A Primer on Data Security

How CPAs Can Help

By Ted Brown

In Brief

Data security represents a defining technology issue for any enterprise. Organizations need a strong information technology (IT) and security strategy in order to protect against the loss of data or financial resources. Nevertheless, the most important defense against intrusion is an informed and knowledgeable user. This article aims to help financial managers become those users by enhancing their understanding of cyberattacks and the motivations behind them, as well as the means to prevent them.

Data breaches that cause millions of dollars in damages to individuals, companies, or the government have become a common occurrence. The Internet was originally designed for computers to transfer data rapidly and communicate into and out of a computer system. In the early days of the Internet, security was little more than an afterthought. With no regulation or standards, the web provided opportunities for apps, tools, websites, and programs, each with their own vulnerabilities and weaknesses. As the Internet becomes more ubiquitous, information that is increasingly profitable in the right (or wrong) hands has become available in some capacity. The solution thus far has been a steady stream of fixes and patches, with new software and hardware sometimes tipping the balance of power back into the hands of businesses and users, albeit temporarily. This has resulted in an acceptable—but nowhere near perfect—wall between hackers and users' data.

One of the leading factors in security breaches is the mistaken belief that a single user couldn't possibly be a target. At its most basic level, this belief stems from the misguided assumption that the average user doesn't touch enough sensitive data to be a liability. Furthermore, it indicates a misunderstanding of what "sensitive data" actually is. How much personal information is stored somewhere on a company's servers? What about corporate data belonging to customers or clients? With such data readily available, almost any employee can be a security risk if proper computer usage habits aren't followed. In order to enhance their data security, companies must look to knowledgeable professionals to better understand security breaches and develop a strategy for prevention. In one observer's opinion, CPAs are those professionals: "increased globalization of business and the huge growth in information due to technology will enhance the role played by CPAs. Accountants in industry are increasingly becoming strategic advisors, rather than just record keepers" (Cynthia Krom, "The Future of the Accounting Profession and the Value of the CPA: Opinions and Insights from Young Professionals," *The CPA Journal*, August 2014, pp. 14–23). Krom also pointed out that maintaining data security is an increasingly important role for today's CPA financial managers, who "are responsible for the privacy and security of financial and other data."

Who Breaches Security?

In popular media, a "hacker" is a malicious user who illegally accesses data and systems for personal or financial benefit. Historically, this term referred to hobbyists who altered consumer electronics, either through hardware modification or programming. In the security and IT industries, however, it generally refers to anyone who uses computer knowledge and skills to bypass network and device security. Several types of hackers exist:

- "White hats," also known as ethical hackers, often work as part of a larger team that attempts to break into an organization's systems hoping to find holes and patch them before one of the other types of hacker discovers them. Most white hats are either security professionals, government workers, or contractors trying to fix network weaknesses.
- "Black hats"—sometimes known as "crackers"—violate "computer security for little reason beyond maliciousness or for personal gain" (Robert Moore, *Cybercrime: Investigating High-Technology Computer Crime*, Matthew Bender & Company, 2005, p. 258). Their motivations range from monetary gain to the simple desire to cause as much damage as possible.
- "Grey hats" fit somewhere in between, often using their skills to find holes in systems they don't have permission to access, then informing proper security personnel of the breach. Many grey hats hack simply for the challenge, whereas others genuinely want to help, notwithstanding their use of somewhat unscrupulous methods.
- "Hacktivists" are hackers who aim to further an ideological agenda by attacking corporations, governments, political parties, terrorist organizations, or other hacker groups. Hacktivists often won't steal money or destroy data but will attempt to impede organizations that they disagree with, especially via visible tactics like website takedowns or vandalism.
- State-sponsored hackers use their skills to target assets of other countries. They have access to top-of-the-line equipment and act as agents of their home government, generally receiving its protection and blessing. As such, it's nearly impossible to catch these hackers (Kenneth Rapoza, "On China and Russia Hacking into the US, 'No Hard Feelings,'" *Forbes Online*, Nov. 8, 2011).

The Human Element of Hacking

The biggest factor in data loss and security breaches isn't a virus or a hacker group like seen on popular TV shows. Instead, it's the security risk sitting at the keyboard: a human. In fact, the strongest security measures are no match for an uninformed or negligent user.

