Computer and Information Science; Vol. 11, No. 1; 2018
ISSN 1913-8989 E-ISSN 1913-8997
Published by Canadian Center of Science and Education

Improving Backup System Evaluations in Information Security Risk Assessments to Combat Ransomware

Jason E. Thomas[1,2,3,4] & Gordon C. Galligher[5]

[1] Graduate Student, Bush School of Government and Public Policy, Texas A&M University, College Station, Texas, United States

[2] Adjunct Faculty, School of Business & Technology, Excelsior College, Albany, New York, United States

[3] Adjunct Faculty, Colangelo College of Business, Grand Canyon University, Phoenix, Arizona, United States

[4] Chief Operating Officer (COO), The Collective Group, Austin, Texas, United States

[5] Vice President of Managed Services, The Collective Group, Austin, Texas, United States

Correspondence: Jason E. Thomas, Bush School of Government and Public Policy, Texas A&M University, College Station, Texas, United States. Tel: 1-512-518-0351. E-mail: jason.thomas@tamu.edu. Gordon C. Galligher, The Collective Group, Austin, Texas. Tel: 512-900-7481, E-mail: gcg@colltech.com

Received: December 15, 2017 Accepted: December 24, 2017 Online Published: January 3, 2018

doi:10.5539/cis.v11n1p14 URL: http://dx.doi.org/10.5539/cis.v11n1p14

Abstract

Ransomware is the fastest growing malware threat and accounts for the majority of extortion based malware threats causing billions of dollars in losses for organizations around the world. Ransomware is a global epidemic that afflicts all types of organizations that utilize computing infrastructure. Once systems are infected and storage is encrypted, victims have little choice but to pay the ransom and hope their data is released or start over and rebuild their systems. Either remedy can be costly and time consuming. However, backups can be used to restore data and systems to a known good state prior to ransomware infection. This makes backups the last line of defense and most effective remedy in combating ransomware. Accordingly, information security risk assessments should evaluate backup systems and their ability to address ransomware threats. Yet, NIST SP-800-30 does not list ransomware as a specific threat. This study reviews the ransomware process, functional backup architecture paradigms, their ability to address ransomware attacks, and provides suggestions to improve the guidance in NIST SP-800-30 and information security risk assessments to better address ransomware threats.

Keywords: information systems, information system security, risk assessments, computer security, ransomware, computer security, computer information systems, backup, disaster recovery, business continuity

1. Introduction

An information security risk assessment is the process of performing an objective analysis of the effectiveness of a firm's security controls in protecting assets and then determining the likelihood of loss that could be incurred by those assets (Landoll, 2012). Guidance for conducting risk assessments is provided by the United States Department of Commerce's National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30 (NIST, 2017a).

An important part of risk assessment is examining systems, networks, and information storage solutions (Landoll, 2012). Backup systems are especially important because they are the foundation for recovery and the last line of defense for many critical threats. However, the guidance provided by NIST SP 800-30 is high-level and does not provide sufficient detailed information to assess whether backup systems are fully protected or set up to effectively protect assets against threats.

For example, the word "ransomware" does not appear in NIST SP 800-30. Ransomware, though, is growing rapidly and becoming one of the most significant threats to data and system availability (Allen, 2017; Collier, 2017; Lelii, 2017; Mansfield-Devine, 2016). This paper explores the potential of ransomware as a generalized threat and how backup evaluations in information security risk assessments might be strengthened to better assess their readiness to address this threat.

2. Methodology

The methodology for this study was a combination of a literature review and review of technology consulting best practices. The literature review was conducted according to guidelines of a systematic method of reviewing literature that included the following steps (Jesson, Mattheson, & Lacey, 2011):

1) Using a scoping review to conduct field mapping
2) Comprehensive searches
3) Extracting the data
4) Synthesizing the data
5) Reporting on the findings and authoring a discussion

A research plan was designed using research questions, keywords, and sets of both inclusion criteria and exclusion criteria. The goal of this study was to explore how backup system evaluations in information risk assessments, as guided by NIST SP 800-30 (NIST, 2017a), can be improved to address the generalized ransomware threat. The research questions were as follows:

1) What is the ransomware threat?
2) How pervasive is the ransomware threat?
3) What guidance does NIST SP 800-30 provide for backup evaluations in information security assessments?
4) How might the guidance in NIST SP 800-30 be strengthened to help address the ransomware threat?

Keyword searches were utilized to identify relevant peer-reviewed literature and industry data. Sources for research comprised online research libraries and associated databases such as ProQuest and Google Scholar, along with general searches of the Internet. After all data were compiled, they were analyzed, and findings were reported and analyzed.

3. Literature Review

Information security risk assessments are the primary tool for organizations to assess their security and viability to combat generalized threats (Landoll, 2012). Ransomware is a generalized threat that affects the global community (Lelii, 2017; Mansfield-Devine, 2016). Ransomware attacks are increasing at an astonishing rate and now account for the vast majority of extortion-based malware attacks (Thomas, 2017a). NIST SP 800-30 is a primary tool for providing guidance to information security risk assessments (Landoll, 2012; NIST, 2017a). Yet, NIST SP 800-30 does not mention the word ransomware.

