11-2000

InfoTech Update, Volume 9, Number 6, November/December 2000

American Institute of Certified Public Accountants. Information Technology Section

InfoTech Update

Information Technology for CPAs by CPAs

IN THIS ISSUE

WIRELESS COMMUNICATIONS

VIRTUAL OFFICE: THE WIRELESS SIDE

By Carolyn S. Sechler, CPA and James A. Subach, PhD

Carolyn Sechler operates a Virtual Accounting Firm—now in its fifth Virtual year. She is a frequent contributor to regional and national publications. Dr. Jim Subach is a former NASA scientist and long-time collaborator with Sechler in numerous consulting, writing and software visioning projects.

What is your Virtual Office quotient? Have you considered operating a virtual organization? Most likely you already are "virtualized" and don't even realize it! Aren't there folks on your team working from their homes, airports, audit-related sites and other places accessing your network and otherwise communicating with co-workers, clients and vendors??? Thought so!

How about your Wireless status? Guess what? You already are, at least, at the beginning stages of "wireless" as well as virtual! Simply by virtue of your use of cell phones and personal digital assistants (PDAs — Palm Pilot, Visor), you have entered the *wireless* arena. OK, now we have established that you are in the early stages of being both virtual and wireless, let's review some of the emerging options available to you and the value that could be delivered to your firm, clients and vendors.

continued on page 2

COMMUNICATIONS TECHNOLOGIES

WORKSTATION VOICE RECOGNITION

By Roman H. Kepczyk, CPA

Roman H. Kepczyk, CPA, is president of InfoTech Partners North America, Inc. in Phoenix, AZ, which focuses exclusively on strategic technology management for the CPA profession. He is a member of the *InfoTech Update* Editorial Advisory Board.

Voice recognition technology is old hat; these applications enable us to talk to our computer to enter data, invoke commands or dictate letters, making us less reliant on our keyboards. In the right circumstances, it could be the savior for personnel who are digitally-challenged (in that they have never learned to type effectively). Over the years, the technology has changed dramatically. Here's an overview of how this technology works, the major products and specifications, and our view of the market and viability for use at your workstation.

How it Works

Voice recognition technology translates your voice into a digital format that can be compared to a database of sound files that identifies words of similar sound. It then takes these sounds and by using "fuzzy" logic, selects the most likely match based on the location within the phrase and the context. These applications can differentiate sentences such as "going **to** the ice cream store and eating **too** much

continued on page 5

AMERICAN INSTITUTE OF CERTIFIED PUBLIC ACCOUNTANTS

AICPA

Virtual Office: The Wireless Side *continued from page 1*

A WAP on the Side of the Head

A virtual team member currently primarily uses dial-up connectivity to the Internet while working in the company office, client's office, home office or almost any place where a connection to company information is available. A virtual organization, however, also can work in coffee shops, reception areas, cars (hopefully not while driving), remote field sites and similar locations where a conventional dial-up connection may not be available. Wireless access technology extends flexibility to a team, releasing them from traditional dial-up connections.

In the never-ending alphabet soup of acronyms, there is a new one to remember: WAP. This is short for Wireless Application Protocol. Get used to it, and begin to work "WAP" into conversations at holiday parties this year!

To become a WAP-enabled virtual organization requires adding the means to access the Internet without the necessity of connecting to a traditional land telephone line. This may be accomplished through an installed wireless modem or cell phone connection. This connectivity feat is becoming easier and less expensive to acquire, for instance, through local telephone providers.

You may begin your entrance to the WAP technology arena by using a cell phone as a wireless connection to the Internet. This procedure usually involves a special cable to connect from your computer to the cell phone. In some cases, a special modem needs to be added, but some computers have the wireless modem component built in. The downside of this approach is the slow speed of these connections: usually around 19.2Kb compared to more common dial-up speeds of 24Kb to 40Kb. In addition, the airtime charges can become a significant expense.

A better, slightly more complicated—though not cost prohibitive option—is to use dedicated wireless modems such as those from Richocet and Alphacom. These models connect automatically to the Internet. They connect to your computer through a serial port, PC card or other device. The bandwidth is usually 128Kb, although this number is misleading. Although the underlying speed is around 19.2Kb, just as with a cell phone, these modems use compression to increase the amount of data they can transmit. Normally, text information is received at the top speed, while graphics might be received at half that speed.

Depending on your location, reception through dedicated wireless modems occasionally may be poor, in which case your speeds will be slower, or you might not be able to get and hold a reliable connection. At press time, modems ran about $400 and the monthly, unlimited service was in the range of $30 to $80 per month. Still, the mobility and speed makes this solution attractive. In some cases, a wireless modem makes a good replacement for a standard dial-up connection.

