2003

Top 10 technologies 2003 and their impact on the accounting profession

Roman H. Kepczyk

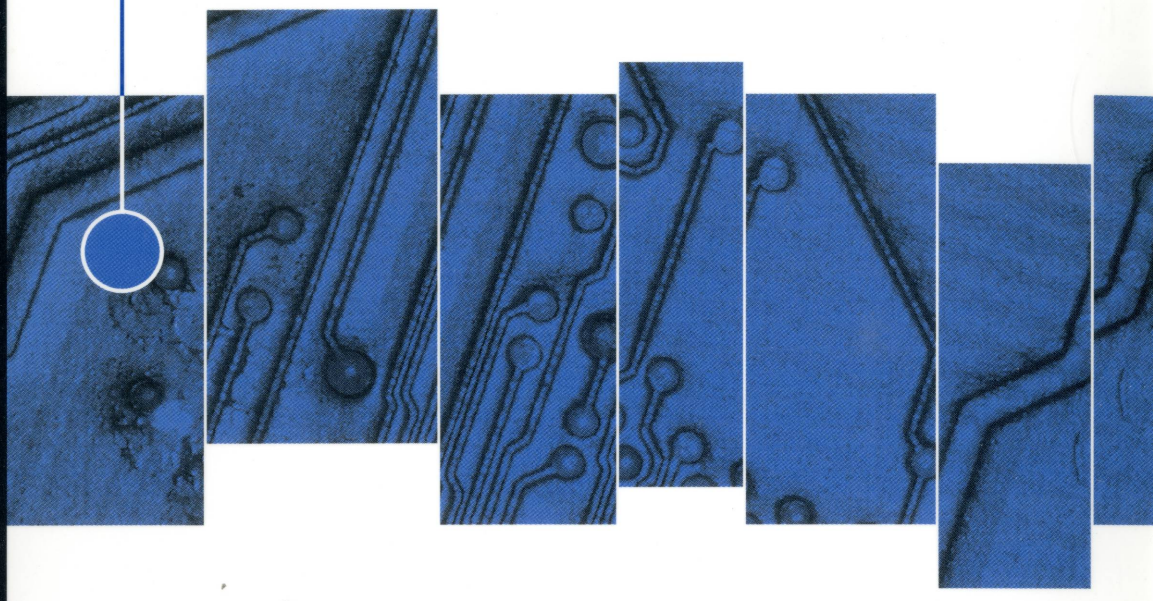
Scott H. Cytron

TOP 10 TECHNOLOGIES 2003

AICPA

AMERICAN INSTITUTE OF CERTIFIED PUBLIC ACCOUNTANTS

Information Technology Section



TOP 10 TECHNOLOGIES 2003

and Their Impact on the Accounting Profession

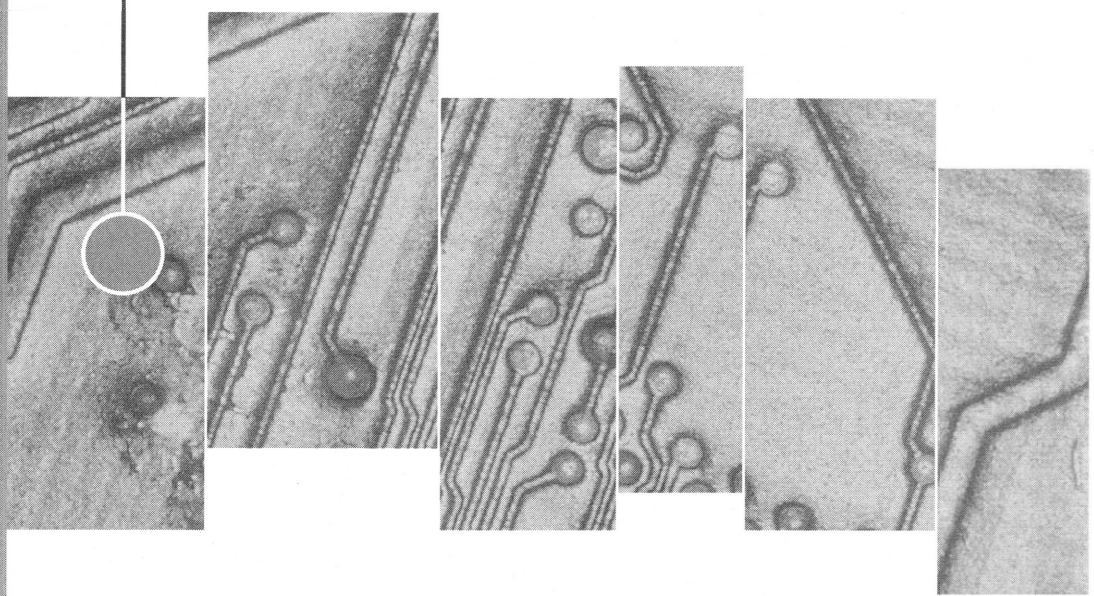
Roman H. Kepczyk, CPA, CITP
Scott H. Cytron, ABC

AICPA

NOTICE TO READERS

Top 10 Technologies 2003 and Their Impact on the Accounting Profession does not represent an official position of the American Institute of Certified Public Accountants, and it is distributed with the understanding that the authors and publisher are not rendering legal, accounting, or other professional services in this publication. If legal advice or other expert assistance is required, the services of a competent professional should be sought.

Information
Technology Section



TOP 10 TECHNOLOGIES 2003

and Their Impact on the Accounting Profession

Roman H. Kepczyk, CPA, CITP
Scott H. Cytron, ABC

American Institute of Certified Public Accountants

AICPA

1 2 3 4 5 6 7 8 9 0 MI 0 9 8 7 6 5 4 3

About the Authors

Roman H. Kepczyk, CPA, CITP

Roman H. Kepczyk, CPA, CITP, is president of InfoTech Partners North America, Inc. and the lead technology management strategist for the firm. His primary focus is assisting firms throughout North America to more effectively use information technology and directing them toward today's "paperless" or digital CPA firm environment. Using the Executive Strategic Technology Resource Management (ExSTRM) Process, Kepczyk optimizes each firm's tax, audit, accounting, and administrative production capabilities based on that firm's clients, applications, and network infrastructure.

Kepczyk spent the past 7 years consulting exclusively with CPA firms and before that, 10 years with the CPA firm of Henry & Horne (Arizona's largest regional firm), where he was the partner in charge of the firm's management advisory services and microcomputer consulting practices. Kepczyk also served as the firm's administrative partner, overseeing the internal accounting, marketing, and human resources departments and managing the creation and implementation of the firm's technology plan and budget.

Kepczyk is currently the chairman of the AICPA's Information Technology Executive Committee, where he analyzes the impacts of technology on the future of the accounting profession. He has served as past chairman of the AICPA's Top 10 Technologies Task Force. He is also a board member of the Association for Accounting Administration and has served on the board of the Arizona Society of CPAs. Kepczyk was included in *Accounting Today*'s Most Influential People list for 2000, 2001, and 2002, and has been named a Technology Pathfinder by the AICPA's Vision Project.

Kepczyk may be contacted at roman@itpna.com or www.itpna.com.

Scott H. Cytron, ABC

Scott H. Cytron, ABC, is an accredited business consultant specializing in public relations, marketing, and communications activities for clients in the accounting, collections/debt recovery, medical, financial planning, legal, and high-tech industries.

Within the accounting profession, Cytron delivers marketing/communications services for a variety of associations, firms and publications. He is managing editor for the AICPA's bimonthly *InfoTech Update* newsletter for the IT

Member Section and assists on other projects in the AICPA. He was key in developing many of the messages and communications materials used in the CPA Vision, working with the AICPA, state CPA societies, and other constituent groups.

Cytron's work is regularly published in the *Journal of Accountancy*, the *CPA Letter*, *Accounting Technology*, the *CPA Software News*, and the Ohio Society of CPAs' *Ohio CPA Journal*, along with its newly created magazine *Catalyst*.

Cytron also currently consults with several CPA firms in practice management activities, communications, and collateral materials/Internet activities; he counsels a national accounting group working in business valuation as well as an international group of CPA firms.

Cytron may be contacted at scott@cytronandcompany.com or www.cytronandcompany.com.

ACKNOWLEDGMENTS

The authors wish to thank the following individuals who participated on the AICPA Top 10 Technologies Task Force, contributed to this book, or both:

SUSAN BRADLEY, CPA, CITP, CISA—*Tamiyasu, Smith, Horn and Braun*

DAVID COLGREN—*Colcomgroup, Inc.*

TOM C. DAVIS, CPA—*Davis, Nichols & Associates, LLP*

DAVID CIESLAK, CPA/CITP, GSEC—*Information Technology Group*

HOLLY HOLT—*Microsoft Business Solutions*

TIM STULL—*Continental Airlines HQSSC*

MARY WAREJCKA—*Freelance writer/editor*

TABLE OF CONTENTS

INTRODUCTION

OVERVIEW OF THE TOP 10 TECHNOLOGIES

Technology is an integral part of our business and personal lives, affecting virtually everything we do and experience in some form or fashion. New technologies continue to be introduced at an increasing pace, and often at a lower cost, providing users more opportunities than ever to advance their competencies and their professions. For business owners, effective use of information technology (IT) provides a competitive advantage that directly leads to improved profitability. The difficulty lies in determining which technologies should have the biggest impact and who would be best suited to create such a list.

Because CPAs are believed to be the most "trusted" business advisers and because they are intricately involved in the flow of information within business, they became the logical choice for evaluating and recommending IT solutions. In that light, the AICPA created the top 10 technologies process in the late 1980s. The AICPA brought together many of the most technologically astute members of our profession to create a list ranked according to priority of technologies that members needed to be aware of in order to be effective with customers and clients.

In the past, this list served as a focal point for the development of guides, articles, and case studies for the AICPA's IT section and various committees to direct the planning of conferences and seminars. In addition, various accounting organizations across North America relied on this list each year to plan their own education endeavors. Over the years, the list was released in the form of articles, books, videotapes, accounting industry newspapers and magazines, and even a domain-specific Web site.

Today, almost 25 years later, the AICPA top 10 technologies program continues to serve as a tool to educate members in business and industry, public accounting, government, and education.

HOW TO USE THIS GUIDE

This guide is designed to provide readers with an introduction to each of the top 10 technologies, followed by a more thorough explanation and practical examples of how that technology is applicable. Even though the items on the list are referred to as technologies, they incorporate technology issues and applications of technology, as well as specific technologies. Wherever possible, such resources as Web sites, actual products, authoritative

documentation, industry statistics, or supporting materials are included to add depth and independent thought to the item discussed.

We encourage you to familiarize yourself with each of the top 10 technologies by reading the introductory paragraph of each chapter and then ranking the chapters according to priority and the issues and opportunities that most directly affect you or your business. We then encourage you to read the entire chapter, review the supplemental Web sites and resources, and discuss the technology with other CPAs and technology professionals. This groundwork should lay an effective foundation for you to more effectively understand and implement the item discussed.

HISTORY OF LAB PROCESS

Beginning in the late 1980s, members of the AICPA IT Research Subcommittee met to evaluate the most important technologies to serve as the research agenda for the coming year. This process became more formalized when a new type of software developed by the Ventana Corporation called a Group Decision Support System (GDSS) allowed a small group of people (approximately 30+ invited guests) to collaborate on the same topic at the same time. Participants met at the University of Arizona in Tucson, in a special technology lab that was equipped to help groups seamlessly collaborate using a small network of computers. Over the years, this GDSS allowed participants to simultaneously vote, add comments, and rank issues in an independent fashion.

To ensure that the laboratory process met the needs of the membership as a whole, selected participants included a comprehensive cross-section of member CPAs working in business and industry, public accounting, government, and education. In addition, individuals with a specific focus in technology consulting, tax production, auditing, and accounting processes were included to add their specialized insights. The process of physically meeting and voting continued through the creation of the 2001 list, at which time a Web-based solution replaced the classroom process.

Over the last several years leading up to the Web-based solution, the evolution of Internet technologies had a profound impact on virtually every business process. With this in mind, AICPA leadership began looking for a method to expand participation in the development of the list, while at the same time lowering the cost to create it. In May 2002, the Top 10 Technologies Task Force opted for a Web-based survey and invited all Certified Information Technology Professionals (AICPA's CITP designation,

awarded to CPAs who have both an extensive knowledge of business process/management and experience in the practical application of technology) and members of the Information Technology Alliance (ITA) to participate in the voting. The Web-based process allowed the voting to be open for a longer period of time and participants to vote at their convenience, rather than having to be physically present at the laboratory for three days. After voting was closed, the results were tabulated and released in a matter of days (rather than the months needed in previous years to fully calculate and assess the results), all at a fraction of previous costs. The following year, 2003, also saw the return to the Emerging Technologies list—absent for one year—created with the assistance of the ITA.

Current Web Process

The Top 10 Technologies Task Force has already begun the process to develop the 2004 list, which begins by reviewing the findings of the previous year. The comprehensive list of items to be voted on will be updated for any new items, and the entire list of definitions will be reviewed and updated as required. The task force then will narrow the list to a manageable number of items to minimize the time spent online to vote. These items, along with specific open-ended questions, are placed within the survey application (Zoomerang), at which time the task force invites others to participate.

The current intention of the Top 10 Technologies Task Force is to include as many technologically astute individuals in the voting process as possible. Although the initial Web-based lists were limited to previous lab participants, CPAs with the CITP designation, and members of the ITA, the task force is evaluating options to expand participation in future years. We invite individuals with exceptional technological knowledge and business insight to submit a request to be included in future top technologies developments. Please e-mail infotech@aicpa.org or this book's authors (see "About the Authors") for more information.

2003 Top 10 Technologies and Emerging Technologies Watch List

The 2003 top 10 technologies tabulation was one of exceptional change. Six new items broke into the final listing, including Business Information Management, Application Integration, Wireless Technologies, Intrusion

Detection, Customer Relationship Management, and Privacy. Not surprisingly, Information Security moved to the number one slot. Disaster Recovery Planning and Remote Connectivity held their own on the list, but participants voted to move Web Services to the number four position, up from number eight in 2002.

The 2003 list boasts the largest participation in the history of this program, with 201 members of the AICPA and ITA voting. Those participating included 142 CITPs.

For reference purposes, here are the 2002 top 10 technologies:

1. Business and financial reporting applications
2. Training and technology competency
3. Information security and controls
4. Quality of service
5. Disaster recovery (business continuation and contingency planning)
6. Communication technologies—bandwidth
7. Remote connectivity tools
8. Web-based and Web-enabled applications
9. Qualified IT personnel
10. Messaging applications (e-mail, faxing, voicemail, instant messaging)

The AICPA top 10 technologies for 2003 are as follows:

1. *Information security.* The hardware, software, processes, and procedures in place to protect an organization's information systems from internal and external threats. This includes firewalls, antivirus protection, password management, patches, locked facilities, Internet protocol (IP) strategy, and perimeter control.
2. *Business information management.* The process of capturing, indexing, storing, retrieving, searching, and managing documents electronically, including knowledge and database management (using PDF and other formats). Business Information Management brings to fruition the promise of the "paperless office."
3. *Application integration.* The ability of different operating systems, applications, and databases to "talk" to each other with

information flowing freely regardless of application, language, or platform.

4. *Web services.* Applications that use the Internet as their infrastructure and access tool, including both Web-enabled and Web-based applications. Examples include Java applications, Microsoft's .NET initiative, today's Application Service Providers (ASP), and business portals.
5. *Disaster recovery.* The development, monitoring, and updating of the process for organizational business continuation in the event of a loss of business information resources due to impairments, such as theft, virus infestation, weather damage, accidents, or other malicious destruction (includes business continuation and contingency planning).
6. *Wireless technologies.* The transfer of voice or data from one machine to another via the airwaves without physical connectivity. Examples include cellular, satellite, infrared, Bluetooth, wireless (WiFi), 3G, and 2-way paging.
7. *Intrusion detection.* Software or hardware solutions that list and track successful and unsuccessful login attempts on a network such as Tripwire. Intrusion detection capabilities are being built into many of today's firewall applications.
8. *Remote connectivity.* Technology that allows a user to connect to a computer from a distant location outside the office. Examples would include Remote Access Services (RAS), Windows Terminal Server (WTS), Citrix, MangoMind, and PCAnywhere.
9. *Customer relationship management.* Processes that manage all customer touch points, including call center technologies, ecommerce, data warehousing, and all other technologies used to facilitate communications with customers and prospects.
10. *Privacy.* As more information and processes are converted to a digital format, this information must be protected from unauthorized users and from unauthorized usage by those with access to the data. This includes complying with local, state, national, and international laws.

2003 AICPA EMERGING TECHNOLOGIES WATCH LIST

The Top 10 Technologies Task Force also worked with the ITA to develop a "watch list" of technologies that may not have current financial viability, but show significant future promise for business owners. More than 20 members of the ITA met at the fall ITA Conference in November 2002 to discuss and vote on the list of emerging technologies created by the Top 10 Technologies Task Force. The four emerging technologies that members should be aware of in the year ahead include:

1. *ID/Authentication.* Includes current and evolving technologies for verifying the identity of a user who is logging onto a computer system or verifying the integrity of a transmitted message. Examples include password scenarios, digital signatures, biometrics, and dealing with such issues as IP spoofing.
2. *M-Commerce.* Mobile commerce uses smart phones and handheld computers with wireless connections to place orders and transact business over the Web. Although accepted in Europe and the Far East, M-Commerce has had slow adoption in North.America.
3. *Tablet PC.* Tablet PCs include the next evolution of the personal computer in a tablet format that allows both handwritten and voice input to interact with the applications found on a computer. The system uses a pen-based stylus, in addition to the traditional keyboard (not required). Tablet PCs provide expanded portability because they can be used in a wireless environment.
4. *3G Wireless.* 3G, or third generation, wireless is designed for high-speed multimedia data and voice. Its goals include high-quality audio and video, and advanced global roaming—the ability to go anywhere and automatically be handed off to whatever wireless system is available (in-house phone system, cellular, or satellite).

Information Security

chapter 1

Information security is once again at the top slot of the AICPA's 2003 Top 10 Technologies list, where it was in 2001 after dropping below business and financial reporting, and training and technology competency last year. Information security is defined as the hardware, software, processes, and procedures in place to protect an organization's information systems from internal and external threats, including firewalls, antivirus protection, password management, patches, locked facilities, Internet protocol (IP) strategy, and perimeter control.

Information security's importance is echoed by many recent high-profile news stories:

- Federal authorities report an identity-theft ring that relied on low-level employees of a Long Island, N.Y., software company that stole credit histories of more than 30,000 people and used them to empty bank accounts, take out false loans, and run up charges on credit cards, among other crimes. This may be the largest-ever identity-theft case in the nation.[1]
- The names, addresses, telephone numbers, birth dates, and Social Security numbers of about 562,000 troops, dependents, and retirees were on laptops and computer hard drives stolen from a nondescript building in an industrial park on December 14, 2002.[2]
- Intruders broke into a computer system and accessed more than 5.6 million credit card account numbers from Visa, MasterCard, and American Express in what is believed to be the largest security breach of its kind.[3]
- Internet job board Monster.com, acknowledging a growing problem for online career sites, is e-mailing millions of job seekers, warning that fake listings are being used to gather and steal personal information. An e-mail message from Monster, which arrived in many users' computer mailboxes, cautions that "regrettably, from time to time, false job postings are listed online and used to illegally collect personal information from unsuspecting job seekers."[4]

[1]Benjamin Weiser, "Identity Ring Said to Victimize 30,000," *The New York Times* (Nov. 26, 2002).

[2]Adam Clymer, "Officials Say Troops Risk Identity Theft After Burglary," *The New York Times* (Jan. 11, 2003).

[3]Jon Swartz, "Hackers Get Credit Card Numbers," *USA Today* (Feb. 19, 2003).

[4]Associated Press, "Monster.com Warns About ID Theft," *Wired.com* (Feb. 27, 2003).

- Hackers broke into a University of Texas database and obtained the names, Social Security numbers, and e-mail addresses of more than 55,000 students, former students, and employees, officials said.[5]

From these incidents, it is obvious that the threat of an attack on an entity's network and information infrastructure is more real then ever, and the methods of attack are evolving rapidly both inside and outside these organizations. In addition, the sheer volume of attacks in recent years has become much more pronounced. The CERT (Computer Emergency Response Team) Coordination Center (www.cert.org) tracks the number of reported computer incidents. CERT listed 82,094 incidents in 2002, up some 36 percent from 52,658 in 2001 and up almost 300 percent over 21,756 in 2000. Along with an organization's direct losses attributed to computer attacks are the difficult-to-quantify "soft costs" associated with a damaged reputation, along with the liability exposure associated with confidential information getting out.

This chapter begins by explaining information security threats, and details solutions in three areas: physical security, technology, and applications. Also presented are security policies and procedures, and how to assess your vulnerability. As your business and technology evolve, protecting your organization requires a combination of solutions that you need to regularly review and update.

EXTERNAL THREATS

To no one's surprise, today's press and trade publications' coverage of information security is on external threats to networks—unauthorized users breaking into a organization's network to steal information or create damage. In general, companies must understand and seek protection against three groups of hackers.

Extreme Hackers

At the top are the extreme hackers who attack information networks for financial or political gain. These professional hackers target business and financial institutions for theft, extortion, or information that can be further

[5]National Desk, "Hackers Steal Data on 55,000 at University of Texas," *The New York Times* (March 7, 2003).

exploited, such as credit card or Social Security numbers. Extreme hackers also target military, law enforcement, government, and university networks because of the confidential, sensitive information contained within those locations, the interconnectivity between the entities, and the political havoc that can be created by attacking these networks.

Extreme hackers have exceptional programming skills and an intimate understanding of the network and security infrastructure; the knowledge allows them to attack undetected and cover up any evidence of their intrusions. Extreme hackers often are stereotyped as self-directed loners hacking for their own personal gain, but some hack into systems under the employ of governments or business competitors—and they see this as legitimate work. Although small businesses usually are not the primary target of extreme hackers, these enterprises often are targeted as a relay or attack point against their intended victims.

Common Hackers

Attacking sites for personal reasons, such as recognition or revenge, common hackers have good programming skills and an exceptional understanding of network infrastructure. This group represents a large portion of the hacker community that threatens governments and businesses, often connected with other hackers through a loose-knit association that shares tools and techniques for exploitation, as well as successful attacks. Common hackers often have access to network administration resources, are comfortable using the network maintenance tools available, and are aware of new, existing security holes.

Script Kiddies

The final group of hackers, "script kiddies," usually have minimal computer skills, and, instead, use automated wizards and tools created by extreme or common hackers to deface Web sites or cause damage to networks. Their attacks are premised on scripts (step-by-step instructions) that explain how to exploit documented vulnerabilities in networks. Often, after a network vulnerability is announced and a patch released, a script to exploit this vulnerability will be shared among hackers and loaded to Web sites where the script kiddies get them. They use these and other programs to scan the Internet for any open connections with the specific vulnerability, and then run the programs to get through the security opening. Because script kiddies' attacks usually are indiscriminate, organizations that do not immediately load network security patches and updates are the most vulnerable.

INTERNAL THREATS

Even though most of the awareness and discussions regarding information security are geared toward external attacks, a large percentage of security breaches and information threats originate from within the organization. In many ways, it is much easier for a person with physical access or network privileges to be a threat. Here are six examples of internal threats. How many of these occur in your own organization?

1. An employee downloads files from the Internet to his or her computer, and those files subsequently are used by hackers to gain access to the network.
2. A user logs on as another user who has better access rights and gets into confidential files, visits illicit Web sites, and sends obscene e-mails to everyone in the address book.
3. A disgruntled employee deletes or damages files on the network by overwriting them. In addition, former employees whose presence is not known to management may hack into the system and do ever greater damage.
4. A computer technician loads a "sniffer" application on the network to capture passwords and logins.
5. A customer service representative copies Social Security information and other confidential information from the default screen.
6. A network administrator delays installing a security patch for the SQL server; six months later, the server is hit by Slammer (Sapphire Worm-SQL Slammer).

In some cases, employees did not even realize they violated security because of a lack of awareness, for example, passwords written on post-it notes attached to computer monitors or piles of documents ready for shredding that fall into the night janitor's hands. Regardless if the incident is driven by ignorance or malice, organizations that understand and evaluate the myriad of possible threats are best suited to prepare a comprehensive defense strategy to secure their information infrastructure. All organizations must make a concerted effort to protect the entity from being a victim, and train employees on recognizing and avoiding compromising situations.

■■■

INFORMATION SECURITY SOLUTIONS

According to a 2002 CSI/FBI (Computer Security Institute [www.gocsi.com]) study, 80 percent of network security attacks could have been prevented had the company put in place even the most basic security steps. Any company with a computer containing information is susceptible to a security breach from internal sources, and any computer with dial-up or Internet connectivity is susceptible to an external attack. Accordingly, companies must develop a comprehensive security defense strategy to protect the enterprise, which includes overall security policies and procedures, and multiple layers of defense, including firewalls and antivirus applications, intrusion detection systems, and vulnerability assessment.

Firewalls

When most organizations think of implementing information security, the first defense that comes to mind is using a firewall or router to protect the network from outside hackers attacking from the Internet. A properly implemented firewall is one critical component of a comprehensive security plan.

Routers are devices used to segment portions of a network and move information to the appropriate location. These devices are aware of the different routes between computers and can immediately redirect information if a targeted path is blocked. Conversely, firewalls have the capabilities of routers, but can do much more. Rather than just ignoring or pushing on information, firewalls closely examine the traffic (data) that requests to go *through* the firewall to the portion of the network protected by it. The firewall determines what traffic is permitted or denied access, depending on the rules set by the company on the firewall. For example, inbound Internet traffic can be limited by the company to specific computers, Web sites, or vendor partners. In addition, the types of files or services that can pass through them also could be limited. The "inspection" done by the firewall on the information is done in one of three ways: packet filtering, stateful inspection, or application processing.

As information moves through the network or the Internet, it is broken into smaller, more manageable pieces of data called packets. As the packet is created, a header is added that describes who the packet is from and where it should go, the size of the packet and number of packets that make up the file, and the method by which the file should be transferred. Depending on the rules fixed in the firewall's memory, packet filtering is the process in which the firewall looks at these headers and determines if a specific packet

is allowed through. Packet filtering firewalls connected to the Internet can be set up to deny all traffic through the firewall except what is specifically given permission by the rules.

Stateful inspection is the next filtering level and much more thorough and detailed than packet filtering. All packets that go through the firewall are inspected, and such information as the specific sender and port to be used are verified to their source. When an employee requests a Web page, not only does the firewall verify the specific user that sent the request; it documents that request in a "state" table and matches incoming pages to ensure they were authorized. Because of the higher level of scrutiny, most organizations today are using firewalls with stateful inspection capabilities.

The third method, application proxy, acts like an intermediary between the two parties on opposite sides of the firewall. Like packet filtering and stateful inspection, the company sets rules about who and what type of traffic is authorized to work through the firewall. Unlike the other methods, once information is deemed to be allowable, the application proxy strips off the sender's address and moves the information through to the intended recipient. As the application proxy handles traffic both ways, neither the sender nor receiver of the information exposes its actual address, providing an additional layer of protection.

Selecting and implementing an organization's firewall should not be a decision taken lightly. Unless the company has individuals with prior security experience, it is recommended the organization get the assistance of experienced professionals. Organizations should look first to their external network integrator because of the inherent, in-depth understanding of the network infrastructure. Some of the more popular firewall companies include Cisco Pix (www.cisco.com), Checkpoint (www.checkpoint.com), Symantec VelociRaptor (symantec.com), and SonicWall (www.sonicwall.com).