3.1 The Ransomware Threat

Ransomware is a form of malware that can attack computers from many different avenues, such as users opening infected emails, users opening infected email attachments, users clicking on bad or malicious links, or by means of social engineering tactics like phishing or instant messaging (Allen, 2017). Ransomware is a pervasive threat that has been growing for many years (Collier, 2017; Mansfield-Devine, 2016; Richardson & North, 2017). However, in the last few years, the growth of ransomware has proved nearly epidemic. For example, the WannaCry ransomware attack affected more than 100,000 organizations (Lelii, 2017). Another cyber-attack against more than 60 trusts in the United Kingdom's National Health Service bred violently to over 200,000 computers in over 150 countries in a very short time (Collier, 2017).

Further complicating the situation, ransomware attacks designed to target only a specific set of systems or technology can quickly expand out of control to hit the international and global stage, such as the Petya ransomware targeting M.E.Doc tax accounting software users in Ukraine, which landed in at least 64 different countries by the time it was stopped (Ghosh, 2017). These attacks caused chaos—facilities could not gain access to patient records, surgeries were delayed or canceled, and ambulances had to be diverted to different facilities. Just over 50% of trusts in the National Healthcare System (88 of 260) fell victim to ransomware for the last half of 2015 and well into 2016. Ransomware is a form of malware that can attack computers from many different avenues, such as users opening infected emails, users opening infected email attachments, users clicking on bad or malicious links, or by means of social engineering tactics like phishing or instant messaging (Allen, 2017).

3.2 The Evolution of Ransomware

While the public may perceive correctly that ransomware is a significant threat, it may also assume mistakenly that it is a new threat. However, ransomware is an established threat that has evolved over time. Ostensibly, the first appearance of ransomware was in 1989 when the AIDS Trojan, also known as the PC Cyborg, appeared

(Longstaff, 1989). This early ransomware virus was distributed on 20,000 5.25 disks to conference attendees at an AIDS conference hosted by the World Health Organization (KnowBe4, 2017).

The disks were labeled, "AIDS Information – Introductory Diskettes." A pamphlet was also included with the disks, stating that the disk could adversely affect other applications, that damages and compensation would be owed to the PC Cyborg Corporation, and that computers would cease to function normally (KnowBe4, 2017). Figure 1 depicts the original ransom notification screen.

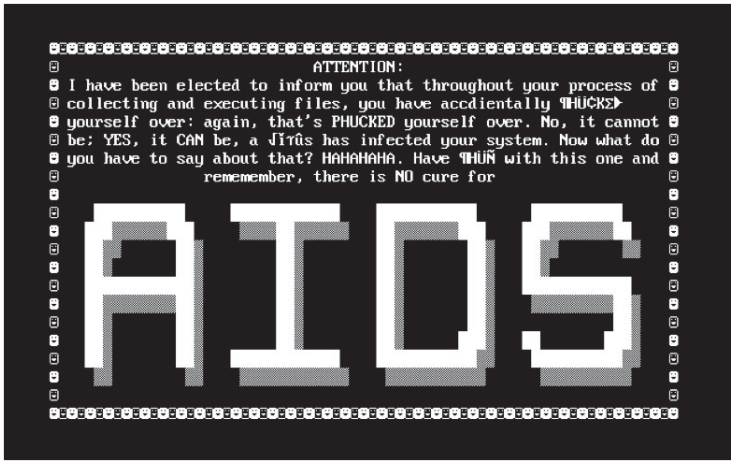


Figure 1. Original AIDS Trojan ransom notification, adapted from KnowBe4 (2017).

The AIDS Trojan kept track of the number of boots experienced by an infected machine, and on the 90th boot cycle, the ransomware locked or encrypted files and hid directories on the main hard disk. The process for regaining access to the system was for the owner to pay a ransom of $189 to the PC Cyborg Corporation in Panama. Tools were developed quickly to decrypt user data.

Ransomware has evolved over the years, with three general paradigms now seen most often: (a) locking up screens, (b) encrypting files, and (c) bluffs that have no real threat. In each case, the software asks affected users to pay a ransom in exchange for having the malware removed (Richardson & North, 2017). Ransomware is becoming more prevalent and now is the largest type of extortion malware attack (Symantec, 2016). The evolution of attack types can be seen in Figure 2, which includes data from the 11-year period of 2005 to 2016.