There are some caveats here beyond the obvious, so if you are considering wireless connections, you can use the following list to check off some of the important issues.

1. Can you still use your current Internet Service Provider (ISP) through the wireless service? In some cases the wireless service provider becomes your ISP (WISP) and you may be unable to access your other ISP (and your email) through the wireless carrier. If this is the case, then you may have to manage two email accounts. If so, it makes sense to consider an independent email service or some of the new WAP mail consolidating tools (Yahoo or *www.wap0.com* for instance) as a way to simplify the receipt of your mail to your WAP device. You could also use Outlook, Eudora or another email program.
2. If you are out of the coverage area for the WISP, is there a way to dial into your WISP using a landline? If so, is

continued on page 3

INFOTECH UPDATE, November/December 2000, Volume 9 Number 6. Publication and editorial office: AICPA, 1211 Avenue of the Americas, New York, N.Y. 10036.

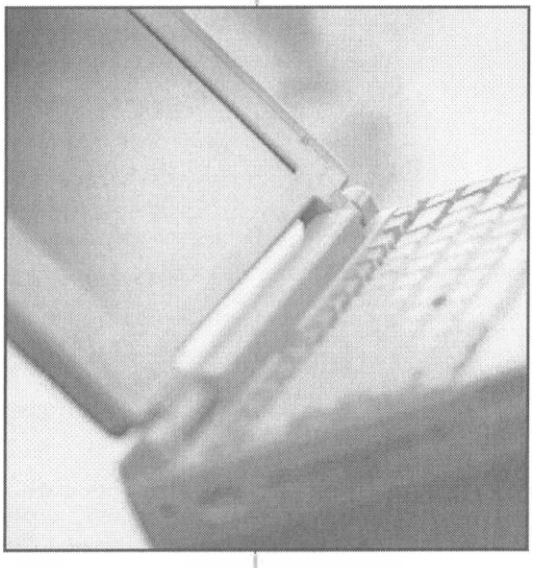
Andrew R. Gioseffi, CPA
Editor
AGioseffi@aicpa.org

J. Louis Matherne, CPA
Director
JMatherne@aicpa.org

Virtual Office: The Wireless Side continued from page 2

there an additional charge for this service or is it bundled with the monthly service?

3. Can you get a fixed price for unlimited service, or are there specific charges? Some WISPs do not charge for connection time, but rather for the amount of data you download. In some cases, this is only for email or only to Web pages. Check this area carefully to make sure that you understand the WISP agreement. There are some WISPs currently offering unlimited access for an average cost of $65 per month, but shop around to ensure you are getting the best price. Prices, too, will surely drop in months to come if past patterns are any indication.
4. Is the WISP local, regional, national or international? Remember, even a national or international WISP rarely operates outside of major metropolitan areas, so the issue of dial-up lines remains if you want to go to a rural area for work or play.



5. Can the WISP support a Virtual Private Network (VPN) connection? Many small businesses do not have VPNs because email provides most of the needs of a small business. Still, if you need to access company information over the Internet, a VPN provides a reasonably secure, effective way to access that information. This issue becomes important in areas like sales force automation. However, there are some potential problems here. A VPN adds some overhead to your computer and the traffic you send and receive. Most computers can handle the overhead, but the wireless connection may appear to bog down. There is the potential for a software conflict between your system and software that the WISP requires for your system and other components, including VPN software on your computer. Discuss this with your technical support and WISP personnel.

How Fast is Fast?

Wireless connections have enormous promise. The current effective speed of 128Kb will soon rise to much higher values. Some vendors are claiming effective speeds as high as 4Mb, though these require proprietary methods. Still, the opportunity to connect to the Internet remotely and have a real-time video conference, access client financial data at a high speed, and update proposals and forward them to the client on the fly, can clearly enhance your current practice.

Still, the need for access to company data and computer systems goes far beyond the basic use of a wireless phone. Consider the following sampling of some recent announcements to *www.thinkmobile.com* a "portal for the mobile community:"

- MSN.CA launched MSN Mobile in Canada, using Internet-enabled cellular telephones and wireless devices to bring MSN to devices throughout Canada.
- Ericsson launched the enterprise WAP Gateway, which allows enterprises to bring mobile e-commerce services to their customers. It also provides mobile office users access to corporate intranet resources. "The WAP Gateway offers huge business potential as a building block for partners who want to provide customized solutions," said Mats Victorin, marketing director, Ericsson Enterprise. "Banking including stock trading, travel requirements like ticketing … can be mobile-based."
- "TelePost, Inc. today unveiled the release of its wireless Conference Center product, a self-administered conference calling service on any wireless platform with Internet access. Using either a Windows CE or Palm operating system, wireless PDA users will now be able to initiate and control multi-participant calls anytime, anywhere with the TelePost Conference Center.

