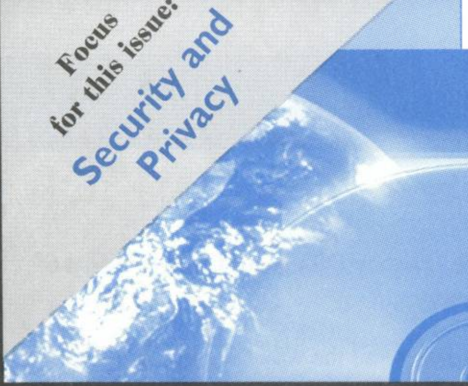
9-2002

InfoTech Update, Volume 10, Number 5, September/October 2002

American Institute of Certified Public Accountants. Information Technology Section

Roj.



InfoTech Update

Information Technology for CPAs by CPAs

IN THIS ISSUE

American Institute of Certified Public Accountants

AICPA

PRIVACY

PRIVACY IS A RISK MANAGEMENT ISSUE

An Interview with Everett Johnson, CPA, CISA

Everett Johnson, CPA, CISA, is a partner and international director of Deloitte & Touche Enterprise Risk Services in Wilton, Conn., and serves as chairman of the AICPA/CICA Enterprise-Wide Privacy Task Force. *InfoTech Update* recently sat down with Johnson to learn how privacy affects the accounting profession, and what CPAs can do to get ahead of the curve in complying with privacy regulations.

ITU: What is the definition of privacy and what obligations do individuals and companies have as it relates to privacy?

Everett Johnson: Privacy is about protecting personal information and ensuring that it is only used in ways the customer wants it to be used. Individuals have choices as it relates to their privacy and how companies can use their information, but these choices mean that individuals also have certain obligations.

ITU: What kinds of privacy obligations are there?

EJ: Individuals need to exercise their right to choose how companies or organizations with which they do business use their information. This means deciding with whom it should be shared or if it should be shared at all. If information can be shared with other parties, the individual is obligated to make sure that private information about them is accurate. The best example of this is in credit reports. If individuals find incorrect information in a credit report, they need to find out what the process is for correcting that information, and then take action.

In addition, entities that maintain private information also have certain rights and obligations to make sure the information about individuals is correct and accurate. This is why the definition of privacy encompasses the rights and obligations of *both* individuals and organizations that maintain the private information. Unfortunately, most individuals focus on their privacy rights, but forget that they also have certain obligations. If you look at the responses to the privacy notifications under the Gramm-Leach-Bliley Act, there was a very low response rate from consumers notified of the new law as it related to personal financial information protection.

ITU: Is privacy a risk management issue? Do you see the need to elevate it to the executive management level?

EJ: Yes on both counts. Privacy violations create a loss of trust and confidence with companies that violate promises, as the promises relate to the treatment of private information. Once this trust is broken, there could be a loss of revenue, decreased customer

continued on page 2

Privacy is a Risk Management Issue continued from page 1

loyalty, diminished reputation or brand, and declining share value or market value. In addition, certain regulatory requirements require that some organizations take specific steps to protect the private information of their customers. Once privacy laws or regulations are broken, privacy often can become a management issue, and I think we're starting to see more interest at the higher levels within companies.

ITU: What developments are putting privacy on the radar screen of top management?

EJ: Reported incidences of privacy violations and their impact on businesses is a major factor, and as a result, we're starting to see companies appoint "Chief Privacy Officers." Currently, however, we're seeing more interest from executive management teams than with corporate boards. In fact, privacy is such an important issue that President Bush has recommended the hiring of a Chief Privacy Officer for the new Office of Homeland Security.

INFOTECH UPDATE, September/October 2002, Volume 10, Number 5
Publication and editorial office: AICPA, 1211 Avenue of the Americas, New York, N.Y. 10036. Copyright © 2002, American Institute of Certified Public Accountants, Inc. Opinions of authors and the AICPA staff are their own and do not necessarily reflect policies of the Institute or the Information Technology Section. Any hardware or software products mentioned do not in any way represent an endorsement by the Institute or Section.

For questions about your subscription to *InfoTech Update* or other questions about the IT Membership Section please contact the AICPA at *infotech@aicpa.org* or leave us a voicemail at 212–596–6211.

ITU: Can companies use the way they handle private information as a competitive advantage? Is there a perceived market advantage for having good privacy policies and controls?

EJ: Today's focus is on mitigating risks associated with the reputation of, and trust in, a company. Companies are beginning to realize that reported privacy breaches mean lost business. I also think there is an opportunity for companies to use good privacy management as a competitive advantage in the marketplace, especially in certain sectors like financial services and healthcare, where information privacy is being required by law.

ITU: Are there mandates from state or Federal governments that require companies to protect consumer privacy? Which business sectors are affected? Are there opportunities for CPAs to leverage these mandates when offering privacy services to companies?

EJ: There are several areas in which the government has issued regulations or approved legislation that requires organizations to protect private information. Gramm-Leach-Bliley requires financial services institutions to protect financial information of individuals. CPA firms also are included under this law if they handle financial information, including tax or personal financial planning information for their individual clients.

Another area affected by privacy laws is the healthcare sector. Under the Health Insurance Portability and Accountability Act (HIPAA), the Federal government is in the process of issuing final privacy requirements that will affect most medical organizations. These will become effective next year. Another area of concern is the protection of children's privacy.

In addition, several privacy laws and guidelines exist in overseas jurisdictions requiring U.S. companies that do business in these countries to protect the privacy of their customers. Most European Union countries have much stricter laws than the United States when it comes to the protection of privacy. So, if companies have customers in Europe, for example, they are obligated to protect customer information — deemed to be private information, in accordance with European law. However, many companies don't realize their obligations. This represents an opportunity for CPA firms because government mandates present firms with significant opportunities to provide privacy services to companies to help them comply with the law, while demonstrating to customers and business partners that they have the proper privacy and security policies and controls in place to protect private information.

continued on page 3

Privacy is a Risk Management Issue *continued from page 2*

ITU: Is privacy only something that large companies should be concerned about?

