AICPA

FVS Eye on Fraud

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

Cyberfraud – Current issues and trends

Issued by AICPA FLS Fraud Task Force
Lead authors: Howard M. Silverstone, CPA/CFF, FCA, CFE
and Jessica L. Pezzato, CPA

Summer 2018, Issue 3

Inside this issue

"As the United States attorney in Manhattan, I have come to worry about few things as much as the gathering cyber threat."

said Preet Bharara, who served as the United States Attorney for the Southern District of New York from 2009 to 2017.

As technology and mobile connectivity have become more prevalent in daily life and the trend towards cloud-based storage continues, it is not shocking that 77 percent of Americans use the internet daily — including 26 percent of American

Continued on page 2

Although it is not surprising that so many individuals are accessing the internet, it may be shocking that monetary damages from cybercrime are estimated to total six trillion dollars by 2021.

adults who use the internet "almost constantly," according to a Pew Research Center survey[1] conducted in January 2018. Although it is not surprising that so many individuals are accessing the internet, it may be shocking that monetary damages from cybercrime are estimated to total six trillion dollars by 2021, according to the website CSO Online[2]. *Cybercrime* is defined as "an intended illegal act involving the use of computers or other technologies." *Cyberfraud* is a specific area of cybercrime, which can specifically be defined as "the intentional act of depriving another of property or money by deception, misrepresentation, or other unfair means using computers or other technologies."

Cyber challenges exist in many forms, some of which an individual or business can control and others over which they have limited, if any, control. Cyber challenges can also be a result of internal or external conditions or both. First and foremost, it is important to consider that technology itself poses a challenge for an individual or business because of its nature of frequent changes and advancements. Therefore, users are not always familiar with the changes and do not recognize the vulnerabilities that can inherently exist until the occurrence of a cybercrime. Some cyber challenges can be controlled through cybersecurity and safeguards such as encryption and two-factor authentication; however, like all aspects of fraud, these security measures are inherently most effective when they are implemented prior to the occurrence of any intrusion.

Phishing is the perfect example of a potential cybercrime that presents challenges. Although this intrusion is the result of an external condition (that is, someone sending an email that is not legitimate), the response to the receipt of that email is the internal condition that affects the ultimate result — providing the perpetrator with sensitive data. Consider an employee receiving a phishing email. If the employee does not recognize that an email is suspicious, he or she may, for example, provide a key password to the intruder. If that occurs, there are two likely scenarios: (a) if the business has weak cyber protection, it may fall victim to the perpetrator; or (b) if the business has two-factor authentication, the perpetrator will not be able to gain access to any business records; this potential cyberattack will be thwarted.

Simply put, two-factor authentication (also known as "2FA") adds a second level of authentication to an account that requires any type of login. If one only needs to enter a username and a password, that is considered single-factor authentication. A 2FA login requires users to have two types of login credentials before accessing an account. For example, a username and password are required when using Microsoft SharePoint. However, using 2FA, Microsoft has an authenticator app for a smartphone. The authenticator app requires users to approve access from the app. Under this 2FA, even if someone obtains a user's name and password via a phishing email, the user still maintains access control because of the authenticator app.

Continued on page 3

[1] pewresearch.org/fact-tank/2018/03/14/about-a-quarter-of-americans-report-going-online-almost-constantly/

[2] csoonline.com/article/3153707/security/top-5-cybersecurity-facts-figures-and-statistics.html

Even with 2FA, an attacker may still find a way around the system. For example, although sending an SMS text as part of 2FA seems secure, if the user's carrier account is compromised, the authentication can be hijacked. As with all aspects of fraud, we may never prevent it, but we can prepare for it. The more we know, the better we can advise our clients and be prepared for the threat.

