Mountain Plains Journal of Business and Technology

Volume 21
Issue 2 *Focus on Technology*

Article 6

Date Published: December 2020

Ransomware - A Strategic Threat to Organizations

James Frost
Idaho State University, frosj@iri.isu.edu

Alan R. Hamlin
Southern Utah University, alanhamlin@yahoo.com

Recommended Citation

Frost, J., & Hamlin, A. R. (2020). Ransomware - A Strategic Threat to Organizations. *Mountain Plains Journal of Business and Technology, 21*(2). Retrieved from https://openspaces.unk.edu/mpjbt/vol21/iss2/6

RANSOMWARE - A STRATEGIC THREAT TO ORGANIZATIONS[1]

JAMES FROST
IDAHO STATE UNIVERSITY

ALAN HAMLIN
SOUTHERN UTAH UNIVERSITY

ABSTRACT

Ransomware is a strategic threat to government, business, and academic organizations. It has both short term and long term consequences, requiring strategic planning to create defenses, assess options, and create policies.

The purpose of the study is to answer three questions: What is the strategic risk of cyberattack to organizations? What are the current attitudes and practices of executives who are vulnerable to such threats? What are specific options that organizations should consider to prevent and deal with possible incidents in the future? The article is thus comprised of the following components: A) a history of the development and complexity of ransomware; B) a survey of IT professionals in government, business and education; and C) recommended strategic options for organizations to defend against cyber threats.

We conducted a survey of ninety-two cybersecurity professionals in government, education, and business. Attitudinal divergence occurred in the areas of cyber-defense, perpetrator negotiations, ransom payment, and involvement of law enforcement. The authors recommend thirteen specific solutions to assist organizations when dealing with ransomware.

Keywords: ransomware, cyber security, cyber strategy, password protection, data breach

INTRODUCTION

In a 2015 discussion, Cheri F. McGuire of Symantec identified a series of vulnerabilities that would rapidly expand. They included data breaches, mobile and social environments, ransomware, cyber-espionage, and the "Internet of Things" (McGuire 2015). These observations paralleled a study by IBM Security that found that attackers focused on "inflicting physical damage, stealing intellectual property and lodging political protests" (Security 2016). The primary effects are still cybercrime and hacktivism. This paper deals with cybercrime as a rapidly growing threat fueled by ransomware (as a part of advanced persistent threats – APT) that have expanded greatly since the year 2000. The problem is so serious that, in certain vulnerable industries, "over 70% of companies hit by ransomware attacks are out of business within six months (Kon 2017), while those which survive can lose millions of dollars (Fitzpatrick and Griffin 2016).

REVIEW OF THE LITERATURE

Significance of the Problem

[1] Submitted: 8 Jan 2020; Revised: 27 Jun 2020; Accepted: 20 Sep 2020

On April 25, 2020, ATM maker Diebold Nixdorf discovered a ransomware attack on its IT systems. The company was one of many government and private organizations that were hit by ProLock, a ransomware related to PwndLocker that demanded ransoms between $175,000 and $660,000 each (Kovacs 2020). Fortunately Diebold was able to quickly restore service and inform law enforcement. Others are not so lucky.

Ransomware is not a new threat. Justin Pope provided a historic link to what was probably the first occurrence. "The first ransomware virus was disseminated almost 30 years ago when Dr. Joseph Popp, a World Health Organization consultant and AIDS researcher, mailed 20,000 informational floppy disks containing ransomware to a group of international conference attendees. The virus encrypted computer files and demanded that the victims send $189 to a physical mailing address" (Pope 2016). Ransomware is malware (software that damages or allows unauthorized access to computer systems) that creates a form of digital extortion for users that is often delivered by a Trojan Horse (Heartfield and Loukas 2015). It usually requires a digital payment to the extortionist after which the users are provided a key to unlock files that are encrypted. There is also a strong financial reason to distribute ransomware. According to SentinelOne, hackers behind a ransomware family called CryptXXX collected over $50,000 in three weeks (Fenton 2016). The Federal Bureau of Investigation (FBI) estimated that $209 million in ransom payments were made in the first three months of 2016 (Fitzpatrick and Griffin 2016). It continues today. On July 19, 2020, the computer servers at the College of Social and Behavioral Science at the University of Utah were hacked, rendering them "temporarily inaccessible." This resulted in the university paying over $457,000 in ransom monies to the "unknown entity" who attacked it (Pierce 2020).

The chances of a hacker being discovered, prosecuted, and penalized for conducting a cyberattack are low due to several factors. First, many ransomware payments are relatively small but distributed over many organizations, so the victim will often not report it. Second, the payments are hard to track due to the use of crypto-currency. Lastly the companies are reluctant to publicly admit that they were hacked. These factors result in the unintended consequence that many groups, and even governments, effectively incentivize criminals to take the risk even for relatively small amounts of money. The highly publicized WANNACRY ransomware shows the potential for new sets of hackers to adopt this vector of attack. "As the WannaCry ransomware epidemic wreaked havoc across the globe over the past three days, cybersecurity researchers and victims alike have asked themselves what cybercriminal group would paralyze so many critical systems for such relatively small profit. Some researchers are now starting to point to the first, still-tenuous hint of a familiar suspect: North Korea" (Greenberg 2017).