EJ: Privacy protection is independent of the size of a company, especially with government mandates requiring adequate protection in large sectors of the business community. Overall, any time companies are dealing with personal information about their customers or employees, they need to consider the privacy issues surrounding that information. Privacy may be much easier for a smaller organization to deal with than for a large, complex organization, but CPAs can help out in either scenario. We have the skills necessary to understand how to implement effective privacy policies and procedures in an organization — no matter how big or small. CPAs understand business systems, how information flows and how information is managed. What CPAs need to understand to help clients or employers is what privacy is all about. This area of expertise is no different from the CPA learning about a new tax law, or a new set of accounting or auditing standards.

ITU: Besides know-how to develop effective policies, procedures and controls, and the understanding of how information flows within an organization, what other skills do CPAs have related to privacy that makes them a better choice for an organization looking for privacy help? What are the advantages of turning to a CPA for privacy services?

EJ: I think that the CPA's understanding of business systems, business information flows and how information is used is probably unique in the marketplace. While some CPAs are not IT specialists, they do understand the way information is gathered from transactions within an organization and how it is used to manage various aspects of the business. This is a unique skill, and privacy is all about managing information according to the privacy needs of customers or employees.

ITU: Is privacy only an "online" or Internet issue?

EJ: No — it's been an offline issue as well for a number of years. The Fair Credit Reporting Act has provisions dealing with privacy, and there are some enforcement actions in the mail order area where companies have had privacy practices and not followed them. Today, online information is being mixed with information that had been obtained offline. The issue becomes even more complex for an organization when they look at how they handle information with this model.

ITU: Is security necessary to protect private information, and what do CPAs have to know about information security to protect the organization's information assets?

EJ: Security is really a tool to ensure that private information is protected and that access to it is only provided to those people that should have access. That can include physical controls like locking information up in a file cabinet, as well as electronic controls governing information security. There is no doubt that security is an important tool to maintain effective privacy practices. It needs to be there. Again, an organization or the CPA might need help from someone with security expertise if the organization is using a fairly sophisticated information system.

ITU: How big is this privacy assurance market for CPAs? Will it involve both large and small CPA firms?

EJ: It's big … and still growing. While it's hard to estimate the size, if we end up with increased privacy legislation in the United States that is as comprehensive as in Europe, Canada or Australia, it could be as big as tax. I think smaller CPA firms really know their individual clients and understand the privacy needs of their business clients. Small CPA firms know how to implement effective policies and procedures in a very practical way for their business clients. I think this experience is going to be very valuable to small business as it relates to protection and assurance around privacy.

ITU: What are some of the basic steps or actions that any organization can take in the area of privacy?

EJ: The first step is to create an effective, understandable privacy policy. Whether it is formal or informal, it also needs to be written down. The policy should include a declaration of how the organization is going to use and handle private information, and should identify the choices the organization will provide to its customers. A member of management, a business owner or even the Chief Privacy Officer needs to be responsible and accountable for maintaining and enforcing the privacy policy.

ITU: Are organizations starting to pay attention to the importance of privacy policies, especially in light of the current regulatory environment?

EJ: I think there are a lot of organizations that are working with privacy as a business issue and a corporate governance issue — and really trying to do the right thing. I think many organizations right now are focused on complying with the regulation but haven't yet realized the potential business value of having good privacy policies and practices.

ITU: Why should the AICPA be involved in the development of privacy standards, and what does this bring to the table?

continued on page 4

Privacy is a Risk Management Issue *continued from page 3*

EJ: This is an exciting new opportunity for CPAs. The AICPA can bring together practitioners from both large and small firms involved in privacy to develop ways that CPAs can provide valuable and meaningful privacy services to their clients. This ranges from helping a client perform a diagnosis and seeing where the organization stands with privacy, to implementing a complete privacy program or conducting a privacy audit.

ITU: What are privacy audits?

EJ: This service is now being developed by the AICPA. Once complete, it will contain a set of privacy criteria that deal with various issues relating to privacy policies, external communications that companies have with the individuals affected by their privacy policy, procedures companies should have in place, and the monitoring of the whole process. There also will be a number of criteria in each of those areas that will be used for the privacy audit or assurance service the CPA firm will perform. If the company meets all the privacy criteria, they can, in essence, get a "clean opinion" or privacy report about their system from the CPA firm.

ITU: How will this privacy report be used?

EJ: I think companies will use privacy audit reports to tell customers, employees and even business partners that they are following good privacy practices with effective controls in place. The reports can be included in a company's annual report, on their Web site or used as a marketing tool.

ITU: What should CPAs do to prepare for these new privacy services?

EJ: There are three things. First, CPAs need to start learning about privacy, and the AICPA is going to provide some tools, resources and links for them to do that at *www.aicpa.org,* which will include a link to a new privacy section on the site. Second, they need to start talking to clients or employers about privacy and business needs. Finally, they need to start applying their skills and knowledge of privacy to begin to help the organizations they serve.

ITU: Will there be a CPA certification process to offer privacy services?

EJ: I think this still is being determined. CPAs have the basic skills to do an effective job. What they need is the understanding of the privacy subject matter. At this stage, the most important thing to develop is an education and outreach program to keep the membership informed about the growing importance of privacy and the fact that an exposure draft will be coming out later this year to deal with this subject matter area.

ITU: When will these new AICPA/CICA privacy services be available for CPAs to use?

