3-2004

InfoTech Update, Volume 13, Number 2, March/April 2004

American Institute of Certified Public Accountants. Information Technology Section

InfoTech
UPDATE

March/April 2004
Vol. 13, No. 2

Newsletter of the AICPA
Information Technology Section

What's Inside

FOCUS FOR THIS ISSUE:
Information Security and Spam Technologies

INFORMATION SECURITY

Application/Network Vulnerabilities and the Risk Management Process

By Steven Ursillo Jr., CPA/CITP, CFE, CISA, MCSE, CIA

Steven J. Ursillo Jr., CPA/CITP, CFE, CISA, MCSE, CIA, is a principal and director of Information Technology and Assurance Services at Sparrow, Johnson & Ursillo, Inc., in Providence, R.I. He specializes in information system security, privacy, control and risk assessments, fraud detection, data extraction and analysis, and technology assurance services. Ursillo chairs the Rhode Island Society of CPAs' Technology Committee, and is a board member and past president of the Rhode Island Chapter of Certified Fraud Examiners.

Advancements in technology solutions continue to provide added efficiency for the most complex and challenging obstacles. However, this forces technology professionals to adapt to rapidly changing environments. Ensuring the confidentiality, integrity and availability of data continues to be a significant concern, from the smallest businesses to the largest public corporations. Every day, emerging security issues and vulnerabilities put some of the most proactive security professionals and network administrators on guard. The nature and technical depth of some of the methods used to exploit systems and security vulnerabilities makes understanding and communicating the risk a continuous challenge.

We know the Internet is still a popular area for attack. At the same time, Internet access and externally hosted services, including a company's Web, mail and FTP servers, force most organizations to have some external presence on the Internet. This external presence increases the risk of, and potential for, different types of external attacks.

The annual CSI/FBI Computer Crime and Security Survey's results of security incidents and attacks over a five-year period (1999 to 2003) indicate that more than half of the respondents incurred an unauthorized use of computer systems within the last 12 months of the years reported. In 2003 alone, 82 percent of respondents had attacks that originated from independent hackers, 77 percent came from disgruntled employees, 79 percent originated from the Internet and 30 percent were from internal systems.

These are some pretty powerful statistics that deeply affect the risk management process. While many mid- to large-size organizations feel these statistics demonstrate a significant threat, there are other businesses and groups that may respond differently. For example, a common response for smaller organizations is to justify a significant reduction of risk because they believe no one is targeting them. Part of that may be true; however, what some organizations may underestimate is that there are many attackers who don't care whom they attack. It is very common for attackers to scan large ranges of IP addresses for

Continued on page 2

AICPA

InfoTech UPDATE
March/April 2004, Volume 13, No. 2. Publication and editorial office: AICPA, 1211 Avenue of the Americas, New York, N.Y. 10036.

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.

If you wish to update your member profile, please visit *www.aicpa.org/anon/login.asp.*

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 212-596-6211.

Continued from page 1

open services and potentially vulnerable system configurations. These attackers are looking to identify externally accessible hosts with particular ports and services that are available for attack.

Are we Really a Target?

Here's a hypothetical, yet disturbingly realistic example. A malicious attacker quietly takes control of an Internet Service Provider's domain name server. The attacker is skilled enough to know that once the system is compromised and full control is available, all evidence of the intrusion will be removed. The attacker implements a backdoor or stealth way of re-entering the system, unannounced to anyone. We will call this system OWNED1. Not only has this system been compromised, but this is just the beginning.

The attacker is now confident that any attack initiated from this system or the next system in line will be difficult to detect, so s(he) quietly accumulates all the functionality need to perform attacks against another host or range of hosts. Next, the process is repeated to gain the unauthorized functionality of another vulnerable system. We will call this system OWNED2. This may be an organization's vulnerable FTP server.

The attacker repeats the concealment process by removing the access trail in the logs, hiding the attacker's working files and setting another stealth backdoor for easy access when needed. This process can be repeated several times in order to make it increasingly difficult for the attacker to be identified. From OWNED2, s(he) sets up an automated port or vulnerability scanner. This scanner is designed to cover a range of IP addresses looking for particular services that have common vulnerability problems, or specifically for newly released exploits that most administrators have not yet managed to patch or update.

In the process of scanning several hundred public IP addresses, the attacker happens to identify ABC Retail Company's Web server. Using a technique to request the server's banner in conjunction with some other tactics, the attacker can identify the make, version and patch level of the Web server application, and it just so happens s(he) is familiar with a buffer overflow exploit for this version of ABC's Web server application. The exploit was publicized two months ago. The attacker accesses from any number of publicly available sources or develops the appropriate code to take advantage of the application and then uses it against ABC's Web server to gain some privileged access.

From the Eyes of ABC Corporation

ABC Corporation is a $60 million retail corporation with approximately 200 employees. The corporation's Web site is used for marketing and public relations purposes, and does not incorporate any e-commerce activity. The company management does take security seriously and has participated in several risk assessments with its five-person internal technology staff. ABC runs a state-of-the-art firewall with all the latest security updates. They also have restricted access directly against the firewall.

The system administrators have performed several external scans against their Web server and firewall, and were pleased to report to their manager that the only available access from the Internet was over port 80 — the one needed for people to browse the site. The manager also is aware that the Web server does not contain any confidential information on it. The manager does not seem to believe there is a tremendous amount of risk, short of a Web site defacement or denial of service attack. The feeling is that these types of attacks would be embarrassing, but would not seriously jeopardize the retail sale of their very popular product lines. Besides, the sensitive customer account and credit card information is really on a separate database server without a direct connection.