In the last few years, ransomware has become sophisticated and malignant. According to *Best's Review*, "Ransomware tools are increasingly being used to cripple operations and spread rapidly, resulting in the potential for massive business operations and property damage on a global scale" (McNicolas and Cunningham 2017). Companies not only have to consider the cost of building a firewall to protect against such threats and then respond to them if and when they occur, but many firms are also now buying stand-alone insurance in the event they are attacked.

Some nation-states (e.g. North Korea) are beginning to take advantage of personal and small accounts instead of focusing on power infrastructures, banks, and military organizations.

This is becoming a training environment for novice hackers that are honing their skills to prove their merit for their country. Small successes in hacking can provide confidence and experience to move an individual from apprentice to master craftsman (cyber ninja). Foreign nation-states have established training camps in their military organizations and are frequently seeking and attacking foreign resources (Greenberg 2017).

Experienced and financed computer hackers are distributing ransomware for the purpose of developing cash flow; in essence, they're creating and running a business. Their well-defined targets, via pretexting, use a form of "spear phishing" to accomplish their goals. They are conducting business analysis to determine the viability of exploiting the discovered vulnerabilities of potential targets and leveraging that vulnerability to their advantage. The developers of ransomware also continue to develop and mature their attacks to expand the impact of the attack and thus increase the likelihood of payment.

The primary industrial targets in the U.S. in 2015 were healthcare, manufacturing, financial services, government, and transportation (Security 2016). These targets usually adopt a strategy of maintaining a risk averse posture and having "deep pockets" to meet any ransom demands. This is because most are required by law to maintain privacy of their client records. For example, a ransomware breach of a healthcare provider's computer system adds the risk of losing files that are protected by the Health Insurance Portability and Accountability (HIPAA), which could result in a federal fine and negative publicity. Under guidance released in July 2016, the Department of Health and Human Services now presumes that a ransomware attack compromises electronic PHI (public health information)—unless the HIPAA-covered entity can demonstrate otherwise (McHale et.al. 2016). This provides further motivation for the healthcare provider to resolve the issue quickly.

Regardless of the industry or company involved, ransomware is very lucrative as a business model for cybercriminals/hackers. Datto's 2016 survey showed that 42% of those small businesses hit by ransomware paid, even though many of them did not get their data back (Hackman 2017).

Strategic Risk Management Options

The organization faces several options after a ransomware attack. *NIST Special Publication 800-39: Managing Information Security Risk* (2011) defines four approaches to managing risk. The organization may pursue acceptance, avoidance, mitigation, or transference of risk.

ACCEPTANCE. There is a level of acceptable risk in any organization defined by the culture of the organization. Acceptance is "taking your chances." Acceptance is often the norm for cyber protection as organizations do not define or execute a strong plan of response prior to a malware attack. Acceptance (doing nothing) implies that there is a rationale for accepting certain risks. Every organization faces multiple sources of risk in doing business, and therefore must determine which risks require action and which to ignore, based on likelihood of occurrence and impact on the firm. Some level of risk is acceptable. Risk posture, economic viability, and corporate culture guides risk posture, as some organizations are risk averse (such as banking and finance) while others trend to exhibit a higher risk tolerance (often smaller businesses or organizations that perceive they are not vulnerable).

AVOIDANCE. Avoiding the risk means to conduct business in a manner that there would be no chance of being exposed to a cyberattack. This option is getting more difficult every year, with more employees using their own hardware, working from home, and/or operating under "free address" or variable work stations. Since this alternative would require either going out of business, operating without electronic devices, selling the company and taking profits, or merging with another firm that has extreme access to firewalls and protections, this alternative is not viable for most companies.

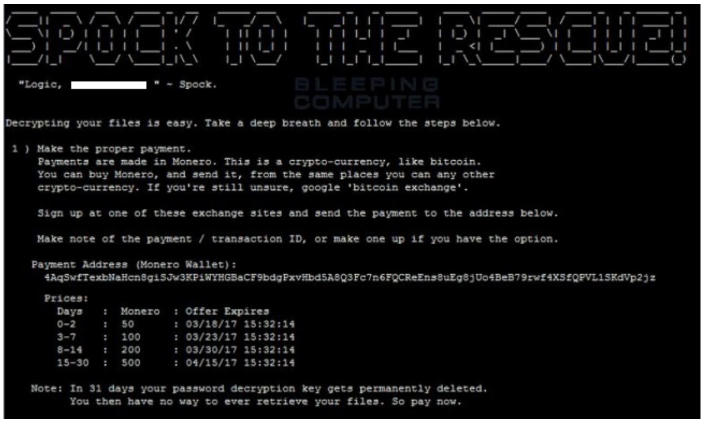
MITIGATION. This means reducing the risk of exposure and loss. For example, the organization may wish to attempt to reverse the encryption executed by the ransomware. The measure of success with this approach may not be successful, however, since the strength of encryption varies with the hacker. For example, it can range from elite encryption to "a poorly executed simple symmetric key cypher to a complex RSA 4,096-bit encryption" (Liska and Gallo 2016). However, criminals make mistakes and sometimes the decryption key is stored in the malware's source code (apparent with the WANNACRY attack). Then the decryption might be a less difficult matter, given time.

Several methods of mitigation are described at the end of this paper; however the strongest response to ransomware is to back up all files often to multiple sites (on-site, off-site and cloud) prior to the breach. It is important to avoid shared drives. These are encryption targets as well. Unfortunately, it is time consuming to store backups in isolated, independent areas. Data backups must be repeated often, with serious intent and testing to insure they are restorable and safe. The backup methodology should be versioning, not incremental. This prevents malware-laden files from over-writing clean files. It provides a safe return to point for the organization. However, it is required that the backup version be on an isolated (not shared) storage device. The very strongest risk mitigation tool is the education, training and creation of an employee awareness to the ransomware threat.

