WILL Hackers WIN THE Battle?

By Robert E. Holtfreter, CFE, CICA, and Adrian Harrington

It's official: Cybercrime is big business.

In July 2013, federal prosecutors announced charges against five men who they believe are responsible for the theft of at least 160 million credit card numbers, which they sold to a network of "resellers" for as little as $10 apiece. The victimized companies whose databases were breached include J.C. Penney, JetBlue Airways, and French retailer Carrefour, resulting in losses that totaled more than $300 million. "This type of crime is the cutting edge," said New Jersey U.S. Attorney Paul J. Fishman, who announced the charges. "Those who have the expertise and the inclination to break into our computer networks threaten our economic well-being, our privacy, and our national security."

Although this particular data breach, the largest such scheme ever prosecuted in the United States, is atypical in terms of the number of records that were compromised, it's as common as the thousands of others that have been verified in the U.S. over the past nine years and continue happening today. Data breaches, also referred to as security breaches, are caused by many internal and external factors, but external hackers are usually responsible for doing the most damage. These criminals steal paper or electronic records containing an individual's personal identifiable information (PII), including names, e-mail addresses, Social Security numbers, passwords, contact lists, medical records, debit/credit card numbers, financial account numbers, and driver's license numbers.

Hacking—An Uncontrollable Problem?

Hacking, mainly the external types, has emerged as the No. 1 driving force behind the tremendous outbreak of data breaches in the U.S. over the past few years. Shawn Henry, a former top cybercop for the FBI, painted a very grim picture of the current status of the cyberwar. As quoted in *The Wall Street Journal* in March 2012, Henry said, "I don't see how we ever come out of this without changes in technology or changes in behavior, because with the status quo, it's an unsustainable model…in that you never get ahead, never become secure, never have a reasonable expectation of privacy or security." (See "U.S. Outgunned in Hacker War" by Devlin Barrett, March 28, 2012.)

Though the cyberwar is far from over, it's obvious that most organizations in every industry (very likely including yours) must wake up and revisit their data security game plan and adopt the latest technologies to help protect the PII of their employees, customers, clients, and others. But even with the use of the best safeguards available, the probability of a data breach is dangerously high as the cybercriminals continue to stay one step ahead of the security experts.

Management accountants need to adopt a proactive approach to data protection strategies.

Implications for Management Accountants

Because management accountants are heavily involved in all aspects of an organization in providing useful information for decision-making purposes, they need to adopt a proactive approach to data protection strategies. To do this, they must first understand the anatomy of a cyber attack. This includes becoming actively involved in continuous training programs that teach the latest defense actions to help stop a cyber attack and learning to exercise a high level of awareness of their network and logs. By sharing the responsibility of safeguarding valuable information from being compromised, management accountants will help maintain the profitability of their organization as well as its status within the public and business communities. As we'll discuss next, organizations in *all* types of business and nonbusiness sectors have been affected by data breaches, which, unfortunately, continue to grow at an epidemic level.

Tracking the Data Breaches

To get a better grasp of the scope of the problem that hackers are creating, several major U.S. organizations identify, track, and classify data breaches according to type and industry sectors. They include the Privacy Rights Clearinghouse (PRCH), Verizon Business, and the Identity Theft Resource Center (ITRC). These groups provide this service because many entities that have experienced a data breach don't volunteer to report it or, if they do, it's because the laws in their states or rules of government agencies require it under certain circumstances. Most state notification laws have loopholes that provide a "safe harbor" for organizations that experience a data breach, which allows them to opt out and not report it. As a result, *most data breaches go unreported.*

And, unfortunately, Congress has yet to pass a data notification or data protection law.