Individuals, specifically CPAs, need to be aware of cyberfraud because cybercrime is increasing in both prevalence as well as in the amount of monetary damages caused by it. However, to be prevented, individuals need to acknowledge the impact of cyberfraud; and they must acknowledge the weaknesses that allow such fraud to occur. CPA firms as well as their clients may be targets for cybercrimes. Small and medium-sized businesses are targeted more frequently than large businesses because they typically have fewer controls in place, making them more vulnerable. CPA firms may be targets for cybercriminals because of the value of the information they maintain (for example, bank account information and other information that can be used for identity theft). Recent examples show that a single fraudulent transaction through wire fraud can result in a loss of $130,000 and, in some cases, can result in losses of more than $1 million. Controls such as internal cybersecurity audits can prevent and detect vulnerabilities. It is estimated that 90 percent of cybersecurity breaches could have been prevented if reasonable controls had been in place prior to the incident.[3] The prevalent themes in all types of fraud prevention are education, knowledge and staying current with technology.

To illustrate the need for change and keeping up with technology, we should look to American history and the city of Philadelphia. It was Benjamin Franklin who said that "an ounce of prevention is worth a pound of cure." Although this advice was in relation to firefighting, it has been applied over the years to all aspects of life and business. For those of us whose business takes us into the world of fraud prevention and investigations, it could not be apter.

Similarly, William Penn, who was born in London, feared that tight living spaces worsened the spread of fires and disease, a fear that emanated from the Great Plague and the Great Fire of London in the mid-17th century. Penn hoped to create a town with wide streets free of the overcrowding, fire and disease that had plagued European cities.

Continued on page 4

Practice tips

As with most aspects of fraud, CPAs should be as knowledgeable as possible about the current threat that exists through cybercrime. CPAs should also help educate and train their clients as they would for traditional fraud prevention. Their clients should be aware of the threats that exist and be regularly updated on new trends and how malware and phishing can lead to attacks.

Although CPAs are not experts on all things IT-related, they need to be informed and know what resources exist to assist their clients from both a pro-active and reactive stance.

At a minimum, the CPA should be aware of

- the latest trends in anti-virus protection;
- how data are backed-up;
- data encryption and firewalls; and
- plans the clients have in place for disaster recovery.

The CPA should have his or her internal or external IT professionals conduct testing of employees, without the employees' knowledge, to see if they fall to phishing or similar schemes. This is an exercise that CPAs should also encourage their clients to undertake.

Encourage clients to have "Bring Your Own Device" programs, where employees are provided training and companies have policies on the ever-increasing issue of employees using their own smartphones and tablets for work-related purposes.

Encryption, encryption, encryption! This has been mentioned more than once here. Even if hacked, a company can protect its data and perhaps its most valuable assets by encryption. Use complex passwords and change them often.

Know the basics of defending against ransomware and other attackers by doing the following:

- Using of 2FA — It is not perfect, but it provides another layer of security.
- Ensuring that data are regularly backed-up to ensure valuable data is stored in other locations
- Making sure updates and patches are made as soon as they are available

[3] ekransystem.com/en/blog/top-10-cyber-security-breaches

Both Franklin and Penn emphasized education, understanding and learning from mistakes to try to shape and influence the future. As CPAs, and for those of us who dedicate our work in the field of fraud prevention and investigation, education is paramount in risk assessment and understanding weaknesses that allow perpetrators to succeed.

The technology-influenced world of the 21st century is not something Franklin or Penn could have envisioned; however, their concepts of prevention and planning still are relevant some 350 years later. In the world of cybercrime, legislators, attorneys, law enforcement officials and the “average” person in the street still do not fully understand what computer-based crime is. Similarly, legislation has been slow to change and has not kept pace with rapidly evolving technology.

Although the traditional concepts of the fraud triangle and the red flags of fraud may still be relevant in some context to white-collar crime, the challenges of cybercrime go beyond these parameters. Those who commit cybercrime often are from another country, and they are unknown to the victim.