The latest point-of-sale upgrade consumed the attention of ABC's IT manager, and as a result, he overlooked a security article

Continued on page 3

placed in his in-box. The article detailed how buffer overflows are a very common type of system vulnerability that can be targeted to hundreds of types of applications, and that a buffer overflow is the result of a lack of programming bounds checking within the program code.

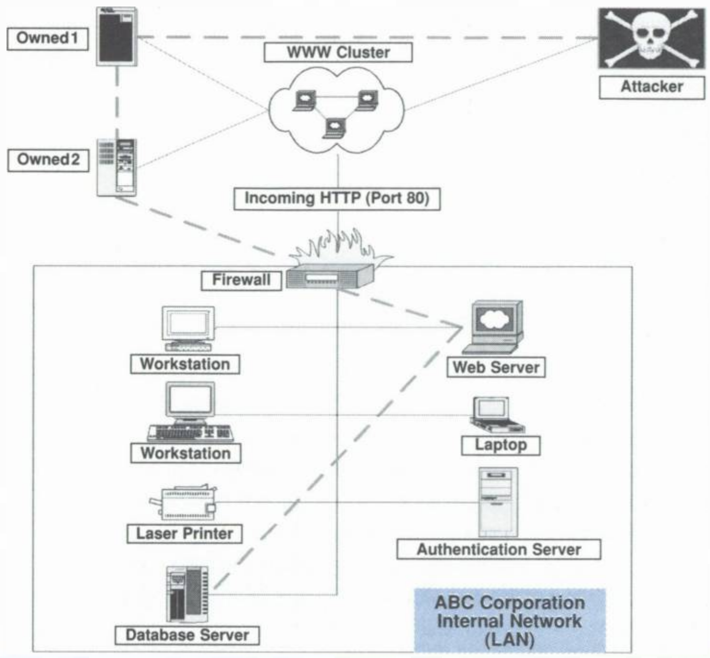
For example, a particular string (sequence of data) of information within an application is not supposed to contain more that 128 bites of data. However, if a user enters more than 128 bites, the excess information forces an override from one area of the computer's memory stack to an alternative location. The result? If the information is entered in a particular way, attackers can inject and execute their own code running at the privilege of the application exploited. If the application is running with system privileges (one step below administrative privileges on Microsoft applications), or, even worse, with administrator or root privileges (powerful access privileges), then the arbitrary code the attacker executes after injecting it from the computer's memory stack will run and function at that same privilege. The overall result would be an attacker gaining full control over the system.

Now Back to the Attacker

The attacker executed a buffer overflow exploit over port 80 — the same port needed for external browsing of the Web site and the only port allowed through the firewall. S(he) has now taken control of ABC's Web server, located on ABC's local area network (LAN) as diagrammed in Figure 1.

ABC's management already addressed the risk of the Web server being compromised. The attacker can deface the site or even shut down the Web server. That was considered somewhat tolerable, right? Unfortunately, it can get much worse! The attacker has fully compromised and controlled the Web server, and this server is on the corporation's LAN. Once this occurs, the attacker can perform "island hopping" or attack one host at a time, similar to what was performed with OWNED1 and OWNED2 in order to hide the trail.

Figure 1



The attacker can now capture network data and traffic with a network sniffer, capture user credentials, capture and map out host information, and view critical configuration settings. S(he) now has a clear line of attack against any host located on ABC's LAN, and the hosts on the LAN do not have any firewall protection between them. After attacking and compromising the database server, the attacker parts with ABC's customer database; including credit card information; hides the entry trails on all systems compromised by deleting access and activity logs, and also hides used files. A back door is set for periodic follow up and undetected remote access back to ABC Company's LAN. This attacker may not have ever heard of ABC Corporation, but only followed the exploit. Let's just hope the attacker does not decide to post the back door access credentials on some underground hacking Web site, chat server or newsgroup for all other hackers to use as well!

An Ounce of Prevention

There are a few actions and controls that could have prevented this attack from occurring. Most buffer overflow exploits that are released force vendors to respond with an update or patch for the program or application flaw. In many ways, this can become a race to keep up. System administrators should follow best practice skills for implementing any patch or program update, which usually requires that the application and system be tested before going live into production.

Sometimes a lack of time or resources allows this process to occur improperly, which initiates added availability issues and risk. However, if an exploit is publicized, attackers may be aggressively trying to identify those companies who have not yet had the time to respond. If the attacker beats the administrator to the punch and sets a stealth backdoor after compromise, the damage is already done. Even though the system was updated and the vulnerability is no longer present, the back door, most likely, is still available. In the ABC Company example, the administrators are balancing the risk of a known system vulnerability and the risk of applying any untested patches that may affect the performance of their production system. Ideally, timely testing and implementation of the updates is the best

