Identity Hack!

Is Your Company Next?

By Elizabeth Mulig, CPA; L. Murphy Smith, CPA; and Clyde T. Stambaugh, CPA

They didn't see it coming.

The current wave of identity theft kicked off on December 19, 2013, with a Reuters headline screaming, "Target cyber breach hits 40 million payment cards at holiday peak." Then on September 18, 2014, another Reuters headline blared news of a second bombshell identity hack: "Home Depot breach bigger than Target at 56 million cards." And less than a month later, an October 2 Reuters headline revealed a still bigger crime, "JPMorgan hack exposed data of 83 million, among biggest breaches in history."

Could your company be next? What can you do to prevent it? Let's take a look at the problem and then identify some prevention tips.

Identity Theft Is Skyrocketing

Identity theft—stealing confidential information to access private financial and other accounts—has skyrocketed. A July 1, 2014, report posted on the website of the Washington, D.C., CBS radio stations reveals that big data breaches increased nearly 20% from last year. At that time there were already more than 10 million cases of identity theft reported in the United States, making it the most common consumer complaint (see "Report: 10 Million Identity Theft Cases, Most Common Consumer Complaint in US").

Table 1 lists the kinds of identity theft seen most often. That crime totalled 14% of the more than two million consumer complaints made to the Federal Trade Commission (FTC) in 2013, the most recent year for which statistics are available. Credit card fraud was the second most common identity crime.

Weaknesses in business or individual practices and procedures may expose identity data, risking significant financial losses. Criminals may open bank accounts, get loans, and rent apartments, homes, or offices. They can buy homes or automobiles, commit utilities fraud, forge checks, or commit other crimes by assuming a stolen identity. Thieves may also declare bankruptcy or obtain driver's licenses, travel visas, or other official government documents in the names of their victims.

What Company Data Is at Risk?

Identity thieves can target your business's financial information, employee information, customers' personal information, and more. That can include anything stored on the company computer system: entries from accounts payable or accounts receivable, business and employee bank account numbers, bank and computer access codes, business plans, employee records, customer information, and vendor data. Cyber criminals love to loot employee or customer personal information, such as Social Security numbers, dates of birth, mothers' maiden names, addresses, account numbers, and passcodes. And if data thieves get some information that they can't use directly, like your accounts receivable or accounts payable entries, they can sell it to business spies who can use it.

Company data accessed using smartphones, tablets, or laptops is also at risk. The trend at some companies to "bring your own device" opens up many more vulnerabilities for identity thieves to exploit. For example, apps on users' smartphones may not be secure. In a March 9, 2014, CNBC story, "Your apps might be spying on you, or worse," Cadie Thompson reported that a growing number of malicious mobile apps are doing everything from tracking people without their permission to completely taking over the smartphone's operating system.

But focusing only on employees and data within the company isn't enough because identity thieves can attack from unexpected directions. In a February 7, 2014, pcmag.com story, "HVAC Vendor Confirms Link to Target Data Breach," Stephanie Mlot revealed that hackers penetrated Target's systems using credentials they stole from a third-party vendor that makes heating, ventilation, and air conditioning (HVAC) systems.

What Are the Consequences?

Businesses suffer when trade secrets or other types of confidential information are breached. But one of the biggest business risks involves the theft of customer or vendor personal information from business records. Laws often require companies to notify those whose personal information has been stolen. And a data breach almost always causes a loss of public trust, resulting in sizeable financial losses and diminished business.

A breach also has legal consequences for companies. Privacy laws and regulations are complicated and varied—a bewildering tangle of older legacy laws and newer digital privacy provisions. They include everything from the Federal Trade Commission Act of 1914 to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Children's Online Privacy Protection Act of 1998 (COPPA, revised in 2012). Many states also have enacted privacy legislation that goes beyond the federal laws. Compliance with all these laws can be expensive and often requires legal and other professional

Table 1. The Most Common Forms of Identity Theft

Government documents/benefits fraud	34%
Credit card fraud	17%
Phone or utilities fraud	14%
Bank fraud	8%
Employment-related fraud	6%
Loan fraud	4%

This year, the FTC reported that identity theft cases made up 14% of its more than two million 2013 consumer complaints.

Source: FTC's Consumer Sentinel Network, "In the Spotlight: Identity Theft—Facts and Figures," National Criminal Justice Reference Service, January–December 2013, www.ncjrs.gov/spotlight/identity_theft/facts.html.

expertise. For a recent overview of the complex web of U.S. federal privacy laws affecting digital data, consult Eric A. Fischer's report for the Congressional Research Service, "Federal Laws Relating to Cybersecurity: Overview and Discussion of Proposed Revisions."