Privacy Rights Clearinghouse (PRCH)

PRCH is known as "a nonprofit consumer education and advocacy project whose purpose is to advocate for consumers' privacy rights in public policy proceedings." Since January 2005, PRCH has compiled and reported more than 4,000 data breaches and approximately 621 million related compromised records—which, as of December 20, 2013, doesn't yet include the 40 million customer records that Target announced may have potentially been breached—in its "Chronology of Data Breaches" document, which is updated daily when PRCH receives notice of a data breach from one of its collaborating sources. For more information, go to www.privacyrights.org/data-breach.

Verizon Business

The Verizon Business "Risk Team" has produced its annual "Data Breach Investigations Report" for the past nine years, which through 2012 is based on more than 1.2 billion compromised records related to the 900 data breaches included in its caseload. The 2013 report is available at www.verizonenterprise.com/DBIR/2013.

Identity Theft Resource Center (ITRC)

The ITRC is a "nonprofit, nationally recognized organization dedicated exclusively to the understanding and prevention of identity theft." Since January 2005, the ITRC has reported more than 4,200 data breaches and roughly 551 million compromised records. It's sponsored by Intuit, Qualcomm, and the California Consumer Protection Foundation, among others. To learn more, go to www.idtheftcenter.org/id-theft/data-breaches.html.

The Holtfreter and Harrington Model

Continuing with this process, in a recent study we developed a new model that (1) classifies data breaches and related compromised records according to nine internal and external causal factors (or categories) and (2) five general industry categories/sectors and 18 related subindustry sectors. The expanded industry approach will allow related organizations to determine the severity that data breaches have on the loss of PII from their networks.

The methodology we used to develop this new, expanded classification model and define its variables was based on an analysis of PRCH's data, including 3,545 data breaches and roughly 764 million compromised records for the eight-year period from 2005 through 2012. (Beth Givens, PRCH's director, granted us permission to use its data in developing our study.)

Many Types of Theft

As you may have guessed, internal data breaches are those that originate from or are caused by factors inside an organization, whereas external data breaches originate from or are caused by factors outside the organization. Here are the types of data breaches we identified in our study:

Internal Breaches

- **IIPD:** improper protection or disposal of data.
- **ITF:** theft of data by a current or former employee with absolute or high probability of fraudulent intent.
- **ITNF:** theft of data by a current or former employee with low or no probability of fraudulent intent.
- **IH:** hacking or unauthorized intrusion of a network by a current/former employee.
- **IL:** loss of data.

External Breaches

- **XP:** partner/third-party theft or loss of data by improper exposure or disposal.
- **XTF:** theft of data by a nonemployee with absolute or high probability of fraudulent intent.
- **XTNF:** theft of data by a nonemployee with low or no probability of fraudulent intent.
- **XH:** hacking or unauthorized intrusion of a network by a nonemployee.
- **NA:** unable to determine the data breach as internal or external (not traceable).

Hackers Don't Discriminate

As we discovered, there aren't any entities, public or private, that are safe from hackers. Our analysis identified five general industry or sector categories—business, government, education, healthcare, and nonprofit—and the following 18 related subcategories:

Business, Financial

- **BFIV:** investments, mainly asset and hedge fund management and custodial and brokerage services.
- **BFB:** banking, which includes banks, credit unions, consumer finance, and payday loan and other financial companies involved in lending money and issuing and processing debit/credit cards.
- **BFIS:** insurance, mainly underwriters, carriers, agencies, and brokerages involved in annuity, life, health, property/casualty, and retirement products.

Business

- **BPS:** professional services, which includes auditing, tax, and legal services.
- **BM:** manufacturing, which is most commonly applied to industrial production, where labor transforms raw materials into finished goods.
- **BR:** retailers, individuals, and companies engaged in selling finished products to consumers.
- **BTM:** telecommunications/media, which consists of all media-technology companies, including telephone, radio/TV, Internet, newspapers, and film.
- **BH:** hospitality, including lodging, restaurants, event planning, theme parks, and cruise lines.
- **BO:** other, including all businesses not included in the other business subcategories.