Remote Connections

Companies also must protect the remote connections they have authorized to access the organization's network through the firewall. Employees working at remote sites or at home should have personal firewalls to minimize the risk of a hacker accessing their computer and capturing logon names, passwords, or other information that can be used to get into the company. As discussed in Chapter 8, "Remote Connectivity," many of today's cable and digital subscriber line (DSL) connections are targets for hackers, so the risk must be minimized. Companies with a large number of remote users should standardize the personal firewalls used by employees, as well as provide

instructions on implementation and testing. Some of the more popular personal firewalls include Norton Personal Firewall (www.symantec.com), McAfee Personal Firewall (www.mcafee.com), BlackIce (www.securelab.com), and ZoneAlarm (www.zonelabs.com).

Regardless of the connection, it is imperative that the remote computer adhere to the same stringent security policies as those within the firm or company, which include using a password, installing a firewall, using antivirus software, and understanding security policies. Strong passwords minimize the risk of access to the system in the event the computer is stolen. Some consultants recommend using the BIOS password for remote computers; the computer cannot turn on without it, making the machine useless. In addition, remote users should not be allowed to store their logon name and passwords on the computers in a default format so a thief would only have to hit the connect button.

The personal firewalls mentioned here minimize the risk from a hacker attaching a keyboard logging or other sniffer program to the remote workstation in order to log activity or use the computer inappropriately. Antivirus software minimizes the possibility of the remote computer infecting the organization's network through e-mail or file transfer, and education of remote users minimizes the risk of remote users being a victim of the environment.

Intrusion Detection Systems

Another integral component of a comprehensive security defense strategy is having systems that can help determine if the organization is under attack or if unauthorized activity is occurring. This is done through the use of intrusion detection systems (IDSs). IDS applications are designed to monitor the traffic that passes through them, looking for unusual network traffic or patterns associated with network attacks. Network-based IDSs often are set up at the Internet access point within an organization to monitor activity from outside the network, but they can be placed between network segments in different divisions of the organization to determine if unauthorized activity is occurring internally. Even though network-based IDSs monitor the flow of information through the "pipe," host-based IDSs monitor activity on a specific computer. Host-based IDSs are applications that reside on a specific host computer or file server to document all activity on that system and report the results to an individual or central console so the results can be analyzed. IDSs are able to compare traffic or activity with patterns of documented methods of attack and against "normal" activity patterns for that specific computer or segment of the network. For a more thorough discussion on IDS, please see Chapter 7, "Intrusion Detection Systems."

In addition to formal IDS, it is important for an organization's technical personnel to monitor basic network activity and set rules to minimize the chance of intrusion. Network administration rules should ensure that passwords are changed according to the organization's policy, and that activity such as access to Web sites or services on the network, are documented. These activity logs must be periodically reviewed so the network administrator becomes aware of the "normal" activity on the network. Other activity logs that should be reviewed include the verification of tape backup systems, testing of uninterruptible power supplies, and updating of anti-virus applications.

System Maintenance

In January 2003, the Sapphire Worm (a.k.a. SQL Slammer) infected SQL servers throughout the world, creating billions of attacks that affected worldwide Internet performance before the worm could be neutralized. Although its damage was minor compared to previous attacks (ILOVEYOU and Melissa, for example), what made it notable was that the majority of servers affected were infected in the *first 10 minutes* of the attack. The second reason it was notable was that the majority of the infections could have been prevented, because the patch to eliminate the vulnerability had been released six months before.

System maintenance is another critical component of an organization's overall security defense strategy and one of the primary responsibilities of an organization's network administrator. Today's network operating systems and business applications consist of millions of lines of code that can contain programming errors. If taken advantage of, this could pose a security risk. As these flaws are discovered, the software vendors create patches and updates to block these holes. Patches usually are posted to Web sites and notification is sent to users to install the patch. In the period between the time errors are discovered and the customer installs the patch, the customer is vulnerable to someone exploiting the error.

The number of vulnerabilities has increased significantly in recent years. According to CERT, the number of known vulnerabilities reached 4,129 in 2002:

Year	1995	1996	1997	1998	1999	2000	2001	2002
Vulnerabilities	171	345	311	262	417	1,090	2,437	4,129

In most organizations, it is the network administrator's responsibility to keep abreast of such security patches and software updates, and to install them as they become available. In many organizations, unfortunately, the IT depart-

ment either is understaffed or does not have the knowledge, skill, or awareness to keep all systems current. This results in network updates and system maintenance taking a back seat to the daily demands of end users. In organizations where a network administrator or individual responsible for system maintenance does not exist, this responsibility should be outsourced to an external network integrator or resource capable of handling the network.

Administrators must be aware of sites that offer fixes for their operating system and sign up for automatic email advisories, if possible, beginning with specific application vendors the organizations use and include some outside resources. Organizations that provide such advisories include Bugtraq (www.securityfocus.com), NTBugTraq (www.ntbugtraq.com), Network World Fusion (www.nwfusion.com), and Microsoft Security Notification Service (www.microsoft.com).

Individuals also can keep their systems up to date. Because the majority of home computers run Microsoft Windows and Office applications, Microsoft has created a feature to update its applications automatically. The system scans a computer and notifies the user of what updates/patches are available. Users also can sign up with their virus vendor to be kept informed via e-mail of all new releases.

Physical Security

Organizations sometimes overlook obvious security risks, assuming they are being taken care of by someone else. In April 2001, thieves broke into a CPA firm in Littleton, Colorado, and stole four computers that contained hundreds of tax returns with Social Security numbers, home addresses, and listings of bank accounts, and financial investments, including balances. With this personal information at risk of identity theft, the CPA firm instructed clients to close out their current accounts and open new ones, as well as flag their accounts with the three major credit reporting agencies so they would be notified in the event someone began using this information. Organizations must physically protect their information resources as part of a comprehensive security defense policy.

Locking down the physical aspects of information security is usually the easiest portion of a security plan for organizations to understand, as long as they are aware of the risks. This is done by first documenting the physical and network infrastructure responsible for managing and housing the organization's information assets. Organizations must create an accurate network diagram outlining all equipment, including all data connections inside and

outside the organization. The diagram should include a listing of fileservers and computers that run critical applications or contain information to be protected.

A drawing of the physical layout of the facility, with details about where this equipment and data reside, also must be created. This drawing should include the locations of doors, windows, staircases, and any physical security already in place, such as alarms, locked doors, and cabinets used to store data. For a more comprehensive listing of considerations for your physical diagram, see Chapter 5, "Disaster Recovery."

Physical information security begins by limiting access to information resources. Rooms containing critical equipment must be physically locked, with entrance granted only to those with a need to access them. Security systems that monitor physical intrusion (as well as fire/flood alarms) also should be implemented. Computers containing sensitive information, especially laptops, should be physically locked to the workspace. Cable locks and motion sensors from companies such as Targus (www.targus.com) and Kensington (www.kensington.com) can be used to minimize the risk of casual theft of workstations. Also, any file cabinets or closets containing backup tapes or other data media should be included in the documentation, with procedures put in place to ensure they are locked.

SECURITY POLICIES AND PROCEDURES

Businesses must develop security policies and procedures to ensure that digital assets are protected. A written policy signed by each employee is the best assurance that they understand the policy and will adhere to it. There are a large number of resources available on the Internet (a listing of sites are provided at the end of this chapter), but some basic policies to include in your computer and Internet usage policy are included in Exhibit 1-1.[6] Once completed, the policy should be reviewed by the organization's legal council before implementation.

The organization also should document how adherence to these policies will be monitored and put processes in place to ensure that monitoring is done systematically. The policies should list the organization's process for investigating individuals violating policies and the penalties for noncompliance, leading up to and including termination.

[6]Courtesy of InfoTech Partners North America, Inc. (www.itpna.com).

Compliance and Education

Once the policies are written, it is important to educate personnel on what the policies mean and how to adhere to them. This effort should include new and existing employees, and require employees sign the policy as a condition of employment. Companies should provide a training session to discuss computer policies and make individuals aware of the risks involved. This training should be followed up annually and regular reminders sent out to all employees.

Password Policies

Implementation of an appropriate password policy is another of the most effective tools a business can put in place as part of a comprehensive security defense program. Businesses should provide training on what is, and is not, an appropriate password, must train users on how to protect their password, and must mandate they change on a predetermined schedule.

The first step to developing a password policy is to train users to select one that is not easily guessed. In one firm the authors visited, everyone's logon was their first initial and last name and their password was their employee number, making it easy for anyone in the firm (including a disgruntled employee) to easily determine everyone else's logon and password. Passwords should be designed so they cannot easily be guessed by those who know or have access to information about an employee's family members, special dates, or employee numbers.

To further stress the importance of strong passwords, there are hacker tools that can test every known word, including those in other languages, against a system's logon, so individual words should not be used. This "dictionary" attack is known as a brute force attack; today's tools test every word, as well as test for numbers used in the beginning or ending of the password (for example, flower32).

Ideally, the policy should require that the password be at least eight characters long and include a combination of upper- and lower-case letters along with some numbers and characters.

Passwords are one of the key access controls that ensure only authorized users have access to the network and to the areas they are supposed to visit. Getting someone's password conveys to that person all the rights of use that the owner of the password would have, so it is imperative they be protected. Again, passwords should not be written down on post-it notes and stuck to the bottom of the keyboard or in a file drawer where they can easily be discovered. Again, at one top 100 firm, a yellow post-it on one partner's monitor listed not only the password but also the logon. Any person visiting that partner or casually walking into the office could have recorded this information and used it to

log into the network as that partner. Once logged in, the trespasser could have done unimaginable damage if he or she loaded the e-mail program and sent inappropriate e-mails to everyone in the partner's address book.

Employees must be trained on the dangers of giving passwords out and how hackers work around the system to get them. The Internet is rife with stories about how industrious hackers gain access to a system or a user's password through social engineering. A person visiting a business could pick up a phone in an unused office and hit extension numbers until one connected, giving this person an "inside" line (or he could simply dial-in and try different extensions). When picked up, the hacker states he or she is from the MIS department and needs the password of the person to "update" the system. Stories abound about how often this information is given without knowing the person at the other end of the line.

When individuals finish for the day, they should be instructed to turn off their computers or, at a minimum, logout of the system. Network administrators should review the log of network connections to ensure that all users regularly exit the system. Businesses should evaluate the use of screensaver passwords that lock down employees' workstations when they are away from their desk. These screensavers turn off after a specific period of nonuse, usually 5 to 10 minutes, at which point the user has to reenter his or her password.

The network administrator plays an important role in ensuring that all users adhere to a company's password policy. Networks should be configured to require all users to change their passwords on a regular schedule and meet the company's guidelines (for example, no passwords fewer than eight characters).

A suggested policy is one under which passwords must be changed every 90 days and previous passwords cannot be reused. Usually when a person is prompted to change his or her password, this person is given a number of "grace" logins (three to five) before the previous password is no longer usable. In addition, the network administrator should limit the number of password attempts before the user is locked out and must call the administrator.

The network administrator also must be cognizant of the impact of his or her own administrator passwords. Whenever installing any new equipment or application on the network, administrators should immediately change the default password so it cannot be used. In addition, any "guest" passwords also should be disabled.

It should go without saying, but the passwords of terminated employees must be disabled immediately upon termination (remember the fired employee who went unmonitored?). For example, the business should have a process to ensure that when the human resources department is dealing with a termination, it

includes the IT department at the appropriate time. Significant damage can be done by a disgruntled employee in a very short period of time.

In addition to passwords, there also are systems that incorporate smart cards or biometrics to authenticate end users. Smart cards are devices containing specific encrypted information. When used in conjunction with a logon or pass code, smart cards allow access, making it more difficult to bypass. Biometrics are devices that use distinguishing physical characteristics, such as a fingerprint, voice, or iris shape, to authenticate a user. Previously, biometric systems had been expensive to implement and, at times, difficult to administer. Today, they are becoming more cost-effective and reliable.

The Virus Threat

Computer viruses are basically programs that can spread themselves to other computers through a variety of means, such as attaching to computer files and infecting other computers that access the file, or by attacking an e-mail program and stealthily sending the virus to everyone in the victim's address book. Once loaded, they also can destroy data files, reconfigure settings, or create a security hole for future exploitation. Such holes are known as Trojan horses and can damage the computer on a specific date or under specific circumstances or capture information about the computer and pass it on to the sender.

The virus threat will only increase. It is imperative that all businesses and individuals have an antivirus application running on all computers and file servers at all times. In addition, the application should be configured to automatically check for updates and install them when they become available. More popular antivirus applications include Norton Anti-Virus (www.symantec.com), McAfee (www.mcafee.com), eTrust (InnoculateIT) (www.ca.com), F-Secure (www.f-secure.com), and Trend Micro(www.antivirus.com).

In addition to providing antivirus solutions, these sites provide information on virus hoaxes. A virus hoax is an e-mail sent to you to inform you of a "new" virus, urging you to take a specific action (like deleting a system file) or forward the e-mail to everyone you know. There is no such virus or problem the vast majority of the time, but users resend the e-mail, wasting not only their time, but that of everyone else they e-mail it to, who subsequently forward it to others. Users always should verify if a virus is real at one of the above sites before taking any action.

Finally, the organization should implement a process to handle virus infections as part of an overall business continuation plan. This is discussed in more detail in Chapter 5, "Disaster Recovery."

VULNERABILITY ASSESSMENT

After all your security policies, education, and infrastructure are in place, it is important that you test the network infrastructure for vulnerabilities as part of a comprehensive security defense strategy. Specifically within accounting, one of the more well-known programs is the AICPA's SysTrust (www.aicpa.org/assurance/systrust/index.htm) program. SysTrust is an assurance service that independently tests and verifies a system's reliability, and is considered to be a natural extension of the CPA's audit and information technology consulting functions. With SysTrust, a CPA tests whether a system is reliable as measured against four essential SysTrust principles: availability, security, integrity, and maintainability. The new SysTrust Principles and Criteria, applicable to engagements beginning on or after April 1, 2003, are offered by the AICPA as a download format.

The SANS Institute lists the top 10 Windows and top 10 Linux system vulnerabilities under the SANS/FBI Top 20 Most Critical Internet Security Vulnerabilities (www.sans.org/top20). There are tools available on the Web that can test your network defenses to see if you are vulnerable to any of these specific threats, including Qualys (http://sans20/qualys.com), Nessus Organization (www.nessus.org), and Foundstone (www.founstone.com).

For organizations without personnel having extensive computer security experience, vulnerability assessments can be performed by security professionals and organizations focusing in this area. A sampling of companies providing this service at an enterprise level include VeriSign (www.verisign.com), Symantec (www.symantec.com), TrueSecure (www.truesecure.com), and UKSecurityOnline.com (www.uksecurityonline.com).

Individuals working from remote offices or home also should assess their vulnerability to attack. After security policies and procedures are implemented, including a proper firewall, end users should have their security tested. There are tools and resources available to scan computers for open ports and close down any not absolutely required to work. Some of the more popular Internet and security vulnerability tests for individuals include Shields Up (www.grc.com), Microsoft Baseline Security Advisor (www.microsoft.com), and Extreme Tech Web Site (www.extremetech.com/syscheck). (See Exhibit 1-2 for additional security resources.)

EXHIBIT 1-1: SAMPLE COMPUTER AND INTERNET USAGE POLICY

Read before signing.

COMPANY NAME (Company) provides computer and Internet access to employees for business use only. All equipment, applications, information, and data created on the computer system are the sole property of the Company and should be treated accordingly. The Company reserves the right to monitor and record computer and Internet usage of all personnel and to suspend individual user accounts for violation of firm policies. The policies listed here are to be used as a guide to help personnel working for the company determine proper computer and Internet usage. If a questionable situation arises, please contact the chief technology officer for clarification. The Company reserves the right to modify these policies at any time and do what is necessary to ensure the policies are adhered to.

- E-mail and file transfers are to be for business use only by authorized users.
- Use of another employee's account or access to his or her personal files without his or her consent is strictly prohibited. Passwords should not be shared.
- Confidential information is not to be transmitted over the Internet without proper encryption and authorization from the receiving party.
- Antivirus software should be run on all workstations at all times, and all files from outside the system should be scanned.
- All downloaded applications must be approved by the firm's network administrator before being downloaded and installed on the network.
- Transmission of harassing, discriminatory, or otherwise objectionable e-mail or files (as determined by the recipient) is strictly prohibited.
- Access to non-business-related, obscene, or offensive sites is strictly prohibited.
- Disruptive behavior, such as introducing viruses or intentionally destroying or modifying files on the network, is strictly prohibited.
- Any personal use of the network for commercial or illegal activity is strictly prohibited.
- Unauthorized copying of copyrighted material for which the company does not have a license is prohibited.
- Transmission of any religious or political messages is strictly prohibited.
- Game playing is strictly prohibited.

I have carefully read the Computer and Internet Usage Policy. I understand and agree to adhere to these guidelines. I understand that any questions are to be directed to the Company's chief technology officer and any violation of the policies will result in loss of access privileges and disciplinary action, which may include termination.

User signature: _____ Date: _____

EXHIBIT 1-2: ADDITIONAL INFORMATION SECURITY AND ANTIVIRUS RESOURCES

- Antivirus Information Exchange Network (www.AVIEN.org) and its Early Warning System provide virus information.
- Center for Education and Research in Information Assurance and Security (CERIAS) (www.cerias.purdue.edu) includes in its site an exceptional list of topic-specific links under HotList.
- The Computer Emergency Response Team Coordination Center (CERT) (www.CERT.org) maintains listings of current vulnerabilities and has an extensive listing of articles and white papers.
- The Computer Incident Advisory Capability (CIAC) (www.ciac.org) is managed by the U.S. Department of Energy and maintains listing of vulnerabilities and security information.
- Center for Internet Security (CIS) (www.cisecurity.org) provides methods and tools to improve, measure, monitor, and compare the security status of Internet-connected systems and appliances, plus those of your business partners. Systems are developed through input provided by the CIS membership.
- CSI (www.gocsi.com) is the Computer Institute and host site for the CSI/FBI Computer Crime and Security Survey.
- ICSA Labs (www.icsalabs.com) is a division of TrueSecure.
- SANS Institute (www.sans.org) stands for SysAdmin, Audit, Network, Security. The site is one of the most comprehensive regarding all information security issues.
- Security Focus Online (www.securityfocus.com) is another good, general information security site.
- SysTrust Principles and Criteria (www.aicpa.org/assurance/systrust/index.htm) from the AICPA offers the complete set of principles and criteria as an Adobe PDF document.

Business Information Management

chapter 2

We now live in a society that processes information at a rate far beyond our wildest dreams, faster than any of yesteryear's greatest thinkers could have ever imagined. At the end of the day, we find ourselves bombarded with voice and text messages that our brains compute and attempt to process. We all reach a point, however, when we hold up our hands and declare, "Enough is enough—I'm on information overload!"

The way we manage this enormous pipeline of information to provide workable solutions is key to business information management (BIM), number two on the list of the 2003 top 10 technologies for CPAs. For the CPA, working his or her way through BIM involves an understanding of the technology and tools involved in processing information, but more important, learning how to use that information to increase knowledge and services deliverables for the benefit of the firm, business, clients, and customers.

One of the primary attributes and practical ways of looking is BIM is working in the paperless—or less paper—environment. Who would not want to deal with less paper? Ever since the personal computer became an affordable method to conduct business, firms and companies across the world have desired to move to the paperless office, and yet few have actually made the leap to going either entirely paperless or even dealing with less paper.

Why? Factors such as undergoing a total evaluation of your systems, quantifying the costs associated with paperless technologies, implementing required hardware and software, and training employees—let alone your own clients and customers—are just a few of the factors preventing this change.

We are now in 2003, and moving to the paperless office is facilitated by improved technologies, proven techniques, and even a few years of practical experience—an important factor so that employees, clients, and customers understand how the paperless office can become an integral part of daily deliverables.

The paperless office is no longer a myth; it is happening in many of today's more progressive firms and organizations.

MANAGING THE DATA THROUGHOUT YOUR BUSINESS

New to the Top 10 Technologies list, BIM is the process of capturing, indexing, storing, retrieving, searching, and managing documents electronically within a firm or company. Key to the process is to transition all internal and external files and documents to a manageable digital format.

Just as a firm or business would want to standardize its computers and systems, standardizing information within BIM also is important when it comes to creating file names, electronic files, and directories so users actually can *find* the files. Other important BIM components include knowledge and database management, because the firm must capture information from within all of the firm's or company's applications, including tax, audit, and consulting.

■ ■ ■

IMPACT OF TRENDS ON THE INFORMATION TECHNOLOGY INFRASTRUCTURE

According to Bruce Dahlgren, vice president and general manager of the North America Printing Solutions and Services Division with Lexmark International, Inc.,[1] the use of electronic communications technologies by organizations is at an all-time high, and as a result, the Internet, e-mail, personal digital assistants (PDAs, for example, Palm), and electronic calendars actually have a *reverse* effect on the number of documents printed and the amount of paper used.

Why? Perhaps it has something to do with backup on paper or what may be deemed an old-fashioned, yet comfortable, way of doing business. People actually want to *touch* the paper and integrate with print versus electronic documentation. Remember how eBooks were going to be *the* trend in publishing? Tablet PCs and some PDAs certainly might contribute to eBook usage, but reading something electronically versus the same document in print has yet to be a reality within mainstream business.

Take a look at various statistics compiled by Dahlgren:

- According to the Gartner Group, printing is costing corporations an amount equal to 1 percent to 3 percent of their revenue.
- According to the Association for Information and Image Management, the average $1 billion corporation generates 88 million sheets of paper each year.
- According to Xplor International, paper use is growing 6 percent to 8 percent each year.
- According to InformationWeek, up to 60 percent of help desk calls are output related.

[1]See www.lexmark.com/US/virtual_press_room/pdf/printmovemanage.pdf for the full article.

- According to Xplor International, e-mail is increasing printing volumes by 40 percent.
- According to MarketTools, employees, on average, are printing 33 Internet pages every day.

"The poor management of hard copy and electronic documents is slowing down the pace of business, impacting customer service and significantly increasing costs," says Dahlgren. "To address these issues, organizations need partners to help them identify and deploy technology solutions and enable them to print, move and manage information more effectively and efficiently to reap the benefits of a more streamlined information system."

■ ■ ■

IS YOUR OFFICE ADVANCED?

A recent survey was conducted by InfoTech Partners North America[2] of more than 550 members of the Association for Accounting Administrators[3] to assess the degree to which firms are going paperless. Respondents—127 firms with an average firm size of 52 members—answered "yes" to at least 10 of the 20 questions. The highest percentage of "yes" answers included these questions:

- Have you standardized file names and directories on the network and provided training so everyone can create, save, and access files effectively? (84 percent)
- Do you maintain your contract or prospect list in your practice management or GroupWare application? (72 percent)
- Do you use an intranet to store firm-wide information (for example, personnel manual and internal firm procedures)? (69 percent)
- Are you producing financial statements using electronic links rather than rekeying? (69 percent)
- Does everyone maintain his or her calendar and contacts on the firm's GroupWare calendar system as well as respond to his or her own e-mail? (65 percent)
- Do you have a document destruction procedure to ensure all confidential printed documents, as well as outdated electronic files on the network, are adequately disposed of? (66 percent)

[2]See www.itpna.com.

[3]The Association for Accounting Administrators' Web site is www.cpaadmin.org; the full survey may be located at www.itpna.com.

Perhaps more important, however, were the questions with the *lowest* number of "yes" answers. Specifically:

- Are you scanning client supplied information for storage of tax return supporting documentation? (20 percent)
- Do you have a digital fax system that allows you to receive faxes via e-mail and save them digitally to the network? (24 percent)
- Do you deliver firm financial and management reports electronically (via e-mail or post to intranet)? (29 percent)
- Are all audit working papers stored in a paperless audit application (for example, CCH Audit, CSI Audit, Caseware)? (31 percent)

Even though this survey is not statistically valid, it does demonstrate a willingness on the part of the accounting profession to move to standardized processes, intranets, and digital and paperless formats. At the same time, it shows that the profession lacks some of the key, fundamental processes and activities if the paperless office is to become a reality.

■ ■ ■

FIVE AREAS OF FOCUS

Just about every area within BIM concentrates on the movement, capture, and processing of documents electronically rather than manually through paper-based tools and even rows of file cabinets. The five areas that enable BIM technology to be fully realized include information capture, physical capture, information consolidation and storage, information search and retrieval, and knowledge and data management.

Information Capture

The way information is captured or collected is vital to the entire process, accomplished through Web input, file transfer, root source capture, and physical capture.

- *Web input.* Instead of sending paper-based organizers and forms, and asking clients to complete these by hand, firms now provide digital versions of these same pieces of paper through electronic organizers. Once an organizer is completed, the documents are sent by e-mail to the firm, or the client uploads the files through a file transfer protocol (ftp) Web site—a

unique Web address set up by firms and companies to receive electronic files on their server rather than through traditional e-mail.

- *File transfer.* The ability to receive a client's trial balance or other files is essential to the electronic process. This is accomplished through e-mail or ftp. When an important file is received electronically, the company should save it electronically in that client's digital file folder. By standardizing the naming conventions of all files and customer directories, employees can use the system as easily as today's paper file storage methods.
- *Root source capture.* Other methods used to aggregate information include e-mail, fax, and voice mail, and handheld PDAs. To improve accuracy and efficiency, information must be captured at the point of creation from its "root source." Digital faxes delivered electronically to the recipient's e-mail, rather in a paper format, allow the user to easily save this information in the customer's directory file. E-mails that contain confirmation information or document decisions also should be saved as a source document and managed electronically rather than printed out and placed in a client file. In addition, the use of today's handheld Palm and PocketPC computers (PDAs) allow people to take important applications wherever they go and update information as it occurs. If you are meeting with a customer and the customer would like to set up an appointment for next week, the handheld device captures this information and synchronizes it with the information back at the office.

Physical Capture

How firms use their copiers, scanners, and multiple function devices also is key to capturing information and eliminating paper.

Information indexing. One of the key issues in BIM is transitioning manual documents into a digital format. For this to occur successfully, users must get to the same comfort level with digital documents that they have with the physical files and folders they use today. This requires that the company standardize its file directory structure, the way it names the files, how it secures them electronically, and how the company will provide ongoing training to ensure that these standards are met.

File directory structure. In most instances, companies emulate their physical file room layout on the network to ease the transition to a digital environment. Files are organized either by the customer's name or some kind of ID number. Within that file could be the years (which often happens with vendor files) or the product or service provided. Within CPA firms, it is common to see a client listed with multiple tax year files. Again, an emulation of the firm file structure will make it easier for users to transition to the new system.

File naming conventions. Companies also should take extra care to standardize how they name electronic files so they are easily identifiable when viewed by file name on a computer screen. Key identifiers, such as the customer number or name, the type of document stored, and the date created, can be included in the file naming convention, for example, "20030602 Johnson Holdings Engagement Letter.doc." If this file was in the wrong folder, it would be obvious, whereas a letter called EngLtr.doc would not tell you anything.

A good file naming convention also makes it easier to search the entire network for a misfiled document. Remember, it is just as easy to save a document in the *wrong* directory as it is to file a piece of paper in the wrong folder. The primary difference is that the search feature on a computer (see the section "Information Search and Retrieval" later in this chapter) allows you to search through your entire network in minutes, compared to the effort it would take to physically go through every file. Who has that kind of time?