EJ: Later this year. The AICPA/CICA Privacy Task Force plans to issue a Privacy Principles and Criteria Exposure Draft during fourth quarter 2002. These services also can be used to help CPAs design a very good privacy program, not just for the audit assurance service.

Contact Everett Johnson at *ejohnson@deloitte.com.*

PRIVACY

ONLINE PRIVACY ... OFFLINE PRIVACY ... IT'S JUST PRIVACY

By Erin P. Mackler, CPA

Erin P. Mackler, CPA, is technical manager of the Enterprise-Wide Privacy Initiative for the AICPA. She serves as a member of the AICPA's Research and Innovation team, and has also worked previously with the AICPA/CICA System Reliability Task Force to develop the SysTrust assurance service. Prior to joining the AICPA, Ms. Mackler was an auditor with Coopers & Lybrand.

Much has been said about *online* privacy over the last few years. Consumer advocacy groups are on the front lines and in the trenches battling companies that have violated consumer privacy or followed poor Internet privacy practices. Businesses with an online presence are under close scrutiny by many organizations, including watchdogs, regulators and legislators, following just how they collect and use their customers' personal information.

No one can forget the privacy uproar over DoubleClick, Yahoo! and Toys R Us. Research studies also show that consumers are feeling frustrated. In a recent study conducted for Privacy & American Business by Harris Interactive (sponsored by the AICPA and Ernst & Young), 79 percent of consumers said they have lost all control over how companies collect and use their personal information.

Perhaps there is more focus by the media on online privacy breaches and violations because consumers can relate more easily to the Internet — they have

continued on page 5

Online Privacy ... Offline Privacy ... It's Just Privacy continued from page 4

more direct, daily interaction with the Internet through home and office computers. While the Internet is something they understand and are familiar with, consumers may not realize how their private information is gathered and used in the offline world because they don't generally have the same kind of close interaction with it.

When consumers see their information in front of them on a computer monitor, they feel somewhat in direct control of their information. In contrast, when they make a telephone call or purchase something in a store, they seem less aware of what information is being collected and how it is used. For example, movie rental cards track the types of movies rented, supermarket cards track product preferences, credit card companies track purchasing history, and warranty cards gather personal information under the guise of a warranty registration process.

Obviously, there's more to privacy than protecting information online. Much in the way that the marketplace has come to view eBusiness models as just business, it also does not see a distinction between online and offline privacy protection. Whether an organization collects information online, offline or both, the heart of the issue remains the protection of the *information itself*, not the *method* of data collection.

Online and other electronic methods of data collection may require controls and special procedures (such as certain security protocols) to protect that information from being misued, abused or corrupted. Nevertheless, the consumer expects his or her information is *protected*, no matter how or where it was collected. There is a minimum consumer expectation when it comes to the protection of private information, and many consumers will not draw the distinction between online and offline information. However, they *will* distinguish between good privacy practices and poor ones.

The Privacy & American Business study also explores this issue, finding that a majority of consumers would "stop doing business" altogether with a company if it violated their privacy. It did not matter if the business was an eCommerce site or traditional bricks-and-mortar; what mattered most to consumers was that once trust was broken, it would be very difficult for the business to rebuild. Because untrusting customers often tell others about their bad experiences, this represents risk to an organization's brand, reputation, customer loyalty, market share and even shareholder value if publicly traded.

Privacy is a risk management issue for all organizations today — whether online or offline. Good privacy practices make good business sense and happy customers. Instead of companies seeing privacy as a burden, they can turn it into a competitive advantage to increase market share and build brand identity as a company with whom it is safe to do business and provide personal information.

In the end, it's not about *where* or *how* companies collect information, but what they do with it and how they handle it that resonates most with consumers.

Contact Erin Mackler at *emackler@aicpa.org*. For a complete copy of the Privacy & American Business Study, visit *www.aicpa.org/assurance/webtrust/priv_surv.htm*. ITU

AN INFOTECH UPDATE PROFILE

THAREN SIMPSON: SYSTRUST PROVIDES VALUE-ADDED CONSULTING SERVICES

By Scott H. Cytron, ABC

It's no revelation that CPAs working in audit, tax and other accounting arenas often look outside their traditional service delivery to enhance and expand a practice. From Houston CPA Tharen K. Simpson's office in Texas, opportunities, indeed, recently became much more diverse, thanks to the recent SysTrust audit she performed for a local Applications Service Provider (ASP).

Simpson began her own firm in July 2000, having worked for Cox & Lord, PC prior to hanging her own shingle. This University of Houston graduate who passed all four parts of the CPA Exam the very first time didn't actually *intend* to pursue consulting opportunities in assurance services; instead, they found her. eVision Systems, already a client, engaged her to perform the SysTrust audit. As a value-added reseller (VAR) of Microsoft Great Plains hosted applications, eVision was required to have its systems independently examined and tested against a set of system reliability standards. SysTrust

Tharen K. Simpson
Certified Public Accountant

continued on page 6

Tharen Simpson: SysTrust Provides Value-Added Consulting Services

continued from page 5

is one of the industry standards recommended by Microsoft Great Plains for ASPs, and along with WebTrust, is one of AICPA's key assurance services.

"SysTrust services are different from what I primarily do every day," says Simpson. "I find it interesting, challenging and rewarding. In addition to applying a CPA's objectivity, independence and other professional requirements, I use my accounting knowledge and skills in the areas of financial systems, working papers and audit procedures."

Simpson explains she has been very active in forensic accounting issues in an ongoing estate case over the past two years, and for the last 18 months, has provided training and payroll tax compliance services to a large public client during implementation of a new accounting system. Although she hasn't had much time to devote to marketing SysTrust services (her practice is 75 to 80 percent based in tax), she now feels confident that pursuing additional engagements in the assurance arena is very intriguing.

