AICPA®

TOP CYBERCRIMES WHITE PAPER

HOW CPAs CAN PROTECT THEMSELVES AND THEIR CLIENTS

February 2017

AUTHORS:
Jeff Streif, CPA
Koller Enterprises Inc.
Fenton, MO

Lisa Traina, CPA/CITP, CGMA
Traina & Associates, a CapinCrouse Company
Baton Rouge, LA

Steven J. Ursillo Jr., CPA/CITP, CGMA
Sparrow, Johnson & Ursillo Inc.
West Warwick, RI

REVIEWERS:
Susan Pierce, CPA/CITP, CGMA
Associate Director
Information Management and Technology Assurance Division
AICPA, Durham, NC

Iesha Mack, PMP
Manager
Information Management and Technology Assurance Division
AICPA, Durham, NC

© 2017 Association of International Certified Professional Accountants. All rights reserved.

DISCLAIMER: The contents of this publication do not necessarily reflect the position or opinion of the American Institute of CPAs, its divisions and its committees. This publication is designed to provide accurate and authoritative information on the subject covered. It is distributed with the understanding that the authors are not engaged in rendering legal, accounting or other professional services. If legal advice or other expert assistance is required, the services of a competent professional should be sought.

For more information about the procedure for requesting permission to make copies of any part of this work, please email copyright@aicpa.org with your request. Otherwise, requests should be written and mailed to the Permissions Department, AICPA, 220 Leigh Farm Road, Durham, NC 27707–8110.

TABLE OF **CONTENTS**

EXECUTIVE **SUMMARY**

We remember the good old days when the hottest topic linked to cybercrime was identity theft. Today, there's much more to cybercrime than a hacker stealing a Social Security number. In fact, ID theft is only one of the top cybercrimes making its way through today's business marketplace. Others include corporate account takeover, theft of data and ransomware. AICPA Information Management and Technology Assurance Cybersecurity Task Force members Jeffrey Streif, CPA, CFO at Koller Enterprises; Lisa Traina, CPA/CITP, partner of Traina & Associates, a CapinCrouse Company; and Steve Ursillo Jr., CPA/CITP, partner at Sparrow, Johnson & Ursillo Inc., compiled a list of today's top cybercrimes to help CPAs leverage their role as trusted advisers to better protect organizations from data breaches and business interruptions.

This white paper defines cybercrimes, examines the aforementioned crimes and their effect on data and systems, and explains how CPAs must steward organizations in securing data, keeping information both reliable and available.

WHAT IS A **CYBERCRIME?**

A cybercrime is, **"an intended illegal act involving the use of computers or other technologies."**

There are many definitions of cybercrime. Based on information provided by the FBI and our own experience as CPAs, a cybercrime is "an intended illegal act involving the use of computers or other technologies." Some examples include spreading computer viruses, stalking, phishing, perpetrating insider threats and causing a denial-of-service (DoS) attack (when an attacker atttempts to prevent legitimate users from accessing information or services). The criminal activity must take place in a virtual setting over the internet, on a local network or in the cloud.

According to C-SAFE, the Florida Cyber-Security Manual, cybercrimes share three elements:

1. Tools and techniques to perpetrate a crime
2. Approach or methodology for executing the criminal plan (known as a vector)
3. The crime itself that is the end result of those plans and activities; a cybercrime is the ultimate objective of the criminal's activities

TOP **CYBERCRIMES**

In 2012, global corporate account takeover **losses were about $455 million,** and jumped to **$523 million** in 2013.

CORPORATE ACCOUNT TAKEOVER

A corporate account takeover ranks among the fastest and stealthiest types of attack. It's costly and affects entities of all types and sizes. Cybercriminals engaging in this activity obtain an entity's financial banking credentials through social engineering and use malware to hijack the entity's computers for the purpose of stealing funds from that entity's bank account.

In 2012, global corporate account takeover losses were about $455 million and jumped to $523 million in 2013 according to Julie Conroy, fraud expert analyst and research director at the Aite Group. The growth rate continues to be robust and — in information provided by BankInfoSecurity and CUInfoSecurity's Tracy Kitten — is projected to reach nearly $800 million by the end of 2016.

THE CRIME'S COURSE

Although corporate account takeovers can vary, we are discussing primarily electronic-funds-transfer fraud, such as Automated Clearing House (ACH) or wire transfer. To perpetuate these types of schemes, criminals take three steps:

1. *Illicitly acquire login credentials.* The credential compromise usually is accomplished by using a malicious program distributed as an email attachment, unintended web browsing download or file transfer of a seemingly legitimate/safe file. The user inadvertently downloads and installs a malicious program, such as a Trojan, and usually is unaware that anything threatening is occurring.