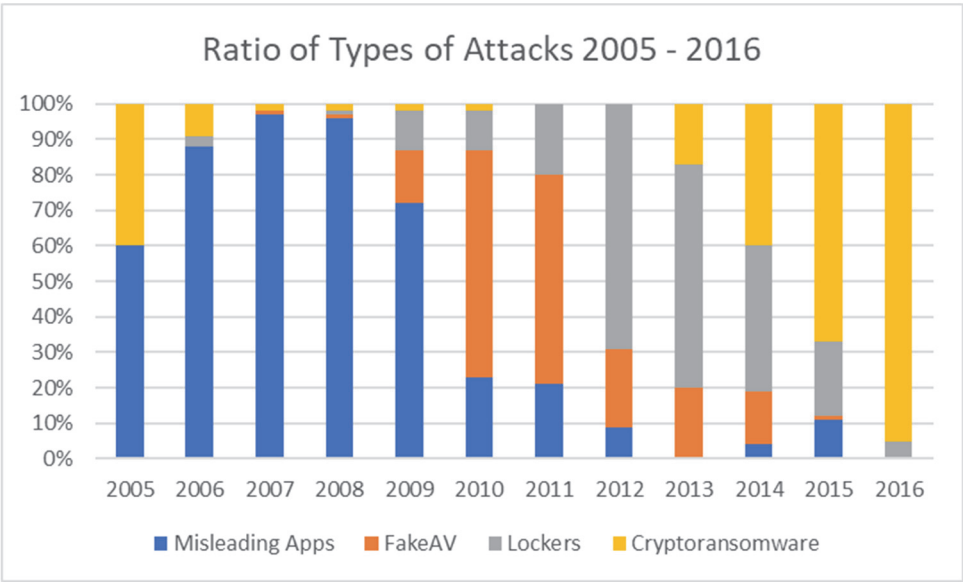


Figure 2. Ratio of types of attacks, 2005 to 2016, adapted from Symantec (2016).

The first major variant in deceptive user interaction that preceded modern ransomware was misleading applications,

appearing in 2005 as third-party spyware removal and system performance enhancement utilities (Savage, Coogan, & Lau, 2015). Programs such as SpySheriff and PerformanceOptimizer affected Windows PCs and Mac OS X machines. For $30 to $90, these programs offered to fix problems that often didn't exist. Later in 2005, a full transition occurred to crypto ransomware, and the first group ransomware threats resembling modern crypto ransomware appeared, such as Trojan.Gpcoder (Symantec, 2017).

The next phase of extortion malware attacks was fake antivirus (FakeAV) programs in 2008 (Savage, et al., 2015). These programs subjected users to specific misleading applications that were very aggressive (Majauskas, 2009). They displayed numerous errors and offered to fix them for $40 to $100. Some asked for fake multiyear subscription fees. Some users proved more sophisticated and removed the software, which lowered the return on investment (ROI) for FakeAV efforts. Figure 3 depicts a screenshot of the Nortel Antivirus FakeAV program.

Figure 3. Nortel Antivirus screenshot, adapted from Majauskas (2009)

Locker ransomware rose to prominence in 2011 to address the ROI challenges of FakeAV (Savage et al, 2015). Locker ransomware was more disruptive than FakeAV, with a definitive call to action. Locker ransomware "locked" users out of the computer by denying access to the computer. Additionally, locker ransomware had a higher price point for relief, generally charging from $150 to $200. The early dedicated locking malware programs were based on the Trojan.Randsom.C paradigm, spoofing itself as Windows Security Center, Microsoft Security Essentials and other valid OEM-based security tools (Richardson & North, 2017). Figure 4 is a screenshot of locker ransomware spoofed as Microsoft Security Essentials.

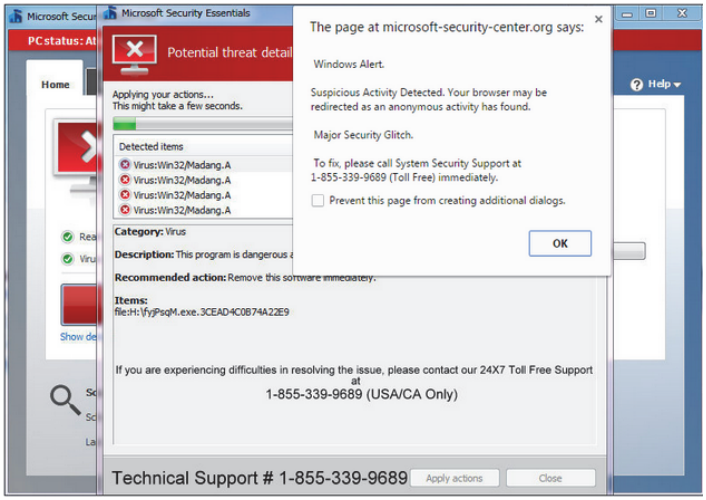


Figure 4. Screenshot of ransomware spoofed as Microsoft Security Essentials, adapted from Bilbao (2015)

Locker ransomware evolved from offering to remove fake errors to creating problems (Savage et al., 20150. Eventually, the facade was dropped altogether, systems were locked, and payment was demanded to restore access. Modern ransomware can be installed without user interaction, but social engineering is still prevalent as a means of enabling infection (Brewer, 2017; Savage et al., 2015). Once the pretense of fixing problems was dispatched, cyber miscreants became more bold and brazen: various storylines for attacks arose such as posing as law enforcement agencies, identifying illegal data on machines, and demanding instant payment of fines to restore access. Though locker ransomware was more effective than previous versions of extortion malware attack, it was still easy for savvy users to remove it with security software, added to the fact that general awareness of threats was growing (Savage et al., 2015).

The growing visibility of malware threats, known as path to removal, as well as need for a stronger value proposition (need to pay), led to the development of modern crypto ransomware. Since 2013, there has been a strong pivot back to crypto ransomware (Savage et al., 2015). In fact, crypto ransomware accounted for 95% of all extortion malware threats in 2016 (Symantec, 2016). When executed with sufficiently sophisticated encryption, victims do not have the option of freeing up their data in timely manner; they must pay the ransom or restore from backup (Thomas, 2017a). The average crypto ransomware request is about $300 per machine (Savage et al., 2015).