Continued on page 4

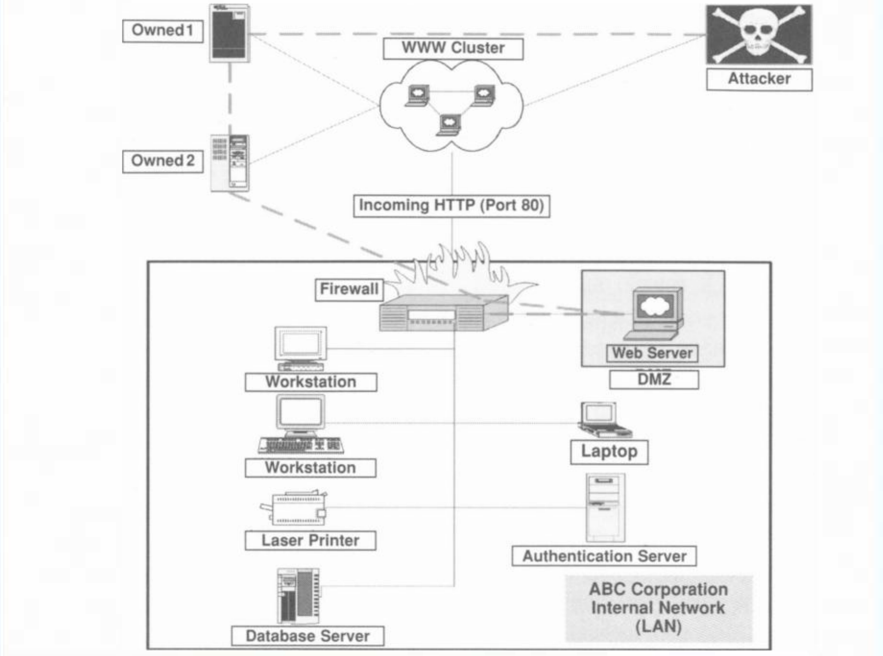
Continued from page 4

solution, but this decision comes from the managers and those who have an intimate knowledge of ABC's systems and infrastructure.

ABC's network architecture is another area the company could have modified in order to manage the risk of compromise. Had ABC's Web server been placed on an isolated network segment, otherwise known as a demilitarized zone (DMZ), the risk would have been reduced by containing the single vulnerability to the Web server. The same attack with a change in the network architecture is diagrammed on right in Figure 2.

In this figure, we see that once the attacker gains control of the Web server and the rest of the internal LAN is still protected by the firewall. The attacker would have to initiate an attack back through the firewall from the Web server to try to get to the LAN.

Figure 2



A buffer overflow — one of the most common types of Internet-based attacks — is just one of many types of system vulnerabilities that can come about over time or as new application flaws are discovered. Even though statistics show that an organization's most significant risks comes from insider abuse, it is clear that external threats are something that should not be underestimated. Proper risk assessment, proactive security monitoring, assessments and assurance services should be used in order for management to obtain a comfort level that follows the organization's security policies and culture.

For more information on risks associated with security vulnerability, plan to attend Steven Ursillo Jr.'s session on this topic at Tech 2004, May 3-5 at the Venetian Resort & Casino in Las Vegas. Visit *www.cpatechconf.com* for registration and an online brochure.

Contact Steven Ursillo Jr. at *sursillojr@sju.com*. ●

INFOTECH UPDATE PROFILE

News at 11: Michelle Samuels Channels Fulfilling Career at Broadcast Giant TBS

By Tim Elsner

As a self-described "business and industry gal," Michelle Samuels, CPA/CITP, CQM, prefers the type of accounting work she calls "in the action" — or in the details, creating a company's financial statements while serving as an integral part of its decision making process.

Michelle Samuels

Ten-plus years after joining Atlanta-based Turner Broadcasting System, Inc. (TBS), one might say that as director of Financial Compliance, Samuels is certainly *in* the action — and more. After all, this is the 8,000-employee, multifaceted company whose cornerstone property revolutionized broadcast news coverage with its groundbreaking 24-hour news channel, CNN. And that's just one network (albeit a key one) in the news division. Today, TBS includes, among other businesses, numerous entertainment networks (TBS, TNT, Cartoon Network), the Atlanta Braves, many Internet sites (cnn.com, nascar.com, pga.com), other professional sports interests and even real estate.

These holdings add up to Samuels' appreciation and exposure to a variety of businesses within a business, as well as many aspects of information technology (IT) and accounting.

Continued on page 5

IT Accident Triggers Career Course

"I started in the accounting world and fell into IT by accident — and loved it," says Samuels, referring to her earliest career days in the international accounting department at Sony Pictures Entertainment, Inc., in Burbank, Calif. She was with Sony before joining TBS, where she's since managed a number of progressively responsible software development and IT positions.

"After more than a decade, I can honestly say that there's hardly been two days alike," she says, reflecting on an array of responsibilities at the global TBS — from help desk analysis in the early days to business analysis, project management and data conversions in more recent years.

"I've been able to work on so many different business aspects of IT – while staying within the same company. There are so many nuances and complex requirements in this highly customized environment. For example, the business process for the Braves can be quite different from CNN. We haven't forced standardization among the businesses — so you can imagine the differences!"

Aside from the variety of business exposure, this mother of two is effusive about the company's "phenomenally family-friendly" culture. "I've literally raised my kids in my office," she says, recalling each child's first visits to mom's home away from home. "The upside is that I think my children see me as someone who likes what she does — and even better — they can look forward to some day having a professional position. That can be a positive thing."

The life in the land of sleepless networks and courageous baseball teams is not without its challenges — quite the contrary. "I probably hold the record for crashing Turner's financial systems more often that any other individual still employed by the company. The reason I'm still here is that I wasn't afraid to take responsibility for my mistakes. In fact, I often reported them. I also am eager to be a part of the solution; everyone messes up sometime, but it's your reaction that shows your true character."