TRANSFER THE RISK. Also called "shifting the risk," the organization can transfer the cost of the ransom and related expenses by purchasing insurance. The organization still gambles that the ransom agents will provide a valid key to decrypt the files; however, the organizations act under the comfort that any ransom expenses are reimbursable. The cost of insurance for future events are dramatically higher without indications of enhanced protection of the cyber assets of the organization. According to the Organization for Economic Co-operation and Development, the market for such insurance in 2016 was over $3.5 billion. With the new EU General Data Protection Regulation taking effect in mid-2018, the worldwide market for cyber-insurance was projected to reach $25 billion by 2020 (McNicholas and Cunningham 2017).

How It Works

As an obvious alternative, after the ransom payment (typically ranging from $300 to $1,000 per infected storage device, usually made in Bitcoin or another digital media), a key for the encrypted device is provided. Note in Figure 1 (a screen capture of an infected machine), the ransom increases as time passes. This has become another social engineering technique, depending on time as a factor to hasten a decision. In the ransom note below, the “monero” price doubles very quickly. This decision is a business option incorporated into a disaster recovery plan. It is important to plan for such an action before the incident to avoid a decision made in panic mode under high stress.



```
 "Logic, [redacted] " ~ Spock.

Decrypting your files is easy. Take a deep breath and follow the steps below.

 1 ) Make the proper payment.
     Payments are made in Monero. This is a crypto-currency, like bitcoin.
     You can buy Monero, and send it, from the same places you can any other
     crypto-currency. If you're still unsure, google 'bitcoin exchange'.

     Sign up at one of these exchange sites and send the payment to the address below.

     Make note of the payment / transaction ID, or make one up if you have the option.

    Payment Address (Monero Wallet):
      4AqSwfTexbNaHcn8giSJw3KPiWYHGBaCF9bdgPxvHbd5A8Q3Fc7n6FQCReEns8uEg8jUo4BeB79rwf4XSfQPVL1SKdVp2jz

      Prices:
        Days   :  Monero  : Offer Expires
        0-2    :  50      : 03/18/17 15:32:14
        3-7    :  100     : 03/23/17 15:32:14
        8-14   :  200     : 03/30/17 15:32:14
        15-30  :  500     : 04/15/17 15:32:14

    Note: In 31 days your password decryption key gets permanently deleted.
          You then have no way to ever retrieve your files. So pay now.
```

Figure 1 - Star Trek Ransomware

The decision to pay the ransom and receive the key for the encrypted files is viewed as the organization “doing nothing” to avoid the situation (acceptance). The first or “gut” reaction of many CEOs is an emphatic NO to the payment of the ransom. However, this illustrates the advantage of having a strategic disaster recovery plan in place prior to the attack. Cooler heads need to prevail in the time of a stressful ransomware cyberattack. Often it is advantageous to have a cybersecurity firm hired as a management consulting aid to help with strategy and decisions in preventing and responding to ransomware attacks. Diebold Nixdorf used this tool effectively in dealing with the ATM problem in April 2020 (mentioned earlier), and paid no ransom (Kovacs 2020). It is important to recognize that there is no guarantee that the criminals will provide a valid decryption key. Dave Packer is quoted as saying “that a recent consumer survey found more than one in three ransomware victims ultimately pay up, despite the fact that nearly half of the victims don't get their files back anyway”(Olenick 2017).

Using Bitcoin or other crypto-currency as payment makes the transaction anonymous and very difficult to trace. Further, the FBI shows little interest in pursuing thefts or ransoms under six digits. Local law enforcement can make a report. However, it would be rare that they would have the resources to pursue the criminals. Most of the reports reviewed indicated the ransom key was delivered and effective upon payment. There is a problem with trusting these reports since many organizations are unwilling to admit that they made a payment without receiving a valid key in return. Since the payment is made to an anonymous entity, there is no advantage to the hacker to “build their reputation” by doing the honorable thing. Interestingly, it has become prudent for a cyber thief to provide a real key to the organization to decrypt the files once the ransom is received. There are reports of cyber criminals retaliating against fellow ransomware hackers when they failed to provide a valid decryption key. This may indicate a developing culture of “honor among thieves.”

Finally, one major defense is strong and current technology. However, this is not enough, by itself, to assure safety from cyber threats. All three dimensions of the Maconachy, Schou, Raggsdale (MSR) model of countermeasures must be employed to effectively reduce an organization’s vulnerability to cyberattacks. Threats and vulnerabilities are morphing rapidly, and most organizations exist in an open environment. Threats continue to grow from neophytes (operating under the umbrella of Ransomware as a Service – RaaS) to experienced and deeply-financed hackers. Further, some risk is internal, not external. For example, improper employee behavior on computer systems actually causes a majority of all cybersecurity violations (Kon 2017).

This perplexes traditional law enforcement in their efforts to pursue and apprehend the criminals. The traditional thought of "follow the money" to find the perpetrator is confounded by the use of payment via Bitcoin, which is anonymous. In addition, these funds often buy a variety of untraceable products like drugs, prostitutes, or other illegal activities.