To make things even more complicated, new regulators may be getting involved in privacy. Lawyer David Munkittrick specializes in privacy and data security for the New York-based Proskauer law firm. In an October 29, 2014, blog titled "FCC: The New Data Security Sheriff In Town," he reported that the Federal Communications Commission recently assessed a $10 million fine on two telecommunications companies for not safeguarding customers' personal information.

Privacy laws also vary outside the U.S. For companies located or doing business abroad, a useful list of data protection and privacy laws in 26 jurisdictions worldwide has been compiled by Rosemary P. Jay in *Data Protection and Privacy 2014*.

The Red Flags Rule

One important regulation that management accountants in the financial industry should understand is the FTC's Red Flags Rule.

The FTC considers identity theft a very significant problem and has issued a Red Flags Rule for financial institutions or creditors, "Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003" (16 CFR Part 681). The Red Flags Rule requires that certain companies implement a written identity theft prevention program. That program must be able to detect certain incidents or red flags that indicate identity theft. The goal is to identify hackers' suspicious patterns of behavior early so they can be stopped. (To determine if your financial institution or creditor company must comply with the Red Flags Rule, see www.business.ftc.gov).

The Red Flags Rule also includes examples of red flags and guidelines to help financial institutions and creditors develop and implement a prevention program. The program must:

1. Identify relevant patterns, practices, and specific forms of activity—the red flags that signal possible identity theft;
2. Incorporate business practices to detect red flags;
3. Detail appropriate responses to any red flags detected to prevent and mitigate identity theft; and
4. Be updated periodically to reflect changes in risks from identity theft.

Stealing Data the Old Way

Of course, thieves don't need a computer to steal corporate data. They can get identity information many different ways. Several of the more common approaches include:

1. Physically breaking into a business or home to steal data;
2. Pickpocketing or purse snatching to steal money, credit or debit cards, or information on driver's licenses;
3. Bribing employees or other trusted parties who have access to targeted information;
4. Rummaging through dumpsters or trash cans for data (often called dumpster diving);
5. Observing a victim enter a password or passcode, write a check, or complete a document (this is called shoulder surfing) and using the information to penetrate a computer system and steal data;
6. Obtaining credit reports fraudulently;
7. Abusing authorized access to information as an employee or other trusted person; and
8. Stealing credit or debit card numbers directly when the victim presents the card to pay for a purchase.

Stealing with Technology

More sophisticated identity thieves use technology to commit their crimes. These techniques include phishing, pharming, and wardriving.

Phishing uses bulk e-mail messages that entice recipients to reveal personal information. Phishers often lure recipients to a bogus online banking or merchant site that asks for personal information. These criminals usually masquerade as a large, well-known company or a website with a broad membership base, such as eBay or PayPal.

A more precise method of phishing is called spear fishing. This approach uses e-mail-spoofing fraud to target a specific organization and get unauthorized access to confidential data. As with other phishing e-mails, spear phishing messages appear to come from a trusted source. But in this case the spoofed source of the e-mail is likely to be an individual within the recipients' own company and usually someone in a position of authority. Spear phishing attempts typically aren't initiated by random hackers. They are more likely to be done by sophisticated groups seeking financial gain, trade secrets, or military information.

Pharming is a special form of phishing. One pharming approach uses sophisticated technology to send the user to a bogus site where personal data is harvested fraudulently. The thief first uses a malicious stealth program that users download unintentionally, often as e-mail.

Spear fishing uses e-mail-spoofing fraud to target a specific organization and get unauthorized access to confidential data.

Opening a pharmer's e-mail message is all it takes to install some of these stealth programs. Once installed, the malicious program makes changes in the system to redirect the browser to a counterfeit copy of a targeted website. Typing in the legitimate URL address of the targeted site takes the user to the bogus imitation of that site. This occurs because the Internet Protocol (IP) address that corresponds to the URL of the legitimate site is changed by the thief to the IP address of the bogus site. This causes the system's domain-name server (DNS) to redirect the traffic to the fraudulent location. Any account numbers, passwords, or other information the user then enters into the bogus website can be captured.

Another form of pharming secretly installs a key logger, which records all of the user's keystrokes. The thief then analyzes the keystrokes and captures passwords to legitimate websites. The criminal can use the victim's passwords to gain access to the secured, legitimate site to harvest personal information.

