

THE TOP 5 CYBERCRIMES



October 2013

AUTHOR:

Tommie Singleton, CPA/CITP/CFF, Ph.D.
Director of Consulting Services
Carr Riggs & Ingram
Enterprise, AL

CONTRIBUTOR:

Randal Wolverton, CPA/CFF, CFE
Randal A. Wolverton CPA LLC
Kansas City, MO

EDITOR:

Mark Murray
New York, NY

REVIEWERS:

Barbara Andrews
Project Manager
Forensic and Valuation Services
AICPA
Durham, NC

Jeannette Koger
Vice President
Member Specialization and Credentialing
AICPA
Durham, NC

Copyright © 2013 American Institute of CPAs. 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	2
Introduction	3
Scope of Cybercrimes	4
Top Five Cybercrimes	5
1. Tax-Refund Fraud	6
2. Corporate Account Takeover	7
3. Identity Theft	8
4. Theft of Sensitive Data	9
5. Theft of Intellectual Property	10
General Remediation Strategies for the Top Five Cybercrimes	11
Security Audits and Controls	11
Business Insurance	11
Incident Response Plan	12
Conclusion	13
Resources	14

EXECUTIVE SUMMARY

There is no doubt today that virtual environments have introduced new levels of efficiency, connectivity and productivity to businesses of all types the world over. However, along with these undisputed benefits has come an equally real and serious threat that each year results in hundreds of millions of dollars in measurable and unmeasurable losses to businesses — aggressive invasions by criminals into a business's virtual environment.

Among the victims of these cybercrimes are CPAs in public practice and their clients as well as CPAs and the entities they serve in business and industry. The prevalence of cybercrime, and the escalating fervor and inventiveness of perpetrators, have led to a harsh reality: it is not a matter of if CPAs, their clients or their organizations will become a victim, but **when**.

In the midst of such a demonstrated, multi-faceted threat, CPAs have a pressing need for resources and straightforward strategies that can help them avoid the risk of cybercrime, detect and recover from these crimes when they occur, and safeguard the interests of their firm, clients and organization.

The Top 5 Cybercrimes is among the resources that the AICPA offers to assist CPAs in addressing cybercrime. It identifies not only the top five cybercrimes that are of greatest concern to CPAs but also the nature of each crime, the manner in which it is committed and remedial steps that can be taken.

The top five cybercrimes being discussed are:

- 1.** Tax-refund fraud
- 2.** Corporate account takeover
- 3.** Identity theft
- 4.** Theft of sensitive data
- 5.** Theft of intellectual property

The paper concludes with a list of resources offered by the AICPA, cybersecurity/cybercrime organizations, federal government agencies and federal/public partnerships.

INTRODUCTION

Cybercrimes have risen so dramatically in recent years that they have seemingly **replaced old-fashioned, organized crime.**

The proliferation of technology devices and other equipment; their pervasive use across age, gender, socioeconomic and geographic boundaries; and, for many, a false sense of information security have merged to create a perfect storm for cybercriminal activity. In fact, cybercrimes have risen so dramatically in recent years that they have seemingly replaced old-fashioned, organized crime.¹

A cybercrime is defined as an intended act involving the use of computers or other technologies, and the criminal activity must take place in a virtual setting, such as the Internet.² 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.** Crime itself that is the end result of those plans and activities (a cybercrime is the ultimate objective of the criminal's activities)

The Top 5 Cybercrimes focuses on specific cybercrimes affecting CPAs in public accounting and those in business and industry. The list of cybercrimes is tailored to the CPA's perspective and experience, and may differ somewhat from a general list of cybercrimes compiled by other groups or organizations, most of which focus on the vectors or tools.

¹ For instance, *Consumer Reports*, June 2011 issue online, states this fact and produces the actual prices paid on the black market to gangs in Eastern Europe, in particular, that enable theft of credit cards and other cybercrimes. Last viewed Oct. 10, 2012 at consumerreports.org.

² Florida Cyber-Security Manual, Secure Florida, November 2004, p. 150. Available from secureflorida.org.

SCOPE OF CYBERCRIMES

In 2011, online revenue losses resulting from **fraudulent transactions were estimated to be \$3.4 billion**, up from \$2.7 billion in 2010.

