5-2006

InfoTech Update, Volume 15, Number 3, May/June 2006

American Institute of Certified Public Accountants. Information Technology Section

InfoTech UPDATE

MAY/JUNE 2006
VOL. 15, NO. 3

Newsletter of the AICPA
Information Technology Section

What's Inside

INFORMATION SECURITY

The CIO as a Security Threat: *What the CPA Needs to Know to Help Clients and Employers*

By Joel Lanz, CPA

Joel Lanz, CPA, leads a niche CPA practice that delivers IT audit, security and risk management services. He is currently a member of the AICPA's Information Technology Executive Committee.

Sometimes, the least likely suspect is the most likely culprit.

As humans, we are conditioned to trust those around us. In the business marketplace where we hire professionals to take on positions of responsibility, we put our wholehearted trust directly in their hands.

Thanks to today's always-on environment, much of our time is spent dealing with potential system and information threats by internal and external sources; the proactive organizations are those that anticipate hacker behavior and are prepared for an attack. However, even though we plan and prepare for these situations, we cannot always anticipate the outcome — or in this case, the intruder.

Today's technology controls are designed to combat higher threats, such as unauthorized access from external sources. We implement and execute classical controls, including segregation of duties, monitoring of privileged users, security hardening guidelines and management oversight. In many organizations, the chief information officer (CIO) or chief technology officer is responsible for designing, implementing and monitoring the effectiveness of these controls.

What happens if the CIO is the security threat? What if the CIO is a disgruntled employee who seeks revenge based on poor salary or a performance review? What if fraud occurs? The triangle of fraud — three elements used to identify fraud at lower levels of the organization (perceived pressure, opportunity and rationalization) — explains the occurrence of CIO-related fraud.

It is executive management's loss of confidence in the CIO's ability to serve the organization that gives rise to the organization calling on the CPA for help. On numerous occasions, CEOs and CFOs have confided to me that they wanted to terminate the CIO, but were proceeding cautiously or suspending their decisions due to the CIO maintaining access to the organization's system resources and serving as custodian of information, including customer data.

In many cases, the soon-to-be-displaced CIO did not place a high value on controls, leaving the organization with undocumented procedures, mis-configured systems and other fundamental control strategies that a practitioner would otherwise find in a well-managed

Continued on page 2

AICPA

Continued from page 1

InfoTech UPDATE

May/June 2006, Volume 15, No. 3. Publication and editorial office: AICPA, 201 Plaza Three, Harborside Financial Center, Jersey City, NJ 07311-3881.

If you wish to change your e-mail address or update your member profile, please send an e-mail to service@aicpa.org.

For questions about your subscription to InfoTech Update or other questions about your IT Membership Section benefits, please contact the AICPA at infotech@aicpa.org or leave us a voice mail message at 201-938-3828, option 3.

technology function. This opportunity, combined with the rationalization of just getting fired and potential pressures due to financial hardship, may give rise to the existence of all three elements in the fraud triangle.

Obviously, in a situation where a CIO *will* be terminated, the action should be coordinated with the organization's human resource and legal advisory functions. Issues such as age discrimination, contract violation and other employment law-related issues, may impact the firing.

This article will focus on how we can help the organization manage the technology-related risks that a disgruntled CIO (or other privileged user) may seek to exploit based on his or her unique knowledge of the organization's existing technology practices and lack of controls.

Here's a Real Situation

The executive management of a $4 billion regional bank decided its CIO needed to be replaced (the cause and reasons are beyond the scope of the article and not relevant to our analysis). When a decision like this is made, it is typical that management wanted the dismissal to occur sooner rather than later.

At the time, the bank's security posture (hardening applications, networks and server) needed enhancement, and documentation relating to system resources was minimal or non-existent. Management had little knowledge of technological details because they trusted the CIO to do his job and follow through on his tasks. However, for various reasons, the CIO delayed implementation of a variety of internal audit recommendations to enhance the organization's overall technology risk management practices.

Management concerns included how to prevent the "fired" CIO from retaliating against the bank, including inappropriately making copies of confidential customer information. To demonstrate appropriate due diligence, executive management desired to mitigate security risks to the extent reasonable in order to protect the bank and its customers.

Like many other enterprises, this client had a rudimentary incident response plan that placed heavy emphasis on the CIO and his direct reports' ability to respond to emergencies. Now that the primary threat *was* the CIO, applicable risks needed to be reconsidered.

For example, the bank could (and did) revoke access to the system. A complete list of systems, including supporting infrastructure resources such as the routers, was not available. As a result, the bank was unaware of all the resources that the former CIO could access from outside its physical structure. In addition, as is practiced in some other organizations, technical staff shared user IDs and passwords, thereby providing the CIO with additional opportunity to retaliate without accountability.