One test of character came up when Samuels was the project manager for an upgrade to PeopleSoft, an 11-month project that was "almost flawless," she says. "Then we discovered one bug that somehow got through extensive, exhaustive quality assurance. The bottom line is that we couldn't cut checks for about three weeks. Unfortunately, this occurred during a time that Mr. Turner was scheduled to present a check for $100,000 to the Elton John AIDS Foundation … talk about bad timing!"

IT + Accounting = Logical Match

Today, Samuels is co-lead for Turner's Sarbanes-Oxley (SOX) compliance efforts. She believes SOX represents a terrific opportunity to understand both IT and accounting, a co-mingling of skills about which she's most passionate.

"For a number of years, my personal value-add was bringing my accounting background to the IT group. Now, I'm bringing my IT expertise to the accounting group. Some of the biggest challenges and opportunities in the profession today are to get accountants to understand the importance of technology, and SOX is a great example of 'why.' Some people keep IT at arm's length, perhaps because they don't understand it or are intimidated by it. With IT moving as quickly as it is, and because it has become so integrated with all business processes, it is critical to consider it a huge part of doing business."

Samuels, who serves on the planning committee for the American Institute of CPAs' Tech 2004 conference, May 3-6 in Las Vegas, underscores the point by looking at the source of today's financial data. "In accounting, every number that is looked at came out of a system at some point. It is imperative to understand those systems at some level to be a good accountant. It's as if IT is viewed as some 'black box' to be feared, when actually it should be viewed as a friend."

Tim Elsner is a freelance writer based in Dallas, Texas. Contact him at *timelsner1@sbcglobal.net*. ●

SOFTWARE AND SYSTEMS

The "Why" Behind CRM Software

By Anne Stanton

As president of The Norwich Group in Norwich, Vt., Anne Stanton has worked with accounting and consulting companies for more than 18 years, analyzing and helping businesses of all sizes use their available resources more effectively. She most recently was executive vice president for Commercial Logic, Inc, is a member of the AICPA's Top Technologies Committee and a new member of *InfoTech Update's* Editorial Board.

What is the big deal behind customer relationship management (CRM) software? I know my customers and track them using a filing system as well in other applications. Why do I need CRM?

If you only had to keep track of a handful of clients, then it would not necessarily be hard to remember that John Smith uses the XYZ Bank, he is affiliated with the local Chamber of Commerce and his brother is

Continued on page 6

Continued from page 5

president of the regional medical center. You might even remember the talk he gave two months ago when he offered some great ideas on expanding the service offerings of one of your particular departments.

In reality, however, we live in an information-overloaded society. We meet people on a daily basis and the promises we gave yesterday are sometimes hard to remember today. CRM software is designed to help us remember what we promised, whom we talked to and what is so uniquely special about each of our relationships. It is meant to track when we last talked with someone so we can remember to call them again in a timely manner, and provides us with a compass to related knowledge on that contact in the integrated map we like to call our brain.

CRM is a tool that can move us to a higher level with our customers. Have you ever been pleasantly surprised to receive a birthday card from Southwest Airlines? Our birthdays are something we consider fairly unique, so when they are remembered even by remote acquaintances, we are inwardly rather pleased. Have you ever had the pleasure of discovering something about a new contact that was not directly told to you? CRM supports cross referencing of information.

We have moved to a culture where the consultative approach to business is very trendy, and, for that matter, critical as competition heightens. Customers are delighted to be treated well and show a much higher level of loyalty when a firm goes above and beyond what is expected. It is much more expensive to get new clients then to service and sell to our best clients. Our customers are tired of being deceived, used and taken advantage of by retail sales that are not really sales — and services that are only slightly above mediocre. Customer service is about uniquely offering a higher quality of product as we couple offerings with the unique personality of the firm and business.

Well-integrated CRM systems are used daily as the central point of customer contact, and as such, these systems have data that is constantly being updated and should be considered the most current. Accounting firms however, have a more difficult task because they often have a number of disparate applications (depending on the size of the office, legacy systems and other administrative issues) that track customer information.

The important focus is knowing how customers are being managed. If you choose to implement a CRM package, or simply choose to use existing CRM features in software applications that are already in use, you must think carefully about what your goal is with regard to customer relations. CRM software rolled out poorly can be an extremely expensive endeavor. In addition to good software, CRM initiatives require the commitment of many different people and groups of people within a firm. *CFO.com* reported in 2003 that in 85 percent of all cases, CRM users could not show any quantifiable results, and 12 percent of all CRM installations were complete failures. CRM is extremely challenging, and to justify CRM's sometimes multi-billion dollar price tag, users of CRM will need to treat it as a firm-wide initiative and cultural discipline.

A tool as critical as CRM can cause untold amounts of user frustration. Despite its peaks and valleys, the primary task is to track customer information, but that includes all customer information, as well as the ability to easily retrieve the information entered. At the same time, you want to track calls and would like a system to help you remember what was talked about during the last call or visit. The accompanying chart was created by evaluating six of the most popular CRM programs for small organizations: ACT!, CardScan, Goldmine, FileMaker, Maximizer, MS CRM Standard and Outlook Contacts. The evaluation looked at a few critical questions.

Remember that each firm and company situation will differ, so it's best to evaluate each package before choosing the one that best fits your needs.