The idea of someone stealing information solely because of personal or business pressure and rationalizing it under the banner of the fraud triangle may not apply in the world of cybercrime. Traditional fraud prevention methods are not going to prevent the attacks on business for competitive intelligence gathering or denial of service. But the stakes could be much higher than the risk of an internal theft. Loss of trade secrets, theft of proprietary information and loss of reputation and goodwill are far greater.

Continued on page 5

Fraud news: Cyberfraud

- In 2017, Hilderbrand & Clark, a CPA firm in California, reported a data breach as a result of unauthorized access to its computer network from abroad. The CPA firm prepares tax returns and was unable to determine what specific files had been accessed; however, this data breach is related to its clients’ and its employees’ personal information (including, names, dates of birth, Social Security numbers, bank account information and other critical information).

- According to an IBM-sponsored study, the average cost of a data breach was $6.5 million in 2015 with an average cost per lost or stolen record of $217. The amount may not seem like much, but consider the size of your firm and how many client records you have stored on your computer. With the average cost of $217 per lost or stolen record, these costs would add up quickly if you became a cyberfraud target. Additionally, it is important to note that this type of data breach runs in tandem with the IRS’ warning regarding the filing of fraudulent tax returns for “bogus refunds,” which has increased in the past two years.

- In February 2018, 36 individuals in seven nations, including the United States and Ukraine, faced charges (among others) of suspicion of large-scale identity theft. These individuals allegedly operated a global cybercrime ring through an internet forum called Infraud, which had about 11,000 members. Their activities resulted in over $2 billion in intended losses and actual losses of over $530 million during a seven-year period.

- The City of Atlanta recently was hit with a ransomware infection that resulted in the loss of access to files and outages to several online systems and services. Atlanta’s chief operations officer, Richard Cox, was in his first week on the job and noted that it affected services related to paying city bills and accessing court information online. The attackers were demanding payments of $6,800 to decrypt files on each infected computer. Their note also offered the city an option to pay $51,000 in exchange for decryption keys for all computers infected in the attack. According to experts who reviewed the ransom note, the attack was likely SamSam, a strain of ransomware that also affected the Colorado Department of Transportation earlier in the year. SamSam scans the web to locate servers with unpatched software, itself a weakness, which then allows penetration to the victim’s server.

Continued on page 5

Similarly, banks and internet-based businesses are at risk from cyberattacks that often are greed-based. The access to customer information, such as Social Security numbers or credit card and bank account information then provides a gateway to the "dark web" and the financial gains from the sale of such information.

There are many other types of cyberattacks that businesses and individuals face, whether they are grudge attacks a former employee or competitor launches, an ideological attack from an activist opposed to a company's particular strategy, or a military-style attack on intelligence.

Faceless criminals holding companies to ransom using malicious software have replaced masked bandits entering a bank's doors. A lack of education and information resulting in lax controls and ignorance of current events can be costly to a company. The perpetrators only need a one-time hit to be successful. It is costing companies a financial loss and resulting in job losses for top-level executives at companies such as Equifax and others.

In the area of prevention, the corporate world still is at the mercy of the internal budget process, authorization, training, personnel and all the other hurdles that have to be met before everyone agrees to do something. As far back as 2005, at a national credit card conference, Suzanne Lynch, who was then vice president for security and risk services at MasterCard International, noted, "We build a 10-foot wall, and the bad guys build an 11-foot ladder."

The most vexing question is always where to start the process.

In a recent survey the U.S. Secret Service, Carnegie-Mellon University, PwC and CSO Security magazine conducted, 75 percent of those surveyed had a breach within the prior 12 months. The top attacks were from malware, phishing, network interruption, spyware and denial-of-service attacks. Interestingly, over 25 percent of respondents said the attackers were insiders, such as current or former employees.[4] This last statistic may be the one area where companies can cling on to formerly used prevention techniques, because they may be able to protect themselves internally; but the rapidly changing manner in which cyberattacks take place may still not protect them, given the MasterCard comment previously noted. An 11-foot ladder will always successfully scale a 10-foot wall.