It's About Risks, Threats and Probabilities

Our engagement was to assist the bank to eliminate the CIO's access to its sites, assets, networks, systems and applications to prevent damaging bank property and data. I facilitated a risk assessment with the bank's management team to help identify relevant risks and threat vulnerabilities. Although the team believed that the soon-to-be-fired CIO was ethical and honest (thereby identifying the overall probability of a criminal situation as "low"), the team readily understood that if its assumption was wrong, the CIO could cause significant damage to the bank.

At a minimum, the team concluded that it would need defense against an "outside hacker" who had significant understanding of the bank's internal operations and current control practices posture. This defense assumption differed from the assumptions in current plans because the bank previously assumed an outsider would have minimal knowledge of internal operations.

Continued on page 3

Before going further, the team had to identify its assets that were at risk. Although much of the following documentation is normally available in a well-controlled environment, the bank had to develop the following items on the fly (and at considerable expense) in order to identify the relevant assets at risk:

1. **Inventory all devices, systems and applications for which access is provided, including telecommunications.** The team needed to know the universe to which the CIO could have access, so it used automated tools to help identify network resources, including security vulnerability software (QualysGuard) and network utilities (Solar Winds). We also compared the results to existing inventory lists to identify missing contents. Fixed assets and accounts payable journals offered even more resources to identify key vendors and purchased technology resources.

2. **Identify all assigned accounts/user IDs.** We reconciled each asset identified in the inventory in Step 1, and in reviewing the relevant access list (or configuration file), we identified potential user IDs belonging to the CIO. Special attention was paid to anonymous user IDs because these were well known to the CIO and their use could be exploited without providing individual accountability.

3. **Identify all administrator rights or system accounts.** We wanted to determine whether the CIO was aware of privileged access accounts that did not have unique owners, thus enabling him to access resources without fear of accountability. As a result, executive management needed to share the planned ouster with a trusted administrator who could either delete these passwords or enable appropriate monitoring tools.

4. **Identify any non-approved or unknown devices on the network.** Given his position of privilege, the CIO would know of potential devices attached to the network that were not identified on network maps or inventories. These "rogue" devices could be used to gain unauthorized access.

5. **Identify all related data and voice vendors, as well as "consultant" projects in process.** Because the CIO would no longer act as an agent for the company, outside vendors and consultants had to be notified. With their unique insight into the organization, this group was able to supplement executive management's understanding of the technology environment and its potential assets at risk. This step also included communications with vendors/suppliers to request their cooperation in informing the bank if attempts were made to initiate unauthorized contact.

6. **With inventories developed above, ascertain quality, completeness and usefulness of backups if a rebuild or reinstall was required.** If the CIO struck, the team needed to ensure that appropriate backups were maintained in case records needed to be reconstructed. Again, in a well-controlled environment, this would be quite easy. However, due to the CIO's poor performance, identifying and testing these resources proved time consuming.

7. **Plan for eliminating physical access, including badges and combination locks.** To reduce the threat of the CIO being able to access the building and other physical resources, electronic badge readers needed to be adjusted to prevent unauthorized access.

8. **Disable access and change passwords as deemed necessary.** We say "necessary," but this is especially pertinent to perimeter-facing devices (routers, firewalls and modems), as well as easily guessed user passwords (default voice mail passwords that have not been changed). Considering the number of applications an average user has, it is not unusual for a CIO to have access to 20 to 30 different system resources. The CIO also may know of other resources where easily guessed passwords are used. Despite implementing good security, if the CIO could access these devices, he could gain entry. The focus of our efforts was on the perimeter systems, which the CIO could potentially access from outside the bank's physical premises.

9. **Determine what to do about voice mailbox, e-mail mailbox, hard drives and anything stored on company resources.** Communication devices can result in important clues to help identify vendor relationships, projects in process and other technology assets. However, this should be weighed against the risk of allowing the CIO to provide the public perception that he is still a representative of the organization. As with other termination practices, the company should ensure that further information leaks are prevented.

10. **Review authorities for Internet domain name and/or registration contact, including DNS provider for e-mail and Web browsing requests.** Typically, the CIO coordinates the corporation's entry and activity on the Internet, including registering domain names. It is important to contact the domain name registrar to remove the CIO's capabilities to modify or transfer domain name assets.

11. **Minimize or critically monitor external access/ability to perform maintenance on critical resources.** With the heightened probability of activity, the organization may desire to enhance monitoring over critical resources, especially technology assets that may be public facing, including routers and firewalls. Passwords on these devices should be changed.

12. **Fine tune the firewall to prevent sending materials out, or uploading**

Continued on page 4

ASSURANCE AND COMPLIANCE APPLICATIONS

Compliance Software — Is it Time to Invest?

By Bepsy Strasburg, MBA

Bepsy Fakir Strasburg, MBA, is director of BDO Seidman, LLP, Risk and Advisory Services. She leads client engagements in Sarbanes-Oxley compliance, internal audit, business process improvement and change integration.