Of the 268 data breaches the U.S. government faced between 2009 and 2012, more than two-thirds were caused by loss of a device, records, or the negligent disclosure of information (William Jackson, "Forget Hackers, the Fool Next to You Is the Real Threat," GCN.com, Sep. 19, 2012). In a 2011 study run by the Idaho National Laboratory, researchers scattered USB thumb drives and CDs around government and private-contractor parking lots to determine how many people would ignore protocol. Researchers found that 20% of employees loaded the drives and CDs on government and corporate computers, while another 22% clicked on bogus links in e-mails that would give hackers access to their systems (Lucas Mearian, "Government Tests Show Security's People Problem," Computerworld.com, Jul. 6, 2011). Worse yet, at least 40% of the test group gave their passwords to imposter IT professionals.

Because entire industries exist to track technology and security changes, it may not be fair to expect the average user to be acutely aware of current trends; however, hackers can be expected to target ignorant users. Seemingly innocuous actions, such as clicking on a link or responding to an e-mail, can give a hacker access to an entire network.

Unfortunately, there's no panacea for user-caused ills. At present, the best defense isn't antivirus software, firewalls, or other means of intrusion prevention: it's a smart user. Training is invaluable, but it is also expensive, time consuming, and often logistically difficult. Yet, all hope is not lost. Because modern security systems are quite good at mitigating risks (often by preventing initial access by hackers), spreading even the most basic knowledge can be the difference between business as usual and a data breach.

The Most Common Hacks

The most common hacking methods aren't usually associated with programming holes; instead, they target users' propensity to give their own information willingly. Tricking a person into giving away their information is a lot easier than spending the time cracking a system and its security.

"Phishing" refers to a scheme in which hackers simply ask for security credentials. While it seems like an easy ploy to see through, a hacker masquerading as an IT professional or a website administrator can often convince a user to hand over information. If a target isn't easily swayed, the hacker might first try to gain the user's trust over a longer period of time (sometimes called "pretexting"). Another common scheme involves piquing a user's curiosity (or greed) through "baiting." This can be done either online, via malicious webpages or links, or offline through storage devices.

Real IT professionals often say that they will never ask for someone's password, so users should be wary whenever someone does ask for it. Vigilance comes down to common sense: if users are unsure of the legitimacy of a link, webpage, storage device, or e-mail, they shouldn't interact with it. In the aforementioned study, the number of employees loading malicious storage devices dropped to only 2% after employees received basic education on hacking schemes.

Exploring Possible Solutions

Once the human element is removed from the equation via user education, companies can focus on ensuring an IT infrastructure that provides an appropriate level of security, functionality, and ease of use. Technically, an absolutely secure system would reside in a bunker with an on-site power source, automate all system service, and be disconnected from any outside networks; however, such a system would not be particularly functional or usable. On the other hand, functionality and ease of use can weaken security measures.

Finding a balance that works for a user's specific needs is key. A home desktop might benefit from greater levels of functionality and ease of use, especially if personal information is not stored on that computer. Government and large-scale corporate systems that require higher levels of security and functionality must sacrifice usability. This complexity, which can often cause system downtime, results in the need for dedicated IT professionals and network engineers with specialized knowledge.

Security Infrastructure

For CPA financial managers, there are literally dozens of controls to consider when crafting a security infrastructure. In a perfect world, a single piece of equipment or software would handle each job. In practice, however, each device or software can do more than one job at a time to protect systems in multiple ways simultaneously. CPAs designing a prevention strategy should consider both physical and technological security, as discussed in the following sections.

Physical Security

The first line of defense against any kind of attack is physical security—specifically, server location. Considering that nearly all of an organization's management and employees access servers at some point, they represent the main point of attack. Although software vulnerabilities are probably the most common methods of gaining access, servers are most exposed when they are physically located in an unsecured location. Most organizations have figured this out, and, at the very least, lock their servers in a room that only network engineers and IT professionals may access.

It is important to remember that hacking isn't the only way data on servers can be irretrievably lost or rendered inaccessible. Earthquakes, hurricanes, floods, tornadoes, derechos, and other natural disasters can be powerful enough to cause structural damage and knock out electricity for millions of people. This possibility of destruction or inaccessibility of data due to natural disasters (as well as more malicious human intervention, such as an attack) drove the creation of high-security data centers. Data centers often have extreme security measures in place—multiple passcodes, multiple entry checkpoints, closed-circuit television surveillance, 24-hour security personnel, and even biometric scanners—to prevent physical access, but their real utility comes from their ability to survive most natural disasters. In fact, some can even survive physical attacks such as bombing.