Virtual environments have become fertile territory for cybercrime, with the number of crimes escalating each year along with the severity of losses. In 2011, online revenue losses resulting from fraudulent transactions were estimated to be \$3.4 billion, up from \$2.7 billion in 2010.³ Revenue losses are based only on fraud associated with e-commerce and exclude fraud involving theft/loss of mobile devices and other forms of cybercrimes.

Companies participating in a 2012 Ponemon Institute study suffered an **average of 102 successful cyberattacks per week**, up from 72 in 2011.

Credit-card fraud was up 32 percent from 2009 to 2010. The average dollar amount of fraudulent transactions also increased by 34 percent.⁴ Federal Reserve statistics place credit-card fraud costs to U.S. businesses at \$52.6 billion annually.⁵

In 2010, 32 percent of U.S. consumers reported a credit-card fraud had occurred in the last five years. In 2009, that figure was 27 percent over the previous five years.⁶ Most of those credit cards were compromised in a virtual setting and therefore should be viewed as cybercrime.

Growth in cybercrimes and their attendant costs are documented in a 2012 Ponemon Institute study. In the study, 56 large U.S. businesses surveyed reported an average annual cost of \$8.9 million for cybercrimes, with costs reaching \$46 million for one company. The average annual cost climbed six percent from the 2011 study. Companies participating in the study suffered an average of 102 successful attacks per week, up from 72 in 2011. The report concluded that cybercrime appears to be worsening, and that 51 percent of CEOs reported that their companies have been attacked either daily or hourly.⁷

³ Cybersource, 2012 Online Fraud Report (13th annual report), 2012, cybersource.com. Last viewed Oct. 8, 2012.

⁴ "Online Credit Card Fraud Jumps 32 Percent as U.S. Economic Woes Continue," Oct. 12, 2012, Kikabink News, kikabink.com. Last viewed Oct. 12, 2012.

⁵ Fox News, "Mastercard Warns of Possible Security Breach, Visa Also Reportedly Affected," March 30, 2012, online at foxnews.com. Last viewed Oct. 12, 2012.

⁶ Consumer Reports, June 2011. Last viewed Oct. 10, 2012 at consumerreports.org.

⁷ Ponemon Institute, 2012 Cost of Cyber Crime Study, Oct. 8, 2012. Available from ponemon.org.

TOP 5 CYBERCRIMES



A broad range of reports and authoritative sources were analyzed to separate vectors and tools from the actual cybercrimes. The sources include the AICPA, Cybersource Corporation,⁸ Internet Crime Complaint Center (IC3),⁹ IBM,¹⁰ SANS,¹¹ Computer Emergency Response Team (CERT),¹² Computer Security Institute (CSI),¹³ Ponemon Institute,¹⁴ Microsoft, Verizon and Secure Florida.¹⁵

Once the cybercrimes were identified, they were ranked in the following order by relevance to CPAs in public practice and business and industry.

⁸ Cybersource Corporation is a worldwide eCommerce payment-management company. It publishes annual, statistics-based online fraud reports. At cybersource.com.

⁹ IC3 is the Internet Crime Complaint Center, sponsored by the National White Collar Crime Center, the Bureau of Justice Assistance and the FBI. It accepts complaints from the public regarding Internet-related crimes and scams. At ic3.gov.

¹⁰ IBM publishes a security report titled Trend and Risk Report. The March 2012 report was used as a source for this paper.

¹¹ SANS has a global scope, with a focus on information security (InfoSec). It has a certification, Global Information Assurance Certification (GIAC), related to InfoSec. SANS's services and resources are generally free to the public.

¹² Computer Emergency Response Team (CERT) is a partnership between Homeland Security and public and private sectors with the objective of coordinating responses to security threats. At cert.org.

¹³ Computer Security Institute (CSI), for information security professionals, provides an annual survey of cybercrime, CSI Computer Crime & Security Survey, since about 1999. At gocsi.com.

¹⁴ Ponemon Institute conducts independent research on privacy, data protection and information security policy. It has one of the best cybercrime studies, its annual Cost of Cyber Crime Study. The second study was published in August 2011. At ponemon.org.