As many companies head into their third year of compliance with Section 404 of the Sarbanes-Oxley Act of 2002, they are evaluating the lessons learned from implementation experiences and initial assessment of internal controls. Many companies faced challenges during their initial SOX implementation and had more of a short-term "get it done" attitude, with compliance as their main goal. Business process improvement and increased automation of controls were considered, but many companies did not have the time or resources to devote to these efforts. For these companies, serious evaluation of a software tool to manage compliance efforts, to date, has been minimal.

Today, companies are taking a closer look at how they can achieve efficiencies, as well as generate overall savings for the company by using compliance software. They want a tool to assist them in achieving their compliance objectives, rather than serving merely as a repository for compliance documentation. Indeed, many early adopters of software tools have discovered that existing functionality did not meet their expectations. Often, software had to be co-developed with the software vendor to provide a more customized solution for the company.

Forrester Research reports that the majority of companies with more than $75 million market capitalization (approximately 5,000 companies) will invest in a software solution. With that forecast in mind, savvy software vendors have taken increased steps to identify key functional requirements sought by the marketplace.

Many factors need to be considered when evaluating the right compliance software to fit a company's needs. Assessment of whether a company is ready for a software tool includes a review of the available functionality of the compliance software, required implementation efforts and cost considerations.

Continued on page 5

Information Security *continued from page 3*

to, a third-party Web site. Using the firewall to prohibit transferring selected types of data to the outside world provides another level of protection against the disgruntled CIO threat. This includes prohibiting virtual network connections that may prevent the CIO from establishing a virtual connection as an internal machine from the external side of the network. Another example is the unloading, or disabling of, any remote control software, such as pcAnywhere or Windows 2000/xp remote or terminal services. However, managing this risk needs to be balanced against the very valid requirement of providing access capabilities to other employees who may need it.

13. **Discontinue credit cards and vendor-extended business credit.** With all the focus on the technology risks, it can be easy to overlook the more traditional business risks, such as use of company credit cards, and with selected vendors, the ability to incur debt on behalf of the organization. For a larger company, signing limit authorities would also need to be revoked.

14. **Determine the extent of monitoring required, focusing on privileged accounts usage and access to devices.** As enterprises balance the benefits and costs of recording all system activity, the level and extent of monitoring is always an issue. During the termination process, the organization should consider focusing its monitoring efforts on the resources most likely to be abused by the CIO, especially the use of privileged accounts that may be shared or that may not be apparent as belonging to the CIO. Consider using an intrusion detection system to assist in monitoring various audit and log files available to the CIO.

Our Role in Business

Privileged users are no different than other employees, given the right circumstances that can face a "moment" of weakness. When compromised, access capabilities granted to a privileged user can be very expensive to manage at best, and compromise the organization in the most severe situations.

As a CPA working with clients, employers and other organizations, we have the innate ability to analyze the situation, develop an action plan and work with the entity to carry out the plan. And, as stated earlier, it may not be an inexpensive solution if the organization must respond quickly to a potentially disastrous situation.

Some of the 14 steps can be combined or changed depending on the actual situation or makeup of the business at risk, but the bottom line is that, as accounting professionals, we can serve our clients and employers by not only helping them over the barrier of facing the situation, but educating them on the possibilities that a CIO security threat can occur.

.....

Contact Joel Lanz at *jlanz@joellanzcpa.com.*

Functionality

The required functionality for compliance software can be evaluated from two perspectives, operational and technological. In addition, functionality should be further differentiated between essential (must have) versus optional (nice to have).

Operational

- Predefined and customizable enterprise compliance models for all components of the compliance framework. For example, COSO and COBIT® for Section 404 of the Sarbanes-Oxley Act.
- Survey capabilities for entity-level controls, business unit self-assessments or sub-certifications for Section 302 compliance.
- Multiple level organization hierarchy structure with no limit on the number of levels.
- Ability to add/move/delete entities using an interactive user interface without requiring a database administrator to make configuration changes to the software or make hard-coded changes.
- Workflow (ease of routing work among people and systems), issue and task monitoring with drill-down capabilities.
- Centralized access control privileges to fit the operating environment of the company.
- Custom reporting (real-time executive management and Audit Committee dashboards) with analytics (number of exceptions, severity of risk and accumulated significance to the financial statement).
- Integrated with process mapping (flowcharting) capabilities.
- Document management with version control, and check-in/check-out functionality.
- Compliance checklists.
- Audit trail capabilities: who made the change and when the change was made.
- E-mail alerts for users originated from the software in anticipation of test dates, past due items and priority of issues using pre-authorized routing rules, and the ability to e-mail control owners and monitor pending items.
- Selected practice aids. Examples include audit planning or statistical sample size selection based on risk and frequency profile of key controls.
- Project management — the ability to track issues and actions associated with documentation and testing within the software, budgetary reporting and estimated completion time or percent complete forecast capabilities.