Furthermore, data centers typically have multiple backup power sources; thus, even widespread power outages cannot take systems offline. In addition, data centers always have incredibly powerful heating, ventilating, and air conditioning systems to protect equipment from overheating. Given these attributes, it's no wonder that data centers have become the most popular locations for storing servers. Yet, data centers can cost hundreds, or even thousands, of dollars per square foot to rent. This expense tends to keep small to medium-sized businesses out of the space; instead, they rely on locked rooms within their offices.

Another physical security consideration arises at the employee level: the security of workstations and devices. Recently, some of the most severe data losses have come from employee loss of portable devices. Arguably the most widely publicized hacking incident of the last decade occurred in 2006, when a U.S. Department of Veterans Affairs employee lost a laptop containing a database of the personal information, including Social Security numbers and birthdates, of more 25 million military veterans (Hope Yen, "Thieves Steal Personal Data of 26.5M Vets," *Washington Post*, May 23, 2006). Companies can help avoid incidents with computer-use policies that discourage the improper use of workstations.

Technological Security

The following common technology solutions can form the underpinnings of a security-infrastructure strategy.

Firewalls. At the most basic level, a firewall is a piece of equipment or software that screens and, if necessary, blocks packets from entering or exiting a network. Firewalls often work in conjunction and put up multiple roadblocks between the Internet and local systems. For example, a home network probably has two firewalls: a software-based firewall packaged with the computer's operating system and another one on the network router.

Firewalls on consumer computers are not particularly potent, and they wouldn't do a great job against the level of attacks that business and other large organizations face daily. A corporation, bank, or government entity will likely have a hardware-based firewall that can almost singlehandedly prevent malicious packets from getting through without notice. Unfortunately, these solutions are costly, with top-tier firewalls running between $10,000 and $20,000. These costs can lead most small and medium-sized organizations to adopt a less effective, lower-level product. A network engineer or a highly knowledgeable IT professional is integral to the upkeep of any firewall. Finally, like everything else in a computer infrastructure, the solution becomes obsolete over time, requiring a complete replacement and making even large investments a recurring expense.

Intrusion detection and protection systems. Closely related to firewalls is a solution that has proven quite effective. Intrusion detection and protection systems (IDS) filter traffic through the use of a constantly updated list of known IP addresses and websites. When an IDS recognizes a malicious address, it actively blocks traffic to and from that site. Consequently, even if a computer on the network is infected with malware, the IDS will block its attempts to speak back to the malware operator.

Moreover, an IDS acts as a strong countermeasure against state-sponsored hacking. One of the more powerful features of such a system allows it to block any sort of incoming traffic from entire geographical areas, even countries. Nations like China and North Korea, as well as groups like the Syrian Electronic Army, notoriously hack U.S. corporations to steal trade secrets or simply cause mayhem. The IDS has settings that completely block any traffic from those locations. Unlike firewalls, which can do something similar, a top-tier IDS can locate and block the actual origin of an attack.

Skilled hackers will typically hide their tracks using a number of techniques, each of which will throw off most attempts to track and catalog their actual location; however, a strong IDS can recognize repeated attacks from the same place of origin and then stop future attacks. Even going through remote servers—a common method of making one's presence online anonymous—cannot stop an IDS from blocking out malicious users. Of course, determined hackers may eventually figure out a way around this protection, but many hackers rely on tried-and-true techniques. When their comfort zone is taken away, they may not have a response, or they may look for another target.

Considering its effectiveness, why don't all networks have an IDS? Like a high-level firewall, a strong IDS represents a $10,000 investment at a minimum. And, just like a firewall, it requires maintenance from dedicated professionals and it does have a finite service life, requiring eventual replacement.

Antivirus protection. Antivirus software is a system-level protection that filters, quarantines, and deletes harmful software, known as "malware." The term "computer virus" is generally misused, and people usually use it when they actually mean malware—that is, any piece of software that interferes with normal computer processes. For example, a piece of malware can be a self-replicating program that infects programs and spreads to the entire system (i.e., a virus), or it can be a program that allows its operator access to computer processes (i.e., a "backdoor"). In practice, the specifics of malware don't really matter. They can be loaded onto a system by clicking on ads on untrustworthy websites, opening spam, or installing infected hardware. Once malware takes hold in a system, it can be difficult to get rid of, sometimes requiring a full system restore to completely wipe out the virus.