¹⁵ The state of Florida has a department, Secure Florida, that focuses on cybersecurity. It published Florida Cyber-Security Manual in 2007. The Florida Department of Law Enforcement, Florida Cybersecurity Institute and Secure Florida contributed to the manual. At secureflorida.org.

1. TAX-REFUND FRAUD¹⁶

Tax-refund fraud has become rampant in recent years. An article from the October 2012 issue of the *Journal of Accountancy* relayed a single incident where three defendants were charged with filing more than 5,000 false tax returns using the Social Security numbers of deceased taxpayers to claim fraudulent refunds totaling about \$14 million.¹⁷

A second *Journal of Accountancy* article quotes a U.S. Treasury Inspector General of Tax Administration (TIGTA) report that suggests the IRS failed to notice 1.5 million tax returns associated with (potentially identity theft-related) fraudulent tax refunds in excess of \$5.2 billion for the 2011 tax season. The IRS simultaneously reported that it detected nearly 1 million tax returns with fraudulent refunds of \$6.5 billion in the same tax season.¹⁸ The city of Tampa, FL, alone estimates that in the past two years, cybercriminals have cashed in \$450 million in fraudulent tax refunds.¹⁹

THE CRIME'S COURSE

Cybercriminals first obtain a valid name and Social Security number, preferably from someone who will not be filing a tax return. That person could be a deceased taxpayer. They will obtain this information using social engineering or email phishing, purchasing the data on the black market, or using other avenues. Sellers on the black market typically have some degree of access to the necessary personally identifiable information — person's name, Social Security number, address and date of birth — from their workplace. They usually are insiders at high-traffic businesses such as hospitals, doctors' offices or car dealerships that capture such information.

The cybercriminal next makes up wage and withholding information, claims standard deductions or a few itemized deductions, and perhaps tax credits, and completes a return that generates a large refund. He or

she files the fraudulent tax return electronically, which technically makes it a cybercrime and not ordinary fraud. Cybercriminals file electronically because W-2s are not included with electronically filed tax returns, and by the time the IRS discovers that the return does not match up with a W-2, the crime is complete and the cybercriminal has absconded with the funds.

The criminal then simply waits for either a check to be mailed, a direct deposit to be made to a "safe" bank account or, most commonly, a credit to be posted to a debit card. The debit card is bought specifically for accepting the fraudulent refunds. Often, multiple refunds are sent to the same address, bank account or debit card because the cybercriminal will complete dozens, if not hundreds, of fraudulent tax returns.

THE OPPORTUNITY FOR CYBERCRIMINALS

All taxpayers are at some risk of becoming victims of tax-refund fraud. It is not difficult for cybercriminals to use one or more of their tools and techniques to search for and fraudulently obtain personally identifiable information from the Internet or other sources. Surprisingly, the cybercriminals usually do not use a deceased person's personally identifiable information but rather that of a living person. Reports indicate that when a legitimate taxpayer's personally identifiable information is used, it can take about 12 months for the IRS to resolve the issue and release the refund to the taxpayer.

If a cybercriminal can obtain the relevant personally identifiable information, carrying out tax-refund fraud is fairly straightforward and somewhat detection-proof. In addition, tax-refund fraud is exacerbated by the number of entities that have personally identifiable information and the extent of exposure it presents. CPAs engaged in tax work should assess their privacy and security policies, and establish internal controls to keep client data secure.

¹⁶ Also see Identity Theft section.

¹⁷ Schreiber, Sally P., "Dozens Indicted on Stolen Identity Tax Refund Fraud Charges," *Journal of Accountancy* (online), Oct. 11, 2012. Last viewed Oct. 11, 2012, at journalofaccountancy.com.

¹⁸ Schreiber, Sally P., "TIGTA Recommends Identity Theft Safeguards," *Journal of Accountancy* (online), October 2012. Last viewed Oct. 11, 2012, at journalofaccountancy.com.

¹⁹ CNN, "IRS Policies Help Fuel Tax Refund Fraud, Officials Say," March 20, 2012, CNN online. Last viewed Oct. 10, 2012, at cnn.com.