Strategic Notes

As a final note for an organization's consideration, there could be reporting requirements. A health care organization could have to file a Health Insurance Portability and Accountability Act (HIPAA) compliance report. An educational institution may be required to file a compliance report under the Family Educational Rights and Privacy Act (FERPA). Other organizations may be legally obligated to respond to the law described under Sarbanes Oxley (SOX) or Gramm-Leach Bliley Act (GLBA). Although the encrypted files are still on the storage devices, they are under the control of the ransom agents, not the organization.

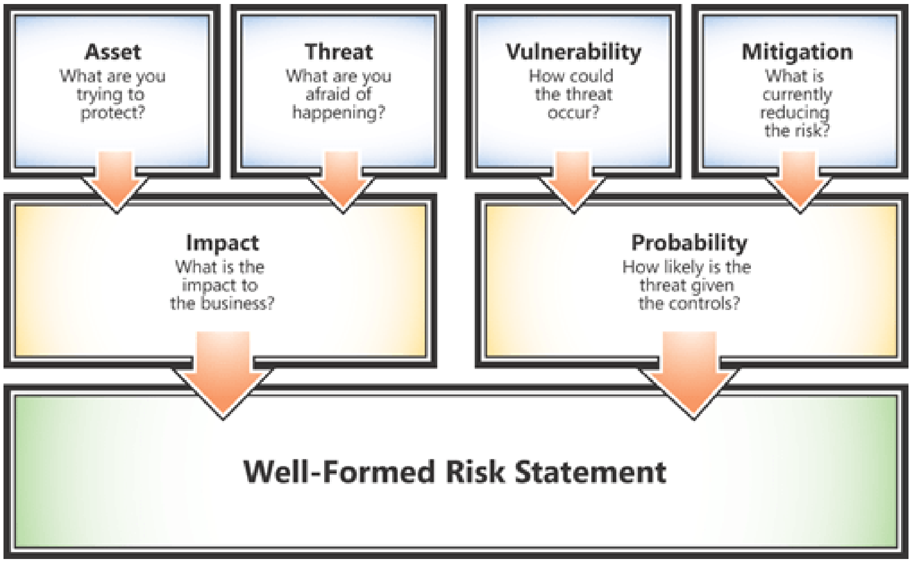

Asset
What are you trying to protect?
Threat
What are you afraid of happening?
Vulnerability
How could the threat occur?
Mitigation
What is currently reducing the risk?
Impact
What is the impact to the business?
Probability
How likely is the threat given the controls?
Well-Formed Risk Statement

Figure 2 - Developing A Risk Statement (from Microsoft)

Tim Rains of Microsoft suggests that corporate management needs to examine the risk associated with the threat category (Rains 2016). To build a well-informed "risk statement," he suggests looking at risk as a combination of probability and impact. The evaluators (strategic planners) should first determine what assets are in need of protection. Different organizations will identify different assets of different values to protect. For example, is the organization interested in protecting data, reputation, or trade secrets and patents? The threat under consideration is a ransomware attack (although organizations must consider all attacks). As the group looks at the issue of vulnerabilities, the critical attack vector is usually the human element via a Trojan Horse. However, there are other considerations, as well, such as unpatched infrastructure and the schedule and methodology of backing up files. Finally, how is the risk mitigated or eliminated? The flow chart in Figure 2 above illustrates the systematic process to constructing an effective risk statement.

ANALYSIS OF SURVEY OF IT PROFESSIONALS

The authors administered a twenty-five-question survey to cybersecurity professionals (see Appendix 1). The response rate was 35% (ninety-two respondents). The results indicate the need for additional training and education. Ninety one percent of the participants were from IT departments in education, followed by government and business. Many of those in education had come from the private sector. Interestingly, ten of the participants experienced a successful ransomware attack. The respondents were aware that the principal attack vector was to healthcare providers. A follow-up question (question ten) indicated that although they recognized healthcare as a target, 38% did not realize that a successful ransomware attack at a healthcare provider creates a HIPAA violation. As mentioned previously, this enhances the potential loss to the organization as it is now possibly subject to Health and Human Services (HHS) fines, penalties, and reports on top of the costs to restore files and the possible payment of a ransom.

There is some variation as to perceptions about just what ransomware actually is. Question two asked whether ransomware was a virus, social engineering, a worm, or a Trojan Horse. Responses showed that most (37%) thought it was a virus, while 31% percent thought it was social engineering and 20% a Trojan Horse. The remainder believed it to be a worm.

Question six asked the respondents about what threats their employers were emphasizing in their organizations. Ransomware led the list with 42%, followed by hacktivists (30%), industrial espionage (16%), and cyber war (11%). Since ransomware has become so prevalent, it is good that employers are giving it more attention than previously.

Question twelve asked about what elements made an organization most vulnerable to an attack by cyber criminals. Correctly, 97% indicated that the "human element" was the weakest link, followed by software (2%), storage devices (1%), and routers (0%). Having this understanding is critical for organizations, in that providing training and practices (such as clean desk policies) can minimize the risk of such an attack.

Questions fourteen and fifteen were scenario-type questions. The scenario was, "You are the System Administrator for a hospital, with a risk averse culture, and you have twenty-five drives encrypted. A ransomware screen is demanding payment of $300 per computer. It will take $7000 of labor to restore the backup files with no guarantees that the backups are not infected. The hackers provided a key to decrypt one computer as a show that their key will function. Which of the following would you implement?" Responses ranged from "contacting local law enforcement and the FBI" (79%) to "pay the ransom before the cost increases" (11%), "attempt to restore the files from backups, then decrypt, then pay ransom" (5%), and "attempt to decrypt the files, then attempt to restore the files, then pay ransom" (4%). It is interesting that the first impulse is to contact law enforcement, even though the chances of them actually catching the perpetrators and getting the money back is very remote. Again, this illustrates the need to have a plan in place to deal with cyberattacks *BEFORE* the incident occurs.