This is the first in a series of profiles spotlighting how CPAs are using technology in their firms, businesses or organizations. Each profile will revolve around a specific *InfoTech Update* issue's theme. If you know someone who would be an excellent profile for an upcoming issue, please send a note to *infotech@aicpa.org*. The theme for the Nov/Dec 2002 issue is Training and Technology Competency, and Qualified IT Personnel.

Through SysTrust, CPAs independently examine a system to provide reasonable assurance that the system is capable of operating without material error, fault or failure during a specified period in a specified environment. A CPA firm's independent SysTrust opinion is designed to increase the comfort of management, customer and business partners with the systems that support a business or particular activity.

When Simpson started the eVision audit, she first researched what was involved in performing the audit, obtained a SysTrust License Agreement from the AICPA, and purchased the Web-based questionnaire and diagnostic application from SysTrust Services Corporation. She then obtained a signed agreement letter from eVision, and requested them to complete their portion of the working papers. After reviewing the client's responses, she met with the client to clarify items and answer additional questions from the material they submitted. The next step was to obtain copies of eVision's written policies and procedures, standard service agreements and other items.

This was followed by requesting specific service agreements and reports pertaining to specific clients within the reporting period. She reviewed the reports on controls and monitoring activities conducting during this period.

"In person, I observed testing of controls and procedures currently in place, and physically visited the off-site location of the servers to assure that procedures were in place," she says. "In the case of eVision, this visit was quite impressive — their off-site location contains high security to obtain entrance, and the facilities are state-of-the-art with raised flooring, limited access, redundant air conditioning and other security measures. I was even able to observe how a server switch-over takes place without interruption to eVision's clients."

Mindy Dunne, eVision's controller, admired the skills Simpson brought to the table, especially in terms of objectivity.

"Tharen was an invaluable resource to eVision Systems during the SysTrust engagement," says Dunne. "CPAs are held to a high standard, and she exemplified all of the professional characteristics of objectivity, independence and integrity."

"The SysTrust Services model helps CPAs and their clients use a set of standards and a framework for the examination process during a SysTrust engagement, according to Richard Oppenheim, CPA/CITP, chairman of SysTrust Services Corporation. Also a member of the *InfoTech Update* Editorial Board, he says, "We leverage a Web interface with our proprietary diagnostic tools to bring CPAs and system owners together who are seeking independent verification that their systems are reliable."

For more information on SysTrust , visit *www.aicpa.org/assurance/systrust/index.htm*. For SysTrust Services Corporation, visit *www.systrustservices.com*

Scott H. Cytron, ABC, is editor of *InfoTech Update*. Contact him at *scytron@sbcglobal.net*.

DISASTER PLANNING

WILL YOUR CLIENT'S BUSINESS SURVIVE A DISASTER?

By Joel Lanz, CPA, CITP

Joel Lanz, CPA, CITP, is a former Big 5 partner who leads a CPA practice that focuses on providing information technology risk management services. A member of the New York State Society of CPAs' Emerging Technologies Committee, he also is an adjunct faculty member of the School of Computer Science and Information Systems at Pace University.

Recent global events have changed the assumptions we make about potential events and their impact on the business that drives the continuity plan. As a result, many clients are in the process of reassessing business continuity risk strategies, and some are considering these strategies for the first time. What are the practical considerations businesses and their CPA advisors should consider as they revise or develop plans in a post-September 11 environment?

Global Events Alter Assumptions

Recent events have triggered a number of lessons learned, resulting in revised assumptions.

- **Greater consideration is given to whether the client might fit a terrorist target profile** by examining the location of client facilities, types of services provided, image of the client, and whether operations are conducted at or near landmark buildings and surrounding areas.
- **There is a greater potential for critical public infrastructures**, such as utilities, transportation and public safety, to be unavailable. Before September 11, especially in areas not historically subjected to severe weather conditions, this threat was generally recognized as a very low probability.
- **Expanded continuity planning actions relating to people now exist.** Although continuity plans always prioritized the safety of personnel, many plans — especially those focused on operational recovery instead of business continuity — gave minimal consideration to employees' mental well-being or the impact of commuting to a "long-distance" recovery site over an extended period of time.
- **The issue of adequate testing should be forced.** The extent of testing varies considerably by client, from none at all to actually shutting down operations and attempting a recovery. Many experts agree that, at a minimum, a *parallel level* of testing needs to be performed in which the plan is tested without disrupting business operations. As a result, participation in the test is limited.
- **Current interest in continuity planning should be leveraged to increase user involvement.** Although highly recommended, key client personnel previously were not extensively involved, partly because continuity planning was perceived to be a technology rather than business responsibility, as well as the low prioritization of these planning projects relative to other business initiatives.

The first step in assessing and reevaluating business continuity strategies is to determine whether the contingency plan is current. This typically would require reviewing the plan's assumptions (risk assessment and business impact) with key manufacturing, service delivery and relationship management personnel. Unless the client has an established process to maintain the continuity plan, the probability is that the plan will be somewhat outdated and irrelevant.

Currency and Relevancy

The following questions can guide the CPA to gauge the currency and relevancy of the plan (each "no" response should trigger suspicion).

- Was at least a parallel level test performed within the past 12 months?
- If yes, has the plan been updated to reflect the "lessons learned" from the test?
- Does the plan contain only currently employed personnel, along with current contact numbers and titles?
- Has the plan received significant review since first quarter 2000? By itself, this would not indicate a problem. However, for many organizations, preparing for Y2K was the last time they devoted significant effort to continuity planning.
- Has a function other than IT raised concerns about continuity efforts?
- Can key personnel access their copy of the plan within a reasonable period of time?
- On an ad-hoc basis, can responsible individuals describe their roles and responsibilities in a disaster accurately and completely?
- Are products/service introduced in the past six months addressed in the plan?