2. CORPORATE ACCOUNT TAKEOVER²⁰

During the summer of 2008, a different type of cybercrime was identified — corporate account takeover. It is costly and ranks among the fastest and most stealthy type of attack. Cybercriminals engaging in this activity surreptitiously obtain an entity's financial banking credentials, use software to hijack one of its computers remotely and steal funds from the entity's bank account, often costing the entity thousands of dollars.

According to David Nelson, FDIC Cyber Fraud and Financial Crimes Section specialist, small- and mid-size businesses (SMBs) and their financial institutions suffered about \$120 million in losses due to electronic funds transfer fraud in the third quarter of 2009, up from about \$85 million from two years earlier. According to the FBI, November 2009 losses alone were about \$100 million.²¹

THE CRIME'S COURSE

Although corporate account takeovers can take different forms, the discussion here primarily is limited to electronic funds transfer fraud, such as Automated Clearing House (ACH) or wire transfer. These types of schemes involve 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 allows this malicious program, such as a Trojan, to be downloaded and executed, and usually is unaware that anything malicious 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."*²² 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 controlled by the cybercriminal.* The cybercriminal transfers most, if not all, of the funds in the victim's bank account, usually by wire transfers. The criminal typically transfers the funds to individuals known as money mules, who move the funds to a protected account such as an overseas bank account in a country that is uncooperative with U.S. banking rules and protocols.

THE OPPORTUNITY FOR CYBERCRIMINALS

SMBs are the targets for this crime because they tend to pay less attention to information security, controls and risk assessments. Thus, their systems tend to be more vulnerable than larger entities. SMBs also have resource constraints, including finances and expertise, which can lead to further risks.

According to David Nelson, FDIC Cyber Fraud and Financial Crimes Section specialist, small- and mid-size businesses (SMBs) and their financial institutions **suffered about \$120 million in losses due to electronic funds transfer fraud** in the third quarter of 2009, up from about \$85 million from two years earlier. According to the FBI, November 2009 losses alone were about \$100 million.

²⁰There is a full article in the *Journal of Accountancy* addressing this cybercrime. Singleton & Ursillo Jr., "Guard Against Cybertheft," *Journal of Accountancy*, Vol. 210, No. 4 (October 2010), pp. 42-44, 46, 48-49.

²¹Savage, Marcia, "FDIC: ACH Fraud Losses Climb Despite Drop in Overall Cyberfraud Losses," *Financial Security*, March 8, 2010, online at searchfinancialsecurity.com.

²²To ensure security of customer accounts, financial institutions create login "fingerprints" of the computer system when customers open their accounts and for all future logins. The fingerprint verifies that the person logging into the account is the legitimate account holder, a process known as authentication. When the fingerprint does not match, the process triggers an additional layer to the login, such as a security question or temporary PIN.

The specific person targeted often is the person most likely to be conducting online banking transactions for the entity, such as the chief accounting officer (CAO), chief financial officer (CFO), treasurer or controller, all of whom are relatively easy to identify online. The savvy cybercriminal also knows the steps that need to be taken to access accounts as well as online banking's typical security features.

There are at least two risk areas for clients of CPAs and CPAs in business and industry 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. According to one source, a survey of small businesses reported that only 18 percent of those surveyed understood they are liable for cyber losses, which reveals a severe lack of basic cybercrime knowledge.²³

Second, there is a lack of adequate controls over the online banking process. However, even fairly stringent controls can be overcome by a cybercriminal's persistent attack, and these controls can create a false sense of security when, in reality, there still is substantial risk.

What makes corporate account takeovers a particular concern for CPAs is cybercriminals preferring to target SMBs — businesses that compose, or could compose, a large segment of public accounting firm clients or have management accountants on their staff.

CPAs can help educate their SMB clients about this type of cybercrime. For CPAs in management accounting, and often in a key position of responsibility for this type of fraud, they should become knowledgeable and vigilant of the full range of controls and vulnerabilities of online banking.

Fifty percent of identity thefts goes undetected for at least one month and 10 percent remains undetected for two or more years.

3. IDENTITY THEFT

Identity theft typically occurs when a cybercriminal successfully steals a person's personally identifiable 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. Thus, 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 identity theft's malicious purposes are:

- ▶ Opening a line of credit
- ▶ Purchasing goods or services
- ▶ Renting or buying a house or apartment
- ▶ Receiving medical care
- ▶ Obtaining employment

Other examples include committing traffic infractions or felonies, auction fraud and wage-related fraud.