The participants strongly agreed in answering a question dealing with encryption of files to thwart a ransomware attack. They were nearly unanimous that the weakest link of the information system in a ransomware attack is the human element. However, it is disappointing that half of those surveyed did not include in their disaster recovery plan (DRP) any guidance or training to deal with ransomware. When a successful ransomware attack occurs, it is past the time to call a planning meeting. Decisions made under stress can lead to greater expense and further problems. The individuals distributing ransomware are conducting the attacks as a business. Likewise, organizations must conduct a financial analysis to outline steps to guide their actions. The plan must include options and alternatives depending on the status of the attack. As a business decision, the individuals experiencing the attack must realize that the ransom usually goes up in price daily if they delay or are unsuccessful in decrypting the files. These alternatives should include:

- Guidance as to whether or not to pay the ransom and the timing of the action. This would include how the organization would use a crypto currency to make the payment. A decision tree of steps and options will guide employees during this issue. A comprehensive cost benefit analysis is required to address the needs of the organization depending on the multiple scenarios of damage to the organization's system.

- Coordination with information technology (IT) employees to attempt to decrypt the files and ***find the point of entry for the hackers***. The concept of encryption techniques may require additional training. However, there are very good massive open online courses (MOOCs) available to provide guidance. As other hackers adopt the ransomware methodology, some are intentionally including the decryption key in the source code so they have the ability to decrypt the files.

- As laws and organizational vulnerabilities change over time, the guidance for contacting law enforcement requires review.

- The reporting implications of a business requires evaluation and definition ahead of time. Is the healthcare organization subject to the requirements of Health and Human Services under HIPAA requirements? Have Sarbanes-Oxley (SOX) requirements for business organizations been met? If this is an educational institution, does the college or university meet the Department of Education guidelines for protection of data under the Family Educational Rights and Privacy Act (FERPA)? Credit card organizations are subject to the laws of Payment Card Industry (PCI) regulations. Other industries have similar laws and regulations.

This list demands a review and modification annually as the environment changes.

Crosstab Analysis of Selected Questions

An investigation via crosstab analysis compared responses based upon whether the individual experienced a successful ransomware attack versus those that did not experience a successful attack. We compared those two groups with respect to responses for questions fourteen, fifteen, sixteen, nineteen, twenty-three, twenty-four, and twenty-five.

Question fourteen states: "You are system administration for a hospital (risk averse culture) and you have twenty-five computers encrypted. A ransomware screen is demanding payment ($300/computer); which single option would you follow? It will take $7,000 of labor to restore the backup files, with no guarantees that the backups are not infected. The hackers provided a key to decrypt one computer to show that they can indeed restore the data they stole." The following table displays the responses into true and false experiences with a ransomware attack.

Table 1: Ransomware payment choices

RESPONSE TO Q14	COUNT	PERCENT
Pay the ransom before the cost increases	10	12%
Attempt to restore the files from backups, then decrypt, then pay the ransom	5	5%
Attempt to decrypt the files, then attempt to restore the files, then pay the ransom	4	4%
Contact local law enforcement as well the FBI	73	79%

Only ten individuals responded that they experienced a ransomware attack. Of the ten respondents, 80% indicated that they would contact the FBI while 22% said they would pay the ransom immediately. Those that did not experience a successful ransomware attack also predominately indicated they would contact the FBI.

Question Fifteen states: "Given the same disaster scenario, you are system administrator for a hospital (risk averse culture) and you have twenty-five drives encrypted. A ransomware screen is demanding payment ($300/computer); which single option would you follow? It will take $7,000 of labor to restore the backup files, and no guarantees the backups are not infected. The hackers provided a key to decrypt one computer as a show that their key functions. Which of the following steps (a. b, c or d) would you implement?"

Table 2: Ransomware payment scenarios

RESPONSE TO Q15	COUNT	PERCENT
Call FBI, contact local law enforcement, attempt to decrypt the files, restore the files from backup, pay the ransom.	78	88%
Attempt to decrypt the files, restore the files from backup, pay the ransom	3	3%
Attempt to restore the files from backup, pay ransom	0	0%
Pay the ransom	8	9%

Both groups liked the choice of the multi-step option of contacting the FBI first, then local law enforcement, followed by restoration steps.

Question sixteen dealt with the payment for ransomware. Both groups recognized that Bitcoin was the preferred method of payment as shown below:

Table 3: Payment vectors

RESPONSE TO Q16	COUNT	PERCENT
PayPal	3	3%
Digital coin (Bitcoin)	85	93%
Western Union	4	4%
iTunes card	0	0%

Question nineteen dealt with inclusion of a ransomware strategy (in case of a ransomware attack) in the organization's disaster recovery plan (DRP). This question shows a descriptive difference between the two groups (attacked by ransomware and not). Whereas 70% of the attacked respondents had a plan that included ransomware considerations, only 47% of the not-attacked group included ransomware in their DRP (Table 4). The respondents not attacked with ransomware responded equally on their inclusion of a DRP response to ransomware or not:

Table 4: Inclusion in DRP

RESPONSE TO Q19	COUNT	PERCENT
TRUE	42	47%
FALSE	45	53%

Question twenty-three deals with the issue of whether the inclusion of a clean desk policy should be adopted in every organization. Surprisingly, although virtually all experts and cyber-threat groups encourage organizations to adopt this policy to reduce espionage and cyber theft, it seems to be perceived as less important, as neither group showed a strong policy orientation on this issue, as shown below in Table 5:

Table 5: Clean Desk Policy

RESPONSE TO Q23	COUNT	PERCENT
TRUE	20%	29%
FALSE	80%	71%

Questions twenty-four and twenty-five are not ransomware-focused questions. Question twenty-four shows that very few respondents use a short password, which is a desirable quality in any organization. In addition, approximately 80% are using passwords between eight and eighteen characters (Table 6). It is interesting that 70% (true) and 58% (false) utilize passwords longer than twelve characters.