Ransomware that encrypts files is particularly debilitating to business firms (Brewer, 2017; Mansfield-Devine, 2016; Richardson & North, 2017). Encrypted files inhibit computer system ability to access the operating system, critical software, and important data (Collier, 2017). Once the system is infected, the ransomware spreads through network connections, shared credentials, and shared storage systems—essentially shutting down the infrastructure necessary to conduct business and process business transactions (Richardson & North, 2017). Experts suggest that comprehensive backup solutions compartmentalized by department and time are required to effectively combat ransomware (Lelii, 2017; Richardson & North, 2017). Compartmentalization does not imply that each department needs to have its own backup infrastructure and technology; indeed, a sprawl of that nature would debilitate the effective corporate response to a ransomware attack and may lead to less secure backup infrastructures, thereby increasing the risk for a widespread ransomware infection. Compartmentalization needs to exist within the enterprise backup infrastructure such that each department has its own set of backup definitions and save sets so that it is easy to identify which systems to restore and from which set of backups.

Enterprise backup solutions provide mechanisms to separate, in a manner similar to an “air gap,” the storage used by the backup system from the storage readily accessible by the servers themselves. Any storage that is readily accessible by infected servers is a target and can be violated; therefore, keeping the backup storage separate and distinct from normal user file storage is key to properly recovering from a ransomware situation.

3.3 How Ransomware Spreads

The process by which ransomware spreads consists of five individual phases (Figure 5 and Table 1) (Brewer, 2017). These phases move from initial exploitation of a secured network to encrypting data and making demands for payment. Each phase is distinct, but not every attack includes facets from every phase.

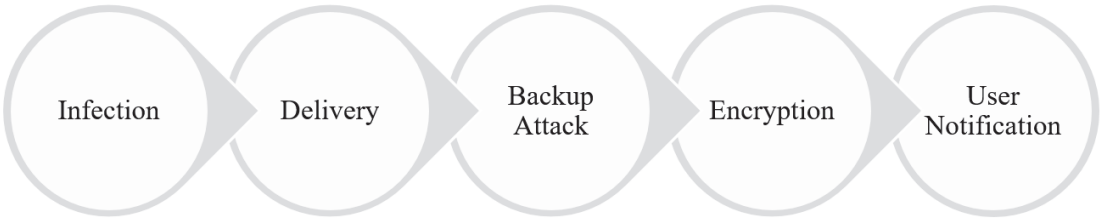


Figure 5. The ransomware process

Table 1. The Five-Step Ransomware Encryption Process

Phase	Name	Description
Phase 1	Infection	During this phase, the network of computing infrastructures is infected. Generally, ransomware makes its initial entry in the system by means of spam email, phishing attack, or an exploit kit. During this stage, the vulnerabilities of human users are exploited. Lapses in user awareness and training and failure to follow corporate

		security policy provide the ransomware entrance into the computing infrastructure (Allen, 2017; Brewer, 2017).
Phase 2	Delivery	Delivery and execution of the ransomware occurs in this phase by means of seeding an executable file into the initial system. Once the executable file is set, persistence mechanisms are established. These mechanisms alter the registry keys to protect the ransomware and hide it so that it is persistent and restarts itself, even after system shutdown. This enables the ransomware to encrypt files at a later date without requiring any other actions on the part of the user or the ransomware command-and-control center (Brewer, 2017).
Phase 3	Backup Attack	Shortly after delivery and execution, the ransomware looks for local backup data and deletes them. This prevents immediate backup as a resolution to the ransomware incident. This is a self-defense mechanism for the ransomware to ensure its effectiveness and to facilitate payment. Cryptolocker and Locky, two ransomware variants, execute commands to remove all shadow copies from infected systems. Other variants search for folders holding backup files and remove them (Brewer, 2017; Harnedy, 2016).
Phase 4	Encryption	After backups are removed and the stage is set, encryption begins. Additionally, the ransomware looks for network connections and for access to other systems that the user has access to write to. The ransomware starts the process of secure key exchange. During this step, encryption keys are established on the local system. Original forms of ransomware included the encryption keys as part of the application itself, making it very easy for security researchers to identify the encryption key and unencrypt the information for users. The encryption time required also varies based on computing infrastructure characteristics, such as file size, network characteristics, and number of connected devices (Allen, 2017; Brewer, 2017).
Phase 5	User Notification	During this phase, the ransomware notifies the user of infection, demands payment, and presents instructions for payment. Generally, the user is given a timeframe for payment, with escalating penalties/ransom payments for not paying. After the ransom is paid, the ransomware cleans itself from the system and tries to remove any evidence that might be identified by forensic investigators (Brewer, 2017; Lelii, 2017).