2. *Covertly gain unauthorized access to the victim's computer to avoid the bank's security features, activated when it does not recognize the login "fingerprint."* When customers open accounts at financial institutions, login "fingerprints" are created as an extra security measure. With every subsequent login, the fingerprint verifies the legitimacy of the person who's accessing the account. If the fingerprint doesn't match, the process triggers an additional layer to the login, such as a security question or a temporary PIN. In this step, the cybercriminal uses a hacker tool to hijack the victim's computer system, using the system as a trusted source to avoid the security check of the bank's login fingerprint. This approach allows the criminal to conduct fraudulent wire transfers out of the victim entity's bank account.

3. *Transfer the victim's bank funds to an account the cybercriminal controls.* The cybercriminal typically wires most, if not all, of the funds out of the victim's funds, usually by wire transfers. The cybercriminal typically transfers the funds to individuals known as money mules who in turn move the funds to an unregulated account, such as an overseas bank account in a country that is uncooperative with U.S. banking rules and protocols.

THE CHALLENGE FOR CPAs

Cybercriminals typically target small- and medium-sized businesses (SMBs) because these organizations tend to pay less attention to information security, controls and risk assessments and are therefore more vulnerable than larger entities. In many cases, SMBs don't have enough staff in the finance function and not all staff have the level of expertise to spot these issues, which can lead to further risks.

Chief accounting officers (CAOs), chief financial officers (CFOs), treasurers and controllers are particularly at risk because they are both easily identifiable online and are most likely to conduct online banking transactions for their entities. The savvy cybercriminal also knows the steps to take to access accounts, as well as the security features associated with online banking.

There are at least two risk areas for CPAs who perform online banking transactions. First, the CAO, CFO, treasurer or controller often is unaware of corporate account takeovers and the repercussions and liability that can follow. Second, there is a lack of adequate controls over the online banking process. However, a cybercriminal's persistent attack can overcome even fairly stringent controls, and these controls can create a false sense of security when, in reality, there still is substantial risk.

There are at least two risk areas for CPAs who perform online banking transactions. **First, the CAO, CFO, treasurer or controller often is unaware of corporate account takeovers**, and the repercussions and liability that can follow. **Second, there is a lack of adequate controls over the online banking process.**

CPAs can help educate their SMB clients about this type of cybercrime. CPAs in management accounting or other key positions of responsibility at an SMB should become knowledgeable and vigilant of the full-range of controls and vulnerabilities related to online banking.

IDENTIFY THEFT

Identity theft typically occurs when a cybercriminal successfully steals personally identifiable information (PII). According to NIST's *Guide to Protecting the Confidentiality of Personally Identifiable Information*, PII is any information about an individual an agency maintains, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, Social Security number, and date and place of birth, mother's maiden name or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial and employment information. This type of cybercriminal does not really benefit unless there is a financial reward for the effort or some type of damage that can be done with the data. Consequently, identity theft serves as a gateway to other cybercrimes, such as tax-refund fraud, credit-card fraud, loan fraud and other similar crimes.

Some examples of the malicious purpose behind identity theft include:

- Opening a line of credit
- Purchasing goods or services
- Renting or buying a house or apartment
- Receiving medical care
- Obtaining employment
- Obtaining prescriptions
- Committing traffic infractions or felonies
- Auction and wage-related fraud
- Extortion

THE CRIME'S COURSE

According to the Identity Theft Resource Center (ITRC), identity theft complaints ranked first in 2014 in the Federal Trade Commission's (FTC) list of complaints. In fact, identity theft was the FTC's No. 1 complaint for 15 consecutive years. A 2016 Javelin Strategy & Research survey shows identity-fraud victims were at the second-highest level in six years, having stolen $112 billion in the past six years.

Identity theft can go undetected for a significant period of time — **50% of identity thefts go undetected for at least one month**, and **10% remain undetected for two or more years.**

Identity theft can go undetected for a significant period of time — 50% of identity thefts go undetected for at least one month, and 10% remain undetected for two or more years. It also is becoming more common for cybercriminals to steal PII, hold that information for some time and then use it. They partly take this approach to build a mass of PII that can later be used to commit a massive crime.

These circumstances can escalate financial or reputational damage that may follow, and add to the challenge of apprehending the perpetrator. In addition, victims spend an average of 200 hours of work over six months to reestablish their identity, making time lost in some cases as damaging as the financial or reputational damage itself.