Education

- **EHE:** higher education, which includes all post-high school educational institutions.
- **EK12:** all kindergarten through high school academic institutions.

Government

- **GF:** federal government, including all agencies (except the military) funded by the federal government.
- **GM:** military, including all agencies and installations funded by the federal government.
- **GS:** state, including all noneducational entities funded by a state government.
- **GK:** county, including all noneducational entities funded by a county government.
- **GC:** city, including all noneducational entities funded by a city government.

Healthcare and Nonprofits

- **HC:** healthcare, including doctors, nurses, and other healthcare practitioners/professionals, and physical facilities, such as hospitals, medical clinics, and pharmacies.
- **NP:** nonprofit, including all formal organizations in the U.S. that qualify for tax-exempt status under the Internal Revenue Code.

Figure 1: Total Data Breaches

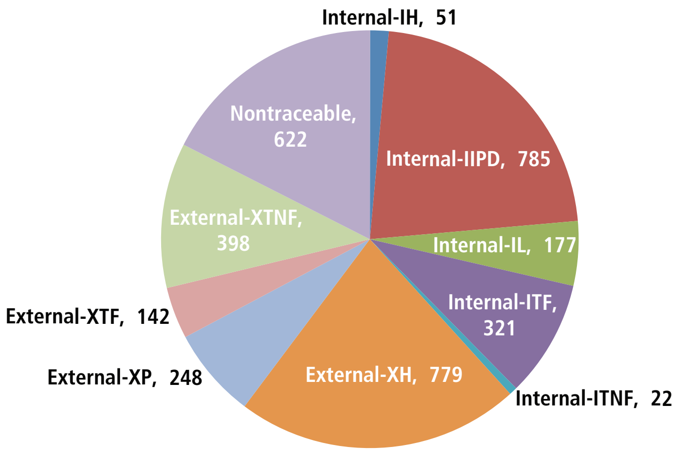


Figure 2: Total Compromised Records

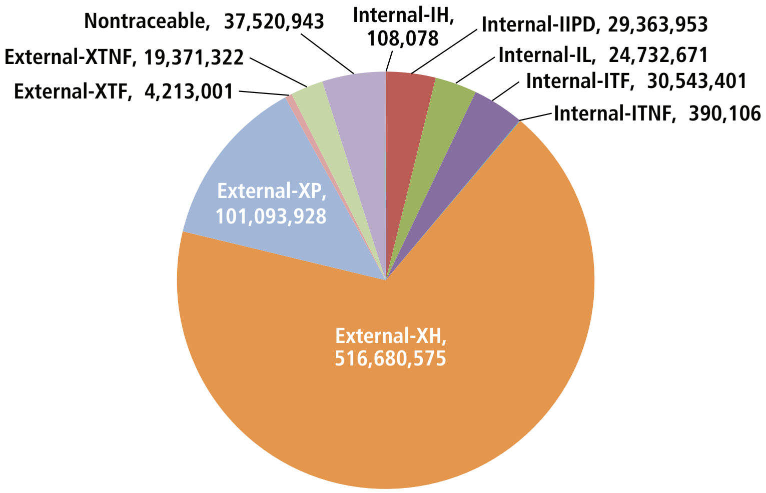


Figure 3: External Hacking Data Breaches: General Industries

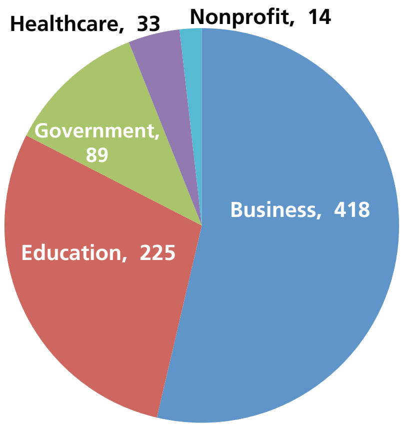


Figure 4: External Hacking Records: General Industries

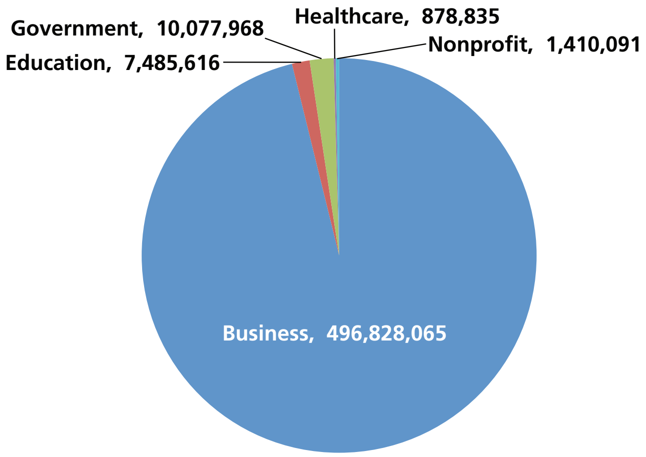


Figure 5: External Hacking Data Breaches: General Industry Subsectors

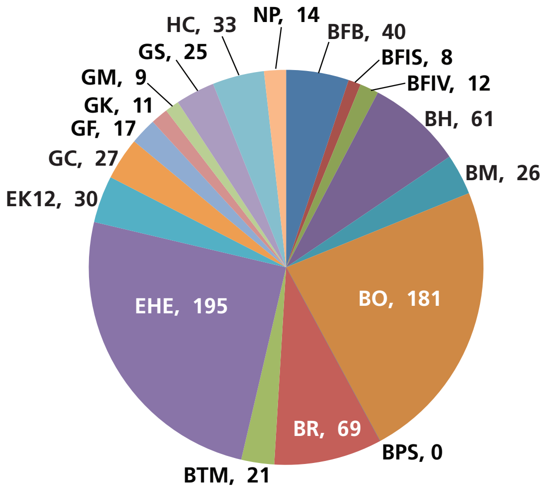
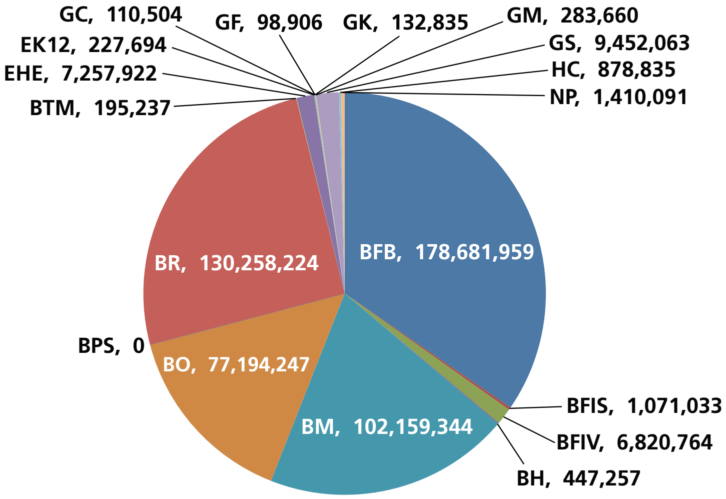


Figure 6: External Hacking Records: General Industry Subsectors



What We Discovered

Because the focus of this article is on hacking activity, we analyzed the nine categories of internal and external data breaches noted earlier, as well as the corresponding compromised records.

In Figure 1, of the 3,545 data breaches reported by PRCH over an eight-year period, 779, or 21.9%,were traced to external hacking, while internal hacking accounted for only 51 breaches, or 1.4%.