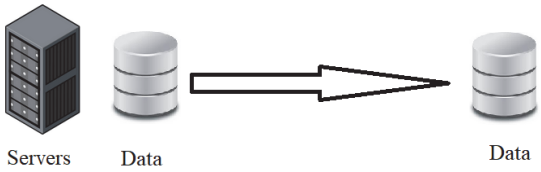
Though early encryption was simple, ransomware encryption evolved such that ransomware creators started to use a form of public-key encryption, which is much more secure and ensures that the encryption key can't be found on the system; that tended to be very slow, however, and was also easily defeated by stopping the ransomware in its tracks before it encrypted much of the system (Richardson & North, 2017). Ransomware has further evolved into a combination of shared-secret traditional encryption using fast algorithms such as the Triple Data Encryption Algorithm and Advanced Encryption Standard combined with a public-key system that encrypts the encryption key so it can't be found. This methodology has two basic paths: (1) using a command-and-control system to provide the public key to use to encrypt the shared-secret encryption key and (2) embedding the public key into the application itself. In the former case, the encryption cannot be truly secured (e.g., encrypting the shared-secret encryption key) until the system can connect with the command-and-control center, and in the latter case, all attacked systems will share the same public key so that once the private key is provided to users who have paid the ransom, the private key can then be shared for all others attacked similarly. Often, the system is tagged with a unique identifier given to the user for payment of the ransom. Encryption methods vary by the type of ransomware infecting the system.

3.4 Backup Paradigms

Backing up is the process of making additional copies of data so that they can be restored at another time (Laudon & Laudon, 2016). There are several processes related to data protection that business managers might consider backup. These include (a) traditional backup, (b) continuous data protection (CDP), and (c) replication. Each of these functions seeks to make data available when needed (Evans, 2014).

Traditional backup is the process of copying files, generally by means of a backup program to a secondary area and storage medium on a periodic basis, which is typically daily, weekly, and monthly (Evans, 2014). The data generated from these daily/weekly/monthly backups are then kept for a specific period of time, often as far back as seven years, depending on business requirements. This process creates an entirely new copy of the data at a specific point in time and can be used to reconstruct a system or its data back to that specific point in time. Backup

strategies generally look at two metrics, recovery point objective (RPO) and recovery time objective (RTO).



Backups make copies of data at a given timepoint to another location.

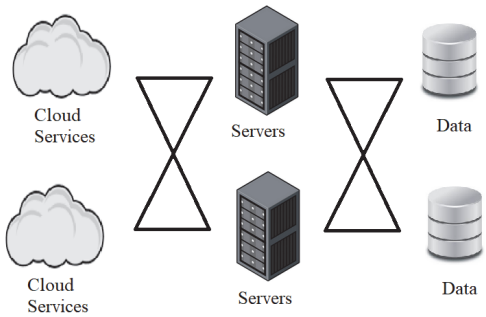
Figure 6. Diagram of traditional backup paradigm, adapted from Thomas (2017b)

RTO is the standard metric to determine the time it takes to effect a restore after an issue or event (Mugoh, Ateya, & Shibwabo, 2011). RPO refers to the point in the system's history or its state at a given time that needs to be restored, e.g., three hours ago (Mugoh et al., 2011). Together, these two metrics establish the business need for restoration/recovery. They answer the questions of how long it takes to get the system back up and what the system should look like when it returns to service.

Remote data replication, otherwise known as snapshot replication, which is often assumed to be backup, is the process of replicating a point-in-time state (snapshot) immediately or with a short delay over a distance (Evans, 2014). This process seeks to keep a current copy of the most recent data available in a geographically dispersed location, ostensibly for more rapid recovery in the event of a disaster. This strategy is commonly used in business continuity plans. However, in this paradigm, changes are replicated immediately. Files deleted or encrypted on the source will be deleted or encrypted on the target immediately or shortly thereafter. Consequently, this form of data protection should not be considered a backup, but rather a replication mechanism to support business continuity.

Another form of protection commonly equated with backup is CDP. CDP can be considered a more comprehensive form of replication, where the target seeks to keep track of all changes as they occur with a limited rollback period (Evans, 2014; Mugoh et al., 2011). However, because of the massive amount of detail required to keep track of these transactions, storage can very rapidly become very expensive. Like replication, changes in the source are quickly replicated on the target—including deletions, corrupt files, and ransomware-encrypted data.

Both of these forms of data replication support high availability, eliminating a single point of failure, and are entirely suitable for "business continuity" aspects of disaster recovery, but are not suitable as "backup" (Thomas, 2017b). Commonly, the data cannot be kept for an extended period of time, either on the source or the destination, if there is a high amount of data volatility due to the storage footprint required for extended periods. Because both these paradigms replicate deletions, defects, and infected data, they are unsuitable as a defense against ransomware.



Rather than copying data directly, high availability eliminates single points of failure with redundant equipment.

Figure 7. Diagram of high availability paradigm, adapted from Thomas (2017b)

3.5 NIST SP 800-30 and Ransomware

NIST SP 800-30 provides guidance for conducting information security risk assessments (NIST, 2017a). Within its pages, there is a myriad of information for security professionals, including types of threats, actions to take against threats, methods for determining risks, etc. However, NIST SP 800-30 does not contain the word

ransomware within its pages (NIST, 2017a). Table E-2 in NIST SP 800-30 identifies phishing attacks and spear phishing attacks as possible threat events. Often, these types of attacks, more commonly referred to as "malware," precede ransomware infection or can be the mechanism of a ransomware infection starting (Richardson & North, 2017). Malware is mentioned in NIST SP 800-30, but ransomware is not.