The extension of Conference Center onto wireless platforms now allows mobile professionals to use a single TelePost account from any PC or PDA device and soon from any mobile phone! Also, a WAP will be released soon that allows anyone on the move to be able to operate a conference call from any web-enabled device, domestically or internationally. Offered at *www.telepost.com,* the TelePost wireless service allows PDA users the flexibility of initiating and controlling calls by adding, muting, holding and disconnecting participants to a conference call dynamically with a simple touch of the screen."

continued on page 4

Virtual Office: The Wireless Side continued from page 3

Vertical Market Example

As trusted advisors, we must be in the business of providing strategic consulting to our clients and not just report on the past. Just like you, few of our clients have time to track the developments in an industry like WAP. What if you could, upon completing appropriate due diligence, identify and recommend a tool that could help distinguish a client as well as potentially increase their revenue?

It is now no longer enough to simply track the WAP developments for your internal use; consider the leveraging opportunities you can bring to your client's attention. Take the healthcare vertical market, for example. If you consider this one of your firm's niches, and you monitor sites that update readers on the latest WAP news, you would now be aware of WirelessMD, Inc. and PayMD.com.

It is now no longer enough to simply track the WAP developments for your internal use; consider the leveraging opportunities you can bring to your client's attention.

WirelessMD, Inc. and PayMD.com recently announced a joint services agreement that will allow physicians to wirelessly access claims information from a handheld device (PDA or cell phone) in a secure, mobile, interactive environment. Consider this: PayMD's business model plans to provide real-time claims adjudication via the Internet, enabling providers to process claims and receive payment immediately.

Their technology is intended to integrate a Medicare and commercial plan-coding compliance system, complete with price checking, eligibility confirmations, verification authorization, and claims entry and processing into one unified processing framework.

The WirelessMD system (the joint venture partner) will automate critical aspects of patient care by interfacing with existing healthcare information systems to facilitate access to healthcare information. This includes clinical laboratory results, patient histories and updates, and potential adverse drug interaction notices, as well as the ability to execute electronic prescriptions in a mobile environment.

The list of applications being developed within specific verticals is growing daily. While no one—least of all accounting professionals—needs additional information overload, there are Mobile portals (called "M*portals") organized in such a way to make sorting and sifting a breeze.

Check out *www.wannawap.com* or *www.anywhereyougo.com* for instance. For device reviews and comparisons consider *www.allnetdevices.com.*

According to a post on *www.thinkmobile.com* in mid-October, "Texas Instruments and TROY XCD have announced a collaboration to offer wireless printing capabilities in cellular phones. Using advanced wireless handsets equipped with TROY's Bluetooth printing software and TI's Bluetooth chipset solution, consumers will have the ability to print emails, stock trade confirmations, address book information and Web site research by wirelessly linking to any Bluetooth-enabled printer more than 30 feet away." Remember that Bluetooth is an example of PAN or personal area network technology (see Sept/Oct *InfoTech Update*).

Have we Got Your Attention?

As our practices, clients and business travels become global, wireless technology will provide the critical leverage which may continue to blur the line between a small- to medium-size firm and its large counterparts. The combination of wireless access and Application Service Provider (ASP) enabled applications used to "virtualize" your client's financial reporting and … Look out!

Imagine the new business you can create or the current client relationships to which you can expand services. For the Virtual Mobile Organization, wireless opens up new opportunities and can speed up and streamline other operations. In spite of the caveats, it deserves serious consideration.

Carolyn Sechler welcomes your comments and communication at *carolyns@home.com.* You can reach Jim Subach at *drjim@bridgealliance.com.*

Workstation Voice Recognition *continued from page 1*

of **two** flavors." While this technology has been around for over 30 years, it was only recently considered practical for business use because of the advances in the applications and personal computing horsepower.

Voice recognition is often confused with *speech recognition,* but the two are different. Commercial speech recognition is commonplace on voice automated telephone systems where we either press a button or respond to a question. Speech recognition is designed to be generic because it can understand a few words spoken by a variety of people with very different voices.

Voice recognition, in contrast, is geared towards recognizing the voice of a specific person. By learning your individual speaking patterns and inflection, voice recognition systems can be trained to recognize a very large part of your vocabulary. In controlled situations, the accuracy of recognition can be more than 98 percent (according to a *PC Magazine* article earlier this year). In addition to translating to text in word processing programs, these applications can be used to invoke commands and actually assist with Web access by inputting data into forms, responding within chat rooms and navigating Web links.