Considering the ways that malware can leak confidential information to its creator, strong antivirus software is absolutely necessary for users in all industries. Servers often come packaged with antivirus software that protects the data on them, but individual workstations should also have such software. It's much easier for malware to find a way into a network when it has already taken hold of a user terminal. Individual accountants often have access to so much data that, even absent a network-wide outbreak, a single infected computer can be disastrous.

It is important to remember that antivirus software is useless unless it is regularly updated. Though the software's creator regularly updates its product, the user's computer must receive regular update patches for protection. Unlike the previously discussed solutions, antivirus software is affordable. Some of the best antivirus software available costs less than a few hundred dollars per year per user. Newer computers often come with antivirus software and a firewall already installed.

Maintenance. Owning and installing the aforementioned solutions is not enough. Constant maintenance keeps systems safe. Every day, new programs are written and new methods are developed to separate a company from its data. Because hacking is lucrative, hackers are often willing to expend much effort to gain access to valuable systems. Realistically, organizations need to put in as much or more effort to keep them out.

For a small startup, individual computers with antivirus software and a prepackaged firewall, as well as a few servers with appropriate software, might be sufficient; however, as a company grows and stores more data on its servers, more care must be taken. Servers and workstations need additional security, firewalls require strengthening, and dozens of programs call for updates.

At some point, hiring a knowledgeable IT professional will be necessary. When this time comes, organizations typically follow two common paths. They might hire an outside IT consultant who usually works on behalf of a larger service firm or is sometimes a small business owner. Unfortunately, because of the high demand for their services and the low supply of quality consultants, their fees can be high and their schedules tend to fill up quickly. Because of this, many organizations choose to hire an in-house IT professional so that any catastrophic issues can be resolved relatively quickly and maintenance can be performed regularly.

The Cloud Option

Another option that is quickly growing within the IT industry is the "cloud"—that is, server-based storage and applications that allow any (or most) Internet-enabled devices to access data. Consider Netflix, perhaps the most widely used consumer cloud application. Movies and TV shows are stored on Netflix's server, and the system (video game console, smart TV, computer) plays the movie or show on the user's device.

Cloud computing marries high-level infrastructure with affordability. Rather than owning, operating, and maintaining equipment and programs, organizations can now opt to use the systems of a cloud services provider. Then, with almost any Internet-enabled device, they access a computing environment created specifically for their individual organization. The cloud services provider manages all system and software upgrading, technical support, equipment purchasing, and even equipment location (typically in top-tier data centers). Perhaps most importantly, these high-level systems experience infrequent downtime, sometimes averaging only minutes or seconds per year. Taking into account IT professional labor costs, consistent software upgrades, equipment replacement, and business lost due to downtime, this solution often ends up being much less expensive than traditional IT solutions, especially for small and medium-sized businesses.

The Role of CPAs

On its website, the AICPA echoes the increasingly important role played by CPAs in data security:

> Fundamentally, a CPA must understand and be knowledgeable about the most pressing security initiatives affecting the profession, be aware of specific solutions to combat these threats and successfully implement best practices for deploying the necessary security measures that protect clients, firms, and organizations in general. CPAs can help with the implementation of these new technologies into a business by consulting with clients to determine critical business decisions such as creating internal controls and meeting industry standard regulations. Additionally, CPAs play a role in designing systems for managing sales, adjusting manufacturing and administrative procedures, and establishing timetables for technology upgrades—all of which play a vital role in protecting a corporation's financial, fixed, and intangible assets.

The AICPA website also stresses the importance of continuing education for CPAs in order to keep them up to date on ever-changing security threats: "When CPAs continue to enhance their education in technology initiatives, they become a more valuable asset to their organization and open the door for career growth and opportunities in today's world of emerging technology."

To the extent that CPA technology advisors and financial advisors can help a business develop a security strategy and create a more secure IT landscape, their professional futures will remain bright. ❑

Ted Brown *is the vice president of IT operations at Network Alliance Inc., a network-management solutions provider in the Washington, D.C., region.*