Plan Quality

To quickly gain an appreciation of the quality of the plan, the CPA should consider the extent to which the plan addresses some of the common mistakes found in business continuity plans.

continued on page 8

Will Your Client's Business Survive a Disaster? continued from page 7

- ❖ Does the plan include public relations strategies and other crisis management initiatives (for example, a media relations strategy)?
- ❖ Are the key business managers involved and supportive of the plan?
- ❖ Is periodic training (briefings on changes, updates and new strategies, for example) provided on key plan provisions?
- ❖ Does the plan include the aggregation and maintenance of records for insurance claims (special documents or approval processing needed to support a claim)?
- ❖ Are critical vendors included in the plan, and do they participate in testing (including exercising vendor continuity plans)?
- ❖ Does the plan include returning production/service delivery from a disaster recovery status back to a normal status?
- ❖ Are strategies prioritized on the basis of criticality rather than organizational political influence?

Critical Success Factors

Timeliness and quality provide only a general impression of how well the client would function in an emergency situation. It is the practical aspects of the plan that will, when the time comes, differentiate businesses that can successfully navigate through a disaster from those that cannot.

- ❖ **Get the right people involved.** Exposure doesn't arise from not assigning "qualified" contingency planners to the project; it comes from not involving those who know the unique aspects of the business and the type of service or product that must be delivered "no matter what."
- ❖ **Expand participation to include specialty skills,** including public relations (to help manage media and client expectations); human resources (to help manage the impact both from the disaster event itself as well as from ongoing "compromises" that employees may have to endure); and insurance/risk management (to maximize recovery form claim opportunities).
- ❖ **Include continuity planning as a key component of the service/product delivery process.** This includes incorporating continuity risk into the business's change management process both on an immediate (daily operational backup) and longer-term basis (designing/modifying continuity strategies as part of new product development).
- ❖ **Recognize that disaster can affect more than the business's internal operations.** A community-based disaster can significantly impact the availability of employees to participate in contingency plans and significantly reduce customer demand (and thus available cash flow) for the business's service or product.
- ❖ **Understand the true cost benefits of continuity planning alternatives** and have the courage to select the strategy that provides the greatest enterprise value. Unfortunately, there are no set rules, and cost-benefit and related strategies will vary significantly based on the individual business' service/product and organizational politics.

A Five-Step Plan for CPAs to Follow

The biggest challenge faced by organizations in planning for business continuity is the ability to communicate and maintain the plan on a current and relevant basis. Although companies emphasize policies and procedures to enforce this, at the end of the day, company culture plays a critical role in ensuring that everyone will be prepared. Many clients find this very challenging. Elements of the following can enable CPAs to help their clients effectively derive the benefits of planning.

1 Stress that continuity planning is people first — safety, family, and, in some cases, the ability of the business to provide for employees and the community.

2 Internally market the need to maintain and periodically review the plan. Depending on the business, the client's campaign can include such awareness items as mugs, calendars or desk items.

3 Send internal email reminders on a periodic basis about the need to review the plan and share war stories about how plans helped other similar businesses.

4 Print wallet-size cards with key instructions for the users. Use positive reinforcement like nominal cash spotter prizes or mention in internal memos that the selected employees had access to their contingency information.

5 Provide peer pressure among the departments to update and maintain their plans by publicizing departments that have successfully reviewed their plan or creating some type of reward promotion for them, like an evening of bowling.

At the end of the day, the best way for the CPA to ensure the effectiveness of the client's continuity plan is to have the client recognize its importance and be personally motivated to maintain it.

You may contact Joel Lanz at *jlanz@itriskmgt.com.*

Disaster Planning eResources

There are many resources on the Internet for review; this is a partial list.

www.contingencyplanning.com
www.disasterrecovery.com
www.fema.gov
www.cpa2biz.com
www.drplanning.org
www.disasterplan.com
www.drj.com

SECURITY AND PRIVACY

IS YOUR COMPANY'S NETWORK A HACKER'S BEST FRIEND?

By Glen Christopher

Glen Christopher is a professional speaker, author and Internet trainer. Since graduating from the Cornell University School of Engineering 23 years ago, Glen has designed, installed and managed networked computer systems for a variety of clients. He is host of The Internet Game Show®, a member of the National Speakers Association and speaks frequently for the North Carolina Association of CPAs.

Wireless networks are everywhere, thanks to the availability of standards and low pricing. Together, these factors offer organizations benefits that cannot be overlooked. However, mitigating the business risk relative to computer operations and information security means understanding wireless technology, auditing the wireless environment at your organization and using hacking tools to test compliance with your wireless policies.

The Business Case

During the late 1980s and early 1990s, I built computer networks for commercial and government facilities, and one of my most memorable projects was at the VA Hospital in Augusta, Ga. I engineered a wireless connection between a 300+ bed facility in the city center and a new healthcare campus on a hillside near the edge of town. The project included engineering, FCC licensing (the frequency that supported Ethernet was regulated then), hardware, cabling, installation and ongoing maintenance. Implementation took about four months, and the link was rated at a whopping 1.5 Mbps, enabling the computer center at the older facility to service all the terminals, PCs and printers on the new campus.

If I were asked to connect these two facilities today, I would use standards-based wireless LAN (local area network) technology, the total solution would cost *one-tenth* the $50K price tag of 12 years ago, the project would last 7 to 10 days and the link speed would be rated at 11 Mbps. What a difference!