THE CRIME'S COURSE

According to the Identity Theft Resource Center (ITRC), identity theft complaints ranked first in 2012 in the Federal Trade Commission's (FTC) list of complaints, with a 32 percent increase over 2011. Identity theft has been the FTC's No. 1 complaint for 13 consecutive years. A Javelin Strategy & Research survey shows an increase of 13 percent in 2011 compared with 2010, and a total of 11.6 million victims in the United States in 2011.²⁴

²³ Yurcan, Brian, "Fraud on the Decline, But Still a Concern," *Bank Systems & Technology*, Aug. 26, 2011, online at niceactimize.com.

²⁴ Javelin Strategy & Research, 2011 survey. Reported by *Digital Trends*, Feb. 22, 2012, online at digitaltrends.com.

Identity theft can go undetected for a significant period of time — 50 percent goes undetected for at least one month and 10 percent remains undetected for two or more years. It also is becoming more common for cyberthieves to steal personally identifiable information and hold that information for some time and then use it. This approach is taken partly to build a mass of personally identifiable information that can later be used to commit a massive crime.

These circumstances can escalate financial or reputation damage that may follow and add to the challenge of apprehending the perpetrator. In addition, victims spend an average of 200 hours re-establishing their identity, making time lost in some cases as damaging as the financial or reputational damage.²⁵

THE OPPORTUNITY FOR CYBERCRIMINALS

The opportunity for identity theft lies in the same source as tax-refund fraud: personally identifiable information. This information can be found in multiple locations across the Internet. There also is an active black market for personally identifiable information, which is relatively easy to steal. Social engineering and dumpster diving are additional ways to gather this type of information.

Entities need to exercise due diligence to protect personally identifiable information — it is good customer service and helps avoid lawsuits or violations of state or federal laws. Forty-six states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have laws regarding security breaches of personally identifiable information.

If a breach occurs, costs for failing to comply are high. 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 audits in Massachusetts, known as MASS 201 audits. These compliance audits ensure that entities have taken "reasonable" precautions to protect the personally identifiable information of Massachusetts' citizens.

4. THEFT OF SENSITIVE DATA

Sensitive data such as unencrypted credit card information stored by a business, personally identifiable information, trade secrets, source code, customer information and employee records all attract the attention of cybercriminals. This cybercrime overlaps with previous discussions of personally identifiable information, identity theft and security breaches. The costs to victims of this type of cybercrime can be high, and involve both 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 sensitive data and steals it. The crime 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.

An incident occurred in 2012 at the South Carolina Department of Revenue that illustrates this cybercrime. Cybercriminals broke into the department's computer systems and stole 3.6 million Social Security numbers and 387,000 credit/debit card numbers. The breach, which began in late August, was not discovered until Oct. 10 by the U.S. Secret Service.

The cybercriminal used a foreign Internet address, which is common to this type of crime. In September, the intruder conducted several attacks and gained unauthorized access to tax returns dating back to 1998. According to department officials, the system was secured on Oct. 20.²⁶

²⁵ Florida Cyber-Security Manual, Secure Florida, 2007, available online at secureflorida.org.

²⁶ Bonner, Paul, "S.C. Taxpayers Social Security Numbers, Credit Cards Hacked," *Journal of Accountancy*, Nov. 1, 2012.

THE OPPORTUNITY FOR CYBERCRIMINALS

Opportunities abound for this type of cybercriminal. First, South Carolina Department of Revenue employees did not discover the breach — the federal government did. Second, the length of time from intrusion to discovery was more than 45 days. It took 10 days to secure the systems upon discovery.

The time lost in discovering the crime and securing the system no doubt created opportunities for additional data losses. The facts also illustrate that the criminals likely attacked the South Carolina Department of Revenue because they believed its security would be weak enough to allow a successful attack on valuable data.

There are other opportunities for an attack on government and state agencies, scores of which have systems that house personally identifiable information and other sensitive data.

5. THEFT OF INTELLECTUAL PROPERTY

Intellectual property, including commercial, copyrighted materials — music, movies and books — also is at risk of being stolen. Although music owners have risen on the list of victims of cybercrime in the past decade, commercial entities that hold copyrights or patents need to also remain on guard.

