WHAT'S YOUR MAIN Technology Concern?

AMONG ONE GROUP OF ACCOUNTANTS, SECURITY ISSUES DOMINATE THE top 10 technologies list.

By William M. Baker, CMA

Whenever new technology raised questions, accountants of the past would flood the IT department with questions. Not today. It's now the responsibility of management accountants to care for all information in the business. To provide this care successfully, they must thoroughly understand the technologies that are commonplace, yet rapidly changing, in all business activities. A top 10 technologies list provides a guide. For the fourth consecutive year, professionals who sit at the intersection of accounting and IT selected information security as the number one technology to watch. Four technologies are new to the list: assurance and compliance applications, IT governance, privacy management, and spyware detection and removal.

To compile the list, the American Institute of Certified Public Accountants (AICPA) surveyed a select group of its members, many of whom are Certified Information Technology Professionals (CITP). This list isn't the end-all list of technological concerns, and by no means does it encompass everything that accountants need to know about today's technologies.

Indeed, some areas not mentioned here may be extremely important to management accountants, such as blocking spam, backing up files, or creating effective, accurate spreadsheets. This list is intended to inform accountants about hot (or soon to be) technologies. Some of these topics are discussed every day, while others are new or confusing. Table 1 features the complete list. It's time to get up to date.

10. SPYWARE DETECTION AND REMOVAL

The creators of the first spyware programs had good intentions. They created software that would remain hidden from users until the users needed to be rescued from a programming or application snag. The spyware would then pop up and help them solve their computer problems. Unfortunately, spyware has turned nasty. Creating legislation to eliminate it has proven cumbersome, and spyware-removal software is, at best, frustrating.

Spyware usually strikes with multiple infections and causes myriad problems. It can create new computer settings and then block attempts to restore original ones. It can change default home pages, download unwanted files, and redirect mistyped URLs to sites that are affiliated with the spyware's creator. It can create unwanted bookmarks, launch pop-up ads, or download Trojan viruses. So-called keystroke loggers can even intercept, record, and then use credit card information, bank data, e-mail addresses, passwords, or Social Security numbers. Worst of all, the user probably won't even know that the spyware exists.

Legislation has been created to attack spyware, but even though different bills have been passed in the Senate and the House, no spyware bill has become law. Such legislation is complicated. If *all* spyware is eliminated, then it will be illegal to use spyware to monitor children's Internet activity, and the original spyware programs that serve as learning assistants for computer users will be eliminated forever.

One compromise has been to make spyware that's downloaded without the user's consent illegal. Surprisingly, though, users often give their consent because spyware is frequently bundled with freeware or shareware! Remarkably, some creators of malicious spyware use a common ploy of bundling their spyware with products that eliminate other creators' spyware. The end-user license agreements (EULAs) for this type of anti-spyware product and for most freeware and shareware are so long and complicated that users rarely read them. When users accept by simply clicking on them, they're accepting the spyware that's present, too.

Creators of spyware go to painstaking lengths to be sure that it's extremely difficult to find and remove spyware once *it is present* on a computer. While some products can effectively remove spyware, it's difficult to recommend them because spyware usually arrives as a set of multiple (perhaps hundreds of) infections, and no one anti-spyware product is effective against all spyware. The best approach may, indeed, involve using multiple anti-spyware software products. Products such as Spyware Doctor, Webroot Spy Sweeper, and Zone Alarm Internet Security often receive high marks, if for nothing else than their ability to block keystroke loggers.

Table 1: THE AICPA'S TOP 10 TECHNOLOGIES FOR 2006

1. Information security
2. Assurance and compliance applications
3. Disaster and business continuity planning
4. IT governance
5. Privacy management
6. Digital identity and authentication technologies
7. Wireless technology
8. Application and data integration
9. Paperless digital technologies
10. Spyware detection and removal

Source: AICPA's Top 10 Technologies, 2006 (AICPA News Release)

9. PAPERLESS DIGITAL TECHNOLOGIES

Digital technologies focus on the process of capturing, indexing, storing, retrieving, searching, and managing documents electronically, including knowledge and database formats. For years, this process has been viewed as creating the paperless office. Paperless digital technologies go beyond that today, however, by focusing on making business data more relevant and reliable. Two concerns dominate here. One is portable document format (PDF), Adobe's file formatting software that enables documents to appear on both the printer and monitor as they're

meant to appear. Using PDF formatting provides a printed-format display of Internet "screens" that usually print differently from how HTML displays them. The PDF format also enables individuals with Adobe Acrobat Reader to view documents created using other applications—applications that the individuals may not be able to access.