In Figure 2, of the 764 million compromised records reported by PRCH for the eight-year period, external hacking accounted for more than 516 million (an amazing 67.6%), whereas internal hacking accounted for just 108,078 breaches, or less than 1%. What stands out in this data is that while external hacking accounted for 21.9% of the total data breaches, it accounted for a whopping two-thirds of the total compromised records. In addition, in terms of compromised records per data breach, external hacking averaged 663,261 records compared to only 2,119 with internal hacking. This indicates that external hackers not only are much more skilled at intruding on organizational networks but are even more skilled at targeting databases that contain the most records once they get inside. In other words, external hackers are getting more “bang” for their buck. (Because of the relative insignificance of the internal hacking data, we will use only external data breaches and their related compromised records for analysis purposes in the following sections of this article.)

As shown in Figure 3, the business industry is clearly the most attractive target to hackers, accounting for more than half of all data breaches (53.7%). This was followed by educational institutions, with about 28.9%; government, with 11.4%; healthcare, with 4.2%; and nonprofits, with a mere 1.8%.

Figure 4 reinforces that the business industry has had the biggest bull’s-eye on its back: It accounted for almost 500 million records compromised by external sources, or 96.2% of the total. Education, government, healthcare, and nonprofits trailed far behind, each making up 2% or less of hackers’ targets. In terms of raw numbers, this amounts to 1,188,584 compromised records per data breach for the business industry, compared to just 33,269 records per breach for educators.

Figure 5 shows the number of external data breaches for each of the general 18 industry subsectors. The top five subsectors accounted for 546 (70.1%) of the 779 external hacking data breaches: Education–Higher Ed ranked first with 195, followed by Business–Other with 181, Business–Retail with 69, Business–Hospitality with 61, and Business Financial–Banking with 40.

Figure 6 illustrates the number of compromised records for each of the 18 industry subsectors. The top five subsectors accounted for almost 498 million of the 516 million (96.6%) total compromised records. Not surprisingly, the business sector took top "honors": Business Financial–Banking ranked first with 178 million stolen records, followed by Business–Retail with 130 million, Business–Manufacturing with 102 million, Business–Other with 77 million, and Government–State with 9.4 million.

Anatomy of a Cyber Attack

We've talked a lot about the depth and breadth of cyber attacks so far, but not much about the mechanics behind them. To learn to spot suspicious behavior on your own network and among unscrupulous individuals in the workplace, it's very important that you and anyone else with access to sensitive information understand the anatomy of a cyber attack. In essence, by understanding how the enemy behaves, you can develop the skills to help defeat them.

A white paper by Dell Software posted on InfoWorld's website states that hackers normally follow four steps to gain access to valuable PII (see www.infoworld.com/d/wp/anatomy-of-cyberattack-231276). They include "reconnaissance and enumeration," which is the art of finding vulnerabilities, either technical (for instance, a porous network security system) or nontechnical (such as an employee who's tricked into giving up sources of PII or works with the hacker to plant malware on the network); "intrusion and advanced attacks," which is the actual penetration of the network; "malware insertion," where hackers secretly leave code behind to enable them to maintain control over the systems; and "clean-up," where the hackers cover up their tracks.

Let's take a closer look at each of these four steps.

Attack Step 1: Reconnaissance and Enumeration

Common vulnerabilities in any network system that's targeted by a hacker include credentials (such as PII), software versions, and misconfigured settings, and the main goal of reconnaissance is to gather information to learn about them. According to the white paper, "one method of gathering this information is through social engineering cons, which fool end-users into surrendering data. This is often perpetrated through phishing (fraudulent e-mails), pharming (fraudulent websites), and drive-by pharming (redirected DNS settings on hijacked wireless access points)." An Internet DNS, or Domain Name System server, is used primarily to look up and match domain names (such as www.cwu.edu) with their corresponding IP address. DNS servers should be configured to handle requests coming from within a specific domain or IP address range. But if they're configured by default to respond to requests from outside their own domain, they become vulnerable to hackers.