Contact Anne Stanton at *astanton@thenorwichgroup.com*. ●

Organizational Activities	ACT!	CardScan	Goldmine	FileMaker	Maximizer	MS CRM Standard	Outlook Contacts
Company Records							
Does a single company record support multiple contacts?	Yes	No	Yes	No	Yes	No, but they can be linked	No
Does a company record handle different addresses? (Or do these become new company records?)	No	No	Yes	No	Yes	No, but they can be linked	No
Does it have customizable views?	No	No	Yes	Yes	Yes	Yes	Yes
Does it track e-mail, web and multi phone #s?	Yes	Yes	Yes	Yes	No	Yes	Yes
Scheduling Tasks							
Do the pending calls show up on a calendar, in a task list or both?	Both	N/A	Both	N/A	List	Both	Calendar
How many key strokes does it take to schedule a call?	~4	N/A	~6	N/A	~4	~4	~10
How cumbersome is it to enter a date? (Manual entry, Drop Down list, Calendar?)	Both	N/A	Both	Manual	Calendar	Both	Calendar
Does it support scheduling a specific time?	Yes	N/A	Yes	No	Yes	Yes	Yes
Does it allow you to set an alarm?	Yes	N/A	Yes	No	Yes	Yes	Yes
Does the calendar interface to Outlook's calendar?		N/A	Yes	No	Poorly	Yes	Yes
Does it handle recurring tasks?	Yes	N/A	Yes	No	Yes	Yes	Yes
Does it easily scroll through companies?	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Can I limit the list of people I am scrolling through by source or other fields?	Yes	No	No	Yes	Yes	No	No
Opportunities							
Can I assign different probability percentages to each opportunity?	Yes	No	Yes	No	Yes	Yes	N/a
Are there built in standard formulas?	Yes	No	Yes	No	No	Yes	No
Does the system do anything to help me classify the opportunity and income potential?	Yes	No	No	No	No	Yes	No
Is a sales system built into the software?	Yes	No	No		No	Yes	No
Report: How many calls were made in a given period of time, does the system handle this?	Yes	No	Yes	No	Yes	Yes	No
Administration							
Do I need to do weekly or Monthly maintenance on the DB?	Yes	No	Yes	No	Yes	Yes	No
Do I need to hire a specialist to come in and configure the system?	Depends	No	For Synchronization & custom fields	To customize	For Synchronization & custom fields	Yes	No
What database is it using?	Unknown	Proprietary cardscan DB	MS SQL, Pervasive	Filemaker	Pervasive	MS Sql	No DB
Will it integrate easily to the other applications I am using?	Yes	Easily	Easily	Difficult	Intermediate	Yes	Intermediate
How hard is the product to learn? Do I need a lot of training?	No	Easy	Intermediate	Intermediate	Intermediate	Intermediate	Intermediate
What is the licensing structure?		Per machine	Per user	Per user	Per user	Per user	Per Machine
Is there a multi-user version available?	Yes	No	Yes	Yes	Yes	Yes	No
What about synchronization licensing?	Yes	No	Yes	No	Yes	Yes	No
Can I create user defined fields?	Yes	No	Yes	Yes	Yes	Yes	Yes
What other features does the package have that I have not thought of?	Groups, E-mail, Custom menus	Image of Business Card scan/stored	Knowledge Base, contact specific addresses	Can easily build the entire interface	Contact specific notes under the company record, Order Entry Model	Reporting security so you don't see peoples contacts that you shouldn't	Displays all e-mail sent and received for a contact with lookup feature.

SPAM TECHNOLOGIES

FACING OFF WITH THE SPAM ISSUE

By Roman H. Kepczyk, CPA, CITP

Roman H. Kepczyk, CPA/CITP, is president of InfoTech Partners North America, Inc. a consulting firm working exclusively with CPA firms on their internal technology utilization. He chairs the AICPA's Information Technology Executive Committee and is a member of the *InfoTech Update Editorial* Board.

E-mail has become a mission-critical tool for virtually every business, but the features that made it so successful are slowly draining its effectiveness away through unsolicited e-mail and dangerous attachments. The impact of Spam and virus-infested attachments are wasting individuals and their IT Departments' time, causing big hits to organizational productivity.

According to an IDC study, 5.6 billion worldwide Spam messages were sent daily in 2002, and that number is projected to top 8.8 billion in 2004. Other studies allude to more than 70 percent of all e-mails being Spam. As a result, it's becoming increasingly clear that no one thing will resolve the evolving Spam dilemma. Instead, it will take a number of approaches, including legislation, new technology, external applications, internal process and solutions, and the education of personnel on minimizing their exposure.

On Jan. 1, 2004, the CAN SPAM (Controlling the Assault of Non-Solicited Pornography and Marketing Act) of 2003 went into effect. This new Federal law calls for penalties of up to $2 million for parties that send "unsolicited commercial e-mail." To avoid being labeled as unsolicited, the e-mail must contain correct header information, an accurate subject line, a functioning return e-mail address (operational for at least 30 days after the e-mail was sent) and a valid postal address. In addition, the e-mail must clearly identify it as an advertisement, and include a conspicuous and working method of allowing the recipient to "opt out" of the list. If an individual opts out, the sender has 10 days to remove the individual from further mailings or the sender will be in violation of the Act.

While the law has done little to date to stem the tide of Spam, the Act requires additional administration for legitimate businesses to ensure that their current practices are not in violation. All organizations will need to evaluate their current e-mail policies, particularly marketing initiatives and the management of e-mail marketing lists. They must make sure that procedures include ensuring that deadlines for updates are met and that they are in compliance with all CAN SPAM requirements. While CAN SPAM compliance is mandatory, it does nothing to manage the amount of Spam that individuals actually receive; a number of solutions such as block lists, filtering and end-user education, should be considered.