Though newer, XML (Extensible Markup Language) will likely have a stronger overall impact. Created by the World Wide Web Consortium (W3C), XML enables the definition, transmission, validation, and interpretation of data between applications and organizations. Accountants will probably be most concerned with a subset of XML called XBRL (eXtensible Business Reporting Language). W3C also created XBRL, which is the standardized set of tags that describes accounting information. Once the term "tags" is mentioned in context with the Internet, most accountants begin thinking about HTML tags, but HTML is different from XBRL. HTML simply describes the *formatting* of information and how the information will appear on the Internet, while XBRL describes and creates business reports.

XBRL offers three major benefits:

- Everyone reports business results in accounting reports using the same format,
- Any computer can extract and use the data, and
- Each company has to enter accounting report data only once. (Without XBRL, the typical company will enter such data three times or more for printing, the company website, and again—maybe several more times—for filing with various governmental entities, such as the Securities & Exchange Commission.)

To learn more about XBRL and see examples of how companies use it, visit www.xbrl.org.

8. APPLICATION AND DATA INTEGRATION

Integrating business and IT applications with data refers to the ability of different operating systems, applications, and databases to talk to each other. The issue is whether information can flow freely throughout the business regardless of the application, language, or platform. Can computer programs and applications talk to each other? This has been a strong concern among accountants since the 1960s.

The few vague attempts to accomplish intercommunication are widely used. Copying data from one application and pasting it to another is common. Importing and exporting files across applications is routine. Much of the popularity of Microsoft Office products comes from the ability to use database, word processing, and spreadsheet operations simultaneously without reentering data.

Today, though, products such as Java and Microsoft's .Net project exist that allow communication servers, applications servers, and routers to at last succeed in fully integrating application software products with each other and database applications. Although this technology provides seamless operations across applications, it involves so many business functions that, once implemented, it seemingly "becomes" the business, much as enterprise resource planning (ERP) software can essentially dictate the way that business is conducted.

7. WIRELESS TECHNOLOGY

Wireless technologies involve the transfer of voice or data from one machine to another, using the airways, without physical connectivity. Well-known examples include cellular, satellite, and infrared applications and services such as two-way paging. Today, much importance is placed on two examples that aren't as well understood: Wi-Fi (Wireless Fidelity) and Bluetooth. Essentially, Wi-Fi refers to wireless technology for the Internet and is driven by communication standards that are defined in IEEE 802.11. A whole family of standards, the 802.11 set defines how wireless gear communicates with the Internet using local area networks (LANs). The most commonly referenced standards are 802.11b, 802.11g, and 802.11a.

While Wi-Fi and the 802.11 family determine how wireless connections with the Internet are made and sustained, Bluetooth can instead be viewed as wireless technology to replace power cords or cables. Bluetooth signals carry only over short distances. If someone wants to create a wireless connection between a PC and a printer or between a car key and the car's ignition system, Bluetooth is appropriate. Bluetooth would also facilitate wireless connections and transfer data from one PDA to another. The key is to remember that Wi-Fi considers Internet connections, whereas Bluetooth alone doesn't provide any Internet protocol support.

Sometimes an area in information technology becomes so important and so widely implemented that it spawns other technologies. Such is the case with wireless technologies. Wireless technologies have led to WWAN (wireless wide area networks), which are used to enable cell phones to connect to the Internet and facilitate applications such as Short Message Service (SMS). With SMS, accountants can receive all of their messages from one source. All instant messages (IM), e-mail, voicemail, and

even faxes are delivered via one central delivery point—a process called unified messaging. Basically, all messages go to an SMS center. Using signal transfers identified by home location registers, messages are then sent to mobile switching centers where cell phones can access them. You need only subscribe to such a service. Privacy is protected by the home location register, which is a database containing the authorized users of the unified messaging service. Similarly, WWANs also enable users to surf the Internet with their cell phones.

6. DIGITAL IDENTITY AND AUTHENTICATION TECHNOLOGIES

Digital identity and authentication technologies verify a user's identity to control and authenticate access, implement authorization schemes, and establish nonrepudiation measures. Nonrepudiation measures make it impossible for the user to deny having accessed the computer. Such technologies include tokens, bar codes, and biometrics. Tokens are security devices, usually cards, that are swiped and read much like credit cards. They usually contain a changing number that serves as a password and is embedded in the software. Some tokens aren't cards but are instead plugged into the computer via a USB port.

Management accountants are aware of bar codes and, if nothing else, they're familiar with the Uniform Product Codes that are scanned at retail stores worldwide. For identity and authentication, bar codes can contain access codes or passwords. Traditional one-dimensional bar-code scanners use the bar code's width to encode a number. Newer, two-dimensional bar codes, which are scanned both horizontally and vertically, can hold considerably more complex passwords.

For more than 30 years, biometrics have used physiological traits, such as fingerprints and retina scans, to identify and authenticate users. They're now common because the hardware and software needed to implement biometric controls are far less expensive than 30 years ago.