Continued on page 6

Fraud news: Cyberfraud (continued)

- In March 2018, police in Spain captured a cybercrime gang that allegedly stole more than $1.25 billion from financial institutions worldwide in a five-year period. They stole amounts up to €10 million (about $11.6 million) in each heist. These cybercriminals used malware to target more than 100 financial institutions and specifically used emails to break into banks and compromise the networks controlling the ATMs. Furthermore, the cybercriminals converted their stolen gains into bitcoins and cryptocurrency to purchase large dollar value items such as houses and vehicles. This prompts another area for concern of increasing cyberfraud, which is digital currency and its increasing popularity and mainstream usage. Currently, cybercurrency is unregulated and not secure, which creates an opportunity for cybercriminals.
- In 2015, 62 percent of law firms had been the victim of a cyberattack in the past year, according to PwC's annual law firm survey. In 2016, it was estimated that hackers had stolen £85 million (about $113 million) from British law firms over a period of 18 months.
- Additionally, recent data indicate that millennials (those between the ages of 20 and 29), are more likely to be victims of cybercrime than senior citizens (those over age 70) as a result of millennials using technology and the internet more frequently than seniors. However, research indicates that the older the target of a cybercrime, the higher the level of loss as a result of the crime. Specifically, the median loss for millennials totaled only $400; whereas the median loss for those over age 80 totaled $1,092. Therefore, even though seniors may be less frequent victims of cybercrime, they may incur greater financial losses as a result.

[4] insights.sei.cmu.edu/insider-threat/2018/01/2017-us-state-of-cybercrime-highlights.html

A company may be able to identify a current or former employee who may feel disenfranchised and therefore recognize the traditional red flags of fraud. However, those who perpetrate cyberattacks fit no such profile. It could be one person, a group of people, a criminal organization, or perpetrators from a foreign country. When a company loses control over its banking information under a corporate account takeover, and its login credentials are undermined, it typically begins at a level within the company where the person has the most information (for example, a controller or CFO). The CPA should recognize this threat and educate his or her client as to how such sensitive information is controlled and make the client aware of phishing and other threats that seek to obtain such data.

Insurance company Camico noted that, according to NAS Insurance,[5] "2016 was the year of ransomware." Such instances went from one every two minutes to one every 40 seconds. In fact, in 2016, 18 percent of cyber claims arose from ransomware, 16 percent from hacking and 13 percent from physical theft. They further noted that, in 2017, they saw an increase in fraudulent wire transfer request claims and phishing attack claims.

In its 2017 "Cost of Cyber Crime Study",[6] the Ponemon Institute noted the following three factors as key to the fight against cybercrime:

- Invest in security intelligence but recognize the need to stay ahead of hackers.
- Undertake extreme pressure testing to identify vulnerable areas.
- Balance spending on new technology such as analytics and artificial intelligence.

Ponemon noted that "spending alone does not always equate to value." Understanding the vulnerabilities and the consequences of failure will allow client companies to build a strategy to start combatting the modern financial enemy. The strategy to combat cybercrime should not be static because, as technology continues to develop, these threats will not be eradicated. They will just become more sophisticated. Continued vigilance in terms of adapting the strategies employed and training employees and clients regarding the risks and ways to combat such risks is the only option for success in combating cybercrime.

As NASA Flight Director Gene Krantz said in the movie "Apollo 13", "Failure is not an option!"

Resources

The AICPA's Cybersecurity Resource Center provides the following resources to practitioners to help assess risk and providing information on risk programs:

- AICPA Cybersecurity Resource Center
- Cybersecurity Fundamentals for Finance and Accounting Professionals Certificate
- Cybersecurity Readiness Assessments
- Cybersecurity Advisory Services: Readiness Assessment Deep Dive

[5] camico.com/blog/cyber-claims-trends-accountants

[6] accenture.com/t20171006T095146Z__w__/us-en/_acnmedia/PDF-62/Accenture-2017CostCybercrime-US-FINAL.pdf#zoom=50