Real-time Block Lists (RBLs, also known as Blackhole and Boycott lists) consolidate the addresses of known Spammers and Spam e-mail addresses that are either identified by their own personnel or reported from clients of the list. These lists are then made available to the organization, which then imports them into their e-mail system. As e-mails arrive, they are compared to the RBL and any item that is black-listed is either deleted or sent to a quarantine area and identified as possible Spam. Some of the more prevalent RBLs include the Open Relay Database (*www.ordb.org*), Mail Abuse Prevention System (*www.mail-abuse.org*) and SpamCop (*www.spamcop.net*). While RBLs can reduce a significant number of abusive e-mails, Spammers are becoming better at generating new e-mail addresses and domains, so the list must be frequently updated to be effective.

The flip side to the "blacklists" mentioned above would be the development of "whitelists," e-mail systems that only accept e-mail from known parties or domains that are specifically listed. While this solution can virtually eliminate unsolicited e-mails to its users, it also potentially denies e-mail from outside legitimate users that are *not* on the whitelist — effectively blocking out potential customers or associates. To handle these e-mail addresses, some organizations have gone to using a "challenge/response" system that directs all e-mail to a server or external Web site. The site automatically transmits a challenge message when it receives e-mail from an unknown sender, asking s(he) to complete a simple task, such as typing in a word shown in a picture. Once the word is correctly entered, the individual is put on the "whitelist" and the e-mail passes through. If no response is sent, the e-mail is deleted after a set number of days.

While this solution is good for individuals sending an e-mail, it can block legitimate messages sent by automated processes, such as e-mail newsletters or services for which the intended recipient might have signed up. Examples of challenge/response applications are ChoiceMail (*www.digiportal.com*), SpamLion (*www.spamlion.com*) and SpamArrest (*www.spamarrest.com*). One important consideration when using an outside organization to perform any type of filtering service (blacklist or whitelist) is that the company's e-mail will be accessible by this third party. This may be a major concern for organizations that routinely handle confidential e-mails that may not be encrypted. In addition, if that service were to have server or broadband difficulties, all inbound e-mail would be affected.

Another process used to identify Spam is called Bayesian filtering, developed from the work of 18th century Mathematician Thomas Bayes. Bayesian filters analyze the contents of an e-mail, and, based on how those contents were previously treated, determines the probability of it being a legitimate or Spam e-mail. For example, if an e-mail previously listed as Spam contained the phrase "lower your mortgage rate" or the majority of the phrase in any fashion such as "low3r y0ur mortg@ge r@te," it would learn that this is

Continued on page 9

most likely Spam. Some of the anti-Spam products that incorporate Bayesian filtering include Network Associates' SpamKiller (*www.nai.com*), SAPro (*www.statalabs.com*), and Audiotrieve (*www.audiotrieve.com*).

While enterprise and Web-based solutions are effective for most organizations, they are not always cost-effective or easy for individual users to implement. Today, e-mail services, including MSN, AOL and Yahoo!, provide some level of Spam filtering that can be turned on. The easiest way to figure out how to do this is to go to the vendor's help screen and search on "Spam filtering." There also are some basic junk mail or filtering capabilities built into e-mail clients like Microsoft Outlook, but most users find that the amount of maintenance required does not reduce the volume effectively. Finally, there are also third-party add-on products designed for individual users. Examples include SpamNet (*www.cloudmark.com*), Norton Anti-Spam 2004 (*www.symantec.org*) and SpamCatcher (*www.aladdinsys.com*).

Organizations also must make a conscious effort to educate their personnel about e-mail risks. This can begin by having a policy in place that defines the specifics of acceptable use of the organization's e-mail system and what is seen as proper Internet access. Visiting chat rooms that list e-mail addresses or posting the user's e-mail address on any Web site are some of the primary methods Spammers use to "harvest" e-mail accounts. In addition, signing up for anything "free" or that looks "too good to be true" also often lead to Spammers capturing and misusing personal information. A scam known as "phishing" sends an e-mail from a supposedly valid organization that asks the user to verify personal or account information either by responding directly via e-mail or by completing information on an official looking (but fake) site.

Please note that while the CAN SPAM act requires an "opt-out" opportunity in every e-mail, the reality today is that this is one of the primary methods for Spammers to validate the recipient's address, particularly those Spammers that are offshore. Most resources today recommend that individuals DO NOT opt out of e-mails from unknown sources.

Contact Roman Kepczyk at *roman@itpna.com*. ●

EMERGING TECHNOLOGIES

RFID BASICS EXPLAIN BENEFITS TO BUSINESS

By Dan Bodnar

Dan Bodnar is director of Product Marketing for Intermec Technologies Corp's Data Capture Systems Group, where he is responsible for scanning technologies and products; and radio-frequency identification (RFID) products.

Radio frequency identification (RFID) is one of the most promising and anticipated technologies in recent years. Magazine articles, television shows, analyst papers and others are frequently trumpeting RFID's potential benefits. Still, many companies want to know what RFID is, how it works, the current standard and compliance environment, and some considerations to ensure the most successful implementation and ROI.