File security and authorization. Just as many companies keep confidential documents stored in secured places, so must they also protect their digital documents. Individuals should have access only to the network directories and files that they need to do their work. Individuals on the production line should not be able to access accounting records or human resources information that do not directly pertain to them. In some instances, companies can use passwords to protect applications or portions of the network, whereas in other instances, the network administrators can set up each individual's network "rights," which would determine what they can access on the network. For more information on security, see Chapter 1, "Information Security."

Ongoing training and procedures to ensure compliance. Moving from a paper to digital environment does not happen overnight. Users must be trained on the items listed here and must be reminded frequently of the new solutions. The company must have procedures in place to ensure compliance, such as the reviewing of files created.

Information Consolidation and Storage

The way in which information is collected, consolidated, and stored is key to enabling BIM technologies. A practical way of looking at the importance of consolidation and storage with regard to BIM is to think of what happens when two CPA firms, or two companies or organizations, merge. Both possess databases on their own, but now the databases and other information must be integrated so the firm is left with only one set of files rather than disparate systems with information. In many cases, the companies spent an inordinate amount of time working on these databases and do not want to see them just get tossed aside. For more information on database integration and information consolidation, see Chapter 3, "Application Integration," and Chapter 9, "Customer Relationship Management."

CPA firms understand one of the components of information consolidation and storage: Professional Services Automation (PSA). PSA is an integrated set of business software and services that help project-driven businesses operate more effectively (www.portera.com). PSA helps any professional services organization such as a CPA firm automate assignments, billing and invoicing, time sheets, and similar kinds of labor. Certainly, a CPA firm as well as any size company or organization can benefit from PSA solutions because they can streamline business processes and improve communication and collaboration among internal teams, as well as with clients and business partners.

PSA enables a business to enhance management insight and visibility, increase revenue opportunities and improve cash flow, reduce support overhead, make the most effective use of resources, and collaborate with clients and partners. It also provides the means to effectively retain employees, share knowledge across the organization and access information from anywhere.

Portera's *ServicePort* suite, for example, provides a set of Web services within a configurable portal interface, and integrates with other financial, human resources and CRM packages.

Information Search and Retrieval

Internal search tools. Once an organization discovers how it can find something internally, harnessing the power to search for documents and information is worth its weight in gold.

Windows Explorer, a popular search tool preloaded on all Microsoft Windows-based operating systems, is a folder/file tree method to find specific files. Improvements in advanced versions of Windows, including

Windows XP, have brought more sophisticated ways of searching by keyword, file name, and other means.

A variety of custom search tools written by developers for specific, proprietary use do exist. Many of these developers (or if available, in-house talent) write custom programs for searching an internal network or system, and will incorporate specific expectations when creating these programs.

A number of other internal search systems already exist. 80-20 Software (www.80-20.com) provides scalable, search, and document management software to manage unstructured data in two areas: repository management and search (on both a personal and enterprise level). Specifically, 80-20 Leaders Online, 80-20 Document Manager, and the 80-20 One Search suite allow companies to profile and store, and then search and retrieve documents across an entire enterprise.

External Web query. Many Web search engines populate the virtual marketplace, and most users have their favorites they access on a daily basis. One continuing to build credibility is Google (www.google.com), with its ability to aggregate data in seconds. For added convenience, you can incorporate the Google toolbar on your desktop. Google has become so popular that many uses now refer to it as a verb, as in, "Do you Google?"

Other search engines are ideal for various pursuits and offer various pay and free services. In addition to Google, a few other popular services include Yahoo! (www.yahoo.com), Northern Light (www.northernlight), and MetaCrawler (www.metacrawler).

MetaCrawler, for example, is a meta-search engine that searches various sites, including About (www.about.com), Ask Jeeves (www.ask.com), AlltheWeb (www.alltheweb), FindWhat (www.payperclicksearchengines.com), LookSmart (www.looksmart.com), Overture (www.overture.com), and many more. Of course, users can go to these sites directly to search rather than rely on an engine such as MetaCrawler to get the work done.

In a meta-search engine such as MetaCrawler, you submit keywords in the site's search box, and the system transmits your search simultaneously to several individual search engines and their databases of Web pages. Within a few seconds, you get results from all the search engines queried. Meta-search engines do not own a database of Web pages; they send your search terms to the databases maintained by search engine companies. However, in many cases, note that the idea of meta-searching is much better than the reality; you might think you would save time by searching only in one place and sparing the need to use and learn several separate search engines, but you should not

solely rely on a meta search engine for all of your solutions. Test and retest, then decide which engine best suits you and your firm or company.

Knowledge and Data Management

Effective BIM must not only manage the files in a digital format, but also make information available in a useful manner, in essence a way to harness the company's knowledge. Today, a variety of tools are used by corporations to organize information, such as databases and intranets. Lotus Notes from IBM (www.lotus.com) is one of the more prevalent knowledge management tools, because it is a large database application that can effectively manage diverse types of information in a seamless fashion. Many companies also use intranets to store information that is not found in other applications. An intranet is simply an internal Web site that stores policies, procedures, and information that are available through a browser.

■■■

CASE STUDIES

KAF Group Uses Xerox DocuShare[4]

Every year on April 10, KAF (Kirkland, Albrecht & Fredrickson, P.C.) Group's greatest nightmare was that clients would call and want to discuss an issue on their completed tax forms. Chances are the tax documents were in a filing room, waiting to be stored, along with about 600 others. It could take more than a day to locate the file. Now, locating the file is a couple of computer clicks away because the company is using Xerox's DocuShare online filing system (www.xerox.com).

"I am convinced people will forever work with paper; it's the storage of that paper that we try to improve," explains Barry MacQuarrie, CPA, director of Technology Solutions at KAF Group, an accounting and consulting firm in Braintree, Massachusetts.

DocuShare 3.0 is a Web-based document management application that gives workgroups and organizations a secure environment for capturing, managing, and sharing information. It can be deployed as a secure document repository, robust content management system, portal, or collaborative project management application.

[4]Source: Kirkland, Albrecht & Fredrickson, P.C.

Every one of the more than 50 employees in the company now knows how to scan in documents, although the company still maintains a filing staff who do the bulk of the scanning. Scanning is no more difficult than copying a document on the DocuShare copier. Preprinted scanning request forms are used to communicate to FlowPort, which directs e-file traffic. An e-file location is checked on the request form and then scanned before the document. FlowPort then directs the document to the appropriate e-file. In addition to online file folders, the documents can be sent to anyone's e-mail address. KAF has more than 44,000 files stored so far.

And, there are no worries if the document ends up in the wrong file because the search function allows anyone at his or her desk to type in keywords, such as Social Security numbers or names, to locate the file on the Web-based system. MacQuarrie says he can usually pull up a person's files while exchanging initial pleasantries over the phone so he is ready to do business.

"We don't have lost files anymore and there is less time wasted traveling to the file cabinets," he says.

Another benefit is now everyone knows if the company has worked on certain projects. For example, if one partner does a major research project, it will be filed on the system, allowing other partners to search for the project if they get similar work. Previously, only the people participating in the projects would know they existed, forcing the others to start from scratch each time a request came into the company.

InStranet Offers Web-Based Document Solution[5]

Intermarche had a problem. The company was designing first-class promotional campaigns for its 1,000 stores, but there was no guarantee the stores were receiving the information in a timely manner or that headquarters was receiving timely feedback to analyze the promotions' effectiveness.

So the $10 billion French version of America's Wal-Mart decided to give New York City-based InStranet application a try. This application, which operates on Intermarche's server, provides a Web-based system that allows for real-time transfer of all sorts of documents. As a result, the system eliminated the need to send reams of faxes to the 1,000 stores.

In addition, the stores were able to quickly give feedback, which helped improve sales for each store's 5,000 to 10,000 products. For example, if a competitor were selling snow blowers for less, headquarters could adjust its

[5]Source: InStranet (www.instranet.com).

promotional price for snow blowers just in that city or region. The system also allows for security; Intermarche provides access levels for all employees.

The results include a $400,000 savings in paper, but more significantly the company's fresh and seasonal sales have increased 2 percent to 10 percent—a huge increase, says Clinton Stark, director of U.S. marketing for InStranet. The move has also saved store managers time, Stark says, because they no longer have to hunt for all the proper promotional paperwork in the company's annual campaigns, which can run as high as 400 separate campaigns annually. They are online ready for viewing, including written and graphical correspondence, such as the specific shelf placements of products to increase sales. Corporate headquarters also has immediate access to product sales and is able to assess the campaign more readily than before.

The Videre Group and GoFileRoom[6]

The Videre Group, LLP,[7] looked at many e-file systems before choosing GoFileRoom, a Web-hosted document management service from Immediatech Corp. According to Videre, the biggest advantage to GoFileRoom was that the system maintains the electronic files offsite so the firm does not have to worry about training and maintaining its own IT staff.

New Jersey-based Videre provides advisory services, tax, auditing, and financial services to businesses in all industries. The firm moved toward a "less-paper" office to increase productivity, improve customer service and cut operating expenses. The deployment took only two or three weeks, and training was a breeze for the 145-person CPA firm–one of the top 100 accounting firms in the United States.[8]

Not only does the online filing system cut down on paper used, it also makes it easier to find files—especially those that were not filed correctly.

"Before GoFileRoom, someone had to go to the file cabinets, find the document, remove it from its binder, and then fax it to the client," explains Adam Kupperman, Videre's technology director. "Locating lost documents could waste hours of staff time."

GoFileRoom is maintained on a secure server off-site and backed up to prevent loss of files. Users can gain access to the 128-bit SSL encrypted site only by providing a password and user name. Any work done on the system

[6]Source: Immediatech (www.immediatech.com).

[7]The Videre Group, LLP, has its Web site at www.videregroup.com.

[8]*Accounting Today.*

is then tracked and recorded to provide a full trail of use. In addition, CD-ROM backup disks can be provided to prevent loss of data.

HA&W: 100 Percent Paperless[9]

If someone asked you to find a client's file in your office, how long would it take you to lay your hands on the actual documents?

Atlanta CPA Leslie S. Lowthers estimates it took her staff up to five minutes *to find one file*, and even though this does not sound like very much time, it all adds up. Of course, that was prepaperless.

Lowthers is senior manager in the real estate group of Atlanta-based Habif, Arogeti & Wynne, LLP, a full-service accounting and consulting firm with approximately 150 total staff. HA&W also is the largest independent accounting firm in Georgia and regularly makes the industry's top 100 listings.

"When we started upgrading our technology in 1998, we had no intentions of going paperless," says Lowthers. "However when we realized tools that were available on the market, we made the common sense decision to use those tools to increase productivity. We were one of the first firms anywhere to commit to going completely paperless, so there was no one to tell us how to get it done or even help in an advisory capacity.

"One of the main reasons we decided on this direction was the lost productivity that resulted from spending time in searching for files. With the tough market for new hires, we had to think about becoming more efficient, and doing more with fewer people."

When Leslie says the firm went paperless, she means *totally* paperless, not just dealing with less paper or taking some parts of the practice paperless as many accounting firms currently do. Even though the initial goal was simply to update the firm's technology, the process involved in going completely paperless presented two problems.

"The software packages on the market were either very expensive and didn't do what we wanted, or they couldn't handle the volume required by an organization the size of ours," she says.

The firm decided to develop its own document management software that integrated with other applications the firm had selected. This product was named SIAN®, or *Secure Information Available Now.*

---

[9]Source: Scott H. Cytron, "Leslie Lowthers: The Proof is in Paper(less)," *InfoTech Update* 11, no. 2 (March/April 2003).

For its trial balance application, the firm decided on Toronto, Ontario-based CaseWare Working Papers' (www.caseware.com) trial balance product. The firm uses CaseWare Working Papers for all attestation functions (audits, reviews, and compilations) and CCH ProSystem *fx* for tax along with the Microsoft operating system, and Microsoft Office products for word processing, calendaring, and other administrative functions. The firm tied these major applications and many other ancillary applications together by using SIAN to control all documents generated.

The combination of these programs, along with increased electronic storage capacity (a must, according to Lowthers), provided enough resources to capture a minimum of *seven years* worth of data. As part of the process of going paperless, the firm digitally imaged all paper files, including files in dead storage. She says if the file was within the retention period, the firm digitally imaged the document.

The result? The system completely eliminated the firm's storage and filing system. In fact, when the firm moved its offices in 2000, it did not move any paper files in the process, and today, the firm has no central filing area and the only paper relates to interim work.

Obviously, an endeavor like this takes time, planning, and resources to occur. However, there is also a large, human resource element that fits into the process, a component she says most firms overlook because they are totally focused on technology instead of the human element.

"We truly believe the key to the entire process is training. Prior to going paperless, we just threw software programs or other products to the staff and expected them to figure them out without training or education. Now, we focus on not only training on the products, but also training on the firm's process for using the products."

Lowthers says another requirement is to have good IT people either on staff or readily available.

"You just can't go paperless without having the backup system in place and an IT department to support a digital office. Firms who think they're too small should not be afraid of making necessary changes. Different size firms call for different solutions. We have helped implement our system in offices with as few as 10 staff.

Except for the traditional accounting busy season, Lowthers travels across the country as a certified CaseWare trainer, sharing her experience and teaching other firms how to work in the paperless office environment. With her field

experience, she has three recommendations for smaller firms (the largest contention) that want to go paperless:

1. *Get some outside help.* Making paperless happen internally is unlikely, unless the firm's staff is technologically savvy. Most accountants find it difficult to keep up with the latest technology advances.
2. *Attend the AICPA Tech Conference.* This is a good source of information to find out what other CPA firms are doing.
3. *Get training.* Start with basic Word and Excel, learn how to use Windows Explorer, and understand how files are saved electronically.

"Employers let their employees down by not training them on basic products. Management is usually of the opinion that, 'if you know how to type, you know how to use Word, or if you can add one and one together on a spreadsheet, you know how to use Excel.'"

Cost, of course, is another consideration that cannot be underestimated. For starters, she says you have to have enough storage capacity, and while some firms have made great strides in upgrading their servers and systems, they also need to have enough storage for many years to come—not just on an annualized basis because the firm has not planned far enough in advance. HA&W, for example, has 20 terabytes of storage capacity. Loosely translated, that is enough storage for *126 million documents*.

On the software front, she advises that many of the products firms already are using may be equipped to help go paperless, such as CCH, Lacerte, and some of the larger tax packages. SIAN, for example, installs for $18,000, and annually runs $325 per user, with half of that fee spent annually for sales and support.

In addition to the case studies mentioned above, the following have developed CPA firm-specific applications. Creative Solutions Inc. (www.creativesolutions.com) has developed a digital File Cabinet Solution. CPA Software (www.cpasoftware.com) has a Virtual File Cabinet application, and firms are using CCH (www.cch.com) ProSystem *fx* Engagement in this capacity. (See Exhibit 2-1 for further resources.)

EXHIBIT 2-1: RESOURCES

- **Browsers and Searches for Internet Resources**
  - *www.lub.lu.se/netlab/documents/nav_menu.html*—A site from Lund University that offers a multitude of search tools, tips, and resources.
- **Internal Search Tools**
  - *toolsgarage.tripod.com/sitesrch.html*
- **Online Research**
  - *www.wiley.com (Best Websites for Financial Professionals, Business Appraisers and Accountants)*—An A-Z guide by Eva Lang and Jan Tudor that takes the guesswork out of information search and capture.
  - "Moving to Paperless" by Tom C. Davis, CPA; *www.itpna.com/Vision/2002/20020930%20Moving%20to%20Paperless.htm.*
  - "Paperless Audit Opportunities" by Roman H. Kepczyk, CPA, CITP and Tom C. Davis, CPA; *www.itpna.com/Vision/2002/20020416%20Paperless%20Audit%20Opportunities.htm.*
  - "Information Management in the CPA Firm" by John Stein and Tom C. Davis— *www.tcdcpa.com.*
  - Capterra *(www.capterra.com/professional-services-automation-software)*—A virtual clearinghouse that offers a variety of resources for professional services automation (PSA) software, including articles, research and vendor links.
  - *CIO Magazine,* "10 Steps to Choosing the Right PSA Software"; *www.cio.com/archive/031502/roboboss_sidebar1.html.*

Application Integration

chapter 3

One of the key components driving quality customer service is the ability to provide an online seamless user experience, and at the forefront of this experience is application integration.

Application integration is the manner in which different operating systems, applications and databases "talk" to each other, with information flowing freely regardless of application, language, or platform.

Remember word processing of days gone by? Anyone who used a previous version of Word had to deal with a translation problem: Documents written in one version and shared in another were not accessible. For example, a document written in Word 97 could not be read very well by Word 95. Some of the characters could not be translated, and the entire process was labor intensive. A greater problem, however, was the ability to read a WordPerfect document or another word processor's document within a program other than the same one in which the original document was developed. Users had to convert a document to ASCII text and then reformat it as desired.

Today, we are facing an altogether different situation; modern software packages have components to read documents rendered in previous versions of the same software and even in other packages. Office XP, for example, can read any document, regardless of the previous format or program The vendors recognize the importance of this task to retain universal appeal to the mass market; in fact, Microsoft now has a page within its Web site solely devoted to converters and viewers (www.microsoft.com/office/000/viewers.asp). In short, application integration is working through these simple examples.

Back to the user experience: Integrating applications such as word processing, spreadsheets, and presentations is one aspect, but enabling e-commerce and e-business across cyberspace is of much greater importance to an organization's bottom line. As a result, it is a natural progression of thought that to enable these processes to occur, operating systems, databases, and applications *had* to integrate so that any manual process was negated. The manner in which information is translated for sharing is the primary component of application integration.

WHERE DOES INTEGRATION OCCUR?

Application integration occurs in four areas: hardware and software, PC-based hardware and software, suite integration and mechanical integration (translation).

Hardware and Software

Mainframe computers. Most readers probably remember the mainframe that filled an entire room and performed at far less capacity than today's typical PC. However, the market for mainframes continues to prosper depending on an organization's needs, and although you are more likely to find a "mainframe" in a very large company, you also might find one in a smaller size enterprise.

In a client-server based network architecture, one major decision-making point is whether to roll out a fat or thin client to the users of the proposed architecture.

"Fat clients are defined as personal computers with floppy drives, hard drives, CD-ROM drives, ability to add more memory, upgrade the CPU, expandable via cards to add more functions, and the ability to pick the operating system run on the computer," says Arnold. "A fat client then had the appropriate client driver, either ICA or RDP, as used by Citrix MetaFrame or Microsoft Terminal Services, respectively. A thin client is radically different. A thin client is like going back to the dumb terminal of the mainframe days. A thin client in its truest form does not have any moving parts, except for a cooling fan. The client operating system and required driver is preloaded on the memory of the computer."[1]

Midrange computers. Midrange computers refer to all computers falling between mainframes and workstations/PCs, and they are primarily used in a multiuser or multitask environment. It also is assumed to be used as a server in a client/server system based on a network. The midrange computer also is classified into UNIX series servers, NOS (network operating system) servers, and original OS (operating system) servers according to the OS used. PC servers, however, are not included in this classification.

Custom computers. Some companies have discovered that building a "hybrid" solution benefits them in the long run because they will have a customized solution that meets their needs perhaps better than a traditional mainframe or midrange computer. At the heart of the custom computer is storage management, application management, and server management tools that link together.[2]

---

[1]David Arnold, "Does the PC Have to go on a Diet?," http://e-redlands.uor.edu/MSITprojects/Babbage/PC%20Diet.htm, (Sept. 24, 2000).

[2]Source: Jamie Gruener, The Yankee Group.

"Today, larger storage and server vendors provide management products that manage either storage or server environments with a wall between the two environments," says Gruener. "However, large enterprises and many midsized companies continue to base buying decisions on infrastructure where administrators manage both servers and storage."

The convergence of application, storage, and server management follows broader market dynamics driven by IT executives, says Gruener. These executives realized they must stem the tide of infrastructure sprawl of servers and storage systems with better management. Eliminating mundane, manual tasks using provisioning and automation software is a growing trend in server and storage management.

PC-Based Hardware and Software

At the low end (but not less powerful or functional), there are two kinds of PC-based operating systems to consider, Network and Workstation.

Network operating systems have existed for more than 30 years, according to Bradley Mitchell of Computer Networking (www.compnetworking.com). Three of the most popular systems include Microsoft, Linux, and Novell.

Workstation operating systems are similar in nature but are designed for the stand-alone PC. Examples include Windows, Linux, and DOS.

UNIX was designed from the beginning to support networking. In its early form, Windows did not support networking, so Novell NetWare became the first popular NOS for the PC (Windows 95 and Windows for Workgroups were Microsoft's first NOS products). Today, Mitchell says any operating system doubles as a NOS based on Internet capabilities and the need to support Internet Protocol (IP) at a minimum.

A few of the latest Microsoft options in NOS include Windows NT Server, Windows 2000 Server, and the soon-to-be-released Windows Server 2003. According to Microsoft, Server 2003 provides significant improvements in performance, productivity, and security over previous versions, and provides advanced technologies for Web services and components, security, networking, Active Directory, directory service, MS Internet Information Services, and support for IPv6.

Although far less popular than Microsoft's NOS's within an organization's internal network, the Linux operating system continues to gain momentum in the marketplace, primarily because it is not "owned" by anyone and offers the source code so developers and programmers can manipulate it to use for

a variety of custom-built solutions. Linux looks and acts much like UNIX, and you can get it from a number of sources, including the official Web sites for each distribution. For example, at www.linux-mandrake.com, you will find the Mandrake distribution; at www.redhat.com you will find Red Hat Linux.

According to Linux, one Linux.com editor tried to determine the cost differential between Linux and Windows. Using the Mandrake 8.0 "PowerPack Edition," which costs $70, he configured a Windows system that costs more than $1,500 for the same components. Although there seems to be a tremendous cost savings with Linux versus Windows, users must weigh issues such as convenience and training.

The third key player in operating systems is Novell (www.novell.com), which provides a wide variety of network solutions. In existence since 1979, Novell became the de facto network standard for small business throughout the late 1980s and 1990s. Even though Novell has lost significant market share to Microsoft in this market, the company continues to remain on the cutting edge of networking by releasing new products and aligning itself with business partners. For example, in July 2001, Novell acquired Cambridge Technology Partners, an eSolutions consulting firm, to strengthen its ability to deliver both services and products to customers. The combination of Novell's industry-leading technology and Cambridge's business expertise helped Novell deliver networking solutions that help companies solve their e-business challenges.

Workstation operating system solutions for Windows include the still relatively new WindowsXP—Home and Professional Editions, and previous versions of Windows. The primary difference between the two editions is the automated built-in networking capabilities in the Professional Edition and its ability to detect any wired or wireless network without setting the connection up manually—another aspect that speaks to application integration because applications integrate with the operating system. In addition, Microsoft already has announced it will stop providing support for Windows 95 because it wants to force users to upgrade from dated systems to something that really does integrate, such as WindowsXP.

The last consideration for workstation operating systems is DOS, which some readers may consider entirely too dated compared to its successors. According to Webopedia, the term *DOS* can refer to any operating system, but it is most often used as a shorthand for *MS-DOS* (Microsoft Disk Operating System). Originally developed by Microsoft for IBM, MS-DOS was the standard operating system for IBM-compatible personal computers.

The initial versions of DOS were very simple and resembled another operating system called CP/M or Control Program for Microcomputers. Subsequent versions have become increasingly sophisticated as they have incorporated features of minicomputer operating systems. However, DOS is still a 16-bit operating system and does not support multiple users or multitasking.

For some time, it has been widely acknowledged that DOS is insufficient for modern computer applications. Microsoft Windows helped alleviate some problems, but still, it sat on top of DOS and relied on DOS for many services. Even Windows 95 sat on top of DOS. Newer operating systems, such as Windows NT do not rely on DOS to the same extent, although they can execute DOS-based programs. It is expected that as these operating systems gain market share, DOS will eventually disappear. In the meantime, Caldera, Inc. (www.caldera.com) markets a version of DOS called *DR-OpenDOS* that extends MS-DOS in significant ways.

Suite Integration

The power of application integration is illustrated through various suites of applications or products, such as Creative Solutions' Virtual Office (CSI VO). According to CSI, VO actually functions as an application service provider (ASP): Programs operate exactly as if the software were residing on your computer. However, all calculations and data are running on secure Creative Solutions servers through the Thomson Data Center. Like other typical ASPs, CSI, as the vendor, is responsible for hardware, software maintenance, and updates.

Through VO, for example, client depreciation and accounting information are linked to CSI's write-up product, which is linked to the tax return so all the data flows through. This integration would also include getting the address from the practice management system, so you would only have to make a change once.

Mechanical Integration (Translation)

Information must go through some sort of translation to be read and used across any sort of hardware, software, and suite. According to the Information Technology Portal (www.peterindia.com), middleware as a software tool provides elegant and easy mechanisms by which applications can package functionality so their capabilities are accessible as services to other applications. Middleware is able to hide the complexities of the

source and target systems, thereby freeing developers from focusing on low-level APIs and network protocols, and allowing them to concentrate on sharing information. Information in different enterprises has not been organized and formatted in the same manner. As a result, the information to be shared among applications in different places has to go through some sort of translation and conversion as it flows from one application to another.

■■■

APPLICATION INTEGRATION ACROSS THE ENTERPRISE

The most frequently cited reason for an enterprise application integration (EAI) project according to Ankur Larvia and Leo Sayavedra Jr. of the Sequence Group (www.sequencegroup.com), is to integrate disparate applications so they work together in a distributed network.

"Managers often face situations where they're charged with breaking down silos of information within or across business units," they say. "These silos often occur because of decentralization and the transfer of processing to distributed platforms. Another driver is the need to assimilate new information systems after a merger or acquisition. In addition, many companies find they need to modernize or automate parts of their business, but cannot without critical data residing in legacy systems."[3]

Key to the process is to consider process integration issues *before* the beginning of the integration process.

"All applications should support business processes," Larvia and Sayavedra Jr. say. "Often, there's a one-to-one relationship between a business function and the application supporting it. For example, one might use the report writer module of an inventory application to generate a report that's manually passed on to other departments."

Ten Keys to Successful Application Integration[4]

A March 2003 article in the *eAI Journal* by Andy Carl outlines 10 methods in dealing with application integration within your business.

---

[3]Ankur Larvia and Leo Sayavedra Jr., "EAI Business Drivers," *eAI Journal* (February 2003), pp. 27–29.

[4]Andy Carl, "10 Keys to Successful Application Integration," *eAI Journal* (March 2003), pp. 8–9.

"With so many new, exciting technology trends happening in EAI, there's a tendency to lose sight of basic fundamentals for successful implementations," says Carl, an enterprise application architect with SUPERVALU Inc. (www.supervalu.com) in Minneapolis. "Web services, Java Connector Architecture (JCA), integration server/application server convergence, and Business Process Management (BPM) are among the new trends worthy of the attention they're capturing. We should monitor these trends because each promises to add significant value, but we must remain focused on fundamentals. Sticking to fundamentals separates success and failure. Implementation is everything."

The 10 methods, according to Carl, are as follows.

1. Communicate, communicate! It is critical to communicate early and often to everyone. How well your organization understands what EAI is and its value often determines success. You need to deliver the message in waves. The first wave includes presentations to senior management on strategies, Return On Investment (ROI), and implementation timelines. A second wave includes presentations to peers in IT. You will need their support. Other waves can come after you have a few projects completed. Keep sharing your successes. Deliver formal and informal updates. Formal updates can be quarterly updates to management or weekly status reports. Informal updates can be "brown-bag" lunch presentations to many different groups. Seek out your network services, Unix, application development, and database teams to share your EAI story. These meetings are critical for building relationships and developing implementation standards. Do not limit yourself to presentations alone. Use many informal techniques to communicate your message.