THE CHALLENGE FOR CPAs

The opportunity for identity theft lies in PII, the same source as tax-refund fraud. This information can be found in multiple locations across the internet, such as social media, phone registries, school records, etc. There also is an active black market for PII, which is relatively easy to steal through social engineering, dumpster diving, phishing and credit-card skimming.

As CPAs, we hold PII in our records such as client data and records, and thus, have an obligation to protect it. Entities need to exercise due diligence in protecting PII because it is not only good customer service, but also minimizes lawsuits or violations of state and federal laws. Forty-seven states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have laws regarding security breaches of PII.

If a breach occurs, the costs for failing to comply are high, and include legal action. For example, the Massachusetts law, known as MASS 201, allows the Massachusetts attorney general to sue any company that has a security breach if the company is found to be noncompliant with the law's requirements. This law has given rise to MASS 201 compliance audits in Massachusetts, ensuring that entities have taken reasonable precautions to protect the PII of Massachusetts' citizens.

DATA THEFT

Sensitive data, including unencrypted credit-card information a business stores, PII, trade secrets, intellectual property, source code, customer information and employee records, all attract cybercriminals' attention. This cybercrime overlaps with previous PII discussions, identity theft and security breaches. The cost to its victims can be detrimental, and involve public-image damage and financial costs related to loss of business, legal fees and increasing security measures.

THE CRIME'S COURSE

The crime occurs when a cybercriminal gains access to and steals sensitive data. It can be as simple as copying an entity's customer data files onto a flash drive and selling it to a competitor or using confidential or proprietary information to compete with the entity's business.

Sometimes, these crimes target governments or other large organizations with more resources. Often referred to as an advanced persistent threat (APT), a combination of malicious methods are used to first infect an organization's networks. Then, the threat agent proceeds to monitor activity and siphon data in an undetected manner over an extended period of time. (Source: Page H-4 Footnote 82 NIST SP 800-39 *Managing Information Security Risk: Organization, Mission, and Information System View*.)

A prime example of an incident involving APT is the United States Office of Personnel Management (OPM) breach that was discovered in 2015. In one of the more convoluted breaches to make the headlines, it involved not only the OPM, but also two other government contractors, resulting in several breaches over a period lasting longer than a year. The series of breaches induced the loss of background investigation records and affected 21.5 million people and their personnel data, as well as the data of 4.2 million current and former federal employees. Unfortunately, it's not the sheer magnitude of victims that makes this particular incident so devastating but, instead, the extremely sensitive nature of the data. (Source: FCW, "Full dollar cost of OPM breach still a giant unknown.")

THE CHALLENGE FOR CPAs

Cybercriminals could easily target CPA firm data. Most SMBs don't have the resources to recover from the publicity fallout that follows a data theft incident. As seen with the OPM breach, once access is gained, the results can be catastrophic.

RANSOMWARE

Unstolen data is not necessarily safe from cybercriminals who use ransomware, a type of malware that, once installed, restricts access to files or entire systems until extortion payment is received. In addition to siphoning data from your firm, cybercriminals now hold your data hostage in exchange for a hefty sum of money.

THE CRIME'S COURSE

The crime begins when users click on a malicious link and unknowingly install ransomware on their systems. The malicious link can be in an email, website or bundled with software.

> Once the ransomware installs, it can take the form of scareware, which **coerces users to pay for unencrypted files or to unlock access to systems**.

Once the ransomware installs, it can take the form of scareware, which coerces users to pay for unencrypted files or to unlock access to systems. (Source: *PC World*, "How to Rescue Your PC From Ransomware.")

One of the more publicized instances occurred in a February 2016 ransomware attack on Hollywood Presbyterian Medical Center. Initially, the news reports stated the cybercriminals demanded $3.6 million. The hospital defied these demands and was denied access to various servers and systems for 10 days, severely impacting its operations. Ultimately, the hospital negotiated, and, for $17,000, the cybercriminals delivered the key codes. (Source: *Los Angeles Times*, "Hollywood hospital pays $17,000 in bitcoin to hackers; FBI investigating."

THE CHALLENGE FOR CPAs

Ransomware can be a lucrative line of work for cybercriminals. Rendering sensitive data unavailable to its users, and demanding large sums of money, is a crime that likely will not diminish in the near future. Cybercriminals often will select targets whose organizations will fail to function immediately without access to certain types of data.

WHAT **YOU CAN DO**

CPAs need to make timely, informed decisions about the **effective controls that can prevent cybercrimes from occurring, and detect, at their earliest stages**, crimes that already have transpired.

CPAs need to make timely, informed decisions about the effective controls that can prevent cybercrimes from occurring, and detect, at their earliest stages, crimes that already have transpired. Once crimes are detected, it is equally important that CPAs respond deftly. For example, reliable backups are one way to respond to ransomware.