Still another approach that is simpler involves taking advantage of common spelling errors. Once a targeted site has been identified, similar URL addresses that contain common spelling errors are registered as IP addresses that point to a bogus site. The unsuspecting user who misspelled the URL is taken to the bogus site, which steals any personal information he or she enters.

Wardriving is another high-tech identity theft technique. The thieves drive around in a car and use a laptop or special device to locate unsecured Wi-Fi networks they can easily hack. An employee working on company data at home using an unsecured home network could unwittingly divulge sensitive corporate information.

Wardriving threats don't always come from traditional cyber criminals. A March 13, 2013, story from the *GPS Business News* website, "Google Settles WiFi War Driving Privacy Case for $7m in the U.S.," recounted how Google Street View vehicles engaged in unauthorized collection of identity data and more from unsecured Wi-Fi networks as they drove past.

But the most notorious classic case of identity theft that used wardriving involved a hacker named Albert Gonzalez. After wardriving, Gonzalez and his cohorts stole more than 90 million credit and debit card numbers, then sold most of them overseas. They committed ATM fraud with other cards by encoding the card data on the magnetic strips of blank cards and using the forged cards to withdraw tens of thousands of dollars at a time from ATMs. In 2010, Gonzalez was found guilty and received a 20-year jail sentence, fines of approximately $1.5 million, and forfeiture of millions of dollars of assets.

Identity Theft in the Healthcare Industry

Management accountants who work in the healthcare industry have to be especially vigilant and careful. Healthcare identity theft is huge. The Fair Credit Reporting Act (FCRA) provides some recourse for financial identity theft, but no similar recourse exists for medical identity theft. The HIPAA Privacy Rule was enacted to safeguard the privacy of individuals' health information. It attempts to limit sensitive health information to those who are authorized to access it. But to limit access to authorized parties only, HIPAA requires identification and procedures that may make it difficult for patients to access their own records if someone has stolen and misused their information.

With the push to use digital medical records in an attempt to make the transfer of information to authorized parties more efficient and effective, some watchdogs fear that privacy issues may worsen as doctors and medical facilities routinely exchange digital data. Management accountants working in this industry should ensure that internal controls over financial data, patient records, and patient identity data are very tight.

Preventing Identity Theft

Identity theft can be a crime of opportunity, so commonsense measures can help reduce risk. But technology and hackers are growing more sophisticated every day, so management accountants and their companies should also consider more advanced measures. "20 Tips for Preventing Identity Theft" lists some useful ways companies and individuals can protect themselves.

The first step in preventing identity theft is to recognize how vulnerable your company may be. According to a cyber-risk survey by the Association for Financial Professionals (AFP), U.S. companies believe that more high-profile cyber breaches could significantly harm their business. Yet they admit they are woefully unprepared.

20 Tips for Preventing Identity Theft

◆ Don't store sensitive data on laptops, tablets, or cell phones. Encrypt all sensitive files.

◆ In addition to passwords, use more secure biometrics identity verification systems such as fingerprint scans, finger blood vessel patterns, and face or voice recognition to verify the identity of computer users.

◆ Employees should change passwords regularly and safeguard them properly. Employees shouldn't keep them in wallets or purses, and they shouldn't tape passwords to computer monitors or other places where visitors can see them.

◆ Do a data security audit. Call in a data security expert to pinpoint vulnerabilities that might affect CFOs, controllers, and their staffs.

◆ Every firm should have a mobile device security strategy and should consider using software to manage mobile devices and control access to them.

◆ Do a separate smartphone and tablet security audit to spot vulnerabilities and apps that aren't secure or may be spying on the user's activities or data. Investigate security apps like those listed by virus protection company Kaspersky for Android phones.

◆ Establish an employee security awareness and training program that teaches proper cyber security behavior. Update the program regularly to keep up with the latest changes in technology and new data security threats.

◆ Make sure your company has a crisis response and business continuity plan to implement if a large data breach occurs. Update the plan at least once a year because technology and security threats are constantly evolving.

◆ The board of directors should discuss information security regularly and actively participate in overall security strategy and policies.

◆ Use patch-management tools to make sure any software is regularly updated with security patches. Keep sensitive corporate financial data confidential by allowing only privileged user access.

◆ Always use a firewall. Use virus protection software, and update it regularly. Also use malware protection software to guard against malware that might steal identity data.