2. Partner with a leader. It's easy to find product evaluation criteria and even product comparisons. Use research firms' (Gartner, Giga, Meta Group, and others) Web sites to find help in selecting the right EAI tool. Independent sources (*eAI Journal, EAI Toolbox,* and *ebizq*) also have excellent materials to help companies choose the right vendor. Partner with an industry leader. For long-term success, you will need to partner with an existing leader. One vendor might be better suited for a decentralized organization. Another vendor might have a compelling alliance with your application server vendor. Another might be better suited to an all-Microsoft shop. Certainly, pick a vendor that meets your requirements, but pick a leader. The EAI industry continues to be characterized by rapid change and consolidation. Vendors are adding new capabilities almost daily in response to new threats and opportunities. Only a few can survive the pace and magnitude of change. A short list of leaders includes webMethods, SeeBeyond, TIBCO, BEA, Mercator, IBM,

Microsoft, and Vitria. Consider partnering with one of these to mitigate the risks associated with rapid change and industry consolidation.

3. Tap internal and external talent. With the need for a centrally focused EAI competency center as a given, you should find the right staffing mix for your competency center. As with anything, a person's track record, interest level, and motivation outweigh other factors when considering candidates for your new EAI team. Aside from identifying these qualities, recruit talent inside your organization that has experience with distributed programming. This includes Java (most tools are Java-based), messaging, and databases. Distributed programming skills translate well to EAI. One of the best ways to gain credibility early is to recruit respected persons who have a history of success and solid technical skills. Do not rely entirely on shifting existing staff to your new EAI team. Supplement existing staff with partners experienced in EAI projects. Do not accept partners with limited EAI training who are looking to build their practice. Sometimes you have to challenge a consultant's background to ensure they are not fresh out of training. You need expertise to help you get started. Make it a priority to use consultants to perform project work and to share knowledge with existing staff. Make sure consultants do not work alone or handle problems without help from staff. You can use professional services for your EAI project, but these consultants are typically much more expensive.

4. Integrate with an external view. Successful business-to-business (B2B) initiatives require that you build and integrate internal systems with a view toward B2B opportunities. You want to leverage your EAI infrastructure. Do not implement a B2B connection to your enterprise resource planning (ERP) application separate from your EAI connection. Leverage the same EAI connections for B2B connections. You can use different vendors for EAI and B2B, but consider both when designing your integration architecture. Implementing BPM will be easier with a single, complete integration solution, but you can develop connections between vendors. Most tools are Java-based and have features for connecting to applications using open standards, such as Web services and Java Messaging Service (JMS), so connecting vendors is feasible. Use B2B initiatives to sell the need for a more complete EAI infrastructure.

5. Deliver and build off success. Do not try to solve your enterprise integration problems with your first integration project. Plan for doing a few projects with limited scope and high probability of success. Also, plan to use a few initial projects for building skills within your staff. Skill building is critical for long-term success. Having several wins under your belt will make your communication task that much easier. Stay focused on delivering a few

initial projects and building reliable, stable EAI processes and infrastructure. After implementing a project or two, you will be ready to tackle the larger, enterprise projects that promise to bring greater ROI.

6. Build alliances in IT. You will need help from database administrators (DBAs) and members of the network, security, application development, and architecture teams. These technical alliances are critical. Engage these groups early to define standards for implementation. To reuse design patterns for implementing adapters, you will need help. The network team needs to understand the impact of EAI traffic on the network. DBAs need to understand how database adapters affect database performance. Architecture leaders need to bless the general architectural design. EAI touches just about everything in your enterprise. If you have a data warehouse group that uses extraction, transformation, and loading (ETL) tools, you need to work with them to articulate how EAI and ETL are complementary, not competing.

7. Establish basic processes. One of the first tasks when creating a competency center is to standardize development life cycle processes and process templates. Put a stake in the ground on a set of documents that guides your EAI staff through implementation. Emphasize making your templates simple, understandable, and usable. Try to resist the temptation to excessively engineer, especially with your first few projects. Your EAI process should jive with processes already used in other areas. If your IT organization operates at Software Engineering Institute (SEI) level four, then begin with level four-like processes. If you need to migrate to a more robust process, do so after starting out simple and small.

8. Use metrics. In addition to process standards, you need to consider metrics. First, measure your processes. You need to understand how long integration development takes and how much of the total effort is development or testing, or design or other key tasks. Having metrics on processes facilitates estimating future integration projects. Second, measure transaction volume. This includes the number of transactions and number of bytes. This metric helps indicate to management how much the EAI environment is being used and by whom. If you charge back to departments in IT for services, this metric is critical. Get started with metrics and adjust along the way. The results of your measurements will help provide visibility to others about the scope of EAI.

9. Build reusable adapters. Keep adapters simple and reuse standard approaches across many systems. For every company using SAP, PeopleSoft, Siebel, and i2, there are many more who do not. The biggest challenge for most companies starting out with EAI is connecting legacy applications to the EAI hub or bus. Legacy is not just mainframe applications, but all applications

(package and internally developed) without open standard application program interfaces (APIs). By this definition, we all have lots of legacy applications. Do not develop a unique adapter for each unique application. Identify common patterns across many applications and start with basic adapter solutions that meet common requirements. Start with simple, reusable adapters and evolve into more complex adapter implementations as your EAI "business" grows.

10. Monitor trends. Even though the focus here is on fundamentals and keeping things simple, you also need to follow new technologies and understand the implications to your industry and company. Build a foundation with basic, repeatable processes, templates, and code, but think strategically as you act tactically. Follow trends in Web services, JCA, .NET, and Java 2 Enterprise Edition (J2EE) development platforms. Web services hold promise to make application connectivity a commodity, rendering proprietary broker adapters useless. JCA could standardize J2EE-compliant application connectivity. Consider also the trend of application server vendors providing integration broker capability. BEA and IBM are taking steps in this direction. These trends will define EAI in the next few years. (See Exhibit 3-1 for more resources.)

■ ■ ■

INDUSTRY EXAMPLES

The Deutsche Bank Group—Vitria[5]

With a $680 billion investment and banking business, branches in more than 60 countries and more than nine million customers, the Deutsche Bank Group had multitudes of computer applications to integrate. The Frankfurt, Germany-based company wanted real-time communication of independent order management applications, distribution systems, consolidation of IT infrastructure management to one location, and implementation of an e-business platform that would handle high volumes of transactions.

To meet the company's needs, it turned to Vitria (www.vitria.com), which worked with the Deutsche Bank Group to produce a proprietary program, called dBus. The program combines Vitria's BusinessWare, and Java and C++ for the management application system. BusinessWare was chosen because of its e-business platform that can publish and subscribe messaging technology, and provide secure and reliable date communications.

[5]Source: The Deutsche Bank Group, www.db.com.

This solution allowed the company to tie together various order management applications and support systems, give traders global access to real-time buy and sell information, and provide completed trading records, 24/7, to the proper divisions.

Among other benefits, the new system saved money on system support and maintenance because it is centrally located and has improved company-wide distribution of securities information. Also, the dBus has reduced the need for new software and hardware system-wide.

Tenet Insurance—WRQ Verastream[6]

Tenet Insurance Co. LTD managers knew they needed to go to a Web-based system to provide better internal and external customer service. The switchboards were jammed with callers who needed help, and when callers finally *did* reach a customer service representative, they had to wait for their answers.

There was one big problem: how to combine a new Web system with old legacy programs that contained all the critical data. To solve their problem, managers of the subsidiary of Hwa Hong Corp. went to WRQ (www.wrq.com), providing them with Verastream that linked the old and new systems together.

Verastream serves as a conduit, allowing terminal-based legacy applications to "talk" to any other system, including Web-based ones. The way it works is the system sees the different applications as interchangeable components that can be mixed or matched. So, all the developers need to do is mix and match the right applications for their system, with no need to rewrite code or type in data.

The new Tenet system now handles everything from quotations to policy insurance. They even programmed underwriting rules directly into the Web application. Now, customers will find that their calls are answered more quickly and the person on the other end of the phone has easy access to quotations for insurance policies, are able to generate proposals and submit policies, print policy schedules, and search for policies and claims.

Tenet, formerly the Hartford Insurance Co. (Singapore) LTD, also has seen incoming calls and operating expenses decrease because customers can go to the Web for self-service. In addition, when customers call in, customer service has better tools to help them with.

[6]Source: www.tenetinsurance.com.

CSC Enterprise Application Integration[7]

A major North American wholesaler and distributor was on a tight deadline to implement new order management, financial, and warehousing systems, according to CSC. But developing the typical point-to-point interfaces required linking the new systems to the company's old legacy system. The company feared it would take too long and be too costly.

CSC proposed that the company go with an alternative: an enterprise application integration solution (eAI). CSC reports that eAI reduces costs, connects front-back offices, integrates ecommerce transactions and creates better customer satisfaction.

For the wholesaler, a proof of concept was quickly done, two representative interfaces were constructed and the demonstration was done within a week. The data from the old system now could flow into the new systems. Because the project was so successful, the wholesaler plans to use it as it begins implementing new merchandising and e-commerce systems, says CSC.

Some of the savings included cutting down on implementation time and costs for integrating the system. eAI also provided the necessary security, monitoring, and notification that the company desired. At the same time, the company was able to meet its e-commerce requirements.

■■■

CASE STUDY[8]

eonBusiness Corporation develops Internet strategies through Web site design, Internet marketing, electronic commerce, database integration, and hosting services. Recently, it developed an application integration solution for Colorado Intergovernmental Risk Sharing Agency (CIRSA) (www.cirsa.org).

Situation

CIRSA provides property/casualty and workers' compensation to more than 100 member Colorado entities (cities and municipalities) across the state. Before eonBusiness' involvement, CIRSA only processed renewal applications digitally through CD-ROMs sent by regular mail or on paper by fax, methods that were time-consuming and costly for both member municipalities and CIRSA because several man-hours were required for each

[7]Source: www.csc.com.

[8]Source: www.eonbusiness.com.

application processed. More hours and overhead were required for renewal applications confirmations, deductible quote requests, and other member questions.

CIRSA wanted to implement an online renewal application that would allow members to log into a secure site and instantly request deductible quotes, update employee payroll information, enter asset valuations, and submit renewal property/casualty and workers' compensation applications with no recurring overhead processing costs.

CIRSA desired a six-month project timeframe, from initial system requirements documentation to the date of the site to go live. In addition to full system functionality with multiple database integration, CIRSA members needed full documentation and training in the new Web-based renewal application.

Solution

eonBusiness created a professional, multifunctional site for CIRSA. The site design included a database-driven insurance renewal section that allowed various entities to renew their property/casualty and workers' compensation coverage completely online. The coverage renewal application process allowed new deductible quotes to be obtained by more than 100 member entities, allowed property and asset values to be compared and updated from previous years, and allowed customized PDF reports to be printed by each member.

The eonBusiness-designed system enabled members to enter and save individual information into the database before official renewal application submittal, and to easily track the completion status of all 10 sections of the application for each member. In addition, full shopping cart functionality for member purchases of training videos and instructional manuals became available. Each password-controlled member interface contained dynamic content of pertinent news, official information, and membership data.

CIRSA estimates that providing these coverage renewal applications in a Web-delivered environment significantly reduced previous CD-ROM distribution costs, and increased member satisfaction through greater interaction on coverage quotes and property value estimations.

Key Functionalities

Functionalities include the following:

- Dynamic database-driven content
- Complete online insurance application submission and notification processes

- Password-controlled member and employee account interfaces
- Dynamic, custom PDF report-printing capabilities
- Secure electronic commerce
- Fully integrated shopping cart functionality
- Training video and instructional manual download links
- Online application help content
- Dynamic news and information updates

EXHIBIT 3-1: RESOURCES

- *The eAI Journal* (www.eaijournal.com) is an electronic magazine devoted to application integration issues, trends and opportunities.
- "Predictions on Application Integration & Middleware" (www4.gartner.com/1_researchanalysis/rc/b2/b2_main.jsp) is an article for 2003 by David McCoy.
- Bitpipe IT Research (www.bitpipe.com) has quite a bit of aggregated information on application integration. Search for "Application Integration" in the search field.
- Computer Sciences Corporation has a site devoted to application integration (www.csc.com/solutions/enterpriseapplicationintegration/index.shtml) with case studies, white papers, and more.
- Microsoft (www.microsoft.com) offers a keyword search for "application integration" that generates many articles and resources.

Web Services

chapter 4

The power of cyberspace is amazing. Just a few years ago, manual processes that took hours to complete now take a matter of moments, thanks to the integrated world of the Internet and our connected world. Business professionals no longer look at the Web as a means to an end; it has become a necessary tool with which to conduct internal and external business, while maintaining almost instantaneous communications with clients and customers, employees, partners, and vendors.

In general, Web services encompass applications that use the Internet as their infrastructure and access tool, including both Web-enabled and Web-based applications. Examples include Java applications, Microsoft's .NET initiative, application service providers (ASPs), and business portals.

According to CyberAtlas,[1] there are somewhere between 580 million and 655 million worldwide users of the Internet in 2003, and in 2004, CyberAtlas expects this figure to increase to 709.1 million to 945 million. In the United States alone in 2003, there are 122.2 million Internet users through 7,800 Internet service providers (ISPs).

Although these numbers clearly demonstrate our dependence on the Internet as a communications tool, the way Web services are used to increase a firm's or company's service delivery is key. In March 2003, Forrester Research Inc. founder and chief executive officer (CEO) George Colony publicly announced that Web services will be the next big thing in IT: "A new technology thunderstorm hits every five to nine years and we are due one now." It is not surprising, then, that the accounting profession already has discovered numerous ways to incorporate Web services into its environment. (See Exhibit 4-1 for additional resources.)

THE TECHNOLOGY THAT MAKES WEB SERVICES WORK

Several core protocols make up Web services, including XML, SOAP, UDDI, WSDL, and WSCL. In layman's terms, think of these protocols as the innards of a telephone system: SOAP is the dial tone, UDDI is the telephone book, WSDL/WSCL is the conversation, and XML is the communication medium.

- eXtensible Markup Language (XML). XML is a markup language for documents containing structured information. Structured information contains both content (words, pictures)

[1]Source: www.cyberatlas.internet.com.

and some indication of what role that content plays. For example, content in a section heading has a different meaning from content in a footnote, which means something different than content in a figure caption or content in a database table. Almost all documents have some structure. A markup language is a mechanism to identify structures in a document. The XML specification defines a standard way to add markup to documents. Note that XML should not be confused with XBRL (eXtensible Business Reporting Language) (www.xbrl.org), an extension of XML.

- Simple Object Access Protocol (SOAP). SOAP is an XML-based mechanism that bridges different object models over the Internet and provides an open mechanism for Web services to communicate with each other. This process provides a way to create widely distributed, complex computing environments that run over the Internet using existing Internet infrastructure.
- Universal Description, Discovery, and Integration (UDDI). UDDI creates a platform-independent, open framework for describing services, discovering businesses, and integrating business services using the Internet. It also creates an operational registry. UDDI is a comprehensive, open industry initiative enabling businesses to discover each other, and define how they interact over the Internet and share information in a global registry architecture.
- Web Services Description Language (WSDL). WSDL provides a model and an XML format for describing Web services. It separates the description of the abstract functionality offered by a service from concrete details of a service description, such as "how" and "where" that functionality is offered.
- Web Services Conversation Language (WSCL). WSCL allows the abstract interfaces of Web services, such as the business level conversations or public processes supported by a Web service, to be defined. WSCL specifies the XML documents being exchanged, and the allowed sequencing of these document exchanges. WSCL conversation definitions are themselves XML documents and therefore can be interpreted by Web services infrastructures and development tools. WSCL may be used in conjunction with other service description languages like WSDL to provide, for example, protocol binding

information for abstract interfaces or to specify the abstract interfaces supported by a concrete service.

DIFFERENCES BETWEEN WEB-ENABLED AND WEB-BASED APPLICATIONS

A cook does not necessarily want to know the science behind what it takes to make a recipe, so as with other aspects of technology, many business professionals may not want or even need to know the architecture that encompasses Web services technology, let alone detailed descriptions of acronyms such as SOAP, XML, and others. However, any lack of knowledge is not necessarily detrimental to those using the technologies as long as the users are able to conduct the business they want, anytime and anywhere—two of the promises fulfilled by Web technologies.

At the heart of Web services are Web-based and Web-enabled applications, and even though they might sound the same, they really are very different.

Web-based applications bring universal access to applications and data through your Web browser. The three most common browsers are Internet Explorer, Netscape, and Mozilla. There also are several other, lesser-known browsers with unique functionality, including Opera and NetCaptor, as well as a few offered by popular, name-brand providers such as Yahoo! and Google.

However, Web-based applications involve much more than just a way to access a Web page because they offer a significant change in the software model. Most professionals are used to loading off-the-shelf, packaged software on their PCs, but what if you are not at your PC and still want to conduct business? In 2003, moving practical applications from the desktop to the browser is commonplace. Designed and developed for exclusive use on the Web, the real-world magic of Web-based applications provides the foundation for a complete, seamless integration of technology-supported processes between business partners and customers, and employees and managers.

Web-enabled applications also allow us access to business data through a Web browser, but that is where the similarities end. From the underlying technology to basic structure and functionality, Web-enabled applications run *within* a business and are accessed through a firm or company's virtual private network (VPN) or in a Citrix/WTS (Windows Terminal Server) environment.

Web-based applications "are built from the ground up to run over the Web. Web-enabled applications, on the other hand, involve adding a Web

interface to traditional applications that may have been created even before there was a Web."[2]

Carr says to imagine an order entry system that runs off a mainframe and is used by your in-house customer service reps. Web-enabling it will allow customers to order over the Web through a browser. The business still must maintain the same software running on the old mainframe; you would just have a new way to enter information.

"Think of Web-enabling a legacy application as giving a bald man a toupee," she says. "He's still a bald man under the 'rug,' but when he's got it on, he looks like he's got hair. You can't grow it or feel confident that it'll stick in a wind storm, but it gets the job done. As for the guy with the full head of hair, think of him as Web-based. When winds shift and styles change, that hair can—and will—adapt."

Web-enabled applications often are used within a company to broaden access to an old application trapped on a mainframe—better known as a "legacy system." By putting a Web browser on the front end of an old application, you can make it available to more employees and customers, a more cost-effective solution than completely replacing it with a reengineered Web-based system. However, there is a tradeoff: If the legacy application is complex, it may not be economically feasible to build Web hooks into more than its most basic functions because the conversion rate either would take too long or the technology would be too burdensome. As a result, efficiency lags.

Web-based applications and their data files reside on Web servers, usually in some other physical location, instead of on an individual's desktop. Many ASP providers also support Web-based applications, because daily responsibilities—including security, back-ups and upgrades—are centralized. This makes an organization's technology management tasks more efficient and cost-effective.

Three ways to identify whether you are using a Web-based application include:

1. You can gain access, and interact with the application and your data, via a browser from *any* computer or access device.
2. When you can see personal or company data, you can update or send the data to another program.
3. Once you've entered new data, you can instantly view the updated information.

[2]Kathleen S. Carr, "What is a Web-Enabled Application?," *Darwin Magazine*, www.darwinmag.com (Jan. 17, 2002).

One of the more popular ways professionals are using Web-based applications is through Web-based e-mail, and with the ready availability of dumb or stand-alone, fee-based terminals and wireless networks at airports, coffee houses, and other public venues, accessing e-mail and the Web while out of the office (and at home if you telecommute or work from home part of the time) is easier than ever. In addition to e-mail, a large number of vendors provide Web-based business and "virtual" workspace tools. Some of the more sophisticated Web-based accounting and business application vendors are now mainstream, including Netledger (www.netledger.com), Creative Solutions (www.creativesolutions.com), and Best Software (www.bestsoftware.com).

From Best, MAS 90/MAS 200 and MAS 500 offer solutions for integrating the enterprise resource planning (ERP) system with electronic storefronts. For example, DTC Stage & Studio Supply in San Francisco was losing money by printing up thousands of catalogs for their 35,000+ rental items. They used the MAS 200 eBusiness Manager to link inventory management and ordering systems with their electronic storefront, and as a result, customers can choose from all 35,000 inventory items online. As evidence of bottom-line cost savings, DTC no longer had to spend money printing up thousands of huge catalogs.

Also from Best, Peachtree Web Accounting and Peachtree WebsiteCreator Pro/Peachtree Website Trader are available as add-ons to Peachtree Complete Accounting. Peachtree Web Accounting enables small businesses to take their general ledger, reports, inventory, and customer lists from within Peachtree Complete Accounting and post that data to a secure Web site. At the site, users can remotely access data, make changes to it, and synchronize that updated information with their information in Peachtree Complete. In addition, users can build a Web site, take orders from that site and bring the orders back into Peachtree for processing. Because the programs are integrated, there is no need for rekeying data, and users actually can upload their catalog from within Peachtree to their Web site.

Best also offers TimeSlips, a popular accounting time and billing software program. TimeSlips' eCenter is a blended ASP that allows its customers to track their time remotely, then synchronize that information with Timeslips in their office. The eCenter also is helpful for businesses who have some employees on Macintosh computers and others on PCs; those on Macs can use eCenter, which will, in turn, interface with Timeslips on the PC.

Another example within accounting is illustrated by RIA from Thomson.[3] While at the client's office, tax professionals can look up this year's FICA limit by accessing RIA's Checkpoint tax research product from any computer with a Web browser and Internet connection. RIA's GoSystem Tax RS (remote server) Web-based product offers tax return preparation from the office, home, or client's offices.

The landscape has certainly changed, and ASPs have played an integral role in spurring Web services. In 2001 for example, The *CPA Software News* reported that its first review of Web-based accounting products the year before featured only three products: "This [year's] review started out with eight products, with one company going out of business before the review went to press. This gives you some perspective on the tremendous growth (and volatility) of this emerging technology for business. The ASPs that have been around for more than a year are 'old timers' already, with most on their fourth or fifth major software release."[4]

When shopping for an ASP, the *CPA Software News* says you should consider the package's features, stability, performance, and implementation details. "Most of the products that offer monthly subscription-based services base the monthly fee on accessible modules or features. With this setup, you can start with only the functions you need and later add access to other modules as your business grows. Company stability is also important as you will invest a considerable effort converting your existing data and learning the new package. Most of the packages offer data conversion from QuickBooks (for example), but in the event the company discontinues the product, the conversion to another package may be very difficult."

WHAT DRIVES WEB SERVICES

The development of Web services has been driven by the desire to create more interoperable computing assets, combined with a standards-based way to describe and share those assets.[5] Web services provide a standard way to expose application interfaces through XML and WSDL, and rely on a standard way to communicate (SOAP). These features help enterprises to

[3]See www.riahome.com.

[4]Brent Dirks, "Web-Based Accounting Primarily Geared Toward Small Business Users," the *CPA Software News* 11, no. 3 (June/July 2001).

[5]Boris Lublinsky and Michael Farrell Jr., "10 Misconceptions About Web Services," *eAI Journal* (February 2003), pp. 30–33.

integrate disparate systems faster, reduce the cost and complexity of integration and development of new applications, and more easily roll out new and timely goods and services that rely on corporate computing assets.

According to the *eAI Journal*, there is room for growth as standards continuously mature. Vendors and organizations will be more confident with regard to their investment in the technology. In particular, professionals also have heard announcements indicating how the standards relating to Web services are unifying and evolving to address security concerns, transaction control, and business processes and workflow elements. Development tools and environments also are maturing to give applications and interfaces increased capabilities.

Recently, Microsoft (www.microsoft.com), IBM (www.ibm.com), BEA Systems (www.bea.com), and TIBCO Software (www.tibco.com) announced the publication of two new specifications to enable organizations to build reliable, interoperable Web services applications. The new specifications, WS-ReliableMessaging and WS-Addressing, along with a high-level road map written by IBM and Microsoft called "Reliable Message Delivery in a Web Services World: A Proposed Architecture and Roadmap," describe a common architecture comprising the necessary protocols, message formats, and interfaces to enable reliable message delivery for Web services.

According to OpenEnterpriseTrends.com, Web services are on track to make some significant inroads in 2003, especially as vendors put aside costly rivalries and find techniques to set cross-platform standards and other ways to "just get along."

The same source also reports that political skirmishes between the Java and the Microsoft camps also seem to be quiet—at least for now. "By the first quarter of next year, Sun will be on the board of the WS-I (Web Services Interoperability Organization), and that will bring Microsoft, IBM, BEA, and Sun all together under one organization."

Bob Sutor, Ph.D., director of Web Services Strategy for IBM, says, "Two-and-a-half years into the evolution of Web services, the hype surrounding this technology has become *deafening*. The good news is that developers are already finding that Web services technology is starting to pay early dividends for some companies. While the big payoff is still two or three years down the road, considerable momentum is building in the standards communities, and in tools and language development, to empower developers to make Web services the standard for doing business with customers, suppliers and partners."[6]

[6]Source: IBM.

MICROSOFT'S .NET INITIATIVE

The panacea that was Microsoft .NET does not seem to be as popular as it was hailed to be several years ago. While Microsoft has continued to concentrate its efforts on new versions of the Windows operating system, it also maintains that the .NET revolution still is coming.

One vendor of accounting base software, Comtech Solutions[7] in Houston, is banking on this revolution, according to Gary Harrison, vice president of product development. Even though .NET has had its share of skeptics, Harrison believes the fact that Microsoft has worked on .NET since 1995, and put time, money, and effort into the platform is evidence enough of the company's commitment to meet industry expectations.

"Microsoft designed .NET as the next generation Windows," he says. "We know that they would start programming on changing .NET *now* if they were to change directions rather than to just keep perpetuating the idea."

Harrison says Comtech chose to program its Adept Financials .NET product in the .NET platform because it is a base of a protocol for companies to communicate financial applications.

"Computers have done a great job of making companies more efficient; there is no comparison between companies operating several decades ago and the ones that are operating now. .NET helps manage our business more efficiently. It is designed so that it doesn't make a difference which financial application a company is using. For example, you could seamlessly send orders from one company to another."

The .NET framework replaces the Windows engine, and Harrison says it is far more stable than the traditional Windows program. An important distinction is that .NET is not running on Windows—it replaces Windows. For example, if you use Microsoft Word, parts of Windows are shared among many programs. If you install Word, it replaces parts of Windows with newer DLL. Anyone who has received general fault errors immediately will know what Harrison is talking about.

"Eventually, your system all comes crashing down because when you uninstall something, the more it overwrites," he says. "With Version 1.0 .NET, one framework is common to all programs. Microsoft controls this and we (the developers) write to this framework. Any .Net program is just as stable as another because it all works from the same common space."

[7]Source: www.comtech.com.

CASE STUDY: FORWARD AIR—APPFLUENT TECHNOLOGY[8]

Legacy systems that need updating are still a common problem among today's businesses. Companies are missing out on the significant benefits that stem from the ability to make quick decisions based on real-time business information because of associated infrastructure cost and complexity, according to a survey conducted by Appfluent Technology, a provider of infrastructure software to enable real-time business intelligence.