The three major products in the personal voice recognition market today are Dragon Systems (*www.dragonsystems.com*), Lernout and Hauspie (L&H — *www.lhsl.com*) and IBM ViaVoice (*www-4.ibm.com/software/speech*). Earlier this year, L&H acquired Dragon, and then was combined with Dictaphone, creating what most of us feel will be the dominant, long-term player in the market.

In our tests, we used L&H "Now You're Talking" on a 333Mhz laptop with 96Mb RAM. Early on, we could not get the system to recognize our equipment because of the flimsy headset included with the system. This was resolved by adding an upgraded Plantronics headset, making the system much more usable for basic dictation. In our office with very little background noise, the accuracy was not bad (but nowhere near the reported 98 percent). Unfortunately, working in an area where there was more background noise, the system became so unreliable that the converted text was hysterically comical (as witnessed by those participants at this year's AICPA Practitioners Symposium). The other issue with actual usage was that inputting punctuation and general correction took longer than if we would have typed it in the first place.

To give the products a fair shake, we *have* seen these products work effectively, but almost every time, it was in a very quiet controlled environment with a very high-powered workstation. Unfortunately, we do not feel we can create this type of environment in many workstations within a typical CPA practice, where equipment usually is behind the technology curve and where there is so much activity and background noise that it causes significant distortion.

For individuals who have a quiet, controlled environment or as an alternative for individuals who suffer from repetitive stress injuries or other handicap, voice recognition may be a viable solution. We recommend you acquire a very high-end workstation with at least a 600Mhz processor, 256Mb RAM, 16-bit Soundblaster Card and a high-end microphone (such as the Plantronics headset or Andrea hands-free microphone). Get as much RAM as possible, as there could be many applications open at the same time, including email and word processing. Something

else to consider are the handheld dictation products such as Dragon Mobile, which have been effective for those people who would dictate "on the run."

Information technology continues to improve dramatically and bring us more horsepower on our desktops than we ever imagined. With time, speech recognition at the workstation level will become commonplace for all users. Currently though, we feel that those that are able to type or those that are not technologically proficient (or patient), are better off waiting.

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

CYBER-TERRORISM, PART II: AN ARSENAL OF DAMAGE

By Albert J. Marcella, Jr., PhD, CDP, CISA

Albert J. Marcella Jr., Ph.D., CDP, CISA, is an associate professor of management in the School of Business and Technology, Department of Management, at Webster University in St. Louis. He also performs IT management consulting and is a frequent speaker both domestically and internationally on security, audit and IT control issues. His most recent book, *www.stopthief.net*, addresses the issue of identity theft, in the growing presence of virtual markets.

So what exactly or rather who exactly, is this elusive 21st Century mischief maker — the cyber-terrorist?

Potential attackers range from national intelligence and military organizations, lone terrorists, criminals, industrial competitors, hackers and disgruntled or disloyal insiders … phreakers, crackers, newbies, coders, script kiddies and hacktivists. Whatever name you give them, collectively, they cause hundreds of millions of dollars in losses to businesses and organizations each year.

In the early days, a hacker or hacking was considered more benign, more of a "closet" activity, reserved for those individuals society labeled "geeks." Over time, the term, along with the concept of hacking, has evolved, as did the technology with which the hackers ply their trade.

1960s	Hackers were the more creative programmers and scientists
1970s	Hackers were viewed as "computer revolutionaries"
1980s	Hackers were described as individuals, actively involved in breaking copyright on computer games
1990s	Hackers are now commonly referred to as "criminals or cyberpunks"

Hackers are no longer the technical elite; greed, power, revenge and malicious intent motivate them. A new taxonomy breaks down the term "hackers" into novices, cyberpunks, insiders, coders, professionals, cyber-terrorists, and perhaps a category of malicious political activists known as hacktivists (*www.infowar.com*, 1999).

Novices, also known as newbies or script kiddies, have limited computer skills, use hacking software that can be found on the Internet, and basically "stage" nuisance attacks. However, they can cause extensive damage to networks because they don't understand how the software works, and sometimes unleash more than they accounted for in the beginning. While cyberpunks have better skills and tend to engage in malicious attacks, "insiders" are very computer literate and often fall into the category of disgruntled ex-employee or current employee. Coders are highly technically skilled, and write the scripts and programs others use to hack systems. They often mentor novices and cyberpunks and are motivated by power and prestige.

Cyber-terrorists are very highly trained, use state-of-the-art equipment and are highly motivated. This professional group comprises criminals, thieves, corporate spies and general guns-for-hire. While cyber-terrorists overlap with professionals, are well-funded and mix political rhetoric with criminal activity, they pose a serious threat to national governments.

