AICPA

FVS Eye on Fraud

The AICPA Forensic and Valuation Services quarterly report on fraud trends and topics

Ransomware

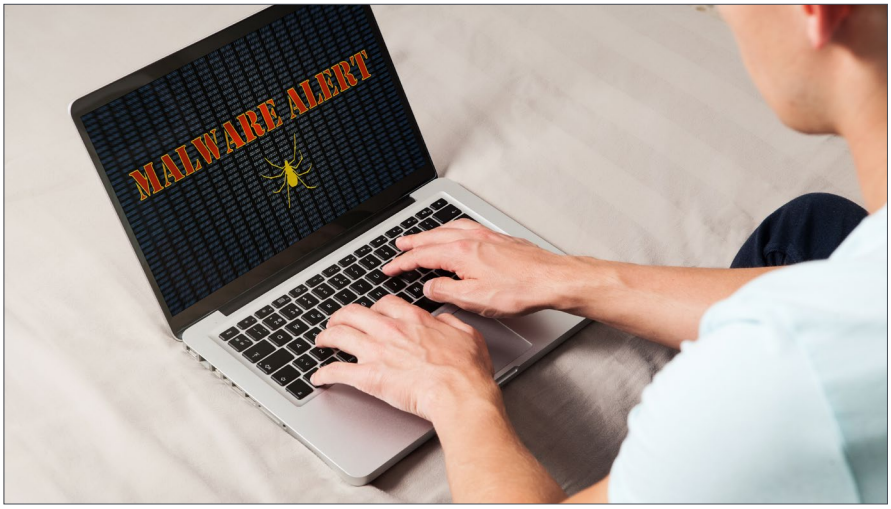
Issued by AICPA FLS Fraud Task Force
Lead author: Rumbi Petrozzello, CPA/CFF, CFE

Personal computers started to gain popularity in the 1980s and, in 1989, Joseph Popp, PhD, an evolutionary biologist, sent 20,000 computer floppy disks to attendees of the World Health Organization's AIDS conference. Information accompanying the disks claimed that the disks contained a program that, through a questionnaire, would analyze an individual's risk of contracting AIDS. What the disk actually contained was a program that was initially dormant. However, on the computer's 90th restart, the program hid directories and encrypted the names of all the files on the C drive. A message was then displayed on the computer screen, demanding that the user "renew the license" by sending $189 to "PC Cyborg Corporation" with an address for a post office box in Panama. This attack became known as the AIDS Trojan or PC Cyborg and the first known ransomware attack. It was not difficult to overcome, but it was the start of what has become an ever-growing and very expensive problem.

Continued on page 2

Fall 2018, Issue 4

Inside this issue



Ransomware is popular among criminals because it is a quick moneymaker (most attacks demand the ransom be paid in less than a week) and has the potential to be extremely lucrative.

In 2005, Susan Schaibly authored the article, "Files for Ransom",[1] stating that "(t)he good news is that documented attacks have been rare. The bad news is that cases are on the rise." And these attacks have grown exponentially, not only in frequency but also in magnitude. Proving Schaibly prophetic, 2006 brought a rash of ransomware, including Cryzip, MayArchive, and the Archiveus Trojan, which worked by encrypting every file in the "My Documents" folder. These files were decrypted by making purchases on certain websites. It was at this point that ransomware truly took off.

Ransomware is a form of malicious software, also known as malware, which mostly works in one of two ways:

- Crypto-ransomware encrypts hard drives or files and folders.
- Locker-ransomware only locks users out of their machines, without encryption.

When a computer has been compromised by ransomware, attackers will find various ways to keep victims from reporting the attack, including implying that the user has somehow broken the law or that the hackers are holding proof of illegal or shameful acts. To motivate victims to pay up and pay quickly, ransomware will often impose time limits for payment, with threats of punishment. This punishment could be releasing embarrassing information to the public, the threat of legal action such as jail or deportation, the destruction of the encrypted or locked files, or it could be a periodic increase in the ransom being sought.