Table 6: Password Length

RESPONSE TO Q24 (# of characters in an important password)	COUNT	PERCENT
1-7	1	1%
8-12	37	40%
13-18	41	45%

>19	13	14%

Responses to questions twenty-four and twenty-five (see Table 7) indicate two things: First, a lack of knowledge that special (cryptic) characters are not a deterrent to hackers. Second, that password length is one of the most critical factors in preventing hacking behavior. A contributing factor to this perception is system administrators that require special characters for passwords, thereby forcing users to include special characters. The inclusion of special characters does not make it more difficult for a hacker to access private files of an organization, especially when using a program like Aircracker or Crowbar (not to mention more sophisticated hacking programs). Raising awareness of administrators, managers, and users on the importance of emphasizing the length for a secure password is a critical issue.

Table 7: Inclusion of Special Characters

RESPONSE TO Q25	**COUNT**	**PERCENT**
True	84	92%
False	7	8%

Crosstab Summary

The crosstab analysis of questions fourteen, fifteen, and sixteen revealed little difference between the two groups in their attitudes toward ransomware responses. Although not a focus of this survey, one author's personal interactions with FBI agents indicates that organizations are hesitant to contact the FBI after cyberattacks. The strong response to inform law enforcement may be an academic response (this is what we theoretically do) rather than an industry response (this is what happens in the real world). We note parallels to organizations not reporting security breaches to a lack of industry filings to the SEC, although such reporting is required.

There appears to be a difference in these two sets for questions nineteen, twenty-three, and twenty-five. These questions do not compare ransomware issues specifically, but just general security issues. In question nineteen, the largest group of respondents (not having experienced a ransomware attack), were split evenly on whether they included a response to a ransomware attack in their DRP. It appears that too many organizations are not planning for a very-likely event (a successful ransomware attack). In addition, question twenty-three shows a disturbing lack of inclusion of a clean desk policy in their organization. A clean desk at the end of a workday is a strong security policy to adopt in any organization to combat espionage and cyber theft.

Finally, question twenty-five indicates a need to raise the awareness of system administrators, managers, and users to the importance of password length over the use of cryptic special characters. The computer is not confused with the inclusion of special characters since cracking a password involves all characters equally, whether numeric, alphabet, or special character. Further, adding special characters makes it more difficult for human users to adopt the policy and remember their passwords. A simple acronym is just as powerful. For example, using a password like "mfmotyi06" is easily remembered as "my favorite month of the year is June."

We suggest that all organizations adopt a clean desk policy to minimize desktop theft of valuable data, both during and after work hours. In addition, it is important to remove the misguided policy of special characters in a password and replace it with the use of long passwords and the adoption of passphrases. These last two techniques assist in creating a strong password environment. The organization may also wish to raise the awareness of its users of the advantages of a password manager and/or the use of a vault to store multiple passwords instead of using the same password for all protected resources.

STRATEGIC OPTIONS AND RECOMMENDATIONS

Potential strategic actions to reduce the effect of ransomware include:

1) Educate employees with innovative educational techniques that include hands-on activities rather than just a list of do's and don'ts. It is important to act and raise the awareness of employees as well as provide training in security methods. There needs to be random, unannounced drills and teaching tests of employees using ransomware techniques. This would include a well-developed feedback scenario to provide confirmation of the results of each ransomware vector in the organization. A memorandum of understanding between the chief executive officer (CEO) and the systems administrator needs to be defined to identify expectations and actions to be taken during the drills and teaching tests.

2) Backing up data is a principle action to employ prior to the breach. See the previous discussion that requires infrastructure security actions. This includes the use of version control, not just incremental backups.

3) Users should run their computer in a user mode, not supervisor or administrator mode. This will prevent some programs from running on a user's computer without their acknowledgement.

4) Autorun should be disabled for media (see above).

5) Top management establishes risk mitigation methodologies as a corporate responsibility. End users implement these methodologies in a top-down approach.

6) The review of the disaster recovery plan (DRP) is an annual event. This DRP guides actions when the breach occurs. DRP guidelines are proactive, not reactive. This DRP includes defined actions to deal with the effects of ransomware attacks.

7) The organization should restrict or definitely scan all email attachments for malware (a primary vehicle for the attack). This is a control issue for the systems administrator in charge of email. This may require a group policy object (GPO) to block older versions of Microsoft products (Word, Excel, PowerPoint) that permit the macro programming language. Newer versions of Word files include a docx extension to indicate this file does not allow macro programming. It is up to the organization to determine what actions will be permissible for Adobe Flash on the user's computer.