4. Discussion

One of the principal dangers of ransomware is that it takes advantage of access controls and storage file sharing to propagate itself (Richardson & North, 2017). Another issue with ransomware is that it can lay dormant for some time before activating (Brewer, 2017), meaning it can avoid detection until it has established enough of a foothold to prove significantly malicious. If data are being protected and stored for only a short period of time, as is the case with replication and CDP-based mechanisms, that data might be compromised because the threshold of snapshot retention is easily overrun and no record exists of a time without having the ransomware infestation (Thomas, 2017a).

For example, if a system using real-time replication were infected with ransomware, the ransomware would be replicated to the target immediately. If the ransomware then encrypted large amounts of storage on the system or all the data on the system, the "backup" created by that system of replication would be immediately transferred to the replicated data (Allen, 2017; Evans, 2014). The data encrypted by the ransomware would be the backed-up data, essentially making the backup useless because it would be encrypted and inaccessible, just like the original data trying to be protected or backed up. CDP would have the same problem, but because of its nature, CDP might be able to go back a few versions or a few hours. However, since ransomware rarely exposes itself immediately, seeks to prevent its removal, and propagates to other storage and systems, it is unlikely that anyone would notice the ransomware infection and take action in a few hours (Brewer, 2017).

This makes traditional backup a strong tool for dealing with ransomware once a system becomes infected (Allen, 2017; Lelii, 2017; Richardson & North, 2017). One can go back into many versions of backups, even as far back as a month previous. If someone gets infected by ransomware and they do not wish to pay the ransom, they can work to find a system state free of ransomware at a specific point in time. Once this point in time is identified, that system state can be restored and operations can resume free of the ransomware. The length of time to recover from a ransomware attack varies, but is ultimately tied to the amount of storage media (e.g., disk or tape) used by the backup system and, with more modern backup technologies, the rate of daily change (delta) in the underlying data itself. This change rate means that only those files changed each day are backed up, also known as an incremental backup. Incremental backup can also be used as a "canary in the coal mine" process: if an environment suddenly experiences a significantly higher change rate in a nightly backup, this is indicative of many more files being changed in that day than is considered normal, such as would occur during a currently undetected ransomware attack.

For these reasons, the author recommends that NIST SP 800-30 consider ransomware-specific threats a generalized threat, as it does phishing and malware, and that content be added to address ransomware specifically. Further, backup evaluations should consider the paradigm of backup (traditional versus replication versus CDP) so they can address this dangerous generalized threat. Also, although it is beyond the scope of this short work, other NIST publications related to SP 800-30 should be updated appropriately to address ransomware. For example, guidelines such as NIST SP 800-115, The Technical Guide to Information Security Testing and Assessment (NIST, 2017b), should consider adding ransomware-specific information.

The current version of NIST SP 800-115 suggests three types of assessment methods: interviewing, examination, and testing. Perhaps another type of interaction should be considered: best practices comparison. Where generalized threats, particularly in the information technology area, are known to exist, functions that operate against these threats might be compared against best practices. An example of this might be the backup paradigm discussion in this paper. Firms without the traditional backup paradigm and no multiple RPO strategy cannot rebuild data and systems to recover from a ransomware attack. They either have to pay the ransom or lose precious data and productivity (Evans, 2014; Mugoh et al., 2011). Traditional backup could be added as another method, or perhaps a specific tactic, under evaluation guidance.

4.1 Adding Rigor to Information Security Risk Assessments

Two categories that must be considered in ensuring the capability to properly respond to a ransomware attack include having an appropriate backup architecture and protecting the backup systems from ransomware infection and subsequent encryption. The backup system itself is also a potential target of ransomware attack and must be protected, as it is the tool ultimately required to respond to an infection and restore data (Brewer, 2017). Any strategy that backs up systems by means of a network file share is susceptible to a ransomware corruption of the

datastore. Even if the length of time that the datastore is mounted is kept as short as possible, an active ransomware attack can latch onto this newly mounted datastore and implant itself to be caught at a future time and then begin encryption again. In this way, more traditional backup paradigms, where data flow to a backup server that is the only machine with direct access to the storage, ensure that backups cannot be corrupted in situ. Of course, nothing prevents the traditional backup system from backing up already-encrypted data, but the mere presence of the backup system does not, in and of itself, prevent another attack from surfacing for the unsuspecting ransomware victim.

Because ransomware seeks to implant itself in a system, incubate itself for a period of time while simultaneously eliminating backup capability, and spread itself as far as possible in the infrastructure, a backup paradigm with sufficient RPO capability is necessary to restore the system back to the healthy state existent prior the ransomware infection (Allen, 2017; Brewer, 2017; Lelii, 2017; Richardson & North, 2017). The author recommends three levels of RPO guidance specifically for addressing ransomware restores. A minimum RPO, in the author's opinion, would ensure system restoration back to the state at least three days prior. A conservative approach would be to have the ability to restore system data up to 14 days prior, and an aggressive state would be to have the ability to restore a system state up to 21 days prior. Furthermore, for some systems, having a weekly or monthly "full backup" that is kept for even longer periods, such as 13 months to seven years, provides even more protection for some insidious situations where ransomware might go undetected for an extended period of time. Of course, it would be necessary to analyze the usefulness of data that old, as well as the cost to the business for the extended RPO, but in terms of recovery of old and possibly unsupported (by the primary vendor) systems that are critical to a function but cannot be upgraded due to point-specific applications, having an older backup of that unique technology might be acceptable.