The evolution of methods of payment that are increasingly more difficult to track has been a boon for those perpetuating ransomware attacks. Dr. Popp demanded people put a check or money order in the mail, but by the 2000s, people were being asked to send money through websites or by money transfer services, such as Western Union. The arrival of Bitcoin and other cryptocurrencies has been a gift for cybercriminals. Bitcoin has become the go-to form of payment for Ransomware attackers. Cryptocurrencies make it easier for attacks to happen on a global scale, and the anonymity of cryptocurrencies makes it harder to track down, along with the perpetrators, who are often located outside of the United States and in countries that are out of reach of the Department of Justice, such as some Eastern European nations and North Korea. Both areas have been fingered in recent ransomware cases. The general advice is to not pay the ransom demanded, but some individuals and companies may feel they have no choice. However, that brings up a new challenge — finding the cryptocurrency to pay. Although buying it has become easier, Bitcoin is not something one can pick up at a local bank, and sometimes, it is difficult to obtain the amounts demanded on short notice.

Ransomware is popular among criminals because it is a quick moneymaker (most attacks demand the ransom be paid in less than a week) and has the potential to be extremely lucrative. Frequently, the amounts demanded of each victim are relatively small. In the case of the attack on the city of Atlanta in March 2018, the ransom demanded was $52,000 (as written about in the

Continued on page 3

[1] Susan Schaibly, "Files for Ransom," *NetworkWorld*, September 2005, networkworld.com/article/2314306/lan-wan/files-for-ransom.html.

summer 2018 edition of *FVS Eye on Fraud* focused on cyberfraud), and the WannaCry ransomware demanded $300 from each computer it locked. However, these amounts very quickly add up to a lot of money for attackers who spread their attacks across the globe. According to CSO Online,[2] about $1 billion was made by ransomware cyber criminals in 2016. At times, the funds demanded are nominal because the cybercriminal has an ulterior motive: accessing the victim company's customer and vendor files to extract data, such as personally identifiable information and credit card information. In addition to the theft of the data, the cost of ransomware attacks is even greater than a ransom paid. According to Wired Magazine,[3] the city of Atlanta spent $2.6 million to recover from its ransomware attack. Cybersecurity Ventures[4] predicts that ransomware damages will hit $11.5 billion by 2019, a massive increase from $325 million in 2015.

How does ransomware get into computer systems? One way is through human engineering. An email could come through with an attachment or a link that the receiver believes is innocuous. With the amount of email people receive daily, it is very easy to click on an email that appears to come from a trusted source. This is especially true when one is scrolling through mail on a smartphone or other mobile device. A very effective way to reduce this risk is through user training. This should include lessons on being careful about clicking on links and attachments and augmented with phishing tests, which are performed by sending mock phishing emails to employees and seeing how many click on the links in these emails. Results can be shared with employees with the goal of raising awareness. Another way in which ransomware affects machines is by exploiting weaknesses in the system. EternalBlue is a tool that was used by the National Security Agency that exploited a flaw in Microsoft Windows. A hacker crew called Shadow Brokers released this tool, and Microsoft released a patch for it in March 2017. A few months later, in May, the WannaCry ransomware infected machines around the world that had not been updated with this patch.

Continued on page 4

[2] Maria Korolov, "Ransomware took $1 billion in 2016, improved defenses may not be enough to stem the tide," *CSO Online*, January 2017, csoonline.com/article/3154714/security/ransomware-took-in-1-billion-in-2016-improved-defenses-may-not-be-enough-to-stem-the-tide.html.

[3] Lily Hay Newman, "Atlanta spent $2.6M to recover from a $52,000 ransomware scare," *Wired*, April 2018, wired.com/story/atlanta-spent-26m-recover-from-ransomware-scare/.

[4] Steve Morgan, "Global ransomware damage costs predicted to hit $11.5 billion by 2019," *Cybersecurity Ventures*, November 2017, https://cybersecurityventures.com/ransomware-damage-report-2017-part-2/.

Practice tips

CPAs should work with clients to keep ransomware attacks from happening in the first place. Working with other knowledgeable professionals is also key. Prevention is always best. In addition to prevention measures, CPAs should emphasize that mitigation is imperative — clients should have a clear discovery and recovery plan, including a roster of professionals with expertise in investigating, diagnosing, and remediating the damages incurred by a ransomware attack. Cybercriminals work very hard to find the smallest weaknesses in a system, and clients should know how they are going to react before anything happens. CPAs should speak to clients about the cost, beyond the ransom payment, of ransomware attacks. Some advice and training that CPAs can provide to their clients include the following:

- **Perform a risk assessment.** An assessment of your clients' systems and processes can help identify where weaknesses are and indicate areas in which to provide recommendations. This assessment will include who in the company has access to various levels of privileged data, how access is limited, and how duties are segregated.
- **Perform periodic penetration testing.** Penetration testing, also referred to as pen testing, is a way to evaluate the security of an IT infrastructure through authorized simulated attacks. Pen tests can identify vulnerabilities in the system, including how easy it might be for unauthorized parties to gain access to the system, and it also will identify strengths in the system. With the constant evolution of threats to IT infrastructures, CPAs should recommend that pen tests be performed at least annually, using a third-party vendor, and periodically rotating the vendors that they use. Some firms may choose to conduct the tests internally, but you should recommend that they also use the services of third parties, sometimes referred to as white hat hackers, and spread the internal and external testing across the year.
- **Conduct regular staff training on computer security best practices, including avoiding falling for phishing communications.** Training should be part of the staff member's onboarding process and updated at least annually. The entities should conduct phishing tests to gauge how many staff members recognize possible

Continued on page 4

A vulnerable system or a duped individual is all ransomware needs to wreak havoc. The WannaCry ransomware attack emphasizes the importance of regular software updates. CPAs should talk to clients about setting up their systems to automatically update all the computers in their business and not give employees the ability to opt out. One vulnerable spot is all it takes for malware to bring expensive damage to a company.

Dispelling rumors is an important part of protecting against ransomware attacks. Incorrect assumptions can lead to lax behaviors, and these lax behaviors can lead to very expensive recovery from an attack. One misconception is that Apple machines cannot be affected by ransomware. Although the most notorious attacks have been on Windows machines, Apple products are not immune. In 2017, the BBC[5] reported on ransomware specifically targeting Mac computers. Where there is money to be made, it only makes sense that criminals will be working hard to find ways to make that money. Another misconception that people have is that they are safe on their phones or tablets. Consumer Reports[6] wrote on the ransomware called Charger, which was embedded in an app sold on Google Play. This ransomware texts the phone owner's contacts requesting admin permissions. Once it has these permissions, it can get to work, locking phones and demanding payment. A very big mistake people can make is believing that only big companies are attacked. We hear a lot about big companies being compromised because big companies generate big news. However, CPAs should be sure to educate all their clients about how to protect themselves because any one of them can be targeted, and the WannaCry attacks are an excellent example. CPAs should remind their clients that often the cost of the ransom may not be high, but the cost of recovery, if the client is not prepared, may be much higher.

Ransomware attacks tend to be more expensive than the money demanded on the locked computer screen. Those who decide to pay the ransom should be aware that they are trusting a criminal to restore their systems. There is no guarantee that payment of a ransom will fix things, and victims may find themselves with less money and a locked machine. Paying a ransom also leads to a growing market — if criminals know that ransomware will make

Continued on page 5

Practice tips (continued)

scam emails. Regular reminders should be distributed to staff with information on real-life current threats. Recommend that clients use outside vendors for some of this training. There is a great benefit to bringing in a specialist to teach on current risks and issues.

- **Provide training to staff on being careful about clicking on attachments and links in emails.** This training should include guidance on smartphone use. Care must be taken regardless of whether staff is using a computer or mobile device. Remind them to check the sender's metadata to ensure that the email is coming from a valid source. Make it easy for the clients' employees to report suspicious emails by providing an email address to which they can send questionable messages and a button in the email service that an employee can easily click on to share a suspicious email with the IT department. The IT department must be trained to be responsive to these emails, as their lack of responsiveness could lead to a reduction in reporting.
- **Update software to protect against weaknesses. Work with clients to have their staff update software on their machines regularly.** IT should set up computers to install security updates automatically, and the ability to opt out should not be available to staff.
- **Consider upgrading from software that is no longer covered by the vendor.** When software is no longer covered, security updates and patches are no longer provided by the vendor. The WannaCry ransomware took advantage of the fact the Windows XP was no longer covered by Microsoft.
- **Create a regular backup system that includes off-site backups.** The backup program should also include a recovery plan, which should be tested on a regular basis to make sure it works and that employees know what to do. The backup and recovery plan should be documented and known by appropriate staff.
- **Have a constant monitoring system to identify anomalies in the system.** The attack on LabCorp could have been far worse if it did not have a round-the-clock system that was monitoring for something amiss.

[5] Maria Mark Ward, "Apple Mac computers targeted by ransomware and spyware," BBC News, June 2017, bbc.com/news/technology-40261693.