◆ Strengthen your monitoring of the security threat from third-party providers who have had access to data, including current and former service providers, consultants, and contractors. Consider establishing a program to regularly monitor and report on this.

◆ Shred financial statements and other paperwork that contains sensitive information. Destroy sensitive data files that you don't need.

◆ Share personal information only with trusted parties.

◆ Guard your mail.

◆ Be very careful which files you download and which hyperlinks you click.

◆ Follow the FTC's Red Flags Rule if applicable to your company, and implement an identity theft prevention program.

◆ Routinely monitor financial accounts and statements.

◆ Use data redaction techniques such as blanking out sensitive information in printed or electronic documents.

◆ Do you take work home and work on your home Wi-Fi network? Turn the network off when you aren't home. Change the service set identifier (SSID) and administrator's password that came with your router, use the highest security protocol available (consult your router's owner's manual for instructions), and enable encryption. These steps will help prevent wardrivers from hacking your Wi-Fi network.

Smartphones, which are everywhere in the corporate world, may be an even greater security risk.

Despite grave concerns, 21% of the organizations surveyed hadn't updated their crisis response and business continuity plans in the last year, and another 12% revealed they had no such plans at all (see www.afponline.org/attack). Make sure your company and your department staff know what to do if there's a data breach, and update the plans at least once a year.

Does your company still use passwords so employees can access data? Identity thieves are finding more inventive ways to bypass traditional security measures. Computer users easily forget passwords, and hackers often get around them using a few personal details and a call to the company. Banks that issue credit cards are now embedding computer chips in them for enhanced data security. And many security systems are switching to biometric measurements—like fingerprints, finger blood vessel patterns, or iris scans—because they are tougher to fake or steal. Others use face or voice recognition to verify the identity of computer users. Consider upgrading to these more secure ways to verify a user's identity.

In "The Global State of Information Security Survey 2015" issued by PricewaterhouseCoopers (PwC), experts recommend strengthening due diligence of third-party providers, employee security awareness and training programs, and technologies such as patch-management tools (to automatically update software with the latest security patches), firewalls, and virus protection software. The report found a spike in insider threats from employees and third parties, including current and former service providers, consultants, and contractors. So companies should regularly monitor and report on security for any third parties that have had data access.

But the PwC report also revealed that, despite media attention after a series of high-profile retailer breaches, in many companies the board of directors doesn't discuss information security. Only 42% of survey respondents said their board actively participates in the overall security strategy, and only 36% said the board is involved in security policies. Companies that are serious about data security need to get their boards involved.

One security risk that has become more worrisome involves devices such as laptop computers, tablets, and smartphones, which are especially vulnerable to identity theft because they are portable. For example, a September 29, 2014, story in the *Birmingham Business Journal* by Ryan Phillips, "American Family Care alerts customers of stolen laptops containing patient information," reported that two laptops containing sensitive information were stolen from an employee's vehicle earlier in the summer. The laptops contained information about work-related injuries, physicals, immunizations, and drug screens. The company admitted that the laptops might contain sensitive patient information, including patient names, dates of birth, addresses, phone numbers, medical record numbers, and dates of service.

Smartphones, which are everywhere in the corporate world, may be an even greater security risk because employees carry and use them all the time. Every company should have a written mobile device security strategy and consider using software to manage mobile devices and control access to them.

Surviving the Era of Identity Theft

You can prevent much identity theft with proper precautions and controls. But no system is foolproof.

In this current wave of identity theft, we feel awash in bad news. But counting the number of data breaches may be an exercise in futility. Many of them are never reported. And while the financial, banking, and credit industries are proactive in protecting their data, there's obviously much room for improvement.

The first two decades of the new millennium may well become known as the era of identity theft. CFOs, controllers, and their staffs must be more aware of privacy risk issues and take measures to keep their companies safe. **SF**

Elizabeth Mulig, CPA, DBA, is an assistant professor of accounting in the College of Business at the University of Dallas. You can reach her at Lmulig@udallas.edu.

L. Murphy Smith, CPA, DBA, is the Dill Distinguished Professor of Accounting at Murray State University in Murray, Ky. He is also an IMA® Campus Advocate and a member of IMA's Louisville Chapter. You can reach Murphy at (270) 809-4297 or msmith93@murraystate.edu.

Clyde T. Stambaugh, CPA, DBA, is a professor in the Department of Accounting at Murray State University. You can reach him at (270) 809-3169 or tcstambaugh@murraystate.edu.