Understanding this broad overview of the evolution of hacking and the hacker in general, we are able to compile a reasonably accurate profile of today's hacker. Most hackers are white, middle-class males, 12 to 28 years old, have limited social skills, and, although they are loners, "crave membership." They tend to perform poorly in school, yet have good computer skills.

This is not to say that all hackers are cyber-terrorists. However, given the recent spat of distributed denial of service attacks (DDoS), talk to any network manager, CEO, CFO or user of the firms targeted in these recent attacks, and you might get a different opinion. Ask if these perpetrators were simply creative programmers or individuals intent on malicious destruction and interruption of national or corporate infrastructure (i.e., commerce, communications, etc.). Cyber-terrorists are among us, and they are assuming many forms and disguises.

Weapons of the Cyber-terrorist

In the battle of bits, bytes and bandwidth, the cyber-terrorist brings with him (and most cyber-terrorists are male), a formidable arsenal of tools and techniques. Traditional weapons of choice include:

- computer viruses (such as logic bombs that wake up on a certain date, worms and Trojan horses);
- cracking (accessing computer systems illegally);
- sniffing (monitoring Net traffic for passwords, credit card numbers and other data);

continued on page 7

Cyber-Terrorism, Part II: An Arsenal of Damage continued from page 6

- social engineering (fooling people into revealing passwords and other information); and
- dumpster diving (sorting through the trash).

Details of intrusion attempts involve multiple attackers working together from different IP addresses, many of which are in different countries and continents. The intent apparently is to make the attacks more difficult to detect, increase the "firepower" and acquire more data.

Another advanced cyber-terrorist tool is monitoring computers, fax machines, printers and other devices by picking up their electromagnetic radiation. If someone truly desires your most sensitive information, and has the time, patience and capital, almost any information can be obtained, most often without the owner's knowledge.

In an attempt to plug this leakage of information, organizations that process sensitive information should consider the installation of TEMPEST—(Transient Electro-Magnetic Pulse Emanation Standard) hardened and certified hardware. TEMPEST products exist to protect against leakage of electromagnetic emissions. Although such protection is available, it is not generally available in the commercial sector; an organization that wants to acquire TEMPEST-hardened products will have to demonstrate a need, as well as secure a place on an approved purchaser's list. For more information, try *www.nsa.gov/isso/bao/tempest1/index.htm.*

TEMPEST-hardened devices are designed to shield radiation leakage(s) that can come from monitors and connecting cables, thus preventing cyber spies from intercepting your password, proprietary business plans or even an embarrassing love letter. All of these can clearly be displayed on an external monitoring device in the cyber spy's van parked across the street from your office. Surveillance reports indicate that such electromagnetic monitoring devices can intercept computer emissions from a distance as far away as 1 kilometer or further, if the cyber snoops are using special fast-Fourier-transform chips.

If this is not enough to scare you, just over the horizon are High-Energy Radio Frequency (HERF) guns. No, this isn't science fiction or prototype hype, but actual weapons of critical mass destruction, that can be constructed via plans downloaded from the Internet and with supplies purchased at your local Radio Shack.

Radio Frequency (RF) weapons consist of a power supply, transmitter and an antenna. One type of RF weapon, a HPM (high-power microwave), generates gigawatts (billions of watts) of short, intense energy pulses focused into a narrow beam—capable of silently burning out electronic equipment. Potential targets of HERF weapons include:

- computers and other electronic devices used in the national telecommunications systems;
- the national power grid;
- the national transportation system;
- and finance and banking systems, including a bank's ability to dispense cash.

Just how credible is the threat of a HERF attack? Members of the Irish Republican Army reportedly intended to acquire powerful radio frequency (RF) weapons for use against the London financial system, and Swedish authorities claim RF weapons have already been used against their financial institutions.

Another flashy but stable tool in the cyber-terrorist's arsenal is a Unix-based port scanner for security auditing. Nmap (network mapper) (*www.insecure.org/nmap/index.html*) surveys remote machines to see what services can be exploited. This is easier to install and run than other port scanners, and one of the few programs that does TCP/IP fingerprinting, a way to identify which operating system is running on a remote machine. Nmap also is one of the most popular attackers' tools.

Terrorists' .38 Special

Buffer Overflow attacks are not glamorous, but they are often devastatingly effective!

A buffer overflow occurs when data input from a program is longer than the buffer (a temporary memory storage area) can handle. A bug in an application causes more input data to be sent to the buffer than it can properly execute.

When the buffer overflows, the hacker/terrorist can overwrite the internal stack space of a program to trick the system into executing arbitrary commands. With carefully written code, the attacker can even gain root-level access on the system. Table 1 lists some additional tools that the average cyber-terrorist will have in his tool kit to use against what you believe to be your protected and secure system.