The December 2002 online survey was completed by 210 U.S.-based companies of all sizes and industry sectors, and more than half of the respondents were from large to very large organizations. Participants held jobs in either business or IT management. The survey's key findings include:

- Almost two-thirds of respondents listed infrastructure management and maintenance as "major pains" in deploying business intelligence systems. Another 60 percent named data freshness and quality as significant headaches.
- Seventy-five percent said their company would benefit from the ability to make quick decisions based on access to real-time information. Of that group, almost 40 percent indicated that benefit would be "significant."
- One in five organizations need fresh, up-to-the-minute business information data, one in 10 need it hourly, and 35 percent need fresh data daily.
- More than half of respondents are likely to implement an intelligent operational data store (ODS) solution to enable real-time business intelligence in their organizations to reduce the cost and complexity of managing multiple data sources for BI reports and analytics.

Recently, Appfluent offered a Web-based solution to Forward Air. When Forward Air managers faced the need to buy new computer hardware to better service and track their trucking and warehousing clients at 80 locations in the United States and Canada, they went to Appfluent for a different Web-based solution. Forward Air decided to use the company's Accelerator system, which off-loads reporting traffic from the production databases.

[8]Source: Appfluent Technology, at www.appfluent.com.

The Accelerator system allows the data to be analyzed daily on separate computer hardware, without taxing the entire system, says Steve Tucker, director of Development and chief technology officer. The reports are important to increase revenue for Forward Air, which does about $250 million in yearly business shipping and warehousing mostly heavy freight, such as computers.

Accelerator, according to Appfluent Technology, comes fully turnkey, with all the software and hardware needed and has been tested with Crystal Decisions, Cognos, Business Objects, and Microstrategy applications.

The move to Accelerator at Forward Air will delay the need for $500,000 of new computer system for another year or year-and-a-half, Tucker says. And, they plan to continue using Accelerator when they buy a new system because they have been so pleased with the performance.

Forward Air has been able to run daily reports for staff—especially sales staff, who use the data to pitch more jobs. This has created greater efficiency, says Tucker. Each month about 1,700 reports are run. Eventually, Forward Air will also use Accelerator to speed up the customer-accessible online tracking system of the 25 million pounds moved weekly.

CASE STUDY: MCDONALD'S—APIGENT ZEOM[9]

When McDonald's needed a Web-based system to integrate its back-end systems, it decided to buy out Apigent for its Zeom technology, says Jim Melvin, past chief executive officer (CEO) of the company and now CEO of SIVA, another technology company in South Florida. Melvin says the technology is attractive because it can link many systems at fast food and casual restaurants. Some of the systems that can feed into the Web platform are inventory, labor time and attendance, scheduling, point of sale, and speed of service.

Melvin says without technology such as Zeom, companies must buy new systems to homogenize their technology—a costly endeavor, especially for big franchises. Typically, a new system would cost $15,000 to $25,000 per store for an Arby's-sized business and $75,000 for a restaurant such as TGI Friday's, Melvin says. "The purpose is to integrate different systems that are out in the field into a common set of data or numbers . . . and bring them back up into a unified accounting system."

[9]Source: Sangoma Technologies, at Sangoma.com.

This is done by connecting the various sites of business to a common point, which turns information into XML format that then can be transmitted to the appropriate reporting site. As a result, management can consistently analyze results from all stores. Melvin says that McDonald's plans to continue selling the software to other restaurants.

EXHIBIT 4-1: RESOURCES

- The Stencil Group (www.stencilgroup.com) offers a collection of white papers, presentations, newsletters, and other articles on Web Services.
- IBM (www-106.ibm.com/developerworks/views/webservices/articles.jsp) has a collection of technical and nontechnical Web services articles.
- *Web Services Architect* (www.webservicesarchitect.com) is an independent online journal dedicated to the concerns of technical professionals designing systems based on Web Services.
- Developer.com (www.developer.com/services) offers articles, discussion groups, tutorials and other resources for Web services. Much of the information at this site is highly technical.
- The O'Reilly Network (http://webservices.xml.com) has links to a variety of articles, papers and discussions about Web Services, particularly XML (www.xml.com). The specific page for Web services articles is www.oreillynet.com/pub/q/all_webservices_articles.
- CPA2Biz (www.cpa2biz.com) has an article called "Have Browser, Will Travel" in its Information Technology Resource Center, Top Techs, under "Applications 2001."
- Microsoft .NET (www.microsoft.com/net) is the home page for .NET technology.

Disaster Recovery

chapter 5

We live in an uncertain world where natural and man-made disasters strike, often at random with no forewarning. Wherever these disasters may strike—and they do occur regularly—organizations are affected. Unprepared firms and companies risk losing everything, while those that have adequate contingency plans are able to recover from the disaster, and continue to service their customers and clients.

UNDERSTANDING DISASTER RECOVERY

A business continuation plan is really a simple method to anticipate a disaster, and yet, many companies and organizations cannot seem to understand the tremendous risk involved. A business continuation plan requires the development, monitoring, and updating of the process by which organizations plan for continuity of their business in the event of a loss of business information resources due to impairments. These impairments include theft, virus infestation, weather damage, accidents, and malicious destruction (includes business continuation and contingency planning).

As businesses rely more than ever on computer technology, the impact of a disaster on this technology is having a more profound impact on an organization's ability to conduct business. You may find the following interesting:

- One in three U.S. businesses would lose critical data or operational capability if a disaster occurred, unless investments are made immediately toward disaster preparedness planning.[1]
- According to Gartner, less than one third of small to medium-size enterprises have comprehensive disaster recovery plans, while only 10 percent have contingency and business recovery strategies. In addition, two out of five enterprises that experience a disaster go out of business within five years.[2]
- Ninety-three percent of businesses that lost their data center for 10 days or more filed for bankruptcy within one year of the disaster.[3]

According to the Gartner study, the main reason cited for *not* having a plan was cost. The difficulty in getting organizations to allocate appropriate

[1]Gartner Dataquest Survey, www.gartner.com (March 4, 2003).
[2]"A Recipe for Disaster," *Computer Reseller News* (May 2002).
[3]National Archives & Records Administration, Washington, D.C.

resources to the development of their disaster recovery plan is that many take their current situation for granted, feeling that "disasters happen to others." These organizations must realize that they are much more likely to be affected by a local emergency or partial loss of service than a full-scale disaster, and that the development of a business contingency plan will help them prepare for many of these smaller scenarios as well, making the organization stronger and more effective. Even though disaster recovery is the title of this chapter, the terms *business continuity planning, contingency planning,* and *emergency response* will be used interchangeably.

To justify the time and cost to develop a disaster recovery plan, it is important for the organization to understand the cost of downtime associated with an emergency. The organization should determine the financial impact if it is unable to provide products and/or services for a period of hours, days, or even weeks. Black and white financials are very helpful in helping the team justify the cost of development and counter measures to the owners and board of directors.

A variety of free Internet tools estimate the cost of downtime in an organization; just try doing a search on "downtime calculator." You'll find some of the following (as of April 2003): HP (http://h18005.www1.hp.com/services/advantage/aa_cod_calc.html), Mimix (www.mimix.com/solutions/DowntimeCalc.asp), Boston PC Networking (www.bostonpcnetworking.com/downtimecostcalc.htm), Data Processing Air Corporation (www.dpair.com/downtime2.htm), and Scientific Software and Systems Inc. (www.sss.co.nz/services/downtimepage.htm).

To develop a disaster recovery plan, an organization must first designate a disaster response team, and provide team members with the authority and funding to complete the plan. This team will be responsible for documenting the current infrastructure and preparedness, as well as doing a business impact analysis that highlights the threats and possible responses to those threats. Finally, the team must catalog this information so it forms a comprehensive document that will serve as guidance in the event of an emergency. These steps are detailed in this chapter.

DEVELOPING THE TEAM

The responsibility for seeing that the organization has a business continuation plan lies with its owners and the board of directors. They should designate appropriate personnel, allocate the needed time, and approve adequate financial resources to develop the business continuation plan. The

organization must designate an individual with the primary responsibility of developing and administering the plan. An alternate or backup also should be designated in the event the primary leader is unavailable. The role of the team leader is to act as a liaison with owners and directors, and should have authority to invoke the plan and direct other team members. Once a leader is selected, team members should be formally designated to be responsible for the various functional departments within the organization in the event of an emergency. Other personnel that should be considered for the team would be the individuals in charge of five areas:

1. *Operations* determines the staffing for meeting the needs and requirements of clients and customers, and coordinates the organization's primary production or delivery services.
2. *Facilities* evaluates the worthiness of the entity's current physical location and coordinates repairs as needed. If necessary, the facilities team member locates and develops alternate locations, and coordinates the logistics of moving to that location.
3. *Communications* coordinates the efforts to restore telecommunications and network and Internet access to the organization.
4. *Network systems* stabilizes the computer infrastructure or rebuilds the system from tape backups if necessary.
5. *Administration* manages accounting, payroll, and the internal resources to resume operations in the aftermath of an emergency.

The team leader also would be the liaison with the media and local civil entities, including the police, fire department, and emergency response teams. Although the size of the team depends on the size of the organization, involving people from various departments ensures that a complete and thorough approach is taken. In addition, it distributes the workload and provides communication channels to and from the various departments. This team should formally be given the responsibility of developing the plan with a budget and timeline determined by the owners and board of directors.

DEVELOPING THE FOCUS

Before developing the business continuity plan, the organization should focus on *why* it exists, the customers and clients it serves, and how it services them. Time should be spent determining the extent to which its customers and clients rely on the organization, and the expectations of service they expect. This focus will help the organization rank according to priority the

functions that are of primary, secondary, and tertiary concern, and help determine the financial ramifications of developing the business continuation plan.

To help garner acceptance for the development of the plan, the team also should emphasize the benefits of developing the plan. In many industries (such as financial) the development of contingency plans are required by law. Having a well-documented, tested plan also can reduce insurance premiums, because it demonstrates to the insurer that the organization is serious about minimizing its risk. Presenting the plan to the organization also can have a positive impact on employee morale, because it provides assurance that the company is doing what is necessary to protect them and their jobs.

DOCUMENTING THE CURRENT INFRASTRUCTURE

After the organization documents its primary service or product focus, and develops a prioritized list of functions and services, it is time to understand the current status of the group's disaster preparedness. A good disaster recovery plan begins by documenting the current organizational structure; layout of facilities and the network/communications infrastructure, including the hardware, applications, and data; and any data backup and existing business contingency plans already developed. Here are examples of the types of information that may already exist within the organization.

- *The business organization chart* includes the contact information, authority, and responsibilities of the members of the organization's disaster response team.
- *The facility analysis* encompasses architectural drawings, including doors, windows, staircases, a layout of the security system, the location of fire suppression equipment, first aid kits, backup media, servers with critical information, and information stored on alternate sites. All water, electrical, and gas mains and shutoffs should be included.
- *The network infrastructure* includes a detailed listing of all computer and network hardware, routers, switches, UPS (uninterruptible power supply) devices, power coverage, and other items, including every serial number. If the list is properly designed to include information such as vendor, in-use date, and asset identification tags, it can be used for insurance and depreciation purposes (or derived from existing documents).

- *The software/application licenses document* includes all applications on the network (capitalized and expensed), including vendor, version, and number of licenses. Vendor contact information and instructions, phone numbers, and hours of operations should be included. For custom applications, special attention should be taken to ensure that backups are made and tested, and any system or operating modifications made also are documented.
- *The data backup procedures* document and test the backups to ensure that all information is being backed up and stored off-site, and that the tapes are valid. The location and access information for the backups should be included, as well as the software/hardware used to make the backup.
- *The communications infrastructure* includes all dial-in and Internet connections, VPN connections to related entities, and business partners.
- *An existing service and product providers listing* should be maintained by organizations to have a centralized location for names of their current service and supply vendors to run their business. Many organizations keep this information within their groupware application (Outlook, Lotus Notes, Novell GroupWise) that can be synchronized to handheld personal digital assistants (PDAs—Palm or PocketPC, for example). In an emergency situation when something must be shipped immediately, having access to the organization's overnight delivery accounts can expedite the situation. Alternate service providers also should be incorporated into this list.
- *The existing documentation* should be reviewed. The team should check any existing policies and procedures for their impact on, or contribution to, the business continuation plan. Employee manuals may already have policies in security procedures, safety programs, environmental standards, and a description what to do in the event of an emergency.

This listing should also include contact information for critical support and response groups, including the police department; fire department; hazardous materials response team; poison control center; local hospital; urgent care and ambulatory service providers; security services; utilities, including telephone, power, and gas; and insurance company. Another component is the contact information for all personnel, including addresses, home/cellular

numbers, and emergency contacts. A word of caution: The organization must consider privacy concerns when determining who has access to this detailed contact information, as well as the documents described above.

PERFORMING THE BUSINESS IMPACT ANALYSIS

The next phase in the development of a disaster recovery plan is performing a business impact analysis. The organization must assess threats and vulnerabilities, and the likelihood of each occurring, as well as the possible financial impact. Threats usually fall into four categories: natural, accidental, man-made or technical.

Natural disasters are usually caused by weather, such as storms and flooding, or disruptions caused by earthquakes. These disasters often lead to power outages and can cause physical damage to facilities. Organizations must assess the probability of each threat occurring, determine the possible impacts, and what insurance or preparation is needed to mitigate them.

Natural disasters in one area can affect businesses in a completely different part of the country. For example, application service providers (ASPs) that lose power and communications capabilities due to freezing rain taking their lines out, will affect any businesses dependent on that provider.

Man-made disasters include theft, vandalism, acts of war and terrorism, and emergencies caused by misuse or accidental destruction of information in systems and directories caused by employees, computer hackers, and viruses. Many of the considerations and resources to minimize these types of disasters affecting computers are discussed in Chapter 1, "Information Security," and Chapter 7, "Intrusion Detection."

Accidental disasters include fires, water leaks, hazardous material spills, and loss of power due to storms, or an accident involving a power delivery system. Incidentally, power outages cause a significant portion of the "data emergencies" that affect organizations. According to one survey, power outages accounted for $26 billion in damage in 2002 alone. American Power Conversion, a maker of UPS and other power protection systems, has an online power availability rating tool that can help organizations respond accordingly to power issues.[4]

Finally, *technical disasters* are related to systems issues, such as failure of a server, individual workstation, or any equipment on the network that

[4]See www.apcc.com/tools/availability.

inhibits employees from completing their work responsibilities. This also includes software upgrades that go bad, making an application inoperable or data unusable.

Organizations should consider these four threats and include any situation that partially or completely eliminates the organization's ability to conduct business in their facilities. Scenarios within each category should be listed. Here are some examples.

- Prohibited access to the building (caused by gas or chemical leak)
- Extended power outage (caused by accident or torrential weather)
- Extended network/Internet access loss (caused by weather or bankruptcy)
- Partial Loss of equipment (whether by theft, vandalism, or fire)
- Complete loss of facilities (fire and resulting smoke and water damage)
- Structural damage or injuries to individuals caused by hazardous material spills

Once the list is completed, the team should assess the organization's vulnerabilities to each one of these, and the impacts on the organization's ability to function. Ratings *will* be subjective, but the organization should do its best to rate possible threats, so priorities can be set. An example for rating the severity of loss would be a numbering or lettering system:

- A: Would put the organization out of business.
- B: Would cause significant problems and long-term financial ramifications.
- C: Would cause short-term financial ramifications and minor inconvenience for customers/clients.
- D: Would have minor or inconsequential impact and financial ramifications

In addition to assessing the impact, organizations should include estimated lost revenue or cost to repair or restore the vulnerability, including temporary or transitional costs. Looking at the historical cost to develop or implement the item associated with the vulnerability often can be helpful in setting a baseline cost or procedure to determine it.

Organizations should assess the likelihood of being a target based on the information they house or resources they contain. Political targets such as

governments, military, education, or high-profile suppliers would have a higher risk, along with businesses that have confidential information. Today's service providers that maintain databases of Social Security numbers or financial (credit card) information would be a higher risk target for hackers and thieves.

Businesses also can have a vulnerability assessment done by an outside party, but some of the better-known suppliers of enterprise disaster recovery services and consulting that can also do a vulnerability assessment include Agility (formerly GE) Disaster Recovery (www.agilityrecovery.com), HP (www.hp.com/hps/tech/continuity), IBM Global Services (www-1.ibm.com/services), and SunGard (www.recovery.sungard.com).

SOLUTIONS AND RESPONSES

Once the vulnerability assessment is completed, the organization should determine what its response will be for each item. For example, an emergency response to a virus infecting an organization could be something like this:

> If a virus is suspected, employees are to inform the network administrator immediately that the organization may have been hit. The network administrator should first attempt to identify what the infection is and scan all machines to see which may be infected by the virus. The infected computers should be disconnected from the network. If entire departments of the company or segments of the network have been infected, they also should be disconnected from the network if necessary. In many cases, the antivirus application will be able to clean up the virus. In instances where this is not the situation, the network administrator should look for instructions to clean up the infection on the antivirus Web site. In extreme cases of infection or damage, the network administrator should be prepared to reformat and rebuild the infected computer to ensure the virus is completely eliminated.

Development of solutions and responses for each item can take significant time but will pay off when the scenario or similar situation occurs. In addition, the organization should evaluate various alternatives for restoring its primary information services. The three most common scenarios for organizations developing backup information processing sites that would be used in the event of a total loss include a hot, warm, and cold site.

A *hot site* is a location that has a live, duplicate network and communications infrastructure that contains all the hardware, applications, and data in a format that is ready to go online on very short notice. Updates to the organization's

network systems also are run at the hot site to keep the location up-to-date. Maintaining a hot site is expensive and time-consuming, because the "twin" system has the same requirements as the primary network infrastructure.

A location that has equipment and Internet connectivity, but does not have the organization's applications or data loaded on the system ready for turn on, is known as a *warm site.* In some cases, data backups and application media can be stored at this site, so the network can be rebuilt in the event of a loss. A warm site may take a few days to become operational, because all applications, updates, patches, and data must be loaded and system settings fine tuned.

A *cold site* is a physical location that is ready to house your network infrastructure in the event that it has to be moved from its current location or completely rebuilt from scratch. A cold site usually has telecommunications and network and Internet connectivity, as well as adequate power and environmental capabilities (such as air conditioning).

When determining which backup scenario to choose, you also will need to consider appropriate staffing levels and personnel alternates in the event they are unavailable due to the disaster.

USING OUTSIDE RESOURCES AND CONSULTANTS

Organizations must evaluate the available resources and time required to properly develop their disaster recovery plan. If the organization does not have the capabilities to complete the vulnerability assessment and disaster recovery plan, it is advised that the company work with outside parties that have experience in this area, or organizations that can provide direction and assistance. Additional disaster recovery resources are listed at the end of this chapter (see Exhibit 5-1).

- *Trade associations.* A good first place to look for resources to develop a disaster recovery plan is within your specific industry. Often, a trade association or peer organization may have developed a disaster recovery plan that incorporates the specific needs of that industry, including resources and suppliers that can aid in a recovery. Sharing of such documents within an organization can save a significant amount of research and development time.
- *Consultants.* There are consulting organizations that focus on developing contingency plans for organizations. Such consultants often bring in-depth experience and background,

and can develop a plan in a significantly shorter time frame than an organization trying to do it by itself.

- *Vendors.* Many hardware, application, and communications vendors provide disaster recovery solutions built around their products. Although not independent in regards to recommended solutions, vendors have extensive experience in implementing their products. If a vendor is entrenched in a specific industry or in close physical proximity to the organization, the benefits can outweigh the vendor's product bias.

IMPLEMENTING THE PLAN

Information collected and developed in the previous steps must be consolidated into a single document that forms the basis of the disaster recovery plan. This document should be stored offsite in a physical format (rather than just saved on electronic media, such as a CD-ROM or tape backup system) and also e-mailed to the disaster response team's home e-mail addresses. As the plan is updated, the new version can be saved—and saved again during future updates—on the team members' PDAs. The PDA serves as a way to retain the most current version because of the synch process.

The disaster response team can prepare wallet-size emergency response cards with instructions on who to call to in the event of a disaster or emergency situation. Employees should receive cards containing emergency contact information for the emergency response team and meeting place instructions in the event that the place of business is not accessible.

A training session can be conducted to ensure all employees are aware of the plan, their responsibilities and responses in the event of an emergency, and the resources contained within the document. Safety posters or visible reminders dispersed throughout the organization keep people aware of the document. Annual updates help ensure employee awareness.

Plans do not always go as expected, so they must be tested. When practical, the organization should consider holding training exercises or drills to test different portions of the plan. Simple drills such as monthly testing of a UPS can dramatically reduce the impact of a real power outage. Finally, the document should be reviewed annually to ensure that the focus still is correct, and if not, the document should be updated for any changes that have occurred in the previous year.

EXHIBIT 5-1: RESOURCES

- CPA2Biz (www.cpa2biz.com) has developed a resource center dealing with business continuity issues important to accountants.
- DR Planning.Org (www.drplanning.org) is a vendor-agnostic information clearinghouse for all things pertaining to disaster recovery and business continuity planning.
- *Disaster Planning for CPA Firms* is a guide provided by the Association for Accounting Administration (www.cpaadmin.org) for member firms with a disaster recovery guide and resources tailored to public accounting firms.
- Disaster Recovery Institute International (www.drii.org) provides education on business continuity, as well as certification for individuals interested in a career in disaster recovery.
- Rothstein Associates, Inc. (www.rothstein.com) is a comprehensive Web site dealing with disaster recovery planning.
- Tennessee Bar Association (www.tba.org/tnbarms/disaster.html) lists a sample of disaster recovery steps that can be incorporated into an organization's business continuation plans.
- "Twenty Seconds Into The Future" (www.tsif.com) is an article in which Dr. Bob Spencer provides a sample disaster recovery plan on his Web site.

Wireless Technologies

chapter 6

The promise of working virtually anywhere, at anytime, is here. Wireless connectivity encompasses technologies and services that transfer voice or data from one machine to another through the airwaves, and includes cellular, radio, and satellite signals. In recent years, providing wireless access has physically untethered workers from their corporate networks, allowing them to work from anywhere to better serve their customers and complete their responsibilities. This ability has translated directly to improved productivity, as evidenced by several recent studies:

- "Wireless e-mail and personal information management (PIM) functions saves five to six hours per mobile employee per week," according to a survey conducted by Oracle of its own customers.[1]
- Since 1999, Sysco Food Systems' 8,000 reps have used wireless laptops for a mobile sales application; the company estimates it has achieved productivity gains of 20 percent to 25 percent.[2]
- According to an Intel Wireless Deployment Case Study, Microsoft Corporation rolled out its wireless local area network (WLAN) to 35,000 users and saw a payback on the investment within 18 months. Fifty percent of individual users stated that the WLAN connection saved them between one-half and one and one-half hours per day.[3]

Wireless technologies consist of a broad range of hardware and applications, and they can generally be split in two groups: those virtually extending the local area network (LAN) capabilities to an individual, and those using a wireless service to access information resources such as the Internet.

The first group—wireless LAN users (WLAN)—want the functionality of being on a LAN without having to be physically tethered to a network cable. They expect to work at network speeds (high bandwidth) to transfer files and access information. To get high speeds and network functionality, users must be within range of a network access point, which is usually 300 feet for WLAN connections. For organizations to have an effective WLAN, companies must place access points wherever their employees may work,

[1]Brian Albright, "Benefits of Wireless Worth the Effort," *Frontline Solutions* 3, no. 5 (May 2002), pp. 22–24.

[2]Ibid.

[3]Courtesy of Intel.

which can be done for an individual office, group of buildings or campus, for example. WLANs are effective ways to extend the network in buildings that are difficult to physically cable, as well as historical buildings where cabling cannot be implemented.

The second group—the mobile information professional (MIP)—needs access to resources, but from a much larger territory that may encompass an entire city or state, or may even extend beyond the nation's border to international usage. To provide such an extended coverage area, MIPs tend to use the public infrastructures developed by communications providers. These include radio, satellite, and cellular systems, and even though these services cover a much larger area, their bandwidth to transfer information is significantly less than a high-speed connection, causing users to send and receive very small packets of information within this limited bandwidth. (See Exhibit 6-1 for additional resources.)

WIRELESS LAN TECHNOLOGIES

Much of the discussion concerning wireless technology revolves around the extension of resources through a WLAN to a limited area, some of which were previously described. WLAN standards were released in 1997 by the Institute of Electrical and Electronic Engineers (IEEE) and referred to as 802.11. The first standard, 802.11b, dealt with devices in the unlicensed 2.4Ghz band, which transmits data at speeds up to 11mbps. The second standard, 802.11a, operated at the higher 5Ghz range and could transmit data between 6 and 54mbps, but was not compatible with the 802.11b standard.

In the late '90s, many companies developed WLAN products, but end users found that different vendors' products were incompatible. An industry group called the Wireless Ethernet Compatibility Association (WECA) (www.weca.org) banded together to make products that could be interchanged under the Wireless Fidelity (WiFi) logo. Today, the WiFi standard, encompassing 802.11a and 802.11b, is the backbone of WLAN technology. The next standard, 802.11g, is expected to be finalized by the end of 2003 and works in the same range as 802.11a, but will be backward compatible with 802.11b devices.

As you read through the scenarios that follow, realize that WiFi devices are affected significantly by distance between devices. Even though often touted as having a working range up to 300 feet, the closer the devices

are in proximity, the stronger the signal. As the signal gets weaker, the WiFi devices will downgrade the transmission speed automatically to improve reliability of the data flow. Here are the three most common scenarios in which individuals and organizations implement wireless LANs.

Home and Peer-to-Peer WLAN

At the low end of the infrastructure are individuals in their home who would like to be able to work from the family room while watching TV, in the kitchen, and on the back patio, as well as from their home office, which usually has an Internet connection. Running physical cables to multiple locations begins to get expensive, not to mention a nuisance with many cords, so setting up a wireless access point solves this issue.

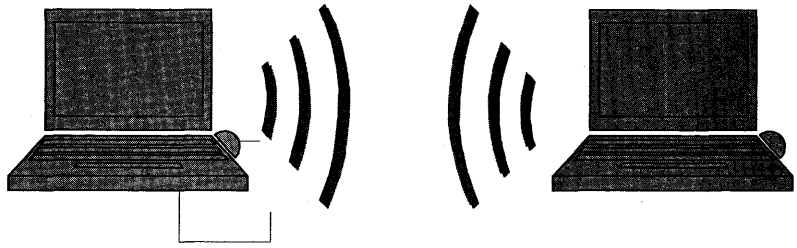
A wireless access point is a device that connects to an individual's digital subscriber line (DSL) or cable modem, and then transmits data to and from that modem to a special network interface card within the user's computer, which has wireless capabilities. As long as the user's wireless card gets an acceptable signal from the base station, the connection works as if the two points were physically connected. This one access point and card is known as a basic service set (BSS) and runs the WLAN in "infrastructure" mode.

Wireless LANs do not require an access point to function, because most wireless cards have the capability to interact with another computer having wireless capabilities. As long as these two computers (or more) are within range of the capabilities of their wireless cards, they can access the information on each other's machines, as well as transfer and share resources in a peer-to-peer or "ad hoc" mode (see Figure 6-1). Known as an independent basic service set (IBSS), this arrangement is used by some companies to set up ad hoc networks in locations without a wireless access point. Newer laptop computers have built-in wireless capabilities. In addition, Intel's release of the Centrino chip set will add wireless capability, as well as greatly extend the battery life of laptops—a necessity for mobile users.