Manufacturers, retailers, logistics providers and government agencies are making unprecedented use of RFID technology to track, secure and manage items from the time they are raw materials through the entire life of the product. Manufacturers, especially, can benefit from RFID because the technology can make internal processes more efficient and improve supply chain responsiveness. According to a study by AMR Research, early RFID adopters in the consumer goods industry reduced supply chain costs between 3 and 5 percent and grew revenue between 2 and 7 percent due to the added visibility RFID provided.

RFID can provide immediate, tangible benefits. Organizations who take the time to understand the technology's capabilities and limitations can modify or create business processes to meet customer requirements, while increasing inventory visibility and streamlining operations.

The Technology

RFID wirelessly exchanges information between a tagged object and a reader/writer. An RFID system iincludes:

- one or more tags (also called transponders), which includes a semiconductor chip and antenna;
- one or more read/write devices (also called interrogators, or simply, readers);
- two or more antennas, one on the tag and one on each read/write device; and
- application software and a host computer system.

Because direct line of sight between the reader and tags is not necessary, there are many more placement options for RFID readers than were possible with bar code labels. Readers can be placed in a

Continued on page 10

Continued from page 9

fixed-position or be portable, just like bar code scanners. Fixed-position readers can be mounted to read items traveling through dock doors, conveyor belts, loading bays, gates, doorways and other areas. Readers may also be attached to lift trucks and other material handling equipment to automatically identify pallets and other items that are being moved. Interrogator capabilities also are engineered to now be able to fit into smaller mobile devices

Performance Features

Radio frequency is not an optical technology and does not require line of site between the tag and reader – an important distinguishing feature that gives RFID many performance advantages compared to bar code and other automatic identification technologies. Because RFID is a radio-based technology, performance considerations for its implementation are that:

- RFID can be susceptible to interference from other radio transmissions and metal,
- some materials absorb RF signals more readily than others, and
- sensitivity to interference varies by frequency and the usage environment.

These factors can impact the tag read/write range and speed. Most scenarios can be handled by using the proper specific tags, readers and applications.

Because no line of site is required, RFID-tagged objects can be read in different orientations at very high speeds. Orientation sensitivity depends on the antenna design and the amount of interference present. In some environments, tags may be read in any orientation. This gives product and package designers tremendous flexibility in tag placement options, and eliminates the need for human intervention to scan labels or ensure items are placed properly for reading in conveyor belt or retail checkout applications.

Some vendors offer systems that can be programmed to search for specific tags within a field. This functionality, "group select," improves processing speed because only the tags of interest are identified and read, and other tags in the field can be ignored. Group select is extremely valuable for logistics and retail operations. For example, distribution center workers could use mobile RFID readers to quickly search dozens of cartons from an incoming shipment to locate items needed to cross dock. Retailers receiving mixed-load shipments could locate hot-selling products and promptly place them on the shelves before the rest of the shipment is unloaded. Special orders also could be prioritized for processing.

With RFID's ability to read and write to tags automatically, every second could easily produce enough data to overwhelm an information system. Properly analyzing the specific data and timing needed for processes and systems is critical. Planning a successful RFID implementation also requires more than simply extensive knowledge of RFID technology. The enterprise and its technology partners need knowledge and real experience with other data collection technologies, mobile computing, industrial and wireless networking, manufacturing, supply chain and distribution processes, and enterprise software.

Security

It is extremely difficult to counterfeit RFID chips. A hacker would need specialized knowledge of wireless engineering, encoding algorithms and encryption techniques. Different levels of security can be applied to data on the tag, so information could be readable at some points of the supply chain, but not others. RFID is very valuable as an authentication technology, as well as an identification technology, and some consumer goods manufacturers are embedding it into their products to fight counterfeiting and diversion.

Standards

Standards initiatives for logistics and item-level tracking also specify these frequencies. For example, Wal-Mart is basing its RFID supplier tagging requirement on the proposed Electronic Product Code (ePC) specifications developed at the MIT Auto-ID Center (and now managed by EAN International and ePC Global).

Applications

Available frequencies, tag and reader designs give users many choices to consider when planning an RFID application. Finding the right combination of features is fairly straightforward once users begin planning their applications and develop an understanding of their needs and goals.

Many highly effective applications take advantage of existing data collection systems and processes as appropriate, and enhance them with RFID for operations where more functionality is needed. This approach fully leverages existing technology and successful systems, which makes the ROI for RFID easier to measure and faster to attain. For unit-level identification, bar code systems provide excellent performance and are still the most cost-effective option. Bar code technologies have some limitations and are not as advantageous at other packaging levels. As a result, carton, case and pallet processing applications provide many opportunities to complement bar code systems with RFID.

Retailers in general, merchandise, grocery, apparel and other categories are piloting RFID programs and reporting improved sales from greater stock availability, cost savings and increased responsiveness, especially in receiving and inventory control operations. As these applications continue to prove their value, more retailers are expected to announce compliance tagging requirements; many manufacturers may find themselves being asked or required by a retail customer to apply RFID tags to shipments.

RFID also is currently being used in conjunction with asset management, production tracking, shipping and receiving, regulatory compliance, returns and recall management, and service and warranty authorizations.

RFID technology is mature, highly functional and supported by current and emerging standards. Companies in all segments of business are proving the value of RFID every day.

Contact Dan Bodnar at *dan.bodnar@intermec.com*. ●

E-BITZ

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

E-BITZ WITH SUSAN BRADLEY

A cup of Java With "Extra Hot" Security

It's a place where you can get cappuccino and frappuchinos, caramel macchiatos and espresso con panna ... refreshment, a bit of talk, a bit of relaxation ... where you can probably count on a connection to the world of "always on" and always doing business.