Intellectual property theft is complicated by state-sponsored hacking, especially China. According to a *New York Times* article, Chinese hackers have stolen product blueprints, manufacturing plans, clinical trial results, pricing documents, negotiation strategies and other proprietary information from a large number of commercial entities in the United States, including Coca-Cola, Lockheed Martin and many others.²⁷

THE CRIME'S COURSE

Cybercriminals usually are extremely specific when identifying the intellectual property they want to confiscate or otherwise use in an unauthorized manner. For instance, they commit commercial espionage if they locate and steal a competitor's intellectual property.

According to the FBI, preventing intellectual property theft is a priority for its criminal investigative program. The FBI is focusing on theft of trade secrets and product infringements, such as counterfeit parts and other products that threaten safety.²⁸

More commonly, cybercriminals access entertainment intellectual property, such as movies, music and books, and use it without payment or they sell it for profit without complying with copyright laws or purchasing it legitimately.

THE OPPORTUNITY FOR CYBERCRIMINALS

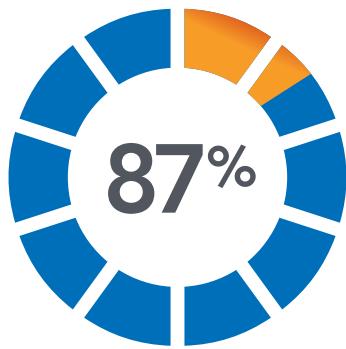
Among the factors making intellectual property in electronic format vulnerable to theft by cybercriminals are Internet features that allow it to be quickly and easily moved, downloaded, uploaded and shared. The only requirement is that it exist on a server connected to the Internet. Music can be purchased once and sold hundreds of times by loading a CD/DVD online then including it for sale on a website.

CPAs therefore need to work with their clients to perform privacy and security reviews to assess the client's level of risk.

²⁷ "Hackers from China Resume Attacks on U.S. Targets," *The New York Times*, May 19, 2013. Last accessed online July 18, 2013, at nytimes.com.

²⁸ Intellectual Property Theft. Last accessed July 18, 2013, at fbi.gov.

GENERAL REMEDIATION STRATEGIES FOR THE TOP 5 CYBERCRIMES



A Verizon study of 600 incidents of security breaches over a five-year period reveals that in 87 percent of cases, investigators concluded that **breaches could have been avoided if reasonable security controls had been in place** at the time of the incident.

CPAs need to make timely, informed decisions about the effective controls that can prevent cybercrimes from occurring, and detect, at its earliest stage, a crime that already has occurred. Equally important is CPAs' adeptness at responding to and correcting a security breach and cybercrime that has occurred.

SECURITY AUDITS AND 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, clients should ask their CPA to audit their privacy and security policies and controls.

Following the audit, preventive controls for the major risks that were identified need to be instituted. Three strategies that can help management develop those controls are:

- ▶ Timely and proactively patching vulnerabilities, including vulnerable software.
- ▶ Using least-access privileges²⁹ and other sound logical access controls to help remediate crimes perpetrated internally. For external threats, sound perimeter controls such as firewalls and Intrusion Detection Systems (IDS) are critical to protection.
- ▶ Monitoring systems, technologies and access, such as various logs created by technologies for those activities, with associated controls varying based on the threat level (also a detection strategy).

BUSINESS INSURANCE

In an age of financially motivated cybercrimes, every entity should have sufficient business insurance coverage to recover any financial losses. Executive management team members, especially the CFO, must evaluate the entity's insurance coverage to ensure that 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 cleanup and restore functions after certain crimes have been committed.

²⁹ "Least-access privileges" is a security concept that grants a person the least amount of access to systems, technologies and data needed to perform his/her duties or that first grants a person no access but then adds privileges to provide access only to needed information.

INCIDENT RESPONSE PLAN

One useful “correction” remediation, although not preventive, 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 top five 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?

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.

