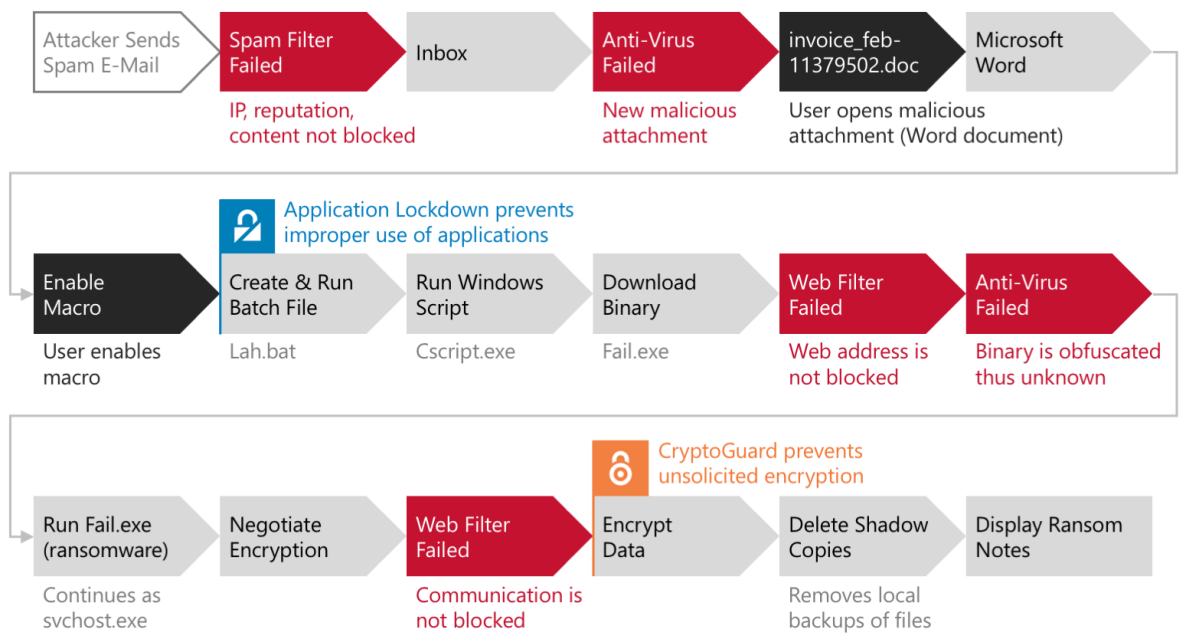

Figure 1. Typical attack sequence for Locky Ransomware. Reprinted from "Are you up all night after getting Locky?" by Mark Loman. Image Retrieved from https://hitmanpro.wordpress.com/

3.6. Plan B: Malware got through -- Now what?

If you cannot stop malware the perimeter, the next best thing is early detection and a solid incident response plan. Non-ransomware malware aims to be quiet within the network but will still have indicators of compromise. Comparatively, ransomware is quite noisy trying to scare the user of the compromised host into quickly paying a ransom. Malware may lurk on a network for weeks or months siphoning data or even staying dormant until ready to be used by the controller. In these cases, there is usually some form of external check-in that the malware will perform to indicate to the controller that it is still active. Referred to as command and control, or C2, malware leaves some tracks, however subtle. Installing a network IDS to monitor internal traffic across the network will provide the manager with visibility into the silent threats lurking on the network. Aggregating the IDS logs into a SIEM that can correlate additional data sources might reveal egress activity to a C2 server with a bad reputation IP address. Having proper detection systems in place is a natural complement to the required preventative systems.

If your tools aren't able to prevent an attack but can detect the intrusion, it is time to engage the incident response plan. The level of detail in incident response process is an excellent

indicator of security program maturity. Per the C2M2 maturity model, a level 0 organization will have no documented process and each response is different. The level 3 organization has clear processes in place prior to an event (Christopher, 2014). Containment will occur quickly, and communication regarding the scope of the event will be clear and concise. In the event of data breach, evidence will be preserved for later analysis.

3.7. Plan A: Critical Security Control #10 data recovery capability

SANS Critical Security Control #10 is perhaps the most critical in regards to ransomware. Ransomware's goal is to restrict access to your data by encrypting it, making it unreadable. Some variants make copies while deleting original files to complicate the recovery of data. Backup and disaster recovery planning needs to be in place before an event occurs to avoid disaster.

Data recovery begins with the classification of data. The manager with astute business situational awareness knows which data is most important to the success of the business and acts accordingly. Critical data stores are not accessible as network shares to hosts that do not need it. Data backup methods and frequency are thoughtfully evaluated and implemented per the pre-defined InfoSec governance expectations.

Cloud-based or off-site backup solutions may provide more recovery options than a network attached storage solution. While Methodist Hospital's backup solution took several days for a full restore to complete, they had a less negative impact than California-based Hollywood Presbyterian Hospital, which resorted to paying a ransom to recover data and restore business operations (Gallagher, 2016).

IT programs with higher maturity levels will perform regular data validation assessments for their data to ensure that the storage solution is performing as expected. This may include regularly scheduled data restorations to test process and ensure data is available.

IT departments that do not backup data on a regular basis are putting the business at risk. In the event of a ransomware attack at an organization without data recovery capability, paying the ransom is the only option short of accepting the loss and wiping the hard drives to remove the

infection. Data backup and recovery is one area where a Plan B solution is not optimal; however, there are still options for businesses that did not implement a full offsite backup solution.

Even IT departments without a budget can implement some form of data backups. Network attached storage devices can be as simple as a USB drive connected to a system with a scheduled data copy. Although this solution is also a target for some ransomware variants, it is possible to hide the shared storage device on the network. As another low-cost solution, consider rotating out the storage device on a regular basis. If you lose the currently attached storage device during a ransomware attack, there will still be a semi-recent copy of data to work with.

Another low cost solution is to enable shadow copy backups on Windows servers and workstations. This service will create periodic snapshot copies of storage devices allowing restoration on request. Although inexpensive, this is not an ideal solution as ransomware often targets shadow copy images when attacking across a network.

3.8. Plan A: Critical Security Control #17 skills assessment and training

Once properly implemented, all 20 of the SANS Critical Security Controls will assist a manager in protecting the business from ransomware attacks. Critical control #17 has a special place in the efforts to prevent ransomware attacks as it works to mitigate the most dangerous threat: the end user (Cave, 2015). Despite having the most modern security appliances and layers of defensive enclaves, a user can still inflict accidental harm on the network by allowing ransomware to encrypt data. Most ransomware infections are the result of untrained staff through bad web browsing habits or inability to recognize phishing attempts. The manager will need to identify this risk and prepare accordingly by implementing a security awareness training program.

A security awareness training program should have several objectives. The primary purpose is to ensure that the non-technical end-users in the network know how to identify common threats and understand the risks associated with those threats. To achieve this goal, the manager needs to create a training program that is understandable by a non-technical workforce. One method is to setup a phishing simulation program such as GoPhish. This tool allows

managers to create email campaigns targeted at their users that generate phishing emails using social engineering techniques to deceive the user. If the user clicks the fake URLs, they will be re-directed to spam and ransomware training resources (Wright, 2015). Managers can set the email campaign to notify the user that they have been tricked, reinforcing the message to be wary of unsolicited emails with links or attachments.

A secondary objective of security awareness training programs is to establish a baseline of user related risk and begin the process of measuring improvement. The manager can create a departmental email address to report phishing attempts and encourage users that detect suspicious emails to report them to the IT department. Over time and multiple email campaigns, the manager can create a trend to report the success of the program. As user awareness increases, the time to report and click through rate of phishing emails should go down.

Beyond focusing on end-user security awareness, a successful manager will develop their internal staffing resources to be able to identify and respond to security threats. By attending security conferences and working within peer groups, information security engineers can learn more about common threats to their industry. Security specific technical training should be a high priority for programs of all maturity levels.

3.9. Plan B: No user awareness planning

Some organizations will not have the time or resources to implement an end-user training program. Consider training as another preventative technique: users that do not infect the network are helping to maintain network security. Plan B for not implementing a user training program is to have a sufficiently trained IT staff that can quickly identify, contain, and clean a ransomware outbreak. Companies with no formal user training program are likely to have a higher risk of ransomware attack, so the IT staff needs to be prepared to act quickly.

Incident response procedures should be developed and practiced by IT security engineers. Ensuring that each employee uses the same tools and process is going to improve the ability to contain and clean a ransomware outbreak. If possible, create an incident response toolkit that contains a hardcopy of the incident response process and a USB drive containing the necessary

forensic and clean-up tools. If your IT organization is not able to prevent the attack, at least strive to be well versed in responding to incidents.

4. Conclusion

Have a Plan A, prepare for it not working

Every business should have a plan in place before an incident occurs. More mature programs will focus on prevention first with a healthy detection program. These programs will have documented processes that are efficient and repeatable. Their plan uses industry standard best practices. Sometimes plan A will fail so make sure your Plan B will get the job done.

Cyber threats continue to grow more complex so the manager must prepare for a variety of scenarios. Spreading security awareness within the organization and helping to develop a security-first mindset will keep all employees vigilant to threats. When building the cybersecurity program start small but aim high. Consider the resources available and create a program that aligns with your businesses objectives. What looks good on paper does not always apply to the real world. IT programs of all sizes and funding levels have resource challenges. What defines a successful information security program is their level of commitment towards improving. Measure the current reality and set a high level of expectations. Create a realistic plan to transition from the current state to the desired goal and stick with it.

Basic controls can mitigate major impacts. By using the SANS Critical Security Controls, a fledgling security program can take battle-tested concepts and apply them in a method that fits their current needs. Create and apply secure configurations for all IT assets to minimize vulnerabilities. Apply administrative access controls to limit the impact of unexpected events. Implementing a layered approach to malware will help to prevent attacks. A reliable and regularly tested backup and disaster recovery program will ensure the business can continue running after an event. Most importantly, share what you have learned to everyone in the business by performing regular training about threats and prevention.

Have a great plan in place but if you cannot afford it or maintain it, have a minimally acceptable plan to fall back on.

Matt Freeman, matt.freeman@hawaiiantel.com

Matt Freeman, matt.freeman@hawaiiantel.com

References

FBI (2016). 2015 Internet Crime Report. Retrieved from https://pdf.ic3.gov/2015_IC3Report.pdf

Gammons, B. (2016). 5 Things to know about the Rise of Ransomware among Healthcare Providers Retrieved from https://blog.barkly.com/rise-of-ransomware-healthcare-stats

Zetter, K. (2016, March 30). Why Hospitals are the Perfect Targets for Ransomware. Retrieved from https://www.wired.com/2016/03/ransomware-why-hospitals-are-the-perfect-targets/

Krebs, B. (2016, March 22). Hospital Declares 'Internal State of Emergency' After Ransomware Infection. Retrieved from http://krebsonsecurity.com/2016/03/hospital-declares-internet-state-of-emergency-after-ransomware-infection/

Savage, K., Coogan, P., Lau, Hon (2015, August). The Evolution of Ransomware. Retrieved from http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-evolution-of-ransomware.pdf

Snyder, D. (2010, May 30). The very first viruses: Creeper, Wabbit, and Brain. Retrieved from http://infocarnivore.com/the-very-first-viruses-creeper-wabbit-and-brain/

Symantec Security Response (2016, February 18). Locky Ransomware on aggressive hunt for victims. Retrieved from http://www.symantec.com/connect/blogs/locky-ransomware-aggressive-hunt-victims

TrendMicro (2016, February 19). New Crypto-Ransomware Locky Uses Malicious Word Macros. Retrieved from http://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/new-crypto-ransomware-locky-uses-word-macros

FBI (2016, April 29). Incidents of Ransomware on the Rise. Retrieved from https://www.fbi.gov/news/stories/2016/april/incidents-of-ransomware-on-the-rise/incidents-of-ransomware-on-the-rise

FBI (2016, April 26). Ransomware: Latest Cyber Extortion Tool. Retrieved from https://www.fbi.gov/cleveland/press-releases/2016/ransomware-latest-cyber-extortion-tool

Charles, D., Gabriel, M., Searcy T. (2015, April). Adoption of Electronic Health Record Systems among U.S. Non-Federal Acute Care Hospitals: 2008-2014. ONC Data Brief, no.23. Retrieved from https://www.healthit.gov/sites/default/files/data-brief/2014HospitalAdoptionDataBrief.pdf

Matt Freeman, matt.freeman@hawaiiantel.com

Methodist Hospital (2016). Mission Statement. Retrieved from http://www.methodisthospital.net/getpage.php?name=mission

National Institute of Standards and Technology (2014, February 14) Framework for Improving Critical Infrastructure Cybersecurity. Retrieved from http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

Christopher, J. (2014, February). Cybersecurity Capability Maturity Model Version 1.1. Retrieved from http://energy.gov/sites/prod/files/2014/03/f13/C2M2-v1-1_cor.pdf

S3. (2015, November 9) Gone in a Flash: Top 10 Vulnerabilities used by Exploit Kits. Retrieved from https://www.recordedfuture.com/top-vulnerabilities-2015/

Abrams, Lawrence. (2016, February 16). The Locky Ransomware Encrypts Local Files and Unmapped Network Shares. Retrieved from http://www.bleepingcomputer.com/news/security/the-locky-ransomware-encrypts-local-files-and-unmapped-network-shares/

McAfee, J. (2015, August 20). I am John McAfee AMA! Retrieved from https://www.reddit.com/r/netsec/comments/3hr9f0/i_am_john_mcafee_ama/cu9uvld

Gallagher, S. (2016, February 18). Hospital pays $17k for ransomware crypto key. Retrieved from http://arstechnica.com/security/2016/02/hospital-pays-17k-for-ransomware-crypto-key/

Cave, K. (2015, December 8). What will be the single biggest security threat of 2016? Retrieved from http://www.idgconnect.com/abstract/10693/what-single-biggest-security-threat-2016

Wright, J. (2015) gophish User Guide. Retrieved from https://getgophish.com/documentation/Gophish%20User%20Guide.pdf