8) Honeyfiles (a honeypot of files) can lure the attacker into a controlled area. When the systems administrator notes (via an automated hash table review) encrypted files, the system administrator can quickly stop the encryption chain from proceeding further. Another option is to create a honey-directory that can keep the ransomware busy until the administrators can take corrective action.

9) Patching of discovered infrastructure vulnerabilities require patches in real-time, along with regular updating of software. The lack of patching on a regular basis is an issue that still plagues organizations. System administrators should be required to do this regularly and thoroughly to remove as much "tech-debt" as possible.

10) Perform penetration (pen) tests of the system, such as an IT audit of the organization, can assist management in understanding any vulnerabilities "One of the more important things internal audit can do is to assure that there's a common understanding as to what the risk appetite and risk culture are" (Jackson 2016). An experienced systems analyst should conduct the audit.

11) Insist on long passwords for all access control and avoid the requirement of cryptic passwords. Cryptic codes are difficult to remember but not difficult for a computer to crack. Over 90% of the cybersecurity professionals included cryptic symbols (*,&,~) in their most robust passwords even though password length is more important than inclusion of cryptic symbols to thwart hackers. This may be a requirement of the computer program they use that demands the use of cryptic symbols.

12) A technology and policy requirement that will not stop ransomware is encryption. The ransomware will merely encrypt your encryption making those files unreadable without a purchase of a key. While it is a good security policy to encrypt sensitive files, this will not stop the effects of a ransomware attack.

13) Establishing a clean desk environment and locking of computers whenever the user is not present will not stop ransomware. However, it sets a tone for computer usage in the organization. It is important for the organization to foster a strong security posture.

CONCLUSION

It is recognized that one study cannot be sufficient to recognize and solve all IT security issues for many different industries. This paper was designed to establish the size and scope of the problem, assess the attitudes and opinions of IT professionals, and make general recommendations to protect organizations from cyber threats in the future. The authors encourage other scholars to investigate the specific needs for each industry in the areas of hardware, software, training, and policy initiatives.

Ransomware is a dramatic threat to the economic and cultural vibrancy of any organization. As companies operate in open systems subjected to multiple stimuli, management must be proactive in strategic planning for cyber threats. Company users continue to open new vulnerabilities by adopting new technologies in an Internet of Things (IoT). A business continuity plan with special attention to disaster recovery planning (including ransomware) must be a requirement for all organizations.

Top management creates the posture of a disaster recovery plan. The implementation of the plan is the job of security professionals in the organization. This is a necessary action since top management and security professionals are more aware of the consequences of their decisions when establishing a disaster recovery plan. They must select from one of four risk management methods: acceptance, avoidance, mitigation, or transference of risk. Each method has inherent advantages and disadvantages. The risk posture of the organization is a strong driver in the decision of any recovery effort. Advanced planning is critical to avoid hasty or poorly formulated decisions on mitigation methods.

Information threats have always been present. Industrial espionage has been in existence since the earliest times of commercial activity. However, technology enables attackers to access data on an unprecedented scale, opening new vulnerabilities for the threat actors to attack and leverage. Attackers have found new vectors to take advantage of the network-centric society in which we live. While some people advise to avoid payment in any illegal action, the problem is now international in scope, with some of the biggest threats coming from less developed countries. We must address layers of complexity in the risk management equation for our increasingly connected and digitalized world.

REFERENCES

Fenton, Caleb. 2016. “New CryptXXX Variant Discovered.” *SentinelOne*. June 27. https://sentinelone.com/blogs/new-cryptxxx-variant-discovered/

Fitzpatrick, David, and Drew Griffin. 2016. “Cyber-Extortion Losses Skyrocket, Says FBI.” *CNNTech*. April 15. http://money.cnn.com/2016/04/15/technology/ransomware-cyber-security/index.html

Greenberg, Andy. 2017. “The WannaCry Ransomware Has a Link to Suspected North Korean Hackers.” *Wired*., May 15. https://www.wired.com/2017/05/wannacry-ransomware-link-suspected-north-koreanhackers/

Hachman, Mark. 2017. “How to Remove Ransomware: Use This Battle Plan to Fight Back.” *PC World,* December, 129-136.

Heartfield, Ryan and George Loukas. 2015. “A Taxonomy of Attacks and a Survey of Defence Mechanisms.” *ACM Computing Surveys*, 48 (3), 39.

IBM X-Force Research. 2016. “Reviewing a Year of Serious Data Breaches, Major Attacks and New Vulnerabilities.” *IBM Security*, April. https://www.autoindustrylawblog.com/wp-content/uploads/sites/8/2016/05/IBM_2016- cyber-security-intelligence-index.pdf

Jackson, R.A. 2016. “Business at Risk.” *Internal Auditor*, 41-45.

Kon, Matti. 2017. “Understanding and Preventing a Ransomware Attack.” *Response Magazine*, December, 49.

Kovacs, Eduard. 2020. “ATM Maker Diebold Nixdorf Hit by Ransomware.” *Security Week*, May 11. m https://www.securityweek.com/atm-maker-diebold- nixdorf-hit-ransomware.

Liska, Allan and Timothy Gallo. 2016. *Ransomware: Defending Against Digital Extortion*. Boston: O’Reilly Media.

McGuire, Cheri F. 2015. “The Expanding Cybersecurity Threat.” *Technology Innovation Management Review*, 5 (3), March, 46-48.

McHale, D, C. Musgrave and P. Nikhinson. 2016. “Cybersecurity and Data Breaches.” *The Doctors Company*, December 1.