[6] Allen St. John, "Smartphone ransomware is a looming threat," *Consumer Reports*, January 2017, consumerreports.org/digital-security/smartphone-ransomware-a-looming-threat/.

them money, they will continue to launch attacks. Beyond ransom, some additional costs of a ransomware attack are as follows:

- **Data recovery costs.** As mentioned previously, payment of ransom is no guarantee that a victim will get their files back. If victims choose to not pay ransom or if files remain encrypted, despite payment, they should consider the cost of data recovery. If victims have not been backing up their systems regularly, they stand to lose data and may have to spend time trying to recreate lost records.
- **Software updates.** If a ransomware attack was the result of vulnerability due to outdated software, those attacked will need to update their systems. CPAs should advise clients to perform regular checks to ensure that the software that they are using is still supported by the vendor and receives regular security updates.
- **New control systems.** After an attack, those affected will need to invest in security and training to protect themselves from future attacks. This will involve both beefing up their systems with tools such as firewalls and filters and training employees.
- **Forensic investigation.** After an attack, businesses will seek to determine the extent of damage caused and get some pointers on how the attack happened and who may have launched it.
- **Lost time.** During and after the attack, a business may either be limited or completely incapacitated. Time lost not doing business is time not making money.
- **Notification costs.** Depending on the types of data that have been exposed by the ransomware attack, the company may be obligated (for various reasons, including regulations, insurance, or contracts) to notify customers, vendors, and other stakeholders about the attack and the potential exposure of their information. According to the 2018 Cost of a Data Breach Study,[7] conducted by the Ponemon Institute, the average cost of a breach is $148 per lost or stolen record.

The cyberfraud edition of the AICPA FLS Fraud Task Force's *FVS Eye on Fraud*[8] noted that "2016 was the year of ransomware", with attacks occurring every 40 seconds. CSO Online[9] predicts

Continued on page 6

Fraud news: Ransomware

Around midnight, on July 13, 2018, the medical testing company Laboratory Corporation of America Holdings (LabCorp) was hit by the same SamSam ransomware attack that crippled the city of Atlanta earlier in the year. By 6 p.m. on July 14, the first computer at LabCorp had been encrypted. Even though it took the company's security department less than an hour to contain the spread of the malware, 7,000 systems and 1,900 servers (including 350 production servers) were affected. In an interview with CIO, Jim Nelms,[10] the Chief Information Systems Officer at LabCorp stated that the company is attacked on a daily basis — about 16 times a day — and has a response plan in place that helped them discover the attack and respond as quickly as they did. Even with that, a week after the attack, LabCorp had not fully recovered from the attack. Health care companies are a prominent target of ransomware and other cyberattacks because of the sensitive information that organizations in this industry hold. On the dark web, information stolen from medical organizations is highly valued. Also, when this information is held for ransom, it can be potentially hazardous for medical entities because this could affect how and when a patient can be treated.

In February 2018, the city of Leeds[11] in Alabama was the victim of a ransomware attack. All the city's computers were locked, including those of the fire and police departments. The city could not even process employee paychecks and had to resort to writing manual checks and delivering them by hand. The city opted to pay the ransom and, after negotiating the payment down

Continued on page 6

[7] IBM Study: Hidden Costs of Data Breaches Increase Expenses for Businesses, IBM News Room, July 2018, https://newsroom.ibm.com/2018-07-11-IBM-Study-Hidden-Costs-of-Data-Breaches-Increase-Expenses-for-Businesses.

[8] *FVS Eye on Fraud, Cyberfraud*, Summer 2018, Issue 3 (Available via AICPA Forensic and Valuation Services Online Professional Library)

[9] Steve Morgan, "Ransomware damage costs predicted to hit $11.5B by 2019," *CSO*, November 2017, csoonline.com/article/3237674/ransomware/ransomware-damage-costs-predicted-to-hit-115b-by-2019.html.

[10] CIO Interview with Jim Nelms, CISO at LabCorp, CIO, September 2018, cio.com/article/3305063/leadership-management/cio-interview-with-jim-nelms-ciso-at-labcorp.html.