Neutralizing the Terrorist Threat

While the threat of a cyber-terrorist attack can never really be totally eliminated, the potential of an attack and its devastating aftermath can be mitigated through the implementation of logical, physical and technical controls.

Proactive steps to protect against the Terrorists' .38 Special (Buffer Overflow attacks), keep abreast of CERT (Coordination Center at Carnegie Mellon University), CIAC (Computer

continued on page 8

Table 1 — Tools the Cyber-terrorist Will Have in his Tool kit

Tool	Action
Password Crackers	Hackers who attempt to decipher user passwords by encrypting each entry in the dictionary and comparing it with the encrypted value. If the encrypted values match, the attacker knows the password.
War Dialers	The tool dials a list of telephone numbers, in increasing or random order, looking for the familiar modem carrier tone. Once the tool generates a list of discovered modems, the attacker can dial those systems to find an unprotected login or easily guessed password.
Netcat	A general-purpose TCP and UDP connection tool, which is an amazingly useful tool for system administration, network debugging and, yes, breaking into networks.
Session Hijacking Tools	A number of applications used to obtain a command-line login to systems that are insecure. In particular, programs such as telnet, rsh, rlogin and FTP, are all subject to hijacking attacks.
Root Exploits	An attack designed to allow an attacker with a user-level account on a UNIX system to gain superuser access, thereby taking over the machine. There are countless ways for an attacker to escalate their privileges on a UNIX system.
Ping of Death	The hacker uses a packet that is larger than the 65,536-byte maximum allowed by the IP standard. When victims' systems encounter a packet of this size, they often crash, hang, or reboot.
Smurf Attack	A brute-force attack targeted at a feature in the IP specification known as direct broadcast addressing.
Land Attacks	Some implementations of TCP/IP are vulnerable to spoofing (a SYN packet in which the source address and port are the same as the destination). Land is a widely available attack tool that exploits this vulnerability.
The Teardrop Attack	Exploits IP's packet reassembly feature by creating packet fragments with overlapping offset fields, making it impossible for the target system to reassemble the packets properly. Any remote user can crash a vulnerable machine.
The User Datagram Protocol (UDP) Flood (denial-of-service)	By spoofing, the UDP Flood attack, hooks up one system's UDP charge service, which for testing purposes generates a series of characters for each packet it receives, with another system's UDP echo service, which echoes any character it receives in an attempt to test network programs. As a result, a nonstop flood of useless data passes between the two systems.

Incident Advisory Capability – U.S. Department of Energy) and vendor advisories that describe different types of buffer overflow attacks and their "patches." You also should consider implementing intrusion detection software tools to identify active attacks.

Examples of Various Attacks

The following paragraphs identify several known cyber-terrorist attack profiles and provide suggested control philosophies. The reader is reminded that each attack can be slightly different and can produce unanticipated results. The best defense against a cyber-terrorist attack is to be prepared, informed and have a viable back-up plan in place.

SYN Attacks

Firewall vendors have incorporated features into their products to shield your downstream systems from SYN attacks. In addition, your firewall should make sure that outbound packets contain source IP addresses that originate from your internal network, so that source IP addresses can't be forged (or spoofed) from the network.

continued on page 9

Cyber-Terrorism, Part II: An Arsenal of Damage continued from page 8

Land Attacks

Defend your network against the Land attack by having your firewall filter out all incoming packets with known bad source IP addresses. Packets coming into your system with source IP addresses that identify them as generated from your internal system are obviously bad. Filtering packets will neutralize exposure to the Land attack.

Smurf Attack

To prevent your network from becoming the intermediary, you can turn off broadcast addressing if your router allows it (unless you need it for multicast features), or you can let your firewall filter the ICMP echo request. To avoid becoming the victim you must have an upstream firewall, preferably a border router, that can either filter ICMP echo responses or limit echo traffic to a small percentage of overall network traffic.

The User Datagram Protocol (UDP) Flood

To prevent a UDP Flood, you can either disable all UDP services on each host in your network, or have your firewall filter all incoming UDP service requests. Since UDP services are designed for internal diagnostics, you could probably get by with denying UDP service access from the Internet community. But if you categorically deny all UDP traffic, you will rebuff some legitimate applications.

Coordinated Large-scale Attacks

Attacks and probes occur when multiple attackers are clearly working together toward a common goal from different IP addresses. Often these IP addresses are also physically separated in different countries or even different continents.

Navy's SHADOW (Secondary Heuristic Analysis for Defensive Online Warfare) software can detect and track such attacks. (Download SHADOW free at *www.nswc.navy.mil/ISSEC/CID* for Unix/Linux/FreeBSD).