Technological

- Secure Web browser protocol enabled.
- Intuitive and easy-to-use navigation tools.
- In-house or hosted application.
- File import and export capabilities – import risks and controls for customization and correlation with business processes, and unlimited storage capability for evidence collected in support of testing and viewed by users based on their access privileges.
- Underlying database structure that integrates to existing IT (ERP and network) infrastructure.
- Integrated with existing network user authorizations, eliminating the need for separate user repositories.
- Third-party upload capabilities to import files from service providers.
- Archive capability.
- "Read only" capability.
- Ongoing compatibility with the company's operating systems.

External Auditor Advantage

Companies are working with their external auditors to refine management's approach to identify and test internal controls. Consideration should be given if the use of a potential compliance software package will facilitate this review process.

For example, the software could provide "read" access to the external auditor for process documentation, management summaries of aggregated deficiencies or the management deliverables timeline. A continuously updated project management timeline can make the audit resource planning more efficient in an integrated audit — and avoid surprises. Customized worksheets can be developed by the external auditor to extract data and import directly into quality assurance tools. Evidence accumulated by management to support testing also can be viewed online.

Vendor and Software Selection

In today's environment, organizational and regulatory requirements are many. Because the compliance software will be a long-term investment for the company, those facing requirements from various organizations will require a comprehensive evaluation process and buy-in from different stakeholders. These include the Federal Financial Institutions Examination Council (FFIEC), the Public Company Accounting Oversight Board (PCAOB), and the Occupational Health and Safety Administration (OSHA) — along with mandates by the Health Insurance Portability and Accountancy Act (HIPAA). It is critical to have an economically viable software vendor with a history of successful implementations for a comparable size company.

Continued on page 6

Assurance and Compliance Applications *continued from page 5*

Key attributes of potential software vendors include:

- Sustainability of the software vendor.
- Product positioning and the vendor product strategy.
- Completeness of the solution set or roadmap – incorporating additional value-add components, such as Section 302 certifications or fraud monitoring.
- Real-time alignment with compliance regulations – particularly if predefined compliance models are provided in product libraries.
- Ease of software upgrade capabilities to enable a smooth migration path.
- Ability of the vendor to provide support as the company grows.
- References of customers.
- Current release number of the software – a higher release number may indicate a product with a sustained track record and product progression.
- Vendor provided training.
- Ease of implementation.
- Overall organizational responsiveness and service orientation.
- Vendor accountability for bundled solutions achieved through add-on packages.
- SAS70 certifications for hosted applications, when applicable.
- Software fit in the vendor product philosophy.

The selection process of the software should include input from practitioners experienced in compliance projects. These team members can develop a custom questionnaire to help the company navigate through the criteria relevant to the evaluation process. Sample questions that could be included in a questionnaire are included in Figure 1. In addition to questionnaires, vendor interviews and live demonstrations are typically used to evaluate the software.

Implementation Considerations

Implementation of the software may take as long as three months. The timing of the implementation should be coordinated with other anticipated changes in the company. Time required to complete current year Section 404 compliance should be factored into the implementation timetable. Other considerations include the company's state of compliance, level of documentation and the conversion effort to migrate to the software repository. Even customization time of existing pre-populated libraries of process narratives and risk control matrices may be significant and should not be underestimated.

Figure 1

Executive Dashboard

Does the product have the capability to display a summary of exceptions, graphs, severity and charts on a single dashboard view?

Can the product assign dashboard views to areas only applicable to the user?

Security Access by Module, by Data, by Specific Compliance Model

Can the product control user access to individual checklist items?

Can users be grouped within the application?

Does the application support security policies, such as password strength and session timeout?

Cost Considerations

Cost of the software is another important condition. Expenses incurred for monthly maintenance and potential costs to upgrade can quickly exceed anticipated costs. Our research indicates that implementation costs may range from $100,000 to $150,000 for a mid-sized, centralized company. Increased scope through decentralization, growth and complexity will add to annual costs. Although some costs may be offset by eliminating manual processes, this saving is hard to quantify. Data related to internal staffing costs to be compliant is not readily available because many companies do not track these costs.

The pricing structure used by the software vendor will vary depending whether the software is hosted by an Applications Service Providers (ASP) or by the user company itself. Software vendors may charge a base price with a variable component based on the number of users or licenses. Hardware investments and additional in-house support services may be necessary as well.

Company Readiness for a Software Tool

Having evaluated the functionality requirements, vendors, software options, implementation issues and associated costs, the company needs to determine whether it is ready to make the investment in a software tool. Several variables in the company's environment will help to determine the success of the software deployment:

- What is the executive management and Audit Committee experience with the compliance process?
- Has the company stabilized its process documentation and identified the key players involved in the compliance process?