A Verizon study of 600 incidents of security breaches over a five-year period reveals that in 87 percent of cases, investigators concluded that breaches could have been avoided if reasonable security controls had been in place at the time of the incident. Thus, a good place to start BEFORE a breach occurs is reasonable security controls as defined by the information security profession as best practices or principles.³⁰

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



³⁰ Verizon’s 2009 Data Breach Investigations Report. At securityblog.verizonbusiness.com.

CONCLUSION



Cybercriminals are drastically different from their gun-toting counterparts, whose menacing presence and intimidating demeanor play key roles in the execution of their crimes.

Cybercriminals rarely are in close physical contact with, and often not in geographic proximity to, their targets. However, their distance and anonymity diminish neither the incidents of their crimes nor the damage they can inflict. Quite the contrary, it is their very remoteness that helps them commit crimes that can be of equal or greater magnitude than traditional crimes, and hide their behavior and crimes from their victims and members of law enforcement.

Cybercrimes also share a number of common characteristics:

- ▶ Cybercriminals usually are located internationally, which makes finding and extraditing them difficult.
- ▶ Cybercrimes often are directed and targeted toward a specific person(s) or entity.
- ▶ Cyberattacks are multifaceted in terms of their tools, vectors and type, and at times, can lead to a cybercrime that is actually a combination of crimes.

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

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

RESOURCES

AICPA

- [AICPA Privacy Principles Scoreboard](#). A downloadable software tool that can help both organizations and CPA firms establish programs addressing the collection, usage, retention and disclosure of customer and employee personally identifiable information. Organizations can use the *Scoreboard*, which is based on the Generally Accepted Privacy Principles (GAPP) framework, internally, and CPAs in public accounting can use it to assess privacy risk and program maturity in client engagements. The *Scoreboard* can also be used when examining and reporting on a service organization's internal privacy controls.
- [Journal of Accountancy](#). The flagship publication of the American Institute of CPAs (AICPA) has been published continuously since 1905. journalofaccountancy.com
- [Complete Guide to the CITP Body of Knowledge](#). A comprehensive review of how to use information technology to effectively manage financial information and help prepare for the Certified Information Technology Professional (CITP®) Exam. CPE credit is available for this self-study course.
- [Cybersecurity webcast series \(archived\)](#). An eight-week series available to Information Management and Technology Assurance (IMTA) and Forensic and Valuation Services (FVS) section members. It provides an expansive overview of cybersecurity.
- [Information Management and Technology Assurance \(IMTA\) Section](#). An AICPA membership section offering tools and networking opportunities that help CPAs increase efficiency and boost profits through technology in areas ranging from information assurance, internal controls and business process improvement to data analytics and enhanced business reporting.
- [Forensic and Valuation Services \(FVS\) Section](#). An AICPA membership section offering tools, publications and networking opportunities that help CPAs who provide forensic and valuation services position their practice for growth and profitability.

CYBERSECURITY/CYBERCRIME ORGANIZATIONS

- *Cybersource Corporation* is a worldwide eCommerce payment-management company. It also publishes annual statistics-based online fraud reports. cybersource.com
- *Ponemon Institute* conducts independent research on privacy, data protection and information security policy. It has one of the best cybercrime studies — its annual Cost of Cyber Crime Study. ponemon.org
- *SANS Institute* has a global scope, with a focus on information security (InfoSec). It has a certification, Global Information Assurance Certification (GIAC), related to InfoSec. SANS's services and resources are generally free to the public. sans.org
- *Computer Emergency Response Team (CERT)* is a partnership between Homeland Security and public and private sectors with the objective of coordinating responses to security threats. cert.org
- *Computer Security Institute (CSI)*, for information security professionals, provides an annual survey of cybercrime, CSI Computer Crime & Security Survey, since about 1999. gocsi.com

FEDERAL GOVERNMENT AGENCIES AND FEDERAL/PUBLIC PARTNERSHIPS

- FinCEN — The Financial Crimes Enforcement Network, U.S. Department of the Treasury, fincen.gov
- FinCEN, *The SAR Activity Review — By the Numbers*, Issue 17, May 2012
- IC3 is the Internet Crime Complaint Center, sponsored by the National White Collar Crime Center, the Bureau of Justice Assistance and the FBI. It accepts complaints from the public regarding Internet-related crimes and scams. ic3.gov



888.777.7077 | service@aicpa.org | aicpa.org