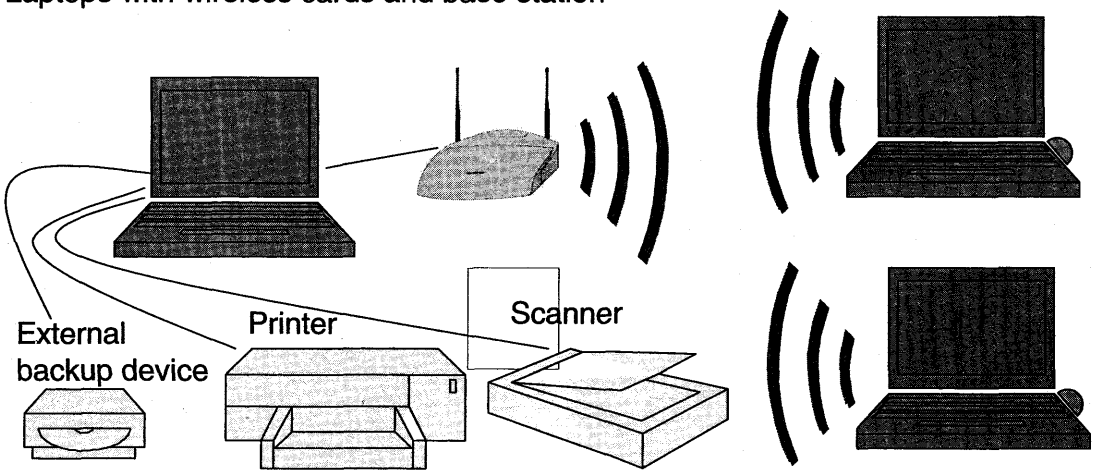
However, because of the frequency being used, WLANs can be negatively affected by some microwave ovens or portable phones operating in the 2.4ghz range. In addition, thick walls or large metal objects and electrical currents can impede the full range of access to a wireless network, so selecting the location for the access point and maximizing the systems directional capabilities is a very important function.

FIGURE 6-1: WIRELESS WANs

Laptops with wireless cards (peer to peer or ad hoc)



Laptops with wireless cards and base station

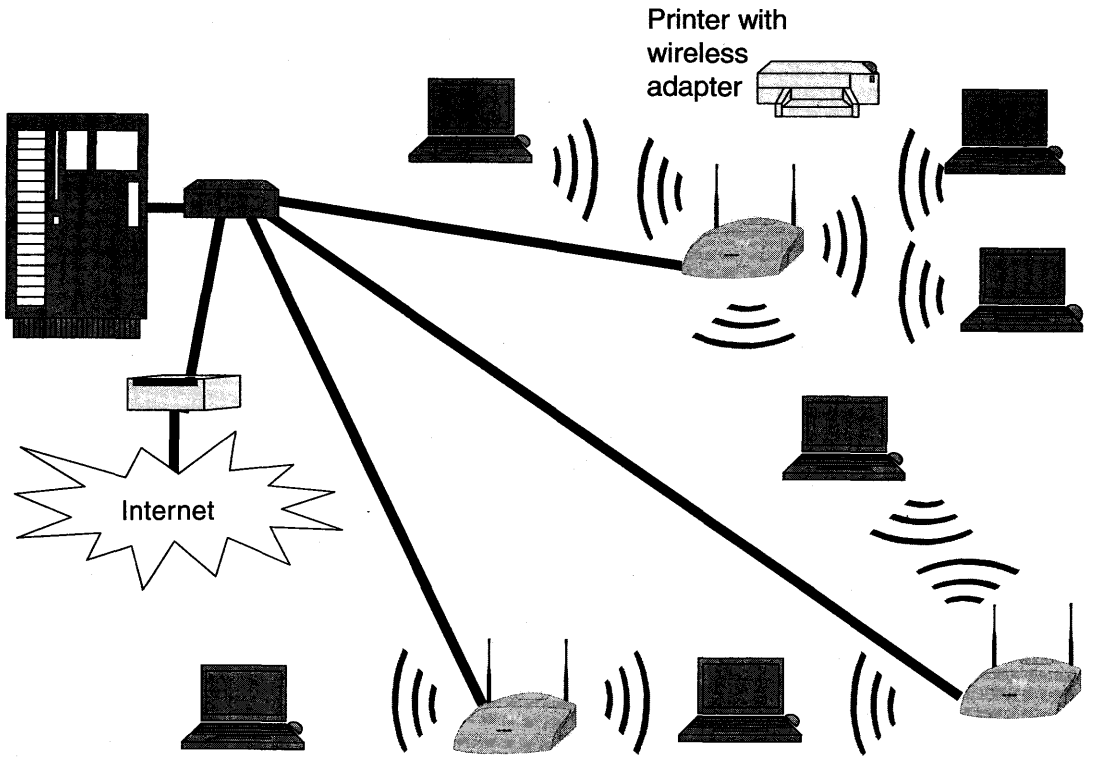


Source: InfoTech Partners North America, Inc. Clip art: courtesy Microsoft.

Extended WLAN

At the higher end of the WLAN infrastructure are organizations that need to extend wireless capabilities in areas beyond the range of a single access point or to specific areas with poor WLAN reception (dead spots). In this environment, multiple access points must be set up to allow the signal ranges of the individual access points to overlap and cover the entire area where individuals need access (see Figure 6-2). In this subnet (or environment), devices also work in "infrastructure" mode and use an extended basic service set (EBSS). The EBSS allows individuals to work in any area of coverage on the best signal available at that time, and minimizes conflicts with other access points. In the case of the Microsoft deployment, more than 4,000 access points were distributed around the Redmond, Wash. campus to ensure that individuals could access network resources with high speed and reliability.

FIGURE 6-2: EXTENDED WIRELESS LOCAL AREA NETWORK



Source: InfoTech Partners North America, Inc. Clip art: courtesy Microsoft.

Commercial or Public WLAN

Another common implementation of WLAN technology is the commercial or public WLAN set up by an organization, company, or any group to allow others to access the Internet from within their facility. This type of WLAN is known as a "hot spot" and is becoming popular in public meeting places, including airports, schools, coffee shops, and restaurants. These WLAN deployments have limited security, but provide access as a matter of convenience and to create customer foot traffic. In addition to chains such as Starbucks and Schlotzsky's already providing some wireless capabilities, McDonald's restaurants recently announced the chain was planning on implementing wireless access points in at least 300 locations in 2003.

Although public WLANs are free, some commercial properties are charging a nominal fee to access their WLAN. However, many users *will* pay simply for the convenience of having a WLAN readily available. In March 2003, Accenture and the Toshiba Computer Services Group announced they will

be setting up hundreds of WiFi access points within hotels, convenience stores, and other public businesses that people can access with a credit card or prepaid vouchers.[4]

A Gartner study stated that the WLAN industry is expected to grow from 4.2 million WLAN users in 2003 to *31 million* users in the next four years. The study also stated that Gartner anticipates there will be more than 100,000 "hot spots" in the next five years, making the technology even more ubiquitous.[5]

Organizations providing users with computers having wireless capabilities also must address the issue of personnel using commercial and public WLANs. In addition to setting up policies and training on how to access public and commercial access points, organizations should provide awareness of any risks involved.

Other WLAN Technologies

In addition to the 802.11 standards for wireless networking, there are other technologies that provide wireless networking capability, including Bluetooth, HomeRF and Satellite.

Bluetooth. An early wireless standard, Bluetooth has attained limited acceptance for devices transferring data within a range of 10 meters (33 feet) or up to 10 times that amount with a power boost. Bluetooth works in the same 2.4Ghz frequency as 802.11b, but only transmits data at speeds of 720Kbps. Some portable devices, such as personal digital assistants (PDAs) and digital cameras, use Bluetooth to transfer information.

While much more limited in range than WiFi, Bluetooth, in some instances, provides a better tailored solution. For example, one of the largest single-site public wireless networks using Bluetooth was installed on a luxury cruise liner called the World of ResidenSea. The 644-foot ship has wireless coverage provided by 250 access points that can be used by laptops, but more importantly by PDAs, mobile phones, or digital cameras with Bluetooth capability. Guests moving about the ship are more likely to carry these smaller devices with them than a laptop; not only are they more convenient, but they use much less battery power that provide longer life.

---

[4]Source: Intel.

[5]Greg Keizer, "Gartner Predicts Wireless Use To Grow Sevenfold By 2007," *TechWeb News* (March 27, 2003).

HomeRF (home radio frequency). HomeRF is an open standard operating in the unlicensed 2.4ghz range that can transmit information between laptops, phones, and PDAs at 1mbps or 2mbps to a distance of up to 150 feet. HomeRF supports the TCP/IP specifications in 802.11. The standard was formalized in 1998 by the HomeRF Working Group (which includes HP/Compaq and IBM), but has been losing traction with WiFi gaining prominence.

Satellite. While not typically a WLAN technology, broadband Internet access can be provided wirelessly to remote locations that do not have access to dial-up or other wired broadband connections. Two-way broadcasting systems capable of downloading data at speeds of up to 500kbps are available from DirectPC (www.directpc.com) and other suppliers. Within the United States, all that is required is an unobstructed southern exposure.

■■■

WIRELESS TECHNOLOGY FOR THE MOBILE INFORMATION PROFESSIONAL

In today's mobile society, individuals work from a diverse variety of locations to service their customers. The ability to send and receive electronic messages, access the Internet, and interact with the organization's network from those locations provides a competitive advantage for those companies. In that light, there are a multitude of wireless technologies to allow mobile professionals to transact business when on the road.

Currently, cellular solutions are the most prolific in regards to the sheer size of territory covered and the number of users. Virtually everyone has access to a cell phone for voice communications, and many newer phones use the existing infrastructure to provide text-based messaging, e-mail access, and Internet connectivity. Currently, there are four major digital cellular systems in use.

1. *Cellular digital packet data (CDPD).* CDPD was one of the earliest systems to send e-mail and download Web data. While rated at 19.2kbps, actual transmission speeds are in the 10kbps to15kbps range. Many early wireless services provided to PDAs used CDPD technology.
2. *General packet radio service (GPRS).* GPRS is a wireless network capable of transmitting cellular data information at speeds of 40kbps to 60kbps. In the United States, AT&T Wireless, T-Mobile, and Cingular Wireless are focusing on GPRS networks.

3. *Code division multiple access (CDMA).* CDMA is currently the dominant cellular data technology within the United States and South Korea, and is provided by Sprint and Verizon.
4. *Global system for mobile communications (GSM).* GSM was developed in the '80s. The most prevalent system in Europe, it possibly also is the most used cellular system in the world. GSM phones have a built-in small messaging system that is capable of transmitting messages of up to 160 characters at 9.6kbps. GSM systems also use a smart card called a (SIM) to hold the user's account information. This SIM is interchangeable with other GSM devices allowing additional mobility.

In addition to the four major cellular systems, new third generation systems are evolving that will have much higher data transmission capabilities, and operating systems are evolving to provide a richer experience. Wireless Access Protocol (WAP) is a standard for providing cellular phones and pagers with a streamlined version of HTML to allow downloads from the Internet through the relatively narrow cellular pipeline. WAP works with phones from all four major networks.

TOOLS FOR THE MOBILE PROFESSIONAL

Laptops with wireless receivers. All laptops have PC card slots capable of adding WiFi functionality. The Meta Group predicts that more than 40 percent of business-class laptops shipped in 2003 will have built in WiFi functionality, and Intel's Centrino chip will add native WiFi capabilities to laptops. In addition to WiFi connectivity, laptops can connect to the cellular data networks with the addition of a PC card such as the Sierra Wireless AirCard (www.sierrawirelss.com), capable of transmitting data to GSM/GPRS networks. Users must purchase a cellular data service to transmit information.

PDAs. Providing wireless connectivity to a PDA can occur through a variety of add-on devices. For users who already have a Palm or Pocket PC, add-on cards can be connected to provide connectivity. This market is slowly being eclipsed by devices that incorporate communications capabilities within the PDA natively.

PDA/phone hybrids and smartphones. As most information professionals are saddled with a number of devices such as phones, pagers, and PDAs to keep in touch, there is a movement to converge the capabilities of these three devices into one, which are called PDA/phone hybrids. These hybrids function like a PDA with e-mail, contacts, calendaring, and notes capability, but they also have a built-in communications system for voice and data communications.

- Within the Palm platform (www.palm.com), devices like the Tungsten W(ireless) uses GSM/GPRS technology to add data transmission capabilities to check e-mail, send small messages, and surf the Web. Handspring (www.handspring.com) has a version called the Treo that uses Sprint's PCS service or the GSM/GPRS services provided by Cingular/T-Mobile. Cellular phone manufacturers also have added the Palm OS to their product lines, as evidenced by Kyocera (www.kyocera-wireless.com) using CDMA technology, and Samsung (www.samsung.com), which is adding GPS support.
- Microsoft OS devices are also in the PDA/phone arena, with a number offered on their Web site (www.microsoft.com/mobile) from Siemens, Toshiba, and AudioVox. The smartphone by Orange (www.orange.com) is one of the latest entries into the market touted by Microsoft.
- A third operating system, Symbian (www.symbian.com), also works on smart phones and provides much of the functionality of the phones running the Palm and Microsoft operating systems. According to TechWeb, Symbian is an open standard operating system for data-enabled mobile phones. Based on the EPOC OS developed by Psion and supported by Ericsson, Nokia, and Motorola, Symbian is finding its way into many smartphone devices.

Pagers. Mobile professionals have long carried pagers to send and receive messages on their hip. Motorola's Skytel pagers were an early entry into this market, but have been eclipsed by the advent of Research in Motion's (www.rim.net) Blackberry device. The Blackberry was one of the first devices to have a QWERTY "thumb" keyboard used to type in and send text messages. As communications capabilities have expanded, Blackberry devices have also incorporated phone technology.

WIRELESS STRATEGY AND SECURITY ISSUES

Before implementing a wireless solution, organizations should evaluate the actual mobile requirements for their users and select the appropriate combination of tools to meet those needs. If all that is required are communications such as SMS (small message service) and e-mail to remote users, the cellular services may be all that are needed, and companies should first select the best service available in their region of operations and then evaluate the tools that work with that service.

For users wanting full network functionality from within the office, cellular services will most likely not be acceptable, and as a result, the organization must evaluate WLAN solutions. The organization must determine which users would most benefit by being portable and approximate the size of the area they would like to work within the office to ensure proper WLAN coverage. The organization should implement policies on WLAN usage, as well as provide training on usage, and must secure the WLAN from unauthorized access, which traditionally has been one of the largest concerns with WLANs.

A group of hackers known as "war-drivers" attempt to access unprotected WLAN networks by driving around with wireless-equipped laptops and finding open signals. At a minimum, the wireless equivalent privacy (WEP) protocol must be turned on to provide a layer of encryption, and the default password to the network should be changed to minimize the risk of casual war-drivers. As access points always broadcast the network connection, companies also can disable this feature and manually configure individual laptops to access it or add a firewall to authenticate users.

Unfortunately, WEP is notoriously easy to break, so organizations with confidential data or a larger number of users should harden their security. The IEEE, which created 802.11 and WEP, also have released extensible authentication protocol (EAP), which will provide additional security if implemented. A white paper by Intel also suggests organizations implement Virtual Private Networks (VPNs), authenticate users by employing RADIUS servers, and regularly scan their networks for individuals that may connect a WLAN without the IT department's knowledge. See Chapter 1, "Information Security," for more information on security concerns within a wireless network.

EXHIBIT 6-1: RESOURCES

- What You Need to Know About (www.about.com) provides additional resources by searching on wireless security and wireless networking.
- Bluetooth (www.bluetooth.com) and its sister site, Bluetooth.org, provide information about Bluetooth applications and hardware.
- Intel (www.intel.com) has white papers on deploying a wireless LAN, as well as implementing security; additional information also can be found on the Centrino wireless chip set.
- WiFi Alliance (www.wifialliance.org) lists WiFi compatible products. Wireless Developer Network (www.wirelessdevnet.com) is a site listing news and technical publications for wireless developers.

Intrusion Detection Systems

chapter 7

A 2002 study by the Computer Security Institute[1] (CSI/FBI) on government and business found that 90 percent of respondents had experienced a computer security breach, with 80 percent of those breaches causing financial damage. Recent high-profile thefts of credit card information and individuals' identities showed that virtually all businesses are susceptible to attack from outside hackers and internal personnel. Much of this confidential information is found within the financial and accounting departments of businesses, and certainly within the tax and payroll departments in CPA firms. Organizations that maintain such financial information are under a moral and legal obligation to secure this data, but how can this be done?

As described in Chapter 1, "Information Security," organizations of any size, line of work, or focus must have an effective, overall security policy to protect their information assets. In addition to strong security policies and procedures, routinely conducting a security audit, and training personnel on security risks, organizations also should evaluate today's tools for protecting their networks, including firewalls, and today's intrusion detection and prevention systems. (See Exhibit 7-1 for additional resources.)

Most businesses with Internet access already have a firewall to monitor Internet connectivity. However, although firewalls can determine what traffic is allowed in and out of the company, they do little to report successful breaches or capture personnel committing unauthorized acts inside the company, where many of the violations occur. According to the 2002 CSI/FBI survey, 33 percent of respondents cited their internal systems as a frequent point of attack. Intrusion detection systems were developed to assist in capturing these types of breaches, and businesses should implement these systems to keep individuals from intentionally or unintentionally gaining entry to areas of the network that they are not authorized to access.

Unintentionally gaining access to parts of the network can be described as a misuse of network resources. Network administrators should set up work and user groups, accordingly, to ensure that individuals can work only in the parts of the network they are authorized to access, and to specifically exclude them from areas outside that area. An individual working in the shipping department should have access to vendor addresses and contact information to verify an order, but there should be no access to accounting, where credit card or electronic funds information is stored. Highly confidential information, such as medical and payroll information stored within networks, also should be off limits to everyone except authorized human resources personnel.

[1]Source: www.gocsi.com.

WHAT IS INTRUSION DETECTION?

According to one of the leading security resources, the SysAdmin, Audit, Network, Security Institute,[2] intrusion detection "is the art of detecting inappropriate, incorrect, or anomalous activity." Inappropriate activity is best described as an individual consciously doing something on the network this person knows he or she should not be doing, such as copying or deleting files, accessing other parts of the network, and attempting to map to network drives.

Incorrect activity usually means violators are making mistakes without knowing the ramifications. For example, an individual who uses Microsoft Windows Explorer to delete or move a file also can affect thousands of other files without realizing an error occurred; this incorrect behavior can be corrected by not giving an individual authorization to do so or by providing training so this person understands the ramifications of his or her actions. Even though some security resources refer to intrusions as attacks from the *outside*, and misuse as breaches from the *inside*, for the accounting marketplace, we consider both to be intrusions.

Intrusion detection systems (IDSs) are a series of tools that examine activity on the firm's network and report unusual items to the network administrator. Activities are captured and documented, such as individuals updating their network status to administrator-level and accessing secured areas of the network where that person is not authorized to visit. Intrusion detection systems also document system information, such as deleting or changing large amounts of files, and multiple passwords being attempted to access the network—both of which are hallmarks of attacks or security breaches.

IDSs examine the traffic that goes through the network or an individual machine, and compares it to a "baseline" view of normal activity. These systems also look for unusual patterns of information flow. Pattern recognition works similarly to antivirus software: All information that flows through the network is analyzed in real-time and compared to a database of known attack methods. Any matched or similar pattern is forwarded to the network administrator for evaluation, and the activity is shut down if necessary.

[2]Source: www.sans.org.

IDSs also use anomaly detection to catch activities that are outside the "norm" for that business. Anomaly detection software documents normal activity for a business, such as the number of users logged in, applications that are open, size of system files, and other factors, and sends an alarm whenever there is any deviation from the norm. Administrators must set the parameters and applicable alarms, and tweak the system as the network evolves. The IDSs must run long enough to get a solid understanding of what is perceived as "normal" behavior. This may pose a challenge to seasonal businesses, such as retail with the holiday rush and CPA firms during busy season; increased activity can create large spikes that are difficult to normalize.

NETWORK- AND HOST-BASED IDS

In general, there are two types of IDSs: network-based and host-based.

Network-based IDSs were the first generation of intrusion detection systems, generally designed to monitor all traffic that goes through a network to look for patterns of attack. They are predominantly passive in nature, because they act like a security camera, recording intrusions, but cannot do anything to stop them from happening. When set up inside of a firewall (some firewalls today have basic IDS capabilities built in), they can analyze external intrusions into the network, as well as internal activity that passes through it. As with any system, to be effective the user must understand the limitations.

Network-based IDSs must read all traffic as it flows through the network. If the traffic gets so heavy that the IDS cannot read it all, the system can become overwhelmed and let through packets that contain unauthorized intrusions. Another issue with network-based IDSs is that they cannot read encrypted traffic. As the IDS attempts to scan the file, it recognizes it cannot decrypt it, and as a result, lets it through the network. Network-based IDSs ideally work well with segments of the network that use a router, because switched networks move data at a higher speed and in a way that network-based IDSs cannot read them as effectively.

Host-based IDSs are the next generation of intrusion detection systems. Loaded directly on a computer that the organization wishes to monitor, including a server or individual workstation that has especially sensitive applications or confidential information. Because these IDS applications are loaded locally on a machine, they can do much more on that machine than a network-based IDS

attached to a router. Encrypted files that are decrypted on that "host" machine can be read, because the encryption has been stripped away.

Host-based IDSs also can monitor all the log files on that computer, which tracks all file activity, and the IDSs send this information to a central repository where it can be analyzed. These logs document items such as who is logged in, what applications they are running, and changes in or deletions of files on that machine. In addition, central processing unit (CPU) activity is monitored, recording times when a machine is being used heavily. If CPU activity is recorded outside of normal working hours, this indicator would show that someone is either working directly on the computer or has found a way to work through it without being physically present. Other user logs also can be monitored, such as if an individual is trying multiple passwords to attempt to log in under a specific user name.

Unfortunately, the downside to host-based IDSs is that activity outside of the host computer is not tested. This can lead to a false sense of security when network administrators see their host computers are well protected but may not realize that critical files or access has been granted to another machine that does not have the host-based IDS running. To maximize the effectiveness of an intrusion detection system, a combination of network-based and host-based IDSs provide the best assurance.

Maintaining an IDS within an organization is not an easy task. It takes a significant amount of time to set up, update, and monitor such a system, and may need to run for weeks or months before a "normal" baseline can be established. In addition, the system will have to be regularly updated for both internal occurrences and newly discovered attacks that the IDS provider writes into its software. Each time the system reports an anomaly, it is up to the network administrator to evaluate the issue and respond accordingly. If there are too many false positives (warnings that turn out not to be a problem), the network administrator may feel like he or she is wasting time checking each item out and may begin ignoring them by letting intrusions get through.

The system can also have false negatives (that is, it allows an intrusion without reporting the error), which can be worse than not having an IDS. In other words, the network administrator may have a false sense that everything is protected. And, if a hacker is familiar with the firm's IDS application, this intruder may have methods to work around that specific product to elude detection. Because intruders know the inner workings of the IDS, they can delete portions of the log files or overwrite them with files that

would not show an anomaly—in effect "covering" their digital tracks. A hacker also could subvert the system if he or she attacked the network in small incremental steps rather than all at once. If these "steps" were taken far enough apart, the IDS may label these intrusions as unusual, but normal activity, and not sound an alarm. Although each individual step may appear to be benign, when combined, they pose a serious threat.

CHOOSING A GOOD IDS

According to the Center for Education and Research in Information Assurance and Security (CERIAS) at Purdue University,[3] there are eight characteristics to consider when selecting an IDS.

1. It must *run continuously* without human supervision. The system must be reliable enough to allow it to run in the background of the system being observed. However, its internal workings should be able to be examined from outside the system.
2. It must be *fault tolerant* in the sense that it must survive a system crash and not have its knowledge-base rebuilt at restart.
3. Similarly, it must *resist subversion.* The system can monitor itself to ensure that it has not been subverted.
4. It must impose *minimal overhead* on the system. A system that slows a computer to a crawl will simply not be used.
5. It must *observe deviations* from normal behavior.
6. It must be *easily tailored* to the system in question. Every system has a different usage pattern, and the defense mechanism should easily adapt to these patterns.
7. It must cope with *changing system behavior* over time when new applications are being added. The system profile will change, and the IDS must be able to adapt.
8. Finally, it must be *difficult to fool.*

IDSs are evolving to include the notification of internal breaches, actively tracking and documenting those breaches to minimize loss or damage. They also are beginning to capture forensic evidence used to prosecute and terminate individuals.

[3]Source: www.cerias.purdue.edu.

MAINTAINING AN IDS

Who is responsible for building and implementing the IDS? The IDS should be managed by internal system administrators or outsourced to experienced external integrators.

As network operating systems evolve and updates are installed, new vulnerabilities occur. The system administrator must have a process to be kept informed of current security flaws, the patches to correct them, and the process to successfully install those patches. As mentioned in the Chapter 1, "Information Security," the number of vulnerabilities reported in 2002 jumped to 4,129 from 2,437 in 2001 and 1,090 in 2000.[4] As a result, IDS must constantly be updated to address those vulnerabilities.

As new methods of attacks occur, the patterns of those attacks also must be updated within the IDS. In addition to the work done by the individual IDS vendors, there is a collaborative effort called the Common Vulnerabilities and Exposures (CVE) Editorial Board. This group begin formally sharing information in 1999 with the intent of creating a standardized list[5] that the vendors would use to be CVE-compliant.

The IDS market is growing. According to Infometics, worldwide intrusion detection and prevention systems product revenue reached $382 million in 2002, and is expected to grow to $1.6 billion by 2006.[6] Today, a number of vendors are offering IDS solutions, and basic capabilities are being built into firewalls. Better known products include Tripwire (www.tripwire.com), CISCO Secure IDS (www.cisco.com), Languard S.E.L.M. (www.gfisoftware.com), RealSecure and BlackICE (www.iss.net), and eTrust (www.ca.com).

In the future, IDS products will provide not only detection services, but also automatic prevention by disconnecting the user or the service being attacked. As firms and companies begin to take security more seriously, intrusion detection systems will become a required tool in their arsenal.

[4]Source: The CERT Coordination Center—www.cert.org.

[5]See www.cve.mitre.org.

[6]Source: biz.yahoo.com.

EXHIBIT 7-1: INTRUSION DETECTION RESOURCES

- Center for Education and Research in Information Assurance and Security (CERIAS) (www.cerias.purdue.edu) is a site set up by Purdue University to house multidisciplinary research and education in the areas of information security and information assurance.
- The SysAdmin, Audit, Network, Security (SANS) Institute (www.sans.org) is one of the most comprehensive sites regarding all information security issues.
- Robert Graham FAQ on Intrusion Detection (www.robertgraham.com/pubs/network-intrusion-detection.html) provides a comprehensive briefing in understanding the basics of IDS.

Remote Connectivity

chapter 8

In our current mobile society, it is becoming increasingly important for individuals to connect to the work environment when they are not physically located in the work environment. Today, there is a remote connection solution available, whether a person wants to work from home on an occasional basis or be connected to e-mail and business resources from anyplace, anytime. In the past few years, improvements in technology and infrastructure have brought about cost-effective solutions for virtually all remote users. This chapter discusses the basics of how you can connect remotely, the applications being used today and the remote "gadgets" available to make remote access more effective. (See Exhibit 8-1 for additional resources.)

COMMUNICATION BANDWIDTH

To understand remote connectivity, you must first understand bandwidth—the "pipeline" available to move information between remote locations. Bandwidth for individuals and most business users can range from traditional dial-up lines to high-speed dedicated leased lines.