Continued on page 7

INFORMATION SECURITY

A Guide to Resources for Information Security

By Chris Fraser, CPA.CITP, MBA, MCP, CISA*

Chris Fraser, CPA*.CITP, MBA, MCP, CISA, a Business Technology consultant in St. Petersburg, Fla., combines the strategic and business skills of a CPA and the technological skills of an Information Technology professional to provide services to various size companies. He is a member of AICPA's CITP Credential Committee and *InfoTech Update*'s Editorial Advisory Board.

**CPA licensed by the State of Florida*

For the fourth consecutive year, "Information Security" once again was #1 on the list of AICPA's Top Technologies. Although in-depth articles and other content will be developed throughout 2006 on Information Security, readers of *InfoTech Update* probably will benefit from a simple resource list of Web sites, products and services that help the profession deal with this very broad, often overwhelming area of concern.

This is by no means an all-inclusive list — but it's a start to giving CPAs and their clients and customers a bit more direction on how to deal with information security. For more information on the Top Technologies, visit *www.aicpa.org/infotech.*

Home Network Security

- **CERT® Coordination Center** — This document gives home users a good overview of the security risks and countermeasures associated with being on the Internet, especially for "always-on"/broadband access services, such as cable modems and DSL.

  www.cert.org/tech_tips/home_networks.html

- **SANS Internet Storm Center** — With this site, you can view the 'Infocon' page, which shows the current status of the Internet, representing changes in malicious traffic and the possibility of disrupted connectivity.

  http://isc.incidents.org/infocon.php

Continued on page 8

Assurance and Compliance Applications *continued from page 6*

Year 2 may be ideal to consider automation due to the joint learning curve of the employees and external audit sign-off of internal controls in the baseline year.

- Does the company have a complex operational and financial reporting environment? For example, the compliance requirements for a single-product, single-location organization with a few employees will be significantly different from a multi-product, multi-national organization.
- What is the company budget and appetite for automation?
- What other compliance requirements beyond Sections 302 and 404 of SOX affect the company's operations?
- Does the company require an integrated enterprise risk management?

Early self-assessment of these factors and corresponding communication plan will yield a better adoption rate of the software by the user community.

Is It Time To Invest?

The timing to implement a software solution will vary by company. The decision depends on a number of the variables discussed above to conduct a careful evaluation.

Consider, too, that potential demand for compliance software has increased the number of compliance software vendors offering compliance software choices — and some with a specific focus area. Not all of these vendors will reach the critical number of installations needed to invest in their product adequately and be a viable long-term player in the marketplace. Therefore, consolidations among software companies are expected over the next few years, particularly to achieve growth by acquiring a competitor's customer base.

This means that selecting the right software vendor is as important as the software itself. In addition, buyers must ensure that customer experience of the software vendor is driving their choice, rather than the "mind share" achieved by the vendor through effective marketing execution (marketing hype) or "cool" technology.

Under this scenario of changes in the software marketplace and the complex operating environment of a company, it is strongly recommended that appropriate due diligence using the best available resources be conducted for this long-term investment decision. The information presented in this article will get you started on the right track in this very important decision. Good luck!

Contact Bepsy Strasburg at *bstrasburg@bdo.com.*

A Guide to Resources for Information Security *continued from page 7*

- **Top 75 Tools for IT Security** — A great list with some free and some fee-based programs that work on Linux, Microsoft Windows and other operating systems.

  http://www.insecure.org/tools.html

- **WindowsSecurity.com** — Security articles and tutorials.

  www.windowsecurity.com

- **Windows Live Safety Center** — New from Microsoft, get a free safety scan to help protect, clean and keep your computer running at its best.

  www.microsoft.com/athome/security/update/windows_live_safety_center.mspx

- **Ten-Minute Guide to Network Security** —

  www.securitypipeline.com/170101586;jsessionid=WT4PGZT1QSVQSQSNDBCCKH0CJUMEKJVN

- **80 Super Security Tips** — This page from PCmag.com offers 80 links to key security issues.

  http://pcmag.com/article2/0,1895,1838690,00.asp

- **More Security Tips** —

  www.earthlink.net/elink/issue72/security.html

- **Network Security Forum** — Information about security, Linux, exploits, wireless, certifications and more.

  www.networksecuritytech.com

General Tips for IT Security

- **Microsoft Baseline Security Analyzer** — This is a great tool that everyone with a Windows system should use. It checks the Windows operating system, determines the security state in accordance with Microsoft security recommendations and offers specific remediation guidance.

  www.microsoft.com/technet/security/tools/mbsahome.mspx

- **Purchase and Update Antivirus Software** — While most PCs come with anti-virus software, some are only 90-day versions. If your subscription has expired, it is not protecting you from current threats. In addition to the big names — Norton, McAfee, Trend and Panda, there are others available for free: AntiVir for home users —*www.majorgeeks.com/download955.html*, and ClamWin for businesses — *www.clamwin.com*.