Table 2 — Steps an Organization can Take to Foil a Cyber Attack.

Step	Action
1	Establish a security policy covering all company information. This involves identifying proprietary information and pinpointing who is allowed to access it—and when.
2	Secure the "human element." Humans are the single most important element of an information security program.
3	Maintain physical security barriers using technology like Biometrics, which include finger, iris, voice and face prints. Biometrics are becoming increasingly attractive as users need not remember or carry anything.
4	Information must be protected both in storage and in transit over computer and telecommunications networks. Protection can come in the form of: ▶ Authentication mechanisms ▶ Encryption ▶ Intrusion and misuse detection systems ▶ Software tools that detect and eradicate viruses, worms and Trojan horses
5	Adopt a strategy for contingency planning and incident handling. The final step of an information security program is to plan for the worst—and then respond to incidents that arise.

Haxor — Intrusion Detection

Haxor is a program developed by IBM, that detects intrusions by monitoring the traffic over a company's network. It recognizes hundreds of telltale electronic signatures of attempted attacks, such as the several thousand efforts per second to log on to the system that give away a hacker's program trying a dictionary's worth of possible passwords.

Haxor also includes scanning technology for stealth attacks, such as low-bandwidth hacks and coordinated attacks from different geographic points, and an ability to detect mangled and overlapping packets.

continued on page 10

Cyber-Terrorism, Part II: An Arsenal of Damage continued from page 9

Foiling Cyber Attacks

Stopping the elusive cyber-terrorist will require a heightened combination of both logical and physical controls. In addition, organizations will have to establish stringent policies and procedures designed to train IT users in better safeguard measures/methods.

What's Ahead

Cyber-terrorism can be as obvious as the DDoS attacks played out against several prime dotcom companies in early February, or as transparent as a seemingly loyal employee, who is actually an industrial spy for one of your competitors. Cyber-terrorism can, and will assume many forms. Organizations must be vigilant, and ready for all of the potential forms such aggressive acts and actions will take.

Table 2 identifies several steps, which an organization can take, as an initial effort in their attempt to foil a cyber attack.

Cyber-terrorism is a reality, it can not be wished away. Corporations, governments, and private citizens are all at risk, and equally all are responsible for preventing such attacks. There is no equivalent "neutron bomb" that affects only infrastructure and spares individuals. A cyber-terrorist's strike, coordinated against infrastructure, will certainly result in loss of life. Society has yet to truly experience and witness the breadth and devastation of a cyber-terrorist's attack capability.The recent outbreaks of malicious code, DDoS attacks and system failures, may simply have been the beta testing of the individual pieces of a more organized, coordinated and comprehensive cyber-terrorist strategy.

Corporations, governments, and private citizens responsible for securing infrastructure must invest the time, energy, and the resources to continually monitor critical systems and to be ever vigilant to the growing threats to those systems. While completely insulating your system or a national infrastructure from the ravages of a cyber-terrorist attack may be impossible, there are several steps, which can be taken to help reduce and prevent the potential of such attacks.

Implementing good internal control procedures/structures, aggressive IT audit programs, subjecting systems to third-party, controlled penetration tests, and proactively attacking, defending and prosecuting malicious intrusions are steps which, if aggressively pursued, can help to minimize the exposure from random as well as coordinated cyber attacks. Organizations should continue the monitoring of high-speed Internet connections so that these connections can not be used as part of a DDoS attack.

Before becoming victims, know where to find the latest security patches and updates of cyber-terrorist activities. Know how to access resources from such sites as the CERT and ensure that all systems are adequately protected with multiple firewalls and hard-to-guess passwords. Verify that backup and recovery plans exist, are implemented, and that they work.

At the end of the day, each of us is responsible for ensuring that we remain watchful of the shifting that engulfs our expanding virtual markets and our virtual society, and realize that each and every one of us is at risk.

Contact Albert Marcella at *marcela@webster.edu.*

WEB-BASED APPLICATIONS

WEB RESOURCES FOR TODAY'S CPA

By Tina Kersen Ferguson

Tina Kersen Ferguson is president of the one80 group, a Dallas, TX-based marketing consultancy that specializes in providing brand awareness and strategic direction for various industry clients. She has published articles on outsourcing, employee retention, employee morale and financial strategies.

If you are like most of today's CPAs and accounting professionals, you use the Internet daily for email, and fall somewhere between Web Wonder and Web Novice. You would probably like to surf the World Wide Web more regularly, but who has the time?

There are many accounting resources on the Web for you, your firm or business, and just knowing where to begin might help you navigate through the maze of information available (and geared) to your special interests. In case you didn't know it, you are part of an elite group that is catered to by many Internet sites.