McNicolas, Edward R and Thomas D. Cunningham. 2017. “A Cyberrisk Grows Up.” *Best’s Review*, December, 59-63.

Olenick, Doug. 2017. “When Ransomware Strikes, Should a Company Pay Up?” *SC Media*, March 7. from https://www.scmagazine.com/when-ransomwarestrikes-should-a-company-pay- up/article/642593/

Pierce, Scott D. 2020. "University of Utah Pays More than $450,000 in Ransomware Attack on its Computers." *Salt Lake Tribune*, August 21, 1.

Pope, Justin. 2016. "Ransomware: Minimizing the Risks." *Innovations in Clinical Neuroscience, 13*(11-12), December 1, 37-40.

Rains, Tim. 2016. "Ransomware: Understanding the Risk." *Microsoft Secure Blog*, April 22. https://blogs.microsoft.com/microsoftsecure/2016/04/22/ransomwareunderstanding-the-risk/.

US Deparment of Commerce and National Institute of Standards and Technology. 2011. "Managing Information Security Risk." *NIST Special Publication 800-39.* March.

APPENDIX

Ransomware Survey Results (N and %)

Note: not all respondents answered all questions

	N	%
1. Which term best describes your profession?		
A) Education	84	91
B) Government	6	7
C) Business	2	2
D) Other	0	0
2. Ransomware is best described as:		
A) Virus	32	37
B) Social Engineering	27	31
C) Worm	10	12
D) Trojan Horse	17	20
3. Have you ever experienced a successful ransomware attack?		
A) True (yes)	10	11
B) False (no)	79	89
4. The first occurrence of ransomware was:		
A) 1980s	25	28
B) 1990s	14	16
C) 2000s	23	26
D) 2010s	27	30
5. The principle target of ransomware in 2016 is:		
A) Government	9	10
B) Transportation	0	0
C) Manufacturing	4	4
D) Healthcare	76	85
6. By your estimate, which threat receives more emphasis in your organization?		
A) Ransomware	37	42
B) Espionage	14	16
C) Hacktivists	27	30
D) Cyber War	10	11
7. Ransomware:		

A) Encrypts files on a local computer	28	30
B) Encrypts on comp. & mapped drives	57	62
C) Deletes attached files	0	0
D) Locks the computer	7	8

8. Ransomware is most likely to attack risk averse organizations.

A) True	32	36
B) False	58	64

9. A successful ransomware attack renders your computer unusable.

A) True	52	57
B) False	40	43

10. A successful ransomware attack on a healthcare provider can create a HIPPA violation.

A) True	55	63
B) False	33	38

11. There are threecountermeasures available to combat ransomware. The most vulnerable element/s that permits ransomware is/are:

A) Human element	89	97
B) Routers	0	0
C) Storage devices	1	1
D) Software	2	2

12. Encrypting your files will thwart the effects of ransomware.

A) True	14	15
B) False	78	85

13. If you pay the ransom demanded in a timely fashion, you will receive a valid decryption key.

A) True	39	43
B) False	52	57

14. You are the System Administrator for a hospital, with a risk averse culture, and you have twenty-five drives encrypted. A ransomware screen is demanding payment of $300 per computer. It will take $7000 of labor to restore the backup files, with no guarantees the backups are not infected. The hackers provided a key to decrypt one computer as a show that their key will function. Which of the following would you implement?

A) Pay the ransom before the cost increases	10	11
B) Attempt to restore the files from backups, then decrypt, then pay ransom	5	5
C) Attempt to decrypt the files, then attempt	4	4

to restore the files, then pay ransom		
D) Contact local law enforcement and FBI	73	79
15. Given the same disaster scenario as in Q14,		
A) Call the FBI, contact local law enforcement, attempt to decrypt the files, restore files	78	88
B) Attempt to decrypt files, restore the files from backup, pay the ransom	3	3
C) Try to restore files from backup, pay ransom	0	0
D) Pay the ransom	8	9
16. Ransomware payment is usually paid via:		
A) PayPal	3	3
B) Digital coin (Bitcoin)	85	92
C) Western Union	4	4
D) iTunes card	0	0
17. Ransomware can:		
A) Encrypt files	47	52
B) Steal passwords	0	0
C) Search and steal digital certificates	0	0
D) All of the choices	44	48
18. If you choose to attempt to decrypt affected files, it is worth it to:		
A) Search the malware code for a key	15	17
B) Go to the Netherland's law enforcement site at https://www.nomoreransom.org.	3	3
C) Begin with transposition options and build from there	10	12
D) Both A and B	58	67
19. Does your organization have a disaster recovery plan that includes what to do when ransomware is successful?		
A) True (yes)	42	48
B) False (no)	45	52
20. When dealing with ransomware, which is the backup system of choice?		
A) Incremental	37	43
B) Versioning	45	52

C) No answer	5	5
21. Historically, if you fall victim to a ransomware attack and pay the ransom, you will not be attacked again.		
A) True	7	8
B) False	84	92
22. Do you use Windows Volume Shadow Copy Service (VSS) in your organization?		
A) True (yes)	19	24
B) False (no)	59	76
23. Do you have a clean desk policy at work?		
A) True (yes)	25	28
B) False (no)	63	72
24. How many characters are in your most important password?		
A) 1-7	1	1
B) 8-12	37	40
C) 13-18	41	45
D) 19+	13	14
25. Do you include special characters (*,&, #) in your most important password?		
A) True (yes)	84	92
B) False (no)	7	8