In addition to verifying a user's identity, accountants may want to verify the validity of a specific message. While tokens, bar codes, and biometrics are less effective for verifying message validity, digital certificates are not only effective, but they are important to securing information and are discussed later (see Technology No.1, Information Security).

5. PRIVACY MANAGEMENT

The Institute of Management Accountants (IMA®) and the AICPA have emphasized the importance of information privacy, especially in relation to confidentiality constraints and industry-specific rules, such as those derived from the Health Insurance Portability and Accountability Act (HIPAA). Since HIPAA became law in 1996, many other local, state, national, and international laws have been passed concerning privacy. During the past decade, accountants have begun to realize that the only way to comply with privacy concerns, especially *information* privacy concerns, is to develop and implement privacy-management strategies.

Privacy management begins with two phases. Initially, existing policies and procedures are reviewed and changed as necessary to comply with laws and management expectations for privacy. Invariably, a second phase creates new policies and procedures to fully achieve management's goals for privacy. Care must be taken to ensure that these policies and procedures are disseminated throughout the organization. Additional procedures are then necessary to facilitate (usually annual) reviews of privacy policies and procedures to ensure that they're still effective in light of new technologies. If these policies and procedures aren't addressed in applicable laws, management should specifically define what data, information, and even cookies are personal and private and outline responsibilities for such items. Strong privacy management also includes facilities for handling, processing, and learning from complaints. Essentially, every other item on the top 10 list is subject to privacy-management concerns.

4. IT GOVERNANCE

Businesses thrive by setting goals and creating and implementing plans to achieve those goals. In the Information Age, companies must then translate these plans into IT processes. Today, businesses—even manufacturing entities—must manage their information technology functions as service enterprises.

Although the concern about IT governance has long been recognized, it's very difficult to measure, and the AICPA doesn't offer much guidance on how to measure the value IT adds. In short, do the benefits of IT outweigh the costs, and does IT add value to the company? The CPAs who responded to the AICPA study seemingly list this item to challenge accountants to develop performance measures for IT. Standardized IT practice is to use return on investment (ROI) measures. Perhaps no one is better qualified to quantify additional performance measures for IT than Certified Management Accountants (CMA®s) and other IMA members.

3. DISASTER AND BUSINESS CONTINUITY PLANNING

Disaster recovery planning became intense after Hurricane Andrew struck Florida in 1992. Such planning became more common each year until 2001; after 9/11, interest in disaster recovery plans changed such that all companies viewed these plans as paramount to ensuring survival and minimizing insurance costs. Since Hurricane Katrina in 2005, many businesses are required to provide evidence of existing disaster recovery plans in order to obtain insurance coverage.

We have learned much about disaster recovery planning in the past few years. Consider two of the biggest lessons. First, the 9/11 disaster and Hurricane Katrina taught us that it's more important to focus on people, rather than information systems, when planning for recovery. Second, the blackout in the northeastern United States in 2003 taught us that recovery is more effective when backup sites for information systems are implemented on utility grids that are separate from those on which the original site is located.

Still, the most important facet of disaster recovery is to realize that it's a *planning* process. Disaster recovery planning refers to the developing, monitoring, and updating of the process by which organizations plan for business continuity. In short, disaster recovery planning implies backing up the entire organization. Management accountants often provide guidance in cost areas for such plans, especially in determining what type of plan to implement. Common jargon refers to plans as either "hot sites" or "cold sites." Hot and cold sites aren't discrete opposites but are opposite ends of a continuum. Generally, the hotter the site, the more expensive it will be. How hot a site is depends on two things: (1) how close the backup site is to being an exact duplicate of the existing original site and (2) how quickly the company can switch from the existing site to the backup site.

2. ASSURANCE AND COMPLIANCE APPLICATIONS

Section 404 of the Sarbanes-Oxley Act of 2002 (SOX) made it necessary for businesses to document and report their abilities to implement, monitor, assess, and test internal controls. The *Enterprise Risk Management—Integrated Framework*, published by the Committee of Sponsoring Organizations of the Treadway Commission (COSO), expanded these needs. At first, companies weren't sure how to approach these requirements, but now most companies have Section 404 documentation in place. Still, companies must provide evidence on a regular basis to show that they comply with Section 404 requirements.

Software tools now demonstrate compliance with Section 404 and even with the COSO *ERM—Integrated Framework*. Most of these tools are simply extremely large computerized checklists because Section 404 requirements are broad and yet incredibly detailed. Since SOX is only four years old and there are so many software products available, it's unclear which products are best or even effective. Assurance and compliance applications are still high on the list, however, because such applications will become essential to demonstrating Section 404 compliance.