- *Dial-up.* At the most basic level, individuals use a dial-up or plain old telephone system (POTS) connection. Even though dial-up connections are available virtually anywhere, they are much slower than other options, which can limit their usefulness. Speed is usually rated at up to 56kbps, but actual throughput is usually less. Although good enough to send and receive e-mail, a large attachment (1mb) could easily take 40 minutes or longer to transfer. Dial-up is traditionally the least expensive form of connectivity.
- *Integrated services digital network (ISDN).* In many parts of the country, ISDN is available on your existing dial-up connection. Most ISDN is rated at 128kbps for the basic rate interface (BRI), so it is at least $2\frac{1}{2}$ times faster than a standard dial-up connection. An advantage to ISDN is the line can be split between data and voice communications, so part of the cost can be offset by not maintaining a separate telephone line. As this service is typically offered by your telephone provider, it is usually under the same contract, which in most places provides a higher quality of service, but at a higher cost. Some ISDN services require that you pay for actual usage (similar to a cell phone contract), which can be very expensive if the connec-

tion is accidentally left on. Other ISDN services are available at a flat monthly rate, which is, of course, preferred. With the expansion of DSL services that typically provide higher bandwidth at a lower cost, ISDN is losing favor. Today, we would recommend ISDN only if other solutions such as xDSL or Cable were not available.

- *Digital subscriber line (xDSL).* In its many formats, xDSL has become very popular in many parts of the country and is generally an upgrade well beyond the capabilities of ISDN lines. xDSL is mostly provided by your dial-up provider but is also available through independent providers that can also deliver access either through their own network or leased through the phone company. xDSL connections generally range from 128kbps to 1,500kbps (depending on the distance from the remote computer to the provider's network connection), with some versions capable of speeds approaching 6,000kbps. Asymmetric DSL (ADSL) is the most common DSL available to home users, but the speed to upload can be significantly less than the rated download speed. There also is symmetric DSL (SDSL), which allows equal upload and download speeds; this may be preferred for remote office connections but usually is too expensive for home connections. In general, most remote DSL connections are rated in the range of 384kbps, adequate for individual users to access e-mail and smaller files.
- *Cable.* The cable television industry has effectively built a far-reaching network by running cable to many homes and neighborhoods. In addition to delivering television programming, many of these systems also are capable of digital bandwidth for moving information. Cable providers usually tout speeds comparable to DSL, but many provide much more—as high as 1,500kbps or more. An advantage to a cable connection is its relatively low cost, especially for individual users who already have a digital television subscription and its simpler installation, which is usually maintained "by the cable guy." The disadvantage to cable is that the remote user shares bandwidth with other digital cable subscribers in the neighborhood. Systems run slower in proportion to the number of online users at any one time, but the greater concern is for the security of your information. As a result, it is imperative to have a personal firewall to ensure the

connection is secure from prying eyes. If you are in a region with reliable cable, this service is great. However, if you are in a region with frequent cable outages, DSL would be a better option.

- *Leased lines.* Although solutions such as dial-up, cable, and DSL "share" the bandwidth with other users, individuals can choose to have a dedicated or leased line available to only the subscriber. These lines usually are arranged through the phone company or a similar provider and give the user a guaranteed connection, but usually at a much higher price than the options previously listed. Businesses needing higher bandwidth on a continuous basis often opt for a T-1 line, rated at 1,544kbps (also known as 1.5mb). In addition, users can pay for "fractional" T-l lines for a portion, such as 1/2 (784kbps), 1/3 (512kbps) and less. Similar to leased lines is frame relay, another bandwidth option that provides a dedicated connection, but a cost that is much more than leased lines. Frame relay is good for moving large volumes of data in bursts rather than in a continuous flow. Both leased lines and frame relay are usually provided by the local telephone company, providing a higher level of service than consumer solutions.
- *Wireless.* In addition to the physical options available for remote connectivity, there are some wireless options to consider. The wireless or radio connections being built into many of today's phones can handle e-mail and minimal access to resources on the Internet. Most of the cellular solutions are rated at 19kbps or less, so they are mostly effective for text messaging and not used for remote application processing. Wireless connectivity, also known as WiFi, also is an option for limited remote access, but to be truly effective, the distance to connection can usually reach only 300 feet before it must be connected to a local area network (LAN) or one of the physical connections previously mentioned. For more information on wireless, please see Chapter 6, "Wireless Technologies," as well as Chapter 11, "Emerging Technologies Watch List and a Look Ahead."
- *Satellite.* Satellite systems are available for remote users who have locations in rural areas with none of the data connection options just listed. For some systems, individuals connect with a dial-up line to make information "requests" and the information (usually Web pages) is downloaded through a stationary satellite dish at

speeds normally in the range of 400kbps. Newer systems are capable of both transmitting and receiving information with speeds close to leased lines, but speed also can be substantially faster. Satellite users must install a disk on the outside of their location, with unobstructed exposure to the satellite. This can sometimes cause a problem with codes and regulations of local homeowners associations or governments.

Cost for the various bandwidth options has come down significantly in recent years. Individuals should reevaluate bandwidth requirements annually and be reluctant to sign contracts beyond one year. To test your current bandwidth, sites such as http://computingcentral.msn.com/internet/speedtest.asp and www.2wire.com have bandwidth meters that provide the connection speed at a given point in time. These tests should be run throughout the day because bandwidth speeds can be affected by other Internet traffic or issues. To find out what additional bandwidth options are available in your area, www.broadbandreports.com and www.getconnected.com provide listings and user ratings.

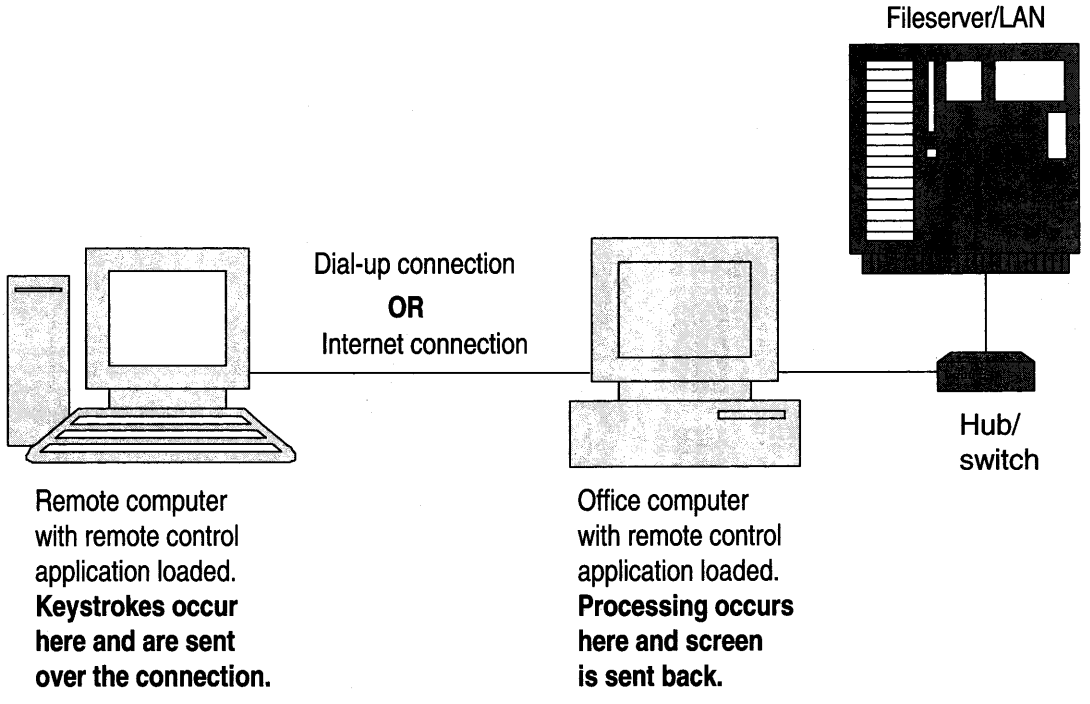
REMOTE CONNECTION OPTIONS

Remote connectivity can occur in a variety of ways depending on user needs. For example, remote control may be the solution for occasional, individual remote access for an individual or to transfer files. Commercial solutions providing a robust user experience may be required if you need to run applications from a remote site. For remote users with adequate bandwidth, virtual private networking may be the best connection scenario. Here are the more common connection options.

Remote Control

With telecommuting still a way to conduct business, individuals may want to connect to the office to access the files and applications on their own computer. In this scenario, users connect either through direct dial-up or the Internet and use remote control applications to "take over" their keyboard in the office computer (see Figure 8-1). Keystrokes are sent over the connection and changes in the screen image are sent back to the remote user. All file processing and updating occur at the office, so when the remote user comes back into the office, there is no need to transfer files. While the host computer is in remote control mode, it cannot be used for any other functions.

FIGURE 8-1: USING REMOTE CONTROL TO CONNECT



One of the downsides for remote control is that the host computer must be kept on, which can be a security risk. As a result, tools allowing individuals to remotely turn their computer on and off are available. This is especially pertinent for remote control users; a system lock-up outside of normal business hours usually means the individual would have to drive back into the office to restart his or her machine, completely defeating the purpose of the remote control application.

An added feature of most remote control software is it can be used to transfer files to the remote PC, where they can be worked on and updated, and then transferred back. These applications often have compression technology built in so the transfer time can be significantly less than trying to transfer the file by copying or e-mailing it to the remote site.

Some of the most popular applications for remote control include PCAnywhere (www.symantec.com), LapLink Gold (www.laplink.com), and CarbonCopy (www.altiris.com).

In addition to these products, Microsoft (MS) Windows XP Professional has some basic, built-in remote desktop features. Although remote control can be a usable solution for an individual connecting with high-speed bandwidth to his or her own computer, many find this to be an ineffective solu-

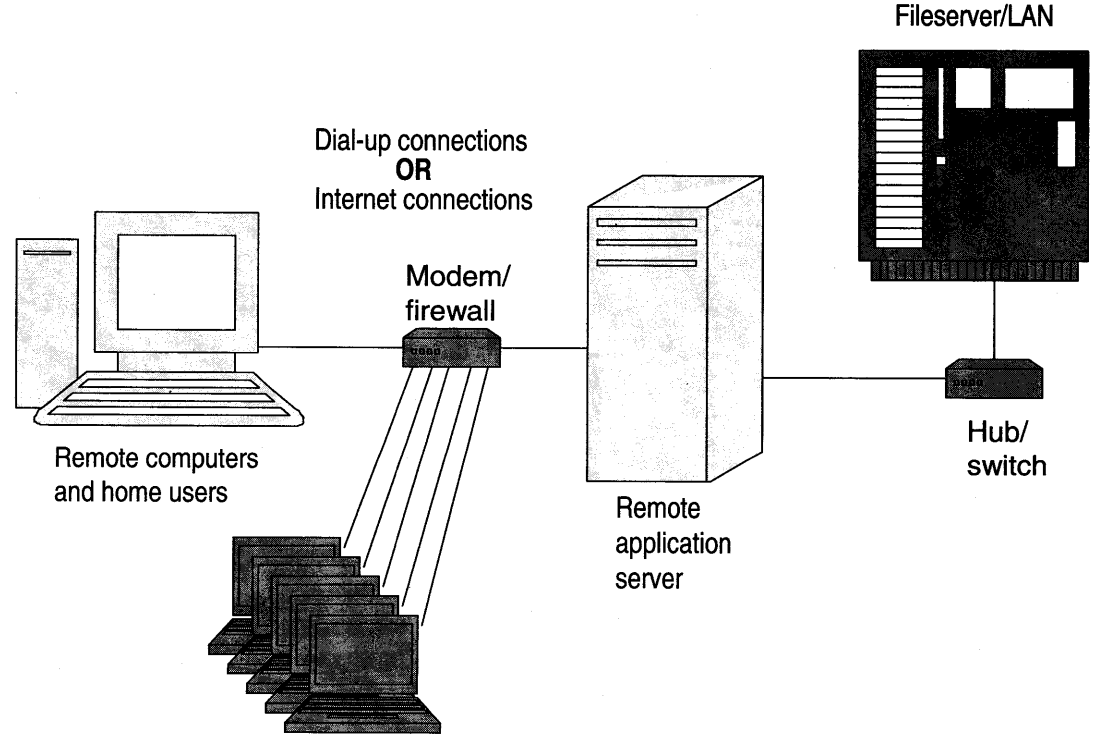
tion for those with underpowered computers, businesses wanting multiple users, or for programs requiring higher bandwidth—the case with many MS Windows applications. For these scenarios, a more robust remote application program is needed.

Remote Application Processing

The next level of remote connectivity, remote application processing, allows users with less powerful computers and slower connections to connect, and it also is a more effective solution for multiple users than remote control products (see Figure 8-2). Also known as "thin clients," remote applications processors are reminiscent of the old mainframe days when a single powerful computer managed all the applications and data, and "dumb" terminals connected to them as input devices. The number of concurrent (or simultaneous) users can be almost unlimited, and the process is as effective for dial-up as it is for Internet connections.

Even though there are a variety of hardware solutions that expand upon remote control applications, most remote application proces-

FIGURE 8-2: USING REMOTE APPLICATION PROCESSING TO CONNECT



sing is currently dominated by two software vendors, Citrix MetaFrame (www.citrix.com) and Microsoft Windows Terminal Server (WTS) (www.microsoft.com/servers).

Both Citrix and WTS should be implemented on a dedicated fileserver, capable of handling the number of remote users expected to be connected concurrently. For businesses wanting to connect 15 users or fewer simultaneously, a single server usually is adequate, and it should have at least 64mb of RAM for each user and 128mb for the operating system. A single processor usually works for seven users or less, but a second (or dual) processor is preferred for businesses needing more capacity based on the number of users. In addition, the server should have high-speed (server-class) disk drives and individual controller cards to speed throughput.

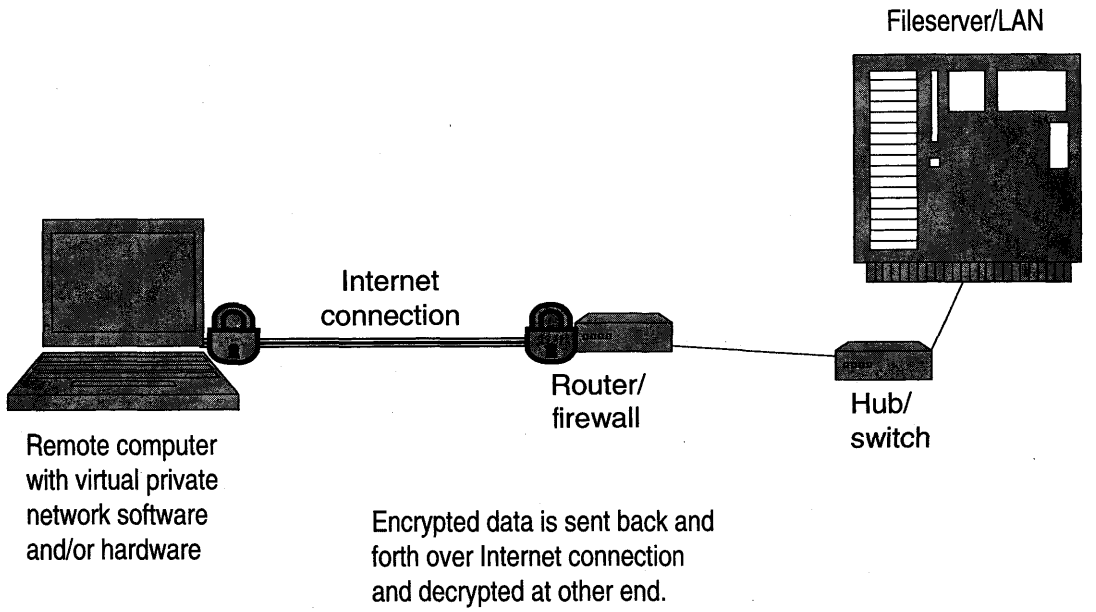
For organizations that want to connect more than 15 users simultaneously, additional servers are required, along with specialized software to balance the load between the various servers. Please note: In some industries with applications requiring very little overhead, a single server can support significantly more users. In fact, some software vendors quote 25 to 30 users per server. The recommendations presented here are designed with more complex Windows environments and applications in mind, such as today's professional service providers that would include CPA firms and businesses.

Virtual Private Networks

Virtual private networks (VPNs) are a secured encrypted connection over a public network, such as the Internet, which is used to transmit information (see Figure 8-3). They use a combination of hardware and software to encapsulate the information and deliver it to the intended location. VPNs can be an effective remote access tool if there is adequate bandwidth between the remote user and the business. In most cases, the business will install a hardware solution capable of virtual private networking—increasingly found in more of today's firewall and router products. The remote user then runs software that encapsulates any information sent in an encrypted packet. In turn, the header of the packet can be stripped off at the other end and the data decrypted, allowing the information to pass through the Internet safely.

VPNs can be used to make the remote user an extended "node" on the network, but that user must have adequate bandwidth to run the applications. If any part of the data path between the remote user and the business has performance issues, the remote user immediately experiences it. Accordingly,

FIGURE 8-3: USING VIRTUAL PRIVATE NETWORK TO CONNECT



the authors recommend VPNs only for those with connections that are very fast, or those with the remote application servers previously mentioned.

Application Service Providers

Application service providers (ASPs) and Web-enabled applications (see Chapter 4, "Web Services") also provide remote connectivity. With an ASP, the remote user connects either to a Web site to work remotely or to one of the business's servers that is running applications that are optimized for the Internet. These applications usually don't require the remote user to load any programs on his or her local computer, and only requires an acceptable Internet connection to be effective.

A remote control product that is an exception to this is GoToMyPC (www.expertcity.com), a Web-based product that manages the security and connectivity between a remote user and his or her office or home computer. The office computer is "registered" with the GoToMyPC Web site and an application is loaded locally for security and authentication. The remote user logs into the GoToMyPC Web site from any Internet connection and "logs in" to the server to connect to the office PC. The advantage to this approach is a third party is administering the security and virtual private networking aspects, so the business does not have to deal

with the additional maintenance required by other remote control and application options.

REMOTE SECURITY

All of the tools listed here are effective for remote connectivity as long as you implement adequate security precautions. For dial-in solutions, a connection should not be left open unless there is adequate password security. For remote control users from a specific location, businesses should consider invoking a dial-back option, where the office computer is prompted to hang up, dial a specific phone number, and connect to only that computer. In addition to minimizing the risk of hackers finding the modem connection, the dial-out feature transfers any telephone connection or long distance charges to the business. For remote users connecting through DSL or cable, businesses should require a hardware or software firewall. A firewall protects the remote user from being the victim of an unscrupulous person loading "keyboard logging" software onto the remote computer and capturing the remote user's logon names and passwords. Individuals transferring files or other confidential information over the Internet also should consider using filename passwords or encrypting files before sending them.

REMOTE CONNECTIVITY TOOLS

In addition to selecting the proper connectivity application and arranging for adequate bandwidth, users also must determine which tools are optimal for working remotely. While personal computers are the most prevalent remote access tool, other tools, including Personal Digital Assistants (PDAs), pagers and cell phones also allow individuals to access company computer resources remotely.

Personal Computer

An individual can use either a desktop or laptop computer when working remotely. Although desktops are less expensive and have bigger keyboards and monitors, laptop computers allow individuals to be mobile and work from customer and client sites. In either case, the PC must have either a modem and a dial-out connection, or a network interface card (NIC) and a router providing Internet connectivity (such as DSL or cable). For modem

users dialing out, it is important that the connection is capable of safely transmitting data. In business centers or hotels that have a data port on the phone, the user usually can dial out safely.

Unfortunately, some of today's digital phone systems operate at a frequency that can damage the laptop's modem or the laptop itself, or cause the laptop to damage the phone system to which it is trying to connect. Remote users should be instructed to never disconnect a phone cord from a phone and plug it into their laptops without checking to see if there is a risk. To mitigate this risk, remote users should carry a digital/analog tester. When plugged into the phone line, this device tells the user whether it is safe to dial out on that line. In instances where the digital signal is unacceptable, a digital/analog converter can be used to allow the remote user to connect. These devices are available from companies such as Targus, Blackbox, and Konnexx, with testers costing approximately $30 and converters in the range of $130.

Personal Digital Assistants

Many individuals use personal digital assistants (PDAs) for remote connectivity. While most PDAs do not have the ability to run the majority of business applications, they can be very effective for accessing and responding to e-mail, arranging your calendar, taking notes, and retaining or maintaining your contact information. These PDAs can connect to the business to synchronize information either through a wireless connection or through a modem and dial-up connection.

Today, the two most prevalent PDA operating systems are Palm from Palm, Inc. and Microsoft's PocketPC. Palm-based devices from Palm and Sony account for the majority of the market, while Compaq, Toshiba, and Dell have significant market share within the PocketPC line. Even though the majority of PDAs operate under the Palm Operating System, PocketPCs are slowly and continuously gaining market share.

Pagers

Pager technology has existed for some time and continues to be an effective remote connection tool. In the past, two-way paging from vendors such as Skytel enabled individuals to receive e-mail messages and respond with short text messages in near real time—a less expensive solution than cellular service at that time. This evolved to today's wireless pagers, including the Motorola Accompli and Research in Motion pagers that not only transmit e-mail, but also have the contact and calendaring capabilities of PDAs.

PDA/Phone Hybrids

The latest PDAs, referred to as PDA/phone hybrids, also have telephones incorporated into them that can be used for messaging and voice conversations. These hybrid phones use both the Palm and the Microsoft PocketPC operating systems and usually come bundled with a specific service provider. The authors recommend that companies always select the digital/cellular provider in their working area with the best reception that supports the company's PDA format, and then select the tool provided by that telephone company.

Internet Appliance

Another remote access hardware solution is the Internet appliance. These devices have traditionally been similar to "dumb terminals" that work with Web-based or remote application servers. Internet appliances have minimal operating systems and must connect to a Web-based application where all programs and data are maintained. Without the Internet connection, the capabilities of the device to run other applications are extremely limited. Even though Internet appliances cost less than fully functional PCs, the reductions in the price of PCs have made the benefits negligible, with most remote users opting instead for the functionality of the PC.

OTHER CONNECTIVITY TOOLS

In addition to using computers to transmit data effectively, today's remote communications tools also allow for video, data, and voice conferencing over the Internet.

Video Conferencing

If your business requires that individuals regularly travel to other locations for meetings or that you need live input from those other locations, you may want to consider video conferencing. More businesses are connecting their locations with high-speed data access to create wide area networks. Rather than incur the costs of travel, this additional bandwidth can be used to transmit live audio and video. Often, only 384kb of bandwidth is needed for effective video transmission, with some newer systems requiring even less.

In addition to the decrease in the cost of these lines, pricing on video conferencing systems also has plummeted in recent years. High-end systems could easily run more than $5,000 per site, but individual solutions today from Polycom and D-link are available for less than one-tenth that cost. Eliminating just a few trips a year between two locations can often immediately pay for the system and its usage. However, while connecting any *two* locations simultaneously is very effective, adding a third simultaneous connection drives up the cost, because the bandwidth and hardware requirements are much more extensive. To see if your business can use video conferencing, Polycom has its own bandwidth meter worthy of review (www.polycom.com/common/scripts/band_start.html).

Data Conferencing

Businesses also should evaluate data conferencing tools that allow people to view or work simultaneously on the same document through an Internet connection. Tools such as Microsoft NetMeeting are ideal for having two people make annotations on a document and see the changes the other is making. This can be very effective if the two parties are also connected through a telephone conference.

Studies done by AT&T on remote conferencing found that the key to success was grounded more in the uninterrupted voice quality than in the continuity of the video presentation (data or video conferencing). This meant that as long as conversation between the two parties was natural, both parties would forgive any choppiness or delay in the image. AT&T also found that video and data conferencing worked better with individuals who already knew each other and that it was not a solution for replacing all face-to-face meetings.[1]

Voice Over IP

The final option gaining popularity in today's business marketplace is using the business's high-speed data connections to transmit voice *and* data. Voice over IP (VOIP) systems cost significantly less than traditional PBX-based phone systems, and can be attractive when used between two locations that must pay long-distance connection charges. In addition to the telecom charges, VOIP systems also allow a central receptionist and messaging system that can route calls to other locations.

[1]Source: AT&T.

EXHIBIT 8-1: RESOURCES

- Citrix (www.citrix.com) has popular solutions for enabling remote connectivity over dial-up or Internet access.
- GoToMyPC (www.gotomypc.com) is an effective solution to allow individuals to safely and securely connect to a specific computer in another location.
- LapLink Gold (www.laplink.com) has long been a popular application to connect to a PC either through a cable, dial-up, Internet, or VPN connection.
- Microsoft Terminal Services (www.microsoft.com) is another popular tool for extending access to business applications from outside the enterprise.
- pcAnywhere (www.symantec.com/pcanywhere) is one of the more popular remote control applications that allow individuals to connect remotely to a home or business PC.
- VNC-Virtual Network Computing (www.download.com) is a free application developed by AT&T and is a remote display system that allows you to view and work on one computer's desktop using a different computer and platform from anywhere on the Internet.

Customer Relationship Management

chapter 9

Customer relationship management (CRM) may be one of the most misunderstood technologies in today's marketplace because of the mysteries surrounding what CRM is *designed* to do and what it actually *can do* for an enterprise.

Just a few years ago, CRM was considered one of the breakthrough technologies, with its much-heralded appeal to sort through customer databases and devise ideal selling situations. If you knew more customers would buy green widgets than orange ones, you would sell more widgets based on an increased demand.

Within the CPA environment, CRM is considered a prime marketing component. It can be used, like the widget example, to enhance service offerings. For example, CPA firms can use CRM technologies to figure out which clients need partnership returns. Any client whose business falls into this area is well-primed for increased services from the firm by providing information, for instance, on some new regulation related to partnerships. There is no doubt that staff could cull through its files manually to find its partnership clients, but with the availability of CRM systems, why spend time doing something manually when you could automate the process?

Still, CRM in 2003 is more than just about databases; CRM is designed to manage *all* customer touch points, including call center technologies, e-commerce, data warehousing and all other technologies used to facilitate communications with customers and prospects. (See Exhibit 9-1 for additional resources.)

THE CRM MARKETPLACE

A recent Gartner survey on the effectiveness of CRM software found that software makers tout CRM as a tool to help companies save money and boost customer loyalty, because CRM is designed to streamline corporate sales, marketing, and call center activities. Competition from vendors working in the CRM space is very crowded, with a $3 billion market led by Siebel Systems, SAP, Oracle, PeopleSoft, and Epiphany.[1]

According to Morgan Stanley *Hot News*, there is a rivalry in the enterprise CRM market between Siebel and SAP. However, "Siebel is expected to remain the market leader given the stumbles of Oracle's CRM efforts and

[1]Alorie Gilbert, "CRM Software or CRM Shelfware?," *CNet News.com* (March 3, 2003).

PeopleSoft's limited resources applied to CRM. SAP is the real threat and that battle will take a few years to play out. However, the overall market for CRM is likely to remain a 6 to 8 percent growth market."[2]

In addition, *Hot News* reports that as the market leader in CRM, Siebel has been successful at penetrating CRM-intensive verticals: Siebel claims 19 of the top 20 pharmaceutical concerns, 15 of the top 20 financial services companies, 15 of the top 20 wireline telecom companies, and 9 of the top 20 mobile telecom firms as customers.

This growth percentage bodes well for CPAs who want to incorporate CRM processes into their firms and companies. In general, CRM was a hot growth area in the business applications market in the late '90s, but sales among the leading providers have declined amid the depressed economy. Gartner predicts that sales will remain flat in 2003, and its latest findings are not likely to make the job of selling CRM applications any easier.[3]

The real losers in all of this are the companies who sank millions of dollars into technology they never used. Although lowering costs is the most common benefit cited by businesses for implementing CRM applications, the survey revealed that almost 42 percent of the total number of software licenses bought by businesses go unused. Other reasons CRM software often goes to waste include the resistance to change and new technology among workers. Declining technology budgets at many companies also have drained the corporate coffers of funding for the consulting services needed to install the applications. Companies spend one to five times as much on CRM consulting as they do on software licenses.[4]

Enterprises that wanted to improve their competitive positions by enhancing customer relationships were the first adopters of CRM technologies, but many companies that implemented early CRM products were disappointed in the business results, witnessed internal department frustration, and saw little customer impact. Fifty-five percent of all CRM initiatives fail to meet executive expectations, and the substantial investment required for CRM compounded these failures. Enterprises spend $60 million to $130 million to implement a typical CRM program, according to Forrester Research.[5]

However, despite these statistics, the potential benefits of a well-executed CRM strategy are too compelling to ignore. In fact, in the face of tighter

[2]Source: Morgan Stanley *Hot News* (Oct. 24, 2002).
[3]Gilbert, *CNet news.com.*
[4]Ibid.
[5]Jill Griffin, "Ensure CRM Success," *Cisco iQ Magazine* (Jan./Feb. 2003).

overall technology spending, the CRM market should experience solid growth over the next several years. The worldwide CRM services market will grow from $25.3 billion in 2002 to $47 billion by 2006, according to forecasts by Gartner Dataquest.[6]

As CRM products and processes have improved, so have the knowledge and capabilities of those using them. In 2002, Baylor University Professor Marjorie Cooper surveyed 99 companies that had recently implemented CRM initiatives. She found that 56 percent completed the initiatives within budget and 85 percent achieved the planned return on investment.[7]

PRACTICAL APPLICATIONS OF CRM

When most of us hear the initials CRM, we think of one of the biggest retailers on the Internet, Amazon.com. Amazon mastered the art of "push marketing" to its customers by tracking the buying habits and areas visited on their Web site to cross-market additional goods and services. And now that the site has expanded into clothing, household goods, and other products, along with their new "corporate" accounts, Amazon's invasion into our daily lives will not soon disappear.

Despite the ability to forecast whether Amazon will ever show a continuous profit, one fact is certain: Firms and businesses want to be just like Amazon in that they want to completely understand their audience so they provide increased "touch points" on a regular basis.

CRM is more than just about technology. In fact, Jay Fruin of the Integration Services Division of Leveraged Technology, Inc.,[8] says most experts agree that CRM "is not about technology any more than hospitality is about throwing a welcome mat on your front porch."[9]

Fruin says that CRM is a philosophy that puts the customer at the center of the design phase—allowing a business to become intimate with that customer. At the same time, a unified strategy that spans all the ways a client or customer can be contacted—fax, e-mail, voice, Web—is an "absolute necessity." In addition, Fruin says, "Although most customer support managers would prefer to provide customer support solely through 'e-channels,'

[6]Ibid.
[7]Ibid.
[8]Source: www.lev-tech.com.
[9]Jay Fruin, "What is CRM?," *InfoTech Update* 10, no. 2 (March/April 2001), pp. 5-6.

the reality is that most customers need a 'safety net' of direct human voice contact with real customer service reps. As customers become comfortable with e-channels, they will eventually come to use them as they would any other customer service capability.

With this strategy in place, Fruin says there are four areas that illustrate practical uses of CRM within the accounting space:

1. *Improved customer service.* Improving client or customer service is the first, most important requirement of any CRM solution because unhappy customers usually do not result in repeat buying—even if what you're selling in the accounting environment is a "service" rather than a "product." In addition, the value of the customer is much greater than first imagined; the customer not only buys more of the products and services already purchased, but also is likely to purchase new ones as well. As a result, quality client or customer service that inspires additional loyalty is paramount to the CRM strategy.
2. *Enhanced product offerings.* Fruin believes there is a tremendous opportunity to cross-sell services to your existing audience and even prospects. To do so, the firm or company must first determine the total relationship it has with the client or customer, and must ascertain which of its products and services are the best fit. For example, you might provide compliance services to a number of clients, but you also can figure out which of these clients also might like technology consulting or investment/advisory services. If the client or customer already has your loyalty, he or she is much more likely to listen to your suggestions regardless of how you might think the suggestion may be perceived.
3. *One-to-one marketing.* This concept goes back to the Amazon example in which Amazon sells products it thinks its customers will want, and the crux of this is to build and expand the client or customer relationship. Fruin says that by understanding previous purchases, coupled with present demographics and a little personal knowledge of the customer (for example, marriage/divorce, recent large purchases), a company can tailor offerings to that particular individual that will be more easily received than a standard, conventional marketing message. As is the case with Amazon, an inexpensive, effective means of communicating through one-to-one marketing is the Internet,

which can generate a much greater response than conventional marketing through opt-in e-mail campaigns, for example. CRM technology is at the center of this effort because it provides a means to deliver and measure these types of campaigns.

4. *Mass personalization.* Fruin says personalization of products on a mass basis can be achieved. For example, Dell offers build-to-suit computers through its Web site or over the phone; customers choose the components and features based on their own needs but still are customizing a product designed for the mass market. Taking this concept to the CPA environment, many firms offer technology consulting, but those that specialize in something for a niche audience and demonstrating intellectual capital are the ones winning customers.

CALL CENTER TECHNOLOGIES

Unsolicited telemarketing is something no one wants, but firms that use call centers are discovering how professional calls win more customers and clients.

Call center technology is the software applications and hardware that control the phone calls received or dialed by call center agents, as well as the database that captures the results of each call. According to the American Teleservices Association (ATA), teleservices generated $661 billion in revenues in 2002 on 180 million sales transactions and, as an industry, employed 5.7 million people—one of the most aggressively growing segments of business process outsourcing.

Because of that growth, the efficiencies of the Internet and the eventual proliferation of voice over IP, the technology investment within the call center market segment has remained robust over the past couple of years, helping create even greater efficiencies.

Call center technology can be defined by the niche a call center serves, as well as the necessities of that niche, including inbound calls, outbound calls, and market research that relies on specific mechanical advantages such as predictive dialers, call routing, and hunt groups. Call centers also tend to be narrow in their focus. For example, agents that primarily make only outbound sales calls probably would not do market research. Many large call centers offer a variety of services, but most have chosen a niche they can profitably serve.

"Sales automation achieved through call centers can provide phenomenal results when used deliberately and strategically," says Toby Gilman, senior

vice president of Dallas-based SalesLogic, LLC,[10] a sales consulting and outsourcing firm focused on consulting, technology, and professional services. "Many people think this is just one step away from telemarketing, but in fact, the entire process is very professional and actually a lot of fun. It's about delivering results."[11]

Gilman, formerly with Ernst and Young, LLP, combined a powerful marketing strategy with college graduates to generate a results-oriented marketing message to contact and set up appointments with 5,000 executives who work for Fortune 1,000 companies. Within 20 months, these appointments resulted in *$100 million* in incremental revenue for the Big Four firm—all at a cost of less than *$1 million.*

"Call centers provide access to the marketplace; however, many variables must come together to drive results," says Gilman. "Our outbound representatives were college graduates who were articulate and could speak in business terms, and the product itself offered incredible results. We were able to leave a message and have the CEO of the company actually call us back."

Although smaller CPA firms may not see the return on investment as quickly as larger firms or businesses in general, CRM through the call center environment can be a viable alternative for many organizations.

DATA WAREHOUSING

Data warehousing identifies trends and cause/effect relationships across the organization. Data is accessed across multiple subject areas, such as sales, cost and manufacturing, and from multiple enterprise resource planning (ERP), supply chain management (SCM), CRM and other applications. Data needs to be mapped, consolidated, and aggregated. For example, businesses should ask, "Who are my most profitable customers?" and "Do I have sufficient inventory and manufacturing capacity to satisfy forecast sales?"[12]

Strategic analytics requires broad source and target support, a rich library of data-warehouse-specific functions, and the ability to graphically represent complex multistep data processes with no coding. Reusable components and prebuilt, conformed data marts that integrate together are important accelerators.

[10]Source: www.sales-logic.com.

[11]Bob Howard, "Using Call Center Technology to Automate the Sales Process," *InfoTech Update* 11, no. 2 (March/April 2003), pp. 5–7.

[12]Harriet Fryman, "Data Drives Your Business: Are You the One Steering?," *What Works* 14 (Nov. 2002).

A few of the data-warehousing-solution providers include Computer Associates International, Inc.; Firstlogic, Inc.; Hyperion Solutions Corporation; IBM Corporation; and Microsoft.

■■■

CASE STUDY—UNION BANK OF NORWAY[13]

Union Bank of Norway, the country's largest savings bank group, serves one million consumer and commercial customers through 175 branches, more than 250 automatic teller machines, six call centers and the Internet.

The Challenge

Union Bank of Norway (UBN) could not easily gather and store customer-specific information because it operated on multiple computer platforms and systems, with disparate data scattered throughout decentralized branches. "We wanted a full view of the customer. We had to use several different systems, which meant it would take us days to find the information we wanted," says Kari Opdal, head of CRM for Union Bank of Norway.

This situation limited the bank's ability to understand how specific customers, products, and services drove profitability. To improve margins and profitability, UBN needed to better target its services to customers, direct business to areas that provide the best return on investment, and manage operational costs.

UBN wanted a way to create, store and access customer-specific information in a responsive, easy-to-use format. The bank decided to build a data warehouse to create a central repository for customer information. The data warehouse uses the Teradata database and a 4700 four-node server. UBN also uses the Teradata CRM analytical solution to create, manage and analyze programs for building relationships with its customers.

The Benefits

The solution, says Opdal, has become "the heart of our organization more and more." Implemented as an investment by the information technology (IT) and marketing departments to help with marketing campaigns, it has paid for itself within a year, thanks to results from direct marketing, says Opdal. Now, she says, all areas in the bank—finance, accounting, and auditing, as well as IT and marketing—rely on the Teradata solution for data analysis.

---

[13]Tom Richards and Bill Bradway, "Case Study: Union Bank of Norway's Analytical, Event-Based CRM Solution," *Customer Knowledge* 4, brief no. 8 (June 28, 2001).

"At first, only a few people in the organization were interested in using the warehouse. Now, nearly 3,000 people have access to our queries and get their sales results from the Teradata system," says Opdal.

UBN was able to increase its market share by reacting faster to opportunities in the marketplace. For example, the bank's marketing team launched a customer loyalty program targeted at the bank's most profitable customers. This dialogue program captures information from customers to use as the basis for the next contact—and this ability, says Opdal, has resulted in an impressive 70 percent response rate.

The bank is better able to analyze each customer's use of different services, as well as an individual's total net worth to the bank. "We can understand the profit and costs associated with each customer, which means better, more customized services for customers and increased profitability for the bank," Opdal says.

Four years after implementation of the data warehouse, UBN realized it could leverage the data it had captured, as well as Teradata's analytical capability to build stronger relationships with customers through CRM initiatives.

"Our customers were saying they were happy with our offerings, but they didn't feel that we were talking to them on a one-to-one basis," Opdal says. "We needed to be more sophisticated, to find a system that could help us be more efficient both with our traditional marketing campaigns and managing event-based campaigns. That led us to the Teradata CRM solution."

With Teradata CRM, UBN is now able to run event-based marketing, managing timely and relevant contact with their customers through all distribution channels. The event-based marketing pilot was a huge success. The sales conversion rate—up to 60 percent—far exceeded that of traditional direct marketing campaigns.

"The Teradata solution gives us the ability to store and track information on each individual customer, react to that information, and find opportunities for growth," Opdal says.

CASE STUDY—MICROSOFT CRM[14]

This year, Microsoft Business Solutions unveiled an offering built to meet the customer relationship needs of the midmarket—Microsoft Business Solutions CRM.

[14]Source: Holly Holt, Microsoft Business Solutions.

Microsoft CRM helps companies build more profitable customer relationships by increasing sales effectiveness and delivering more consistent customer care. Because Microsoft CRM is built specifically for the midmarket, it includes the tools that market space needs to handle a full range of sales and customer services functions.

Microsoft CRM gives businesses a powerful tool for making the most of customer relationships by delivering consistently excellent customer service—the level of service their customers expect, and that keeps them coming back for more rather than checking out the competition.

The solution delivers benefits in three broad categories: It helps improve business productivity; it comes with a lower total cost of ownership than most CRM solutions; and it integrates data and other business applications, which adds business value on an ongoing basis via easy integration with third-party applications and Web services.

Improved Productivity

Microsoft CRM is a complete solution that helps midmarket businesses improve productivity by helping salespeople and customer service representatives perform their jobs more effectively. Microsoft CRM makes it easy for employees to share information across teams and departments. That eliminates redundant data entry and plays a key role in delivering on companies' goals to deliver superior customer service.

At the same time, the comprehensive nature of Microsoft CRM lets management, sales and service teams get up-to-date information that leads to informed, agile business decisions.

Lower Total Cost of Ownership

By integrating data and other business applications, Microsoft CRM keeps the total cost of ownership low—a key consideration for today's midmarket business. Microsoft CRM was developed to be rapidly deployed, easily customized and scaled to adapt to ever-changing business needs. It can also be up and running within days or weeks—far more rapidly than most other CRM solutions.

Powerful Integration

Microsoft CRM is built from the ground up on the Microsoft .NET architecture, which ensures ongoing business value by enabling easy integration with third-party applications and Web services. Microsoft CRM's ability to

integrate data with other business applications gives businesses a more complete view of customers and customer interactions. Microsoft CRM also integrates easily with Microsoft Business Solutions' enterprise resource planning (ERP) products.

Benefits for the Midmarket

Midmarket businesses can benefit from the use of Microsoft CRM in several ways.

Microsoft CRM includes features that have a direct impact on the company's most important constituent— its customers. Midmarket businesses can dramatically shorten their sales cycle and improve close rates with leads and opportunity management, automated sales processes, quote creation, and order management. Having a shared knowledgebase and automated routing and queuing enables businesses to give more efficient and consistent customer service.

It also has a positive impact on customers by streamlining processes and procedures behind the scenes. Tightly integrated sales and customer service modules, for example, let employees view, update, and share information across teams and departments. Microsoft CRM gives employees flexibility in how and where they work, offering them access to full sales functionality online or offline through Microsoft Outlook or online from any location using a Web browser.

In terms of planning for the near and far term, Microsoft CRM helps businesses make informed, agile decisions. Comprehensive reports let business decision makers forecast sales; measure business activity and performance; evaluate sales and service success; and identify trends, problems, and opportunities.

Key Features of Microsoft CRM

Microsoft CRM integrates with Outlook, Word, and Excel, which enables access to full sales functionality from Outlook and the ability to create, send, and print communications to Microsoft Word Mail Merge. Users can also export data to Excel for further analysis.

Microsoft CRM's lead and opportunity management features let leads be easily imported and then automatically assigned to a salesperson based on territory, product, or other criteria. Salespeople can also track opportunities throughout the sales cycle and convert qualified leads to opportunities without data reentry. Drawing on the product catalog feature that includes sup-

port for complex pricing levels, units of measure, and discounts, salespeople can quickly create accurate quotes and convert them to orders.

Using Microsoft CRM, sales opportunities can be tracked and closed consistently with workflow rules that automate stages in the selling process. Workflow rules also make it easy to generate and send auto-response e-mail messages in response to customer requests. And Microsoft CRM's case management features let employees create, automatically assign, and easily manage customer service requests from initial contact.

Microsoft CRM comes with a searchable knowledge base that enables employees to resolve common support issues. And with more than 100 prebuilt reports, employees and management can use Microsoft CRM to make informed decisions quickly; measure and forecast sales activity; and identify opportunities, trends, and problems.

Microsoft CRM has a familiar user interface that is used in both the Outlook and thin clients, allowing for faster training of team members and higher usage of the solution. This ensures the data is in the solution, not just in the heads of your salespeople or in many disparate systems.

Availability

Microsoft developed the solution to meet budget and support needs for businesses in the midmarket. Delivery and implementation through certified Microsoft Business Solutions partners includes hands-on assistance with the setup and maintenance process, as well as 24-hour access to Microsoft technical support services.

EXHIBIT 9-1: RESOURCES

- Knowledge Concepts, Inc./FirmWorks (www.knowledge.org/firmworks.asp) offers information on this CRM tool used in many CPA firms.
- Interface Software (www.interfacesoftware.com), makers of InterAction 5, have a variety of white papers and case studies on the CRM process as it affects the accounting profession.
- Microsoft Business Solutions (www.navision.com/hq/cat524.htm) offers several articles on implementing CRM solutions.
- Business.com offers an entire section devoted to the CRM tool (www.business.com/directory/computers_and_software/software_applications) and a list of industry vendors.
- CRM Community has a collection of articles, networking, information, and research (www.crmcommunity.com/registration/member.cfm?code=QNFIH96).
- The CRM Toolkit (http://www.crm-toolkit.com) is a how-to guide on getting started with CRM initiatives.
- Call Center Magazine has an article called "The Scope of CRM" that addresses the costs associated with CRM (www.callcentermagazine.com/article/CCM20021202S0009). The site has a number of related resources.

PRIVACY

chapter 10

During the heyday of Internet expansion and the ensuing dot-com collapse, Privacy ranked fifth on the AICPA 2001 Top 10 Technologies list and subsequently dropped to number eleven in 2002. With the release of the 2003 Top 10 Technologies list, Privacy once again is prominent on the list as people become more concerned about the issue.

The description of privacy coined by the Top 10 Technologies Task Force was "As more information and processes are being converted to a digital format, this information must be protected from unauthorized users and from unauthorized usage by those with access to the data. This includes complying with local, state, national, and international laws."

To further build on this definition, the AICPA Privacy Task Force defined privacy as the "rights and obligations of individuals and organizations with respect to the collection, use, disclosure, and retention of personally identifiable information." Unfortunately, the privacy of an individual's electronic information is not always being properly protected. In addition to the examples provided in Chapter 1, "Information Security," here are a few stories that highlight the exposure of personal information:

- "Bowing to public pressure and concerns about security, the Social Security Administration this afternoon abandoned a service that lets users get employment histories online."[1]
- "A search page at *www.halllmark.com* made untold numbers of e-mail valentines and birthday cards accessible to millions of strangers."[2]
- "A programming error at drug maker Eli Lilly and Company resulted in the disclosure last week of 600 to 700 e-mail addresses belonging to participants in the company's Medi-messenger service, which was linked to Eli Lilly's Prozac Web site."[3]
- "The hijacking of someone's identity information, such as credit card or Social Security number, to steal money or commit fraud, is one of the fastest-growing crimes in the

[1] Staff Report, "Social Security Site Closed," *CNet News.com* (April 9, 1997).

[2] "Hallmark Web Site Glitch Made Private Messages Accessible to Anyone," *The Kansas City Star* (Feb. 11, 1999).

[3] "Drugmaker's E-Mail Glitch Exposed Patient Info," *eCommerce Times* (July 6, 2001).

> United States. Privacy advocates have said the number of people victimized by identity theft may be as high as 750,000 a year."[4]

Even though privacy issues are exacerbated by the increased use of computer technology, the issue is not a new problem but an already existing one fueled by more information that is stored on the Internet. According to an 1890 issue of the *Harvard Business Review*, privacy was defined as "the right to be left alone" and is a right assumed by citizens as granted by the U.S. Bill of Rights. Our Fourth Amendment, which states Americans will be "secure in their persons, houses, papers and effects, against unreasonable searches and seizures," speaks to the fact that privacy is a right granted by the U.S. Constitution. (See Exhibit 10-1 for additional resources.)

PRIVACY STATISTICS

A study[5] sponsored by AICPA/Ernst and Young in November 2001 and conducted by Harris Interactive to evaluate consumers' trust of privacy policies and data handling found that "both on and off the Internet, consumers are more concerned about privacy today than they have been at any point over the past two years, and they are much more assertive in taking steps to protect their privacy." The study found that 79 percent of consumers felt they had lost all control of how personal information was collected and used. The survey also found that 63 percent of respondents did not believe existing laws and organizational practices provided a reasonable level of protection for consumer privacy, and that 56 percent believed a company not following its privacy policies was a cause of major concern. Other studies done in recent years support these findings and further expose the fact that individuals are concerned with the privacy of their personal information:

- *The San Francisco Chronicle* (May 4, 2000) stated the "No. 1 reason consumers give for not shopping online is fear of losing their privacy."

[4]Wired News Report, "Identity Theft Is Top Complaint," *Wired News* (Jan. 23, 2003).

[5]Source: AICPA, at www.aicpa.org/pubs/insider/innovationres.htm.

- According to a Yahoo! Internet poll, 85 percent of online users regard the privacy of information transmitted online as the most important issue on the Internet.
- An Odyssey study stated that 92 percent of online households agree or agree strongly with the statement, "I don't trust companies to keep personal information about me confidential, no matter what they promise."
- A Forrester Research "Privacy Best Practice" study found 90 percent of online consumers want to control the use of their personal data.
- An AT&T survey found 87 percent of Net users are concerned with threats to their individual privacy while online.

Physical Movements Captured

Privacy is becoming a bigger issue in part because so much more information can be collected and consolidated electronically than ever before—both physically and virtually. Today, physical movements of individuals can be logged, often without the person having any idea that his or her whereabouts are being captured. Some examples of physical information capture that could possibly affect an individual's privacy include the following:

- Security cameras capture images of individuals as they walk in and out of buildings. Facial recognition applications can scan such images in these tapes and compare them to a database of existing employees or known criminals. Technology called FaceIt from Identix (www.identix.com) was used at Super Bowl XXXV in Tampa, Florida.
- A discount card at a grocery store immediately captures what that person purchased and provides discounts for the next visit. This information is tied back to the original application, which often includes the customer's name, address, phone numbers, and other "personal" information. A group called Consumers Against Supermarket Privacy Invasion and Numbering (www.nocards.org) tracks abuses caused by such cards.
- Evolving cell phone technology for individuals dialing 911 will provide that person's physical location. Once this system is implemented and possibly cracked, it may be possible to locate

a cell phone within meters of its location. The Massachusetts Institute of Technology (MIT), working with True Position (www.trueposition.com) together have developed such a system, and other carriers are looking to embed a global positioning system (GPS) chip within the phone handset.

- Keyboard and password logging applications not only let organizations know which computer an individual uses and when, but they also can document every keystroke. These keyboard logs can be sent to an administrator and all activity can be observed. Programs such as Ghost KeyLogger, Key Thief, Key Server, and Password Detector are available through public access Web sites such as CNET (www.cnet.com).
- Technology is also available to implant a computer chip about the size of a grain of rice into an individual that identifies who they are by scanning the individual with a handheld device. The VeriChip from Applied Digital Solutions (www.adsx.com) was first used in 2002 for Alzheimer's patients.

VIRTUAL MOVEMENTS CAPTURED

Virtual movements of individuals as they work on their computers to access network resources and "surf" the Internet also can be captured to create a profile that many privacy proponents feel is a direct violation of that individual's privacy. In addition, many people virtually *give away their privacy without even realizing it.*

- People completing surveys for free travel, subscriptions, prizes, discounts, or newsletters often fill out comprehensive applications. These create a profile that later can be exploited by the company, and usually includes names, addresses, phone numbers, and e-mail addresses. One well-known example is the 10,000 free PCs given out by Idealab in 1999: more than 1.2 million people provided pages of detailed personal information to qualify.
- Completing warranty forms and registering software online also provide the vendor with similar information. This information is often shared between "related" entities and consolidated to create a profile of that individual, which could later be exploited.

- In some cases such as government filings, the consumer can do little to protect personal information. Public filings for home purchase, birth of a child, marriage, and divorce provide companies with targets for specific products, including home warranties, baby supplies, new furniture and appliances, and dating services.

In addition to information collected in these ways, some Web sites employ "Web bugs." As individuals navigate a Web site that has a Web bug, the bug transfers information such as the computer's IP address and browser used, the URL of the page visited and the specific Web bug, and information previously stored in a "cookie."

DoubleClick (www.doubleclick.com) was an early pioneer in this area, as well as MatchLogic (whose URL is no longer live). Recently, NewYorkTimes.com tested "Wide Angle Targeting"—the practice of "putting people into contextual categories by monitoring how many times they visit certain sections of the site, including health and sports."[6] Web bugs can also pose a risk to users of e-mail because they can provide information on when the e-mail was read, and to whom it was forwarded.

The environment in which many people operate today can best be summed up by Sun Microsystems' Chairman Scott McNealy with his now infamous quote, "You have no privacy—get over it!," a fact-of-life largely true for those who do nothing to protect their individual privacy. To protect their privacy, individuals should find out what information about them is available, reduce the amount of new information becoming available, and minimize their exposure when attached to the Internet.

FIND OUT WHAT "THEY" KNOW

Credit reports are used by organizations to determine an individual's credit worthiness, including a history of all loans, credit cards, and payment status. Each time new credit is extended or a new credit card is issued, the matter is filed with one, two, or all three of the nation's leading credit agencies to manage this information: Equifax (www.equifax.com), Experian (www.experian.com), and TransUnion (www.transunion.com). A person's credit report also is one of the first areas affected in identity theft.

[6]Stefanie Olsen, "NY Times.com Gears ads to Surfers' Habits," *CNET News.com* (Feb. 13, 2003).

Individuals should review this information periodically to ensure that all transactions are valid.

In addition, a variety of companies provide credit monitoring services and will inform you as soon as any change is made in your credit: MoniTrust (www.monitrust.com), Online Credit Information (www.onlinecreditinfo.com), PrivacyGuard (www.privacyguard.com), and True Credit (www.truecredit.com).

Individuals also should review the annual personal earnings and benefits estimate statement (PEBES) provided by the Social Security Administration. This statement summarizes the annual earnings credited to your account, as well as Social Security taxes paid. These statements are sent automatically to eligible workers over 25 years of age, three months before their birthday.

The next step is to "opt out" of as many offers to share your information as possible. Financial companies are required to send you a privacy notice to inform you of what information they share and instructions on how to be removed from this list. You also can opt out of preapproved credit card offers by calling (888) 567-8688, which forwards your request to the three credit reporting agencies. Whenever filling out any warranty information, only provide your name, address, and information about the specific product you bought. Ask them in writing not to sell your information. The same goes for any magazine subscription, association membership, or charitable organization. Individuals can also opt out of the Direct Marketing Association's (www.dmaconsumers.org) mail preference service and telemarketing list, which includes the major catalog providers and marketing and telemarketing companies.

It is important to also know what is stored in regards to an individual's medical history. The insurance industry uses a centralized database at the Medical Information Bureau (www.mib.com). If an individual is denied insurance based on information within the Medical Information Bureau records, he or she can request a copy for free.

KEEPING INFORMATION PRIVATE

The second step to protecting individual privacy is to avoid opportunities for private information to be exposed. Armed with little more than a Social Security Number (SSN) and basic information, a criminal can get a fake ID made and begin impersonating the owner of that SSN.

Many people shirk off some of the basic, tried-and-true methods to keep information private based on the "It's never going to happen to me" syndrome. However, it could just as easily happen to you and anyone else—and it often does. Some tips to protect your privacy include:

- Do not give out your SSN unless absolutely necessary—and only when dealing with a trusted party. Currently, 29 states use your SSN as your driver's license number, while other entities also use your SSN as part of their own ID system. If it is possible to use another number, you should request right away that the SSN be changed.
- Minimize the number of credit cards you use and bank accounts you keep open