How Wireless LAN Technology Works

Simply stated, wireless LAN technology lets computers communicate with the rest of the LAN through radio signals rather than over wires. The majority of products installed and used today are based on the standard known as 802.11b and commonly referred to as Wi-Fi (wireless fidelity).

The two key components in Wi-Fi networks are the access point or AP, which is the last wired stop on your network and the wireless-network interface cards located in each PC, laptop or mobile computing device. The range of a wireless network extends 300 to 500 feet in large open areas, but the transmission range is limited to 60 to 80 feet in offices with dividing walls and hallways.

Community Hot Spots and Free Wireless Access

Several companies have emerged that offer fee-based access to the Internet via Wi-Fi networks, and many of these are located in airports, hotel lobbies, cafes and coffee houses. Locations where Wi-Fi access is available are called "hot spots," and many commercial hot spot providers or WISPs (Wireless Internet Service Providers) are listed in a directory at *www.bbwexchange.com.*

The relative ease of setting up a hot spot has fueled a grassroots effort in many cities across the United States where people are setting up parasitic networks. These parasitic networks also are called wireless communities, free networks and personal telecoms. NYCwireless (*www.nycwireless.com*), for example, provides free wireless Internet service using wireless technology to mobile users in public spaces throughout the New York City metropolitan area, including parks, coffee shops and building lobbies. Visit FreeNetworks.org (*www.freenetworks.org*) to learn more about wireless communities.

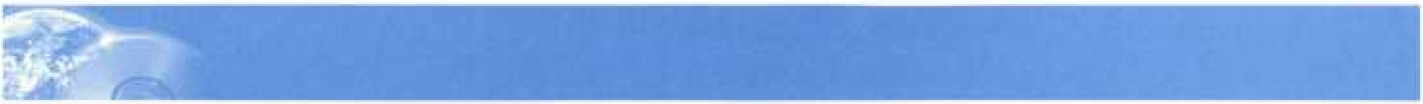
Inside the Hacker's Toolbox

For too many organizations, placing a firewall between the Internet and company LAN is the equivalent of putting an iron door on a tent. A hacker's toolbox includes daemon dialers, port scanners, password crackers and sniffers that make the side and rear of "the tent" an easy target.

Wireless networks create the same type of vulnerability. And, while most hacking activity requires breaking in, here's a technology that is literally breaking *out* of your facility to meet hackers on the street by your building or several miles away. OK — I said that the maximum range of a wireless-network interface cards is 60 to 300 feet, depending on building construction and other environmental issues. What I *didn't* say was adding appropriate antennas, with a good line of sight, can extend the range of typical wireless-network interface cards for several miles. Even a small, external antenna on your client PC can make a huge difference in communications range. The Internet has numerous sites detailing step-by-step instructions on building antennas to boost the signal.

Even more disturbing than the ready availability of inexpensive standards-based hardware is the availability of freeware and operating system features that make discovering wireless LANs

continued on page 10



Is Your Company's Network a Hacker's Best Friend?

continued from page 9

as easy as child's play. Consider Network Stumbler and its Pocket PC 3.0 cousin, Mini Stumbler (*www.netstumbler.com*).

Discovering wireless LANs has given rise to new hacking pastimes: war driving, war walking and chalking. War driving is the practice of driving around with an 802.11b-equipped laptop and scanning for open wireless networks that can be accessed for free. War walking uses similar equipment, perhaps a handheld PC, by hackers on foot in crowded metropolitan areas. Chalking is the practice of writing information about a discovered network on the sidewalk outside a commercial office building or industrial facility.

Each time Network Stumbler identified a wireless network, a bell or chime would ring. Apologies to Frank Capra aside, it is said, "each time the bell rings, a hacker gets his wings." Network Stumbler records a variety of information about each wireless network it discovered, including:

- the MAC address of the access point or wireless-network interface card;
- Service Set Identifier (SSID) … typically referred to as a Network Name;
- the AP node name, the channel for which the AP is set and the manufacturer of the AP;
- whether WEP (Wired Equivalent Privacy) is enabled or disabled; and
- signal strength, and the latitude and longitude of your Network Stumbler client when the signal is strongest.

For the 70 percent of commercial, governmental and residential wireless networks that are set up like community networks, I say, "*yes, your network is a hacker's best friend*!"

Securing Your Wireless LAN and Auditing Your Facilities

Whether your wireless network is deployed by a marketing manager or an IT administrator, there are a number of steps that must, at a minimum, be applied.

1. Place access points near the center of your building, away from windows and exterior walls. Interference from construction materials will limit how far the signal will travel beyond the facility.
2. Change the default network name, the SSID — which is needed to sign on to a WLAN, as well as the default password on your access point. Each manufacturer's default settings are common knowledge among hackers. Using an SSID that correlates with your company name or address makes it easy for hackers to identify you.
3. Disable SSID broadcast in the Access Point Beacon. Disabling this broadcast makes it harder for intruders to recognize your network.
4 Enable WEP and use the stronger 128-bit variety if available.
5. Change your encryption key periodically. The less data transmitted with the same encryption key, the less vulnerable you will be.
6. Enable MAC filtering on your APs. Many access points let you build a list of MAC addresses that are allowed on the wireless network. Those not listed will be denied.
7. Disable DHCP and require all workstations to use assigned IP address in order to gain access to the network.

I cannot overemphasize that these are the minimum steps; even if you do all of them, your data still is at risk and your organization is potentially liable for hacking activities that originated on your LAN. Wi-Fi networks that use WEP have locked the back door, but the key is under the mat!

Last summer, researchers revealed a WEP vulnerability, and within a couple of weeks of their presentation, a number of hacking tools based on these findings were available on the Internet. AirSnort (*http://airsnort.shmoo.com*) is a wireless LAN tool hackers use to recover encryption keys. It operates by passively monitoring transmissions and computing the encryption key when enough packets have been gathered.