- **Install a Compression Utility** — If you don't have Windows XP (XP already has a built in compression utility), some Internet files you want to download will require a program to extract them. The most popular is Winzip — *www.winzip.com*; however, 7-Zip is a freeware program that works with RAR and ZIP files — *www.7-zip.org*.

- **Disable Messenger Service** — Some Internet advertisers misuse Windows Messenger to broadcast ads by having a "messenger service" in the title bar of the pop up box. Note: This is different from MSN instant messenger. It is a good idea to disable the windows messenger service in order to prevent these ads from popping up.

  www.microsoft.com/windowsxp/using/security/learnmore/stopspamv45.mspx

- **Understand Windows Built-In System Restore** — System Restore can be a useful tool for setting your PC back to a previous working state if something were to go wrong. However, spyware and malware also can use System Restore to reinstall itself on your computer after you clean it. If you have a virus or spyware, disable it by following the following steps for Windows XP or ME:

  - **Find and remove Spyware** – You must use additional programs because the current version of Windows (XP or earlier) does not have a built-in feature to protect your machine from spyware and malware.

  - **Free Spyware Scan from Earthlink** —

    http://www.earthlink.net/software/nmfree/spyscan

  - **Microsoft Anti-Spyware** — This one has a great detection rate and real-time protection, and most likely will be Microsoft's default anti-spyware in its next version of Windows (note – even though the Web site says "beta," it is not a beta product).

    www.majorgeeks.com/download4466.html

  - **CWShredder** — Removes the common CoolWebSearch Trojan that infects PCs.

    www.intermute.com/spysubtract/cwshredder_download.html

  - **Spybot Search and Destroy** — Another good spyware removal tool.

    www.safer-networking.org/en/download

  - **Ad-Aware** — One of my favorite spyware removal tools. Note: Ad-Aware Personal is for home users only; they sell a version for business users. Also, remember to install the VX2 Cleaner plug-in for Ad-Aware.

    www.lavasoftusa.com/software/adaware

  - **VX2 Cleaner:** *www.lavasoftusa.com/software/addons/vx2cleaner.shtml*

  - **Crap Cleaner** — Clears out files where malware sometimes hides.

    www.majorgeeks.com/download4191.html

  - **Winsock Fix** — Certain malware destroys your Internet connection when removed. This program can try to repair

Continued on page 9

INFOTECH UPDATE PROFILE

Bryan L. Smith, CPA.CITP, CISA

This month's InfoTech Update profile focuses on Bryan L. Smith, CPA.CITP, CISA. Bryan is co-founder of CPA Crossings, LLC (www.cpacrossings.com) *in Rochester, Mich., a professional services firm deploying an innovative model to work with CPAs to bridge the gap between business and technology for the small- and mid-size business market. He was formerly with BDO Seidman, LLP, and is a member of AICPA's CITP Credential Committee.*

InfoTech Update: With regard to serving other CPAs and their firms, what do you feel is the primary mistake most firms make when it comes to effectively using technology?

Bryan Smith: Simply put: Not fully using the technology they have already invested in. The reasons for this vary from one firm to the next. One of the primary reasons is that the firm will not dedicate the time to learn how to use the more advanced features of an application, or to learn about best practices for leveraging the features of a particular software application.

Another reason is that in many cases, when you fully utilize the capabilities of an application, it means fundamentally changing the way that particular process is performed. This takes CPAs *out* of their comfort zone relative to a traditional approach to the process. The good news is that CPAs, in general, continue to become much more comfortable with all aspects of information technology and are gaining a better appreciation of the overall value proposition of technology. This ultimately results in a higher ROI in their technology investments.

ITU: *What do you think the largest hindrance or barrier has been to companies (not CPA firms) implementing paperless solutions?*

Bryan Smith: The issue is more a matter of priority.

I don't think there has been any significant obstacle preventing business organizations from implementing paperless solutions in terms of electronic document management systems. Unless the organization is in a business model that pushes a lot of paper through its processes, there are likely to be other IT initiatives that will provide the business with a higher ROI. Examples of such initiatives include e-commerce solutions and RFID inventory tracking systems, to name a few. Actually, the examples just cited are paperless solutions in their own right. In terms of document management solutions, I think we will see a continued increase in adoption of this technology because the solutions become easier to deploy and less expensive.

Bryan L. Smith, CPA.CITP, CISA

ITU: *What's the CPAx Technology Best Practices Forum?*

Bryan Smith: This is a new service that we recently announced to provide accounting and tax professionals with direct access to two very valuable resources: IT-focused CPE programs and "best practices" technology experiences shared by their peers in the profession.

The Forum's CPE programs are very focused on advanced tips and techniques for using everyday software applications, such as Excel, Word, Adobe and other programs in traditional accounting, assurance and tax services. The more firms go "paperless," the more important these tools are becoming.