Because of the need for point-in-time restoration, traditional backup methodologies based on full backups with incremental backups between full backups seems to be the best method for achieving the level of stability required to remediate a ransomware issue. Traditional backup paradigms create the ability to go back to any given day backed up and to restore a system to that state (Evans, 2014; Laudon & Laudon, 2016).

Thus data protection methodologies such as replication and CDP are often set up to create an immediate copy of the system or data to respond instantaneously to issues, and they have limited rollback capabilities (Evans, 2014; Mugoh et al., 2011; Thomas, 2017a). While these paradigms often have versioning capability, they are often limited to static images of a short-term retention period, with no long-term retention due to the high expense of storage media and system resources needed for operations and their general availability (Thomas, 2017b). Often, these paradigms operate with a round-robin methodology that does not catch changes between image periods, and versions are not saved after they roll out of utilization. For example, if the system makes weekly images on Mondays, and a file is created on Tuesday and then deleted on Thursday, the file will not show up on next Monday's weekly image. If the administrator is also performing daily images, they will have to know specifically which files existed on which day to try and find the item. This can be a great administrative challenge. Further, once the system is infected, it's very likely that replication and CDP images are infected as well, as they likely replicated the encrypted data instead of taking a copy of the file when it was originally created and storing it in a clean state as a traditional backup would (Evans, 2014).

Once a proper backup paradigm and backup system are in place, the backup system itself must be protected. Generally, the backup system can be attacked by means of network access, infected users having access to the backup system and its storage, and infected user accounts having write access to the backup system (Brewer, 2017). To mitigate this, system administrators must ensure that the backup system is secure. Only administrators should have access to the backup system. User accounts should not be able to mount storage from the backup system and should not be able to write or makes changes to the backup system or its storage. Network connections and storage sharing should only occur and be permitted when aboslutely necessary.

As an additional safety measure, if the backup system or companion technology keeps track of all of the backup metadata for an extended period of time, these data can be mined in a specific way that may just be able to identify a ransomware attack in its early stages. As a ransomware application starts to encrypt the data on the host system and over the network file system shares, it is, by definition, changing those files. The changed files are then copied as an incremental backup by the backup software. If enough historical metadata are available from previous backups of that same dataset on that same day, then as the backups complete a process to compare the sizes of the dataset, in terms of a trend analysis, backup operators can be informed in real time of any systems experiencing a higher-than-normal amount of incremental backups. That information can be relayed to the system administration staff for review and may point to a ransomware encryption attack in process.

While this isn't the main, or even secondary, reason for implementing traditional backups in the environment or as part of the rigor around the NIST SP 800-30 process, it is a side effect and benefit that—with the proper tools for capturing, analyzing, and reporting on that backup metadata in real time—is another justification for adding backups to the rigor around that process and standard. Other tools that detect file changes, such as tripwire, are insufficient to properly detect a ransomware attack because while they take "fingerprints" of files (or at least the file metadata such as size, owner, permissions, access/modify/change times), files are regularly accessed, and for any enterprise of sufficient size, there are files modified on the order of terabytes per day with just daily change rates. It would not be possible to analyze all of the individual files that changed each day from those tools in order to be an effective measure. Due to the aggregate nature of the backup technology and the metadata associated with it, using technology capable of capturing the metadata and analyzing trends in that data as a data warehouse application of sorts can provide yet another use for the backup technology and the large amounts of metadata that, today, largely are ignored. Any early-detection possibility is an added bonus for using such technology and capturing, analyzing, and reporting on the metadata.

4.2 A Tool for Additional Rigor in Information Security Risk Assessments

Table 2 depicts the Information Security Risk Assessment Backup System Evaluation Tool, a tool designed to enhance the rigor for information security risk assessment backup evaluations and to better enable security professionals to determine risk preparedness to combat ransomware. Further, as previously stated, ransomware should be added as a specific risk in NIST SP 800-30 guidelines. These items identified in the tool should be compared to industry best practices and the likelihood of a ransomware attack for the given environment.

Table 2. Information Security Risk Assessment Backup Evaluation Guide

1 Backup Factor	2 General Guidance	3 Success Criteria	4 Findings	5 Recommendations
Backup Paradigm	Does the backup paradigm allow full point-in-time restores?	The system must be able to restore fully to the previous state on a given day.		
RPO Capability	How far back can the backup system create a previous state?	Minimal = 3 days, Conservative = 14 days, Aggressive = 21 days		
Backup Server Access	Who can access the backup server?	Only backup administrators or those with legitimate need should be able to access.		
Backup Server Network Connections	Which systems can be connected to the backup system?	The backup systems should be isolated, and only systems with need should be able to be connected.		
Backup Server Storage Sharing	Can the backup storage systems be shared?	Backup system storage system sharing should be limited. Other systems should not be used as a "bridge" where unintended users can write the backup systems.		