Because it is so inexpensive and easy to implement a wireless network, your wireless network policy should clearly outline the requisition and approval process. Each of the numbered guidelines listed above should become part of the security checklist. Network Stumbler and AirSnort are easy-to-use tools that give you the power to inspect your wireless LAN for compliance without alerting the computer department or IT management of your audit activities.

Periodically, someone in your organization needs to search the netstumbler.com database to find out if your wireless network is listed. If it is, netstumbler.com will remove the record of your MAC address(es) if you send them an email request.

Out of the Woods? Hardly!

There was a time, not long ago, that a hacker would break into a computer in one country, then another computer in another country (and so forth) in order to disguise himself and remain anonymous while hacking and committing digital crimes. With the advent of wireless networking, that same hacker can *visit* you within a couple of miles of your facility, use your wireless LAN to launch an attach and then sign off. Should the victim decide to pursue legal remedies, don't be surprised if the FBI or other agencies show up at your doorstep one day. The digital trail stops there … and legal liability may stop there, too!

Contact Glen Christopher at *glen@christopher.net*.

E-BITZ focuses on practical applications of various technologies to enhance a practice or business.

E-BITZ WITH SUSAN BRADLEY

The Security of Linux

The penguin may be cute, but the black screen that awaits you as you boot up is intimidating. As commands fly across the screen informing you that devices have been properly mounted and loaded, the reassuring words of "OK" fly by. No, this isn't a travel back in time to the DOS days, it's a Windows' user's experience of Linux RedHat 7.3.

Linux (pronounced "linn-icks") is based on an unique concept of "Open Source code," but the software is not given away completely "free." You can "license" Linux as long as you agree to copy Linux as much as you want, sell copies of Linux, modify Linux and redistribute it, and not restrict the abilities of others to copy, modify or distribute your modified Linux!

When you distribute a copy (modified or not), you also must make the source code available. When I bought my copy of Red Hat Linux that came on three CDs, I also received two CDs of source code.

Linux often is touted as being a more secure code and more stable than its Microsoft counterparts, but depending on the sources you read, the answer to that question is unclear. Many refer to studies that indicate Linux can be as insecure as Windows, especially if the installation is set up with defaults and with unnecessary services running. The attitude that Linux is not a target is a complete untruth. Network administrators who set up servers without the most basic security measures, including anti-virus, firewall, changing passwords and physical security measures, will be in for a rude awakening. Linux and Windows machines that are Web servers are attacked on a daily battlefield that leaves many a network administrator ready to tear his or her hair out.

Web servers set up for access without the proper tools for tracking network intrusions, and servers that are Internet-facing and are not regularly monitored for patch fixes and security flaws, are ticking time bombs. Studies have shown that an unpatched Microsoft Web server [IIS] gets attacked and infected with Code Red or Nimda within 24 hours after being put online. Ninety percent of worms, viruses and other Web-based attacks are based on known vulnerabilities that have patches freely available for downloading and installation. Unix and Linux servers suffer their own security vulnerabilities; unpatched and installed on the Internet, they suffer the same risks of compromise as Windows machines.

Linux has numerous tools, sites and other information to keep you updated on its security issues; check out the FAQ for security at *www.linuxsecurity.com/docs/colsfaq.html.* In that document, Linux administrators are reminded to do the same steps that Windows administrators are reminded to do:

- install the most recent security patches for your distribution;
- turn off unused services, and tcpwrap the rest;
- if accessing your computer remotely, replace Telnet and Ftp with more secure equivalents; and
- maintain current backups (via a spare HD, tape drive or backup server).

If you don't have security, you don't have your computer systems when you need them. Security also is a matter of understanding risk and preparing a risk analysis: risk = (threat*vulnerability*impact). Understanding where your risks are the greatest, and assigning appropriate resources, is key to a proper security solution for your office.

Security also means that you or someone in your organization, or perhaps a consultant, knows exactly what each station should be doing, and knows what the standard "benchmark" logs look like in your firm. The ability to understand the ISA log files means that your server is being "probed" for the Code Red vulnerability.

Everyone should have a computer security policy. More that the "Internet use policy" it should be readily understandable and protect the data you're safeguarding, as well as the users' privacy. Consider who has access to the system, who is allowed to install software on the system, who owns what data, disaster recovery and appropriate use of the system. For most businesses, the large number of threats come not from the hackers, but from your very own computer users who download viruses, accidentally delete files and don't fully understand their actions on the

continued on back page

The Security of Linux continued from page 10

network. Ensuring you assign appropriate resources for each risk that your office has is key to ensuring that your network has the maximum amount of up time.

Consider adding Technology Security awareness training to your next staff meeting. Assign a person in your office to be the computer awareness guru. Being aware that vulnerabilities and viruses are on the rampage will reinforce people to be a bit more cautious.

Linux does have its place as an alternative to Windows, and is providing competition in the marketplace. Is it more secure than Windows? No, I would argue it's not, because both Linux and Windows suffer from similar operator and user mistakes. Is Linux right for you? Get informed so that you can assign appropriate risk. On July 30, David Cieslak, CPA/CITP, GSEC, and Michael Dickson, CPA/CITP, presented a Web cast on security issues for firms (*www.cpa2biz.com/webcasts*).

For the record, this document was composed on Star Office 5.2 running on RedHat Linux 7.3.

Susan E. Bradley, CPA/CITP, MCP, is a principal with Tamiyasu, Smith, Horn and Braun in Fresno, Calif. Contact her at *sbradcpa@pacbell.com*.