In addition to raising awareness of the four cybercrimes detailed here, this white paper offers three ways to mitigate risk.

1. CONDUCT A SECURITY AUDIT AND ASSESS CONTROLS

A Computer Security Institute (CSI) survey ranked internal cybersecurity audits as the strongest weapon in preventing and detecting cybersecurity vulnerabilities. An effective internal security audit identifies cybersecurity risks and assesses the severity of each type of risk. For optimal results, CPAs should audit their clients' privacy and security policies and controls.

Following the audit, preventive controls need to be instituted for the major risks that were identified. Some best practices that can help management develop those controls include:

- Proactively patching vulnerabilities, including vulnerable software
- Using least-access privileges and other sound logical access controls to help remediate crimes perpetrated internally; for external threats, sound perimeter controls such as firewalls, intrusion prevention systems (IPS) and intrusion detection systems (IDS) are critical to protection
- Monitoring systems, technologies and access with associated controls varying based on the threat level (also a detection strategy); for example, use various logs created by technologies for those activities
- Data backups, including offline versions

2. RETAIN BUSINESS INSURANCE

In an age of financially motivated cybercrimes, every entity should have sufficient business insurance coverage, such as business continuity/disaster recovery or cyber insurance, to recover financial losses. Executive management team members, especially the CFO, must evaluate the entity's insurance coverage to ensure it could recover estimated losses from any cybercrime.

Reviewing coverage should be done on a reasonable periodic basis. Leaders also might consider enlisting service providers that offer forensic, cleanup and restore functions after certain crimes have been committed.

3. CREATE AN INCIDENT RESPONSE PLAN

Despite not being preventative, one useful correction remediation is to develop an incident response plan. The plan would require employees with the necessary level of knowledge and serving in key positions within the entity to answer the following questions relating to the cybercrimes identified in this white paper:

- Which of these crimes are potential risks?
- What risks would follow from each crime?
- How should we respond to each of these crimes?
- How would we fully recover from each of these crimes?
- Do we have appropriate skill set on staff or on a retainer contract?

The manner in which an entity responds to a cybercrime provides valuable insight into its possible vulnerabilities and preventive steps that could have been taken before the crime occurred.

Time after time, research organizations that report on breach statistics all report that 90% of breaches could have been avoided if reasonable security controls had been in place at the time of the incident. A good place to start *before* a breach occurs is with reasonable security controls defined by the information security profession as best practices or principles. Best practices include employee training.

Remediation measures and controls that apply to one cybercrime often apply equally well to others, which result in multiple cybercrimes being addressed with a single countermeasure. This further supports the position that the measures and controls entities take once a cybercrime occurs are the same measures and controls that should have been in place before the breach.

CONCLUSION

Cybercrime is more prevalent, more damaging and more sophisticated than ever before. CPAs need to gain a clear and general understanding of the major threats, risks, costs and other negative factors associated with it as well as the degree to which these factors relate to their employer (public practice or business and industry) and/or clients (public practice). They also need the ability to identify perpetrators and learn their methodology.

The proliferation of cybercrimes does not require the CPA to assume the role of cybersecurity expert. However, by becoming and remaining informed and aware of the core elements of cybercrime and by seeking assistance from security professionals when necessary, CPAs can best identify preventive, detection and reparative measures. In the process, they can ensure the safety, security and future success for themselves, as well as for the individuals and entities they serve.

ABOUT THE AUTHORS

Jeff Streif, CPA, is chief financial officer at Koller Enterprises Inc. in Fenton, MO. Before joining Koller, Jeff worked on SSAE16 (SOC 1) engagements; SOC 2 engagements; PCI compliance; ITGC and application control reviews; IT risk assessments; penetration and vulnerability assessments; and data mining. Contact Jeff at jstreif@kollerenterprises.com.

Lisa Traina, CPA/CITP, CGMA, is a partner at Traina & Associates, a CapinCrouse Company. Traina & Associates provides cybersecurity audit and consulting services to a number of industries, including not-for-profits, financial institutions; hospitals and medical practices; professional service firms; and others. Contact Lisa at ltraina@capincrouse.com.

Steven J. Ursillo Jr., CPA/CITP, CGMA, is a principal and director of Technology & Assurance Services for Sparrow, Johnson & Ursillo Inc., in West Warwick, RI. Contact Steve at sursillojr@sju.com.

Steven co-chairs the AICPA IMTA Cybersecurity Task Force and Jeff and Lisa serve as members on that task force.

888.777.7077 | service@aicpa.org | aicpa.org

22795-256