Enumeration, the second part of this two-pronged strategy, uses two popular techniques, namely "service scanning" and "war dialing," to surreptitiously expand the knowledge and data gained during reconnaissance. According to the white paper, "service scanning identifies network systems and matches known bugs with software weaknesses. War dialing, on the other hand, involves using an automated system to call each of the telephone numbers owned by a company in hopes of finding a modem that provides direct access to internal company resources." Cybercriminals will do everything possible to locate and exploit weaknesses in a network, and these techniques can result in dire consequences for an organization.

Attack Step 2: Intrusion and Advanced Attacks

Skilled hackers have the ability to access every facet of your network systems. They gain the ability to penetrate a network by exploiting its vulnerabilities once they have been identified and correlated. Sophisticated "zero-day" attacks are more dangerous and are used to exploit soft-

Cybercriminals will do everything possible to locate and exploit weaknesses in a network.

ware weaknesses. A zero-day or zero-hour attack means that the hacker executes an attack as soon as possible before the developer of the targeted software notices the intrusion and patches the vulnerability. We'll describe other intrusion methods later in the article.

Attack Step 3: Malware Insertion

To maintain ongoing remote control over the network systems and ultimately execute code within the network, hackers need to secretly insert malware after infiltrating a network. According to the white paper, "inserted malware can be a nuisance (for instance, spam), controlling (to provide backdoor access or remote control), or destructive (to cause intentional harm or to cover the attacker's tracks)." Once the malware is inserted, the hacker has the keys to your network. It's like having the keys to your car or your home. Game over? Just about!

Attack Step 4: Clean-up

The final stage of the attack cycle is to rid the infected system of forensic evidence. The success of this step depends on how inconspicuous the hacker has been during the earlier steps. For example, so as not to trigger alarms, an attacker may commandeer the credentials of a trusted network user or use common applications, such as instant messaging, to insert malicious files or extract information. According to the white paper, "a primary goal of this step is to erase any traces of the attack from the system. This can be done by manually or automatically deleting command line or event logs, deactivating alarms, and upgrading or patching outdated software post-attack. Additionally, hackers and cyber-thieves often unleash viruses and worms to destroy potentially incriminating evidence." By destroying any evidence of their intrusion before software developers become aware of it, the hackers can return to the scene to gather more PII.

Spotting Common Threats

According to the Data Recovery Reviews website (www.data-recovery-reviews.com), there are five major common threats to network security. In no particular order, they are:

Denial of Service (DoS). By overloading a server with more requests than it can handle, hackers intrude on a network by crashing the server. This is relatively easy for them to do, but it's hard for the organization that's been intruded on to deal with. Commonly used DoS attacks include SYN attacks, ping-of-death attacks, smurf attacks, and ping flood attacks.

IP Masquerading. By pretending to be someone else (with a different IP address), the hacker is able to gain access to the server. This often occurs because the system isn't smart enough to authenticate legitimate users from imposters.

Session Hijacking. In session hijacking, the perpetrator takes control of a user's session, resulting in a very serious security breach in which the hacker could steal critical data, including passwords or credit card information. To make this deception work, the user is led to believe that he has been logged out. When he logs back in—boom!—the hacker takes over.

Illegal Security Break-ins. This is by far the most obvious and dangerous Internet network data security threat. Through faulty software security patches or via access to passwords, the attacker is able to pierce the authentication and authorization checks to get access to corporate databases and mission-critical files. This threat can be resolved only through prevention rather than cure, such as by safeguarding passwords more carefully.

Physical Access to Servers. Unauthorized physical access to corporate servers is still the largest threat to data security. Good data centers protect themselves through fingerprint-based authentication and by verifying the credentials of everyone who visits the data center.

If you suspect that your network has been intruded on, what's your next step? First, work with your IT department to attempt to locate the source of the intrusion by checking for any new or strange access to the computer network. Then look for *past* patterns of intrusions to see if any of these patterns have been repeated recently on your networks.