InfoTech Update

AICPA
Information Technology Membership Section
1211 Avenue of the Americas
New York, NY 10036-8775

ADDRESS SERVICE REQUESTED

September 2002

Dear Information Technology Section Member:

The accounting profession faces many significant challenges and opportunities with the recent enactment of the Sarbanes-Oxley Act of 2002 ("Act"). Many of the provisions of this Act will redefine the way in which CPAs serve their publicly-traded audit clients. The AICPA recognizes that many of our Information Technology Section members will not be directly impacted by the Act because they do not provide services to publicly-traded audit clients. We felt it was important to share the provisions of the Act with you because: 1) many IT section members provide services to or are employed by public companies and 2) the Act may very well influence other federal or state legislation and rule changes that could extend beyond public companies.

The Sarbanes-Oxley Act of 2002

The most significant provision of the Act impacting the CPA IT service provider is the prohibition on certain non-audit services provided to publicly-traded audit clients. Also, all non-audit services that are not expressly prohibited must receive advance approval from the client's audit committee. The remaining provisions affecting the CPA IT service provider relate to disclosure of non-audit related fees.

Provisions of the Act Affecting Firms that Audit Public Companies

The Act has a number of provisions relating to the offering of non-audit services to audit clients. How those services are defined and interpreted could be important for CPA's who provide technology services.

Of particular relevance to IT Section members, the Act specifically makes "unlawful" the delivery of the following "non-audit" services to publicly-traded audit clients:

- bookkeeping or other services related to the accounting records or financial statements of the audit client;
- ***financial information systems design and implementation***;
- legal services and expert services unrelated to the audit; and
- any other service that the Board (Public Company Accounting Oversight Board) determines, by regulation, is impermissible

Non-audit services are defined as those professional services provided to a publicly-traded audit client by a registered public accounting firm, other than those provided to the client in connection with an audit or a review of the financial statements of the client.

Financial Information Systems Design and Implementation

In the list of prohibited services, the most significant concern to CPA IT service providers is the bans on financial information systems design and implementation services. ***This is of particular importance to those CPAs with the Certified Information Technology Professional designation as it is one of the core disciplines of the credential.*** While this service is clearly non-audit and is disallowed by the Act, information system services such as internal control reporting that have been a part of the audit engagement would clearly continue. It is also important to note the Act does not prohibit CPAs from providing information technology services to non-audit clients.

XBRL (eXtensible Business Reporting Language) related services

Those XBRL services that can be characterized as *financial information systems design and implementation* service are likely to be banned for public-company clients, e.g., a new system implementation that includes XBRL functionality. However, a significant amount of XBRL related services either are or contemplated to be an integral part of the core audit service including creating and reviewing XBRL reports with related assurance.

Internal Control Reporting

The Act requires each annual report of an issuer to contain an "internal control report" that describes the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting and assessing the effectiveness of the structure and procedures. The auditor will be required to attest to and report on such assessment. This engagement shall not be the subject of a separate engagement.

Trust Service Engagements (WebTrust & SysTrust)

We believe that Trust Service engagements will be viewed as non-audit services but not as a "banned" service. In fact, because of the raised awareness for internal controls, there could be a greater call for Trust Service engagements by audit committees. However, a Trust Service engagement provided to a public company audit client will be subject to approval by the audit committee and must be disclosed in the issuer's 10K and 10-Qs.

Expert Services

The Act prohibits providing "expert" services to audit clients. Since the Act does not specifically define "expert" services, there are many questions raised by the term "expert". This could generally impact consulting and advisory services. During the implementation phase of the Act the AICPA Information Technology Executive Committee will be working with AICPA leadership to describe the potential issues and offer suggested solutions.

Advance Approval Requirement

All non-audit services that are not expressly prohibited under the Act must be pre-approved by the audit committee. The pre-approval requirement is generally waived when the services were not recognized by the issuer at the time of the engagement to be non-audit services, total fees received during the year from all non-audit services are less than 5% of the total fees received from the audit client, and the services are brought to the attention and approved by the audit committee prior to the completion of the audit. The audit committee's approval of all non-audit services must be disclosed to investors in regular SEC filings.

Disclosure of Fees

As part of the registration process required by the Act, CPA firms must disclose the annual non-audit service fees received from each publicly-traded audit client.

Cascade Effect Beyond Public Companies

Of particular concern is the cascade effect the scope of service restrictions of the Act could have on the CPA providing information technology services. The new law may become the template for similar federal and state legislative and rule changes that would also directly affect both non-publicly traded companies and the CPAs who provide information technology services to them.

Shortly following the President's signing of the Act into law, several states began moving forward with legislation that would result in additional burdens for CPAs. The AICPA and state CPA societies are monitoring this situation closely and will continue to keep you informed.

Conclusion

The AICPA will continue to monitor and update you on legislative activities that impact the accounting profession. We are actively working with the various legislative and regulatory agencies to insure our concerns and suggestions are addressed in current and future legislation and rule making. We encourage you to contact your legislative representatives and the AICPA concerning any current or proposed legislation that may impact CPAs and CPA information technology service providers. If you have any close contacts in your state houses of legislature, you may wish to talk with and help them understand the impact of this cascade effect on privately-owned businesses.

You can view the recent AICPA News Alert on the Sarbanes-Oxley Act at www.aicpa.org/info/aicpa_update_7.htm. Members who have questions about the new law and how it will impact their firm or company, should call 866-265-1977. The hotline will be staffed Monday through Friday for the remainder of 2002. You may also send questions or concerns to the Information Technology Membership Section at infotech@aicpa.org

The summary of the Act serves as a general outline of the issues that may impact the CPA information technology service provider and should not be relied upon for technical interpretation.

Yours truly,

James C. Metzler, CPA
Chair – Information Technology Executive Committee

J. Louis Matherne, CPA
Director – Business Assurance & Advisory Services