The "best practices" forums are small

Continued on page 10

A Guide to Resources for Information Security *continued from page 8*

your internet connection if the malware destroys it. Note: use this only if your connection dies as a result of removing the spyware/malware.

www.majorgeeks.com/download4372.html

For More Technical Information

The NIST (National Institute of Standards and Technology) has a number of resources available over the Internet. Follow these links for more information.

- NIST Computer Security Special Publications — *http://csrc.nist.gov/publications/nistpubs*
- Focus Areas: Cryptographic Standards and Applications, Security Testing, Security Research/Emerging Technologies and Security Management and Guidance — *http://csrc.nist.gov/focus_areas.html#csa*

Contact Chris Fraser at *cnf@frasercompany.com.*

InfoTech Update Profile *continued from page 9*

group online conference sessions with discussions about successes and challenges CPAs are having in their deployment of popular CPA centric software applications, such as CCH, RIA, Creative Solutions and more. We facilitate the forums to keep them focused, documented and free from vendor bias. All of these experiences are delivered via live Web conference sessions that allow the participants to get in and out of a topic within a two-hour time slot *and* avoid the time and cost of traveling to the event. We have priced this as an "all you can meet" service. Individual and firm memberships are available that allow members to attend all of the training and forum sessions throughout the year for one fee. Details are available on our Web site, *www.cpacrossings.com*.

***ITU:** How do you and your business partner, John (John Higgins, CPA.CITP) complement each other with regard to skills, knowledge and client relationships?*

Bryan Smith: John and I make a great team! On one hand, we both have a high level of passion for helping the members of our profession leverage IT to increase their value, quality of service, and yes, quality of life. So we are pretty nicely aligned in our thinking about the strategic direction of CPA Crossings.

On the other hand, we have a diverse and complementary set of skills. John is focused more on getting the CPA Crossings message out to the marketplace through his extensive interaction with members of our profession throughout the country. He also focuses on developing our strategic alliances and partnerships, and overall business development. My primarily role is to leverage my analytical and organizational skills to oversee the value and quality of our client services by managing our team to successful completion of client projects. I am also responsible for overseeing the development of our service delivery methodologies.

Perhaps a simple explanation is that John's focus is on CPA firm strategy that leverages IT, and my focus is on IT that leverages the CPA firm's strategy. That can best be seen through John's work on various executive committees and as board chairperson at the Michigan Association of CPAs, and my studies toward a Master of Science in Information Assurance (MSIA) degree. Together, with the rest of our team members, we serve as a valuable resource to our clients.

***ITU:** What does the CITP credential do for you?*

Bryan Smith: There are two key components of the CITP credential's value proposition. One is market positioning and the other is competency development. In regards to the marketing aspect, I firmly believe the CITP credential is an essential tool, not only for me and CPA Crossings, but for the profession overall.

We (CPAs) are continually challenged with overcoming the stereotype of being tax preparers and auditors. There is a substantial segment of our profession that is directly or indirectly involved in the planning and deployment of IT in their own business organizations or their clients' businesses. We need to proactively communicate to the marketplace that this is a core competency of our profession, consistent with the AICPA's Vision Project. The CITP credential is a great way to communicate that to the marketplace. From this perspective, I believe we should be able to easily identify 5 to 10 percent of CPAs having this core competency. Many of these folks are members of the Business and Industry group that the AICPA is continually working to serve more effectively.

The second component of the CITP's value is the ability to have access to technical information and professional development programs that will improve my skills and qualifications to help my clients successfully address the pertinent technology issues of the day, including security, privacy, Web applications and application integration. We, the current community of CITPs, need to push forward initiatives that will help us expand the depth and quality of these resources to improve our competencies in this discipline. If accounting is the language of business, then information technology is the oxygen that gives breath to the business organization – and necessary to survive and grow in today's competitive global marketplace.

Are you a CISA? You are Automatically a CITP!

Through a recent agreement with ISACA, CPAs holding the Certified Information Systems Auditor (CISA) credential are now automatically eligible to receive the Certified Information Technology Professional (CPA.CITP) credential from the AICPA if they are Institute members.

With the CITP credential, CPA/CISA practitioners will have a complementary set of credentials that demonstrate to employers and clients both their business technology orientation and in-depth knowledge of systems, controls and security. As CITP credential holders, they will receive premium benefits, including discounts on AICPA IT conferences, Webcasts and publications. The CPA.CITP also will have access to a CITP marketing toolkit and monthly communications that focus on the impact that technology has on business.

CPA/CISA practitioners interested in applying for the CITP under this program should e-mail *CITP@aicpa.org*, or visit *http://infotech.aicpa.org/Memberships/CPA.CISA+Application.htm*.

E-BITZ focuses on practical applications of various technologies to enhance a practice or business. Her columns in 2006 focus on "Honorable Mentions" in the 2006 Top 10 Technologies Program.