[11] Howard Koplowitz, "Leeds hit with ransomware attack," AL.com, March 2018, al.com/news/index.ssf/2018/03/leeds_hit_with_ransomware_atta.html.

that this frequency will rise to every 14 seconds by the end of 2019. The cybercriminals launching ransomware attacks are difficult to track down and often beyond the jurisdictional reach of authorities. Sometimes, the attackers are believed to be agents of foreign governments. Very rarely are there arrests for ransomware attacks. Instead, CPAs should speak with clients about the most effective ways to protect themselves from attacks and how to mitigate the effects of any attacks that may occur. Since Joseph Popps' floppy disks were sent through the mail, ransomware has grown into a monster that does not discriminate among victims: they can be individuals or businesses, small and large. As attacks continue to increase and wreak more havoc, it is imperative for CPAs to help their clients be vigilant and prepared for attacks.

Fraud news: Ransomware (continued)

from $12,000 to $8,000 in Bitcoin, the city found that the hackers restored only a limited number of files. This is the price of working with criminals — they often do not do what they say they are going to do. Ultimately, the city of Leeds hired a company to help it restore its data and clean up its systems. Leeds and Atlanta are in no way unique — cities all over the United States have been attacked, from New Jersey[12] to North Carolina[13] and Tennessee.[14]

In July 2018, China Ocean Shipping Company (COSCO) was forced to shut down all its American office networks due to a "local network collapse" allegedly caused by a ransomware attack. COSCO was very close-lipped about what which ransomware was responsible or the extent of the damage caused.

However, this attack was reminiscent of a ransomware attack on shipping giant Maersk,[15] in June 2017. Here, the company was attacked by the NotPetya ransomware, which is believed to be a product of Russian military hackers. What makes NotPetya stand out from other ransomware is that unlike traditional ransomware that encrypts or locks files and then demands ransom, NotPetya pretends to do so. Although a screen appears on computers asking for ransom, the NotPetya's malware proceeds to destroy machines, irreversibly encrypting the computers' master boot records. It doesn't matter if a victim pays the ransom demanded; there is no key to reverse this encryption. Maersk reported that it would suffer losses of up to $300 million to recover from the NotPetya attack, and this recovery included reinstalling 4,000 servers, 45,000 PCs, and 2,500 applications.

In May 2017, WannaCry ransomware swept across the world, first making the news when the UK's health service, the NHS, stated that it had been attacked. In very little time, this attack was estimated to have affected over 200,000 computers across 150 countries.[16] Fortunately, within days of the WannaCry attacks, Marcus Hutchins, a security researcher, stumbled upon a kill switch and halted WannaCry's spread. However, mere months after being hailed a hero, Hutchins[17] was arrested and accused of being responsible for the creation of malware called Kronos, which is designed to steal online banking credentials. In late 2017, the U.S. government blamed North Korea, specifically, a hacker entity known as the Lazarus Group, which works for the North Korean government, for the WannaCry attack. In early September, the Department of Justice (DOJ) made a rare announcement: charges against a perpetrator[18] of the WannaCry ransomware attack. The DOJ released a 179-page complaint against an alleged member of the Lazarus Group, Park Jin Hyok. Although charges have been announced, it is unlikely that Park will even see the inside of a courtroom because the United States has no diplomatic relations with North Korea.

[12] Plainfield, NJ Under 'Ransomware' Cyber Attack, CBS New York Online, April 2016.

[13] Debbie Hightower, "Davidson County, N.C., Still Reeling from Ransomware Attack," *Government Technology*, February 2018, govtech.com/security/Davidson-County-NC-Still-Reeling-from-Ransomware-Attack.html.

[14] Jay Powell, "Spring Hill, Tenn., Hit with Ransomware Attack," *Government Technology*, November 2017, govtech.com/security/Spring-Hill-Tenn-Hit-with-Ransomware-Attack.html.

[15] Andy Greenberg, "The Untold Story of Notpetya, the Most Devastating Cyber Attack in History," *Wired*, August 2018, wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

[16] BBC News, "Ransomware cyber-attack: Who has been hardest hit?", bbc.com/news/world-39919249.

[17] Reeves Wiedeman, "Gray Hat," *Intelligencer* (originally appeared in February 19, 2018, issue of New York Magazine), nymag.com/intelligencer/2018/03/marcus-hutchins-hacker.html.

[18] Greg Otto, "U.S. charges North Korean hacker over Sony, WannaCry incidents," *CyberScoop*, September 2018, cyberscoop.com/north-korea-indictment-sony-pictures-wannacry/.