Even if you only have 15 minutes in the next few months, be sure to check out these Web resources.

continued on page 11

Web Resources for Today's CPA continued from page 10

Search Engines

www.google.com — First, there were single search engines, then there were multiple search engines … and now there is Google. The key difference here is that Google is fast—*really* fast, and dedicated to searching; if you search through Google, you will have a better chance of running across a higher percentage of sites that actually *match* your search criteria. How? Google uses "PageRank" technology that allows it to return more relevant results because it ranks the sites by the number of hyperlinks within the site's pages. The end result is a reliable search engine that screams! There are other search engines, certainly, but for now, Google is the chosen favorite.

News and Information

www.accountingweb.com — Looking for a site where you can get practice development ideas, a quick look at the day's top accounting and business news, and weekly workshops geared to the toughest challenges facing your practice or business? Look no further. Accountingweb.com offers all of this and more — FREE. The site is fully searchable, so if you have a question about an issue, you are just keystrokes from a database of information. The site's top ten articles by hits (*www.accountingweb.com/hits.html*) include *seven* articles about Microsoft Excel tips and tricks and pivot table troubleshooting. This is the place to go for answers!

www.techweb.com — When tech news and information are your desired destinations, start here. This site is loaded with hyperlinks to a plethora of sites that help with your unique information technology question — everything from IT specific issues like C++ questions, to industry issues like banking and technology. The site also sends subscribers free, daily tech updates that keep you informed about what's hot (and what's not) in the tech world.

www.accountantsworld.com — Not sure where to start to find accounting-related information? AccountantsWorld could be nicknamed LinkWorld for its seemingly endless supply of links to all the places an accountant or CPA would ever want to visit. State societies, government sites, portals and resources are categorized by subject. While this site offers a mother lode of links, you'll have to check out each site the old-fashioned way, so you might set aside some quality time to explore.

www.cpaweb.org — Where else can you go to update your AICPA member information and pay dues online? One of the site's most exciting offerings is a fully searchable eMAP (Management of an Accounting Practice) Handbook. This online reference is extensively linked, and includes interactive sample worksheets for effortless customization of productivity tools, forms and letters. If you are looking for CPE, CPAWeb features *InfoBytes*, a "one-fee-covers-all" course offering of more than 1,200 hours of training and resources, delivered in one- to two-hour segments.

On the Job Resources

www.edgar-online.com — When you need SEC information, this site should be your first stop. EDGAR Online is ideal for business, financial and competitive information derived from U.S. Securities and Exchange Commission data. The site offers free and paid member subscriptions.

www.zdnet.com — Ziff Davis offers useful information in an easy-to-navigate site that allows you to follow virus alerts and sign up for Microsoft product (Word, Excel, PowerPoint and others) tips that are delivered directly to your email box. You also can download free software for everything from how to find resumes on the Web to how to better organize your Palm Pilot. This site holds the tools you can use every single day.

www.isyndicate.com — Firms looking to boost their Web site stickiness and traffic may want to check out isyndicate.com.

continued on back cover

Web Resources for Today's CPA continued from page 11

The site distributes a broad selection of written, graphical, audio and video content from 1,175 sources to a vast, diverse network of 285,382 Web sites. The site enables you to register and determine how many news articles you want accessible to your Web site every day, as well as choose only the topics relevant to *your* clients. And the cost? You've got it — *free.*

Old Favorites

www.rutgers.edu/Accounting/raw/fasb — Ah, good ol' FASB. The Financial Accounting Standards Board has stepped up to the Internet plate and is dishing out information in easily digested portions. If you want to understand the latest proposed standard, you'll find it here, along with pertinent press releases, exposure drafts, updates on FASB projects and much more.

www.firstgov.com — The Feds have done it! They've created a Web site that consolidates millions of U.S. Government Web pages. To navigate the site, use topic listings, key word searches and links. The site's topic listing, *Money and Taxes,* includes links to the IRS, FDIC, currency exchange rates and bank ratings. If you are looking for governmental information — check here first.

No doubt, the Internet is changing the way people look at information and approach their jobs, and new sites like *www.cpa2biz.com* come about everyday. Developing a good list of resource bookmarks is your first step to capturing the power the Web has to offer you and your clients. We want to hear your own suggestions on interesting and informative sites that appeal to the accounting community. Send your comments to *scytron@earthlink.net.*

Tina Kersen Ferguson may be contacted at *tina@one80group.com.*

InfoTech Update

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

BULK RATE
ZIP + 4 BARCODED
U.S. POSTAGE PAID
Paterson, N.J.
Permit No. 630