E-BITZ WITH SUSAN BRADLEY

Patch Management, Systems and Tools

It's Tuesday. Not just any Tuesday … but "Patch Tuesday."

It's the day those of us running workstations and servers with Microsoft Windows operating systems need to look at our risks: the risk of patching, not patching, taking mitigation … the risk of determining that you have other means to protect your systems.

What am I talking about? It's a process called Patch Management, the monthly process of risk analysis and change analysis, and something all of us should be doing, even on our home computers.

When software is designed and built, engineers make certain assumptions regarding how their software will be used. If it is used in a manner that wasn't considered or planned on, the software may react in a manner that wasn't expected. In the worst case scenario, this "unexpected behavior" could mean the program would break its processing and leave the processes in a position to be used for other, more harmful things.

This abnormal behavior is better known in the technology industry as "buffer overflow" where unexpected data enters into a process or application. These software bugs can be flaws where the application wasn't anticipated to be used or attacked in such a manner, or they can just be flaws in software caused by human fallacy.

Before you think the process of finding software vulnerabilities is only done by hackers, very large companies spend a great deal of time trying to figure out what could go wrong. For example, firms like 3com's The Tipping Point organization will pay up to $10,000 per vulnerability and work with both researchers and vendors. Why do they provide this type of service? By knowing what problems exist, their products can include pre-release detection for these unreleased vulnerabilities.

The next pressure on the patch and risk management industry is the narrowing of the time between the moment the patch comes out and when the exploit is actually seen as a remote, attackable worm on the Internet.

In recent months, there's been less and less time between when a patch is released and when an exploit is in the wild. Part of this is the process of looking at what the patch fixed and the vulnerability researchers "reverse engineer" with the patch in order to build a "proof of concept" exploit. This is then turned into a real exploit and used widely. The tools for building these exploits are getting easier and easier. Add to that the fact that the malware industry also drives many of these exploits, and you end up where we are at today.

Analyze Your Systems

Inventory Your network. You cannot protect something when you don't know what you need to protect. Begin by understanding the applications and operating systems, and the security requirements of these systems. Is your network standardized? Do you have a mixed network of Linux and Windows? Just Windows platforms? Knowing these answers will assist you in determining the tools you will use for patching.

Set up a test network for patching. Today, with Vmware (provide both server and workstation emulation software) and Microsoft's VPS and VServer offered as free products, any size network should be able to set up a patching test bed to ensure that patches will not harm your key line of business applications. If you can't do even that, the process is as easy as finding a "canary." A "canary" is just like the helper to the coal miners of the past — a computer user in your office, more savvy than the rest, who is willing to test the patches first and ensure that your line of business applications work as they should. Once this person has "certified" the patches, you are ready to roll them out to the rest of your firm.

Review and link to resources. During the patch testing process, any and all of the issues found in testing are included in the "caveat" section of vendor security bulletins. If any issues were found, there is a link to a Knowledge Base article with additional resources. If you cannot patch, due to vendor support or issues, then you also should review the mitigation factors in the bulletin and take appropriate actions. I'd also strongly recommend that someone is your organization keeps his or her RSS reader pointed to the MSRC blog at *http://blogs.technet.com/MSRC,* the location where the Microsoft Security Resource Center will post its late breaking information on security and patch issues.

Patch Tools

At this point, you've reviewed your network, know what patches you need to deploy, tested them and now are ready to deploy them. What tool do you use for deploying patches?

Continued on back page

You can be as low tech as merely turning on automatic updates on all of your workstations and servers, to using Patch Management tools like WSUS, Shavlik or Ecora to deploy patches and keep track of the software in your office. WSUS or Windows Software Update Services is a free patch management solution from Microsoft at *www.microsoft.com* (search for WSUS). Other patch management vendors, such as Ecora (*www.ecora.com*) and Shavlik (*www.shavlik.com*), provide much granular control of patching, including uninstalling.

Susan E. Bradley, CPA/CITP, MCP, GSEC, is a principal with Tamiyasu, Smith, Horn and Braun in Fresno, Calif. Contact her at *sbradcpa@pacbell.net*. Note that the opinions expressed here do not reflect an endorsement or recommendation from AICPA.

AICPA Top Technologies #14

Patch & Network Management Tools — Tools and strategies to centrally patch, manage, upgrade and maintain applications and operating systems across an enterprise, e.g., MS MOM (Microsoft Operation Manager), MS WSUS (Microsoft Windows Server Update Service), Shavlik, Dell Open Manage, ZenWorks and Unicenter TNG.

AICPA IT Section

American Institute of Certified Public Accountants
Information Technology Section
201 Plaza Three, Harborside Financial Center
Jersey City, NJ 07311-3881

ADDRESS SERVICE REQUESTED

ISO Certified

PRSRT STD
U.S. POSTAGE
PAID
Permit No. 5165
RIVERDALE, MD