Once the source of the intrusion has been identified, your data protection procedures should be updated to help prevent any possible future intrusions. While this sounds simple, well-established hackers are very ingenious and diligent in developing new schemes to gain access to valuable PII. As a result, the battle between them and security experts goes on and on and on.

Tips to Stay Secure

No matter what type of setting you work in, there are creative ways to make things tougher on hackers. Here are some examples of what organizations in all industries need to consider to help protect their records and hopefully make it more difficult for hackers to intrude on their networks. The first five examples were provided by Data Recovery, 2007, available at www.data-recovery-reviews.com/intrusion-detection-reviews.htm.

1. Review your service provider's data protection policies to ensure that they're adequate. For hacking attacks in particular, keeping a company's network secure will require both proactive and reactive security strategies. In the end, the costs of security may prove to be minimal as compared to mitigating a successful breach.

2. Decide who should have access to company servers, and put it in writing. A good practice is to outsource the hosting of corporate services to a data center that can focus on providing great Internet network security, including hard-to-penetrate firewalls and provisions for recovering data in the event of a disaster (man-made or otherwise). This will help prevent unauthorized persons from accessing your servers.

3. Have a well-thought-out Internet data security policy. To make your security policy work, you'll need buy-in from employees, who should be given handouts covering what they need to know about your data security. Contractors should receive these handouts, too, plus assist with regular data security audits.

4. Update all software, and use an industry standard network data security firewall. This will help thwart hackers as they attempt to exploit the vulnerabilities of the operating system, the database, or even specialized software, such as customer relationship management (CRM) or enterprise resource planning (ERP) packages.

5. Use new network backup strategies, such as remote data backups and data replication, to make backups regularly, even when your systems are live. Also, always safeguard your backups because careless backup handling could be your biggest network security threat.

6. Encrypt all personal information stored on laptops or other portable devices, or transmitted wirelessly or through a public network, using the Advanced Encryption Standard (AES) 128, 192, or 256 bit size. The commonly used DES 56 bit standard contains hashes that can easily be cracked and returned to plain text for identity theft purposes.

7. Change passwords periodically using a mix of at least eight numerals and letters. Avoid common phrases, names, birthdays, and the like. This should go without saying, but it's amazing how many people fail to follow these important safeguards.

8. Consider keeping all valuable information off the network. If something isn't on the network, it can't be stolen.

Looking Ahead

The results of our study strongly indicate that organizations in every type of industry—especially those in the business subsectors—are experiencing serious problems with external data breaches, giving up millions of compromised records in the process. As we mentioned earlier, PRCH has discovered and tracked thousands of data breaches affecting hundreds of millions of records, which, it says, is a fraction of the actual criminal activity that's occurring. This helps to explain why identity theft is escalating and why fraud accounts for more than 30% of the complaints reported to the Federal Trade Commission every year.

As management accountants, now more than ever you must be proactive in working with IT personnel to develop a strong, comprehensive data protection plan to help defend against hacker attacks. This will require resources—sometimes pricey ones—and a diligent mind-set from everyone in the organization. Our recommendations represent a starting point for creating positive improvements for helping stop data breaches and to protect valuable PII from hackers. The battle is ongoing, but the effect on reducing identity theft will surely be substantial. **SF**

Robert E. Holtfreter, CFE, CICA, Ph.D., is Distinguished Professor of Accounting and Research at Central Washington University in Ellensburg, Wash. Bob serves as the identity theft protection and detection analyst for the Association of Certified Fraud Examiners and writes peer-reviewed articles for their journal, Fraud Magazine. *In addition, he's a member of the editorial review boards of several academic and professional journals. He also is a member of IMA's Washington Tri-Cities Chapter. You can reach Bob at (509) 963-2144 or holtfret@cwu.edu.*

Adrian Harrington, a former student in Bob Holtfreter's fraud examination class at Central Washington University, now serves as his research assistant. You can reach him at aaharrington87@gmail.com.