My view is very different; whenever I walk or drive by the place with the green sign and hot beverages, to me, it's a possible place of hackers, malware, viruses, spammers and what-not. You may call it a Starbucks, a place you count on for high-speed wireless connectivity and efficiency. However, before connecting, you need to stop for just a moment and perform a few checks to ensure you are not jeopardizing more than just the size of your waistline.

Enable your firewall. In Microsoft (MS) Windows XP, there is a built-in basic firewall. To enable it, click start, control panel, click on network connections, right mouse click on properties, click on advanced and ensure that the check box is in place. If you can't navigate that, visit *www.microsoft.com/security/protect* for online help.

Ensure that file and printer sharing are not enabled. Again, in that network connection properties section, review the protocols and ensure that file and printer sharing is unchecked. Then, review that you have not inadvertently shared out your local hard drive. When you click on "My Computer," there should not be a "graphic hand" underneath that C drive. If there is, you have shared out the root drive; combined with file and printer sharing enabled and no firewall means that you are wide open for anyone in that hotel, coffee shop or any other location where you connect to look at and review your files.

Currently in beta is Service Pack 2 for Windows XP that will enable a firewall for all network connections and provide much greater granular control over that firewall to the extent that you will probably want to leave the firewall on while it is inside the office. More information on the changes to XP sp2 can be found at Microsoft.com.

I have a laptop in my office I call "the prostitute" — it decides to "trust" connectivity and share an information highway with fellow travelers without knowing who its neighbors truly are. The prostitute has been connected to high speed access in hotels, coffee shops and airports, and is used to find connections where there should not have been connections. I use it to send dangerous probing packets to other machines and networks (with permission).

Keep in mind as you travel with your laptop, your fellow computer users may not be so kind and may have malicious intent in mind. Therefore, when you take your laptop to locations, give it special attention when you connect it back to the office. Ensure you scan it for vulnerabilities and viruses before you connect it back to your network. A little bit of extra prevention will ensure that your entire network stays safe and secure as well. You may wish to set up a check-in/check-out procedure to ensure that you stay safe. Check with your firm's or business's IT department for a list of steps to check before and after traveling with your laptop.

Remote connections. Don't forget about your home PC you may use to remote back into your corporate network. On a daily basis, that computer may be used by your family, so do you know where it travels on the information highway when you are away? According to Wired.com, if the PC is used by family members to download music and files using a file swapping service called Kazaa, for example, 45 percent of the files on the service contain Trojan horses, viruses, malware and other potentially threatening files. As a result, that seemingly innocent Britney Spears download may damage your corporate network!

Requirements for remote workers. When the worm MSblast was unleashed on the Internet, the primary means of infection in corporate networks were Virtual Private Network (VPN) connections from home personal computers connecting into the network and laptops. What requirements and standards do you require for remote workers who connect to your network? Do you require them to have anti-virus software and a certain level of operating system, and have it patched to a certain level? Many colleges and organizations are beginning to draft minimum standards for their devices that attach to their networks — visit *http://socrates.berkeley.edu:2002/MinStds/AppA.min.htm* for an example. Microsoft and CISCO recently announced products that assist in testing and setting limitations on what VPN clients can connect to the network.

Wireless access in your home and office. When you set it up, did you "AT A MINIMUM" ensure you enabled WEP encryption for the access and included MAC address filtering? The MAC address is the unique identifier for the network adapter, and you can easily set up your wireless access point to only allow specific network devices to connect.

Traveling and connecting from remote locations means you can work as efficiently as you possible, but the next time you order that fancy coffee beverage, turn on your laptop and connect to that Starbucks/T-mobile wireless access. Stop and think about the risks you may be introducing back into your office.

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

APPLY FOR THE CITP CREDENTIAL, ATTEND TECH 2004 AND GET THE CITP APPLICATION FEE WAIVED!

CPAs interested in attaining the Certified Information Technology Professional (CITP) credential will have the $400 application fee waived if they apply and complete the CITP Application *prior* to TECH 2004 Conference. Successful candidates who attend the Conference in Las Vegas, May 3-5, will be recognized at the Conference and immediately welcomed into the CITP community. Start the application process *now* in order to take advantage of this Special, Limited-Time offer!

Becoming a CITP helps you:

- achieve recognition as *the* preferred business and technology professional in your community;
- join the CITP online collaborative community, and share and learn with other CITPs;
- learn how to promote your services through your listing on the CITP Referral Web site and the use of marketing tools in the CITP marketing toolkit;
- share the CITP value proposition with your employers, clients and peers; and;
- increase your practice development opportunities and advance your career, whether you are a CPA employed in public practice, business and industry, education, or government.

To take advantage of this offer, visit *http://citp.aicpa.org* and complete your application. For more information, write to *citp@aicpa.org*. Don't forget to register early for the Tech Conference! IT Member Section members receive $100 discount off the Conference registration, and the earlier you register, the more you save. To register, vist *www.cpa2biz.com* or call 1-888-777-7077. For more information on the conference, go to *www.cpatechconf.com*.

CPA CITP
Certified Information Technology Professional

AICPA

American Institute of Certified Public Accountants
Information Technology Section
1211 Avenue of the Americas
New York, NY 10036--8775
ADDRESS SERVICE REQUESTED