1. INFORMATION SECURITY

While assurance and compliance applications may still be new and untested, information security, the number one technology, is a longstanding number one on the AICPA list. Information security has long been the responsibility of management accountants since they take care of and oversee all business information. While information security is so vast that it could easily spawn additional top 10 lists, we must first discern the difference between information privacy, which we discussed in Technology No. 5, and information security. *Privacy* refers to the right to be left alone. *Information security* refers to the hardware, software, processes, and procedures that are in place to protect an organization's information systems from threats. New threats surface each day, so information security is more difficult than ever. This problem is compounded by stipulations among entities concerned with confidentiality and privacy that security must be in place. For example, HIPAA required that *information security* systems be in place and operational by April 2005.

Who attacks information systems? More than 50% of the time, the attacker is a disgruntled employee. Other attackers, in order of frequency, include independent hackers, U.S. competitors, foreign competitors, and foreign governments. Most businesses, especially small businesses, incorrectly believe that their Internet service providers protect them from attacks.

As a first line of defense, businesses should design firewalls. A perimeter firewall, for example, examines the addresses of all incoming and outgoing messages and blocks unwanted messages. While such a firewall may help detect the source of intrusion, it doesn't effectively handle internal attacks. Instead, businesses often consider a dual-homed gateway (or DMZ), which creates a firewall between the Internet and the company's network. Every-

thing is routed through this firewall. It will usually be combined with an application gateway that examines the content of messages rather than just the addresses.

At least 20% of attacks go through existing firewalls. Further, more than one-third of attacks are initiated and completed using Microsoft Windows, and many additional attacks are initiated using UNIX. Many organizations, such as the SANS Institute, routinely issue lists of common vulnerabilities for both Windows and UNIX systems. For example, instant messaging in Windows and databases in UNIX are commonly on such lists. The high number of vulnerabilities makes it necessary for companies to consider intrusion detection. Intrusion detection provides evidence of any attack, prevents probing once an attack has begun, and provides detection that can lead to correction when prevention fails. To learn more about how these products work, go to www.tripwire.com, the site of one common intrusion-detection product.

One of the most important ways that business is conducted today is B2B. Almost all B2B transactions are conducted using the Internet, so, obviously, information security is a concern in B2B transactions. Much of the information security for business on the Internet is based on the Public Key Infrastructure (PKI), the source for digital certificates and the starting point for digital signatures. These are standard internal control mechanisms for Internet transactions. Digital certificates, which contain public keys, are obtained from Certificate Authorities, and, in the U.S., almost all Certificate Authorities are private companies such as RSA, VeriSign, and Entrust. In 1995, Utah became the first American governmental entity to serve as a Certificate Authority.

Briefly, this is how the PKI works. A company that wants to do business electronically with another company will obtain that company's digital certificate from a Certificate Authority. The digital certificate, which typically lasts about a year, will include subscriber information—everything from type of business to customer ratings to credit ratings. Digital certificates are more than just an optional credit check. They're necessary because they contain public keys. Any company that wants to do business with another company over the Internet obtains that company's public key and uses it to encrypt information that it sends to that company. The public key is an encryption algorithm; it transforms data into an illegible format and language. Information that might be sent using the Internet after public-key encryption would include purchase orders, invoices, or even bank transfers. The public key encrypts data that only the private key can decode. Companies keep their private keys on a *secure* server at all times, and the keys are never copied or distributed to anyone. This public-key/private-key approach essentially creates digital signatures that authorize transactions. Digital signatures always have these three goals:

1. **Integrity:** no alterations occurred during electronic transit,
2. **Attribution:** the source of the electronic transit can be identified without doubt, and
3. **Nonrepudiation:** the sender can't possibly deny the electronic transit of the document.

Hundreds of controls are necessary to provide information security. A certain amount of trust in personnel is necessary, too, because no system of controls for information security is 100% effective. Each new control provides hackers with a new challenge. As controls are devised to enhance information security and privacy, social effects emerge, and dilemmas concerning the constitutional rights of individuals may be challenged. In addition, management accountants must be extremely careful to ensure that their efforts to secure information don't violate the *IMA Statement of Ethical Professional Practice*.

THE REAL NUMBER ONE

The AICPA's list of the top 10 technologies is aimed directly at accountants, a group that understands the importance of information security. Yet even though information security tops the list, businesses don't always place it at the top of their own lists. Although information security is important in all business areas, the biggest concern, the item that would top the lists of both IT departments and CEOs, would be alignment. Alignment doesn't refer to IT governance (see Technology No. 4). Alignment is concerned with how managers and accountants ensure that the goals of a business and the goals of its IT department are congruent. After that is accomplished, alignment considers how those same managers and accountants ensure that business and information technology remain aligned with each other while both continue to change and modernize. These are the ultimate technological challenges for accountants in a world where technology is part of everyday life. ■

William M. Baker, CMA, is a professor of accounting in the Walker College of Business at Appalachian State University. You can reach Bill at (828) 262-6200 or bakerwm@appstate.edu.