5. Conclusion

This paper discussed adding rigor to information security risk assessments, specifically to NIST SP 800-30. Ransomware has been identified as one of the growing threats in the business community, with the potential to cause tremendous damage and representing 95% of extortion-based malware attacks (Mansfield-Devine, 2016; Richardson & North, 2017; Symantec, 2016). Ransomware can be addressed after it occurs with sophisticated backup strategies that utilize a sufficient time-delineated RPO restore point capability (Evans, 2014; Mugoh et al., 2011). Ransomware should be considered a generalized threat, and provisions should be made in the NIST guidance documents to help address it and remediate it once it happens. This paper presented a new tool for conducting backup system evalutations during information security risk assessments that will better enable auditors to effectively analyze backup systems and improve and organization's ability to combat and recover from

a ransomware attack.

References

Allen, J. (2017). Surviving ransomware. *American Journal of Family Law, 31*(2), 65-68. Retrieved from https://www.ncbi.nlm.nih.gov/labs/journals/am-j-fam-law/

Bilbao, B. (2015, April 8). *Microsoft-security-center.org removal manual*. Retrieved November 28, 2017, from Sensors Tech Forum: https://sensorstechforum.com/microsoft-security-center-org-removal-manual/

Brewer, R. (2017). Ransomware attacks: detection, prevention, and cure. *Netowrk Security, 9*, 5-9. http://dx.doi.org.ezproxy.utica.edu/10.1016/S1353-4858(16)30086-1

Collier, R. (2017). NHS ransomware attack spreads worldwide. *CMAJ, 189*(22), 786-787. https://doi.org/10.1503/cmaj.1095434

Evans, C. (2014). *Backup vs replication, snapshots, CDP and data protection strategy*. Retrieved from ComputerWeekly.com: http://www.computerweekly.com/feature/Backup-vs-replication-snapshots-CDP-in-data-protection-strategy

Ghosh, S. (2017, June 28). *The massive 'Petya' cyberattack has hit 64 countries so far and there's no kill switch*. Retrieved November 28, 2017, from http://www.businessinsider.com/petya-cyberattack-hit-64-countries-no-kill-switch-2017-6

Harnedy, R. (2016). *3 better ways to use backup to recover from ransomeware*. Retrieved from Barkly: https://blog.barkly.com/3-better-ways-to-use-backup-to-recover-from-ransomware

Jesson, J., Mattheson, L., & Lacey, F. (2011). *Doing Your Literature Review.* Los Angeles: Sage Publications Ltd.

KnowBe4. (2017). *AIDS Trojan or PC Cyborg Ransomware*. Retrieved November 28, 2017, from https://www.knowbe4.com/aids-trojan

Landoll, D. J. (2012). *The security risk assessment handbook: A complete guide for performing security risk assessments* (2nd ed.). [Kindle version]. Retrieved from Amazon.com

Laudon, K., & Laudon, J. (2016). *Management Information Systems* (14th ed.). Boston: Pearson.

Lelii, S. (2017). *WannaCry ransomware attacks shows value of data backups*. Retrieved from http://searchdatabackup.techtarget.com/news/450418934/WannaCry-ransomware-attack-shows-value-of-data-backups

Longstaff, T. (1989, 12 19). *Information about the PC CYBORG (AIDS) trojan horse*. Retrieved from http://www.securityfocus.com/advisories/700

Majauskas, G. (2009, September 2). *Nortel Antivirus - How to remove*. Retrieved November 28, 2017, from Viruses: https://www.2-viruses.com/remove-nortel-antivirus

Mansfield-Devine, S. (2016). Ransomeware: Taking business hostage. *Network Security, 2016*(10), 8-17. Retrieved from http://www.sciencedirect.com/journal/network-security

Mugoh, L., Ateya, I. L., & Shibwabo, B. K. (2011). Continuous datat protection architecture as a strategy for reduced data recovery time. *Journal of Systems Integration, 2*(4), 54-69. https://doi.org/10.20470/jsi.v2i4

NIST. (2017a). *Guide for Conducting Risk Assessments*. Retrieved from https://www.nist.gov/publications/guide-conducting-risk-assessments

NIST. (2017b). *Technical guide to information security testing and assessment*. Retrieved from NIST: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf

Richardson, R., & North, M. (2017). Ransomware: Evolution, mitigation and prevention. *international management review, 13*(1), 10-21. Retrieved from http://www.usimr.org/

Savage, K., Coogan, K., & Lau, H. (2015, August 6). *The evolution of ransomware*. Retrieved November 28, 2017, from http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-evolution-of-ransomware.pdf

Symantec. (2016). *Ransomeware and Business 2016*. Retrieved November 28, 2017, from Symantec Website: https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/ISTR2016_Ransomware_and_Businesses.pdf

Symantec. (2017). *Trojan.Gpcoder*. Retrieved November 28, 2017, from https://www.symantec.com/security_response/writeup.jsp?docid=2005-052215-5723-99

Thomas, J. E. (2017a, November 6). *Combating ransomware with traditional backups*. Retrieved November 28, 2017, from https://www.linkedin.com/pulse/combating-ransomware-traditional-backups-jason-thomas-phd/

Thomas, J. E. (2017b, November 30). *Is your backup a real backup? Part II: Combating ransomware with traditional backups*. Retrieved December 5, 2017, from https://www.linkedin.com/pulse/your-backup-real-part-ii-combating-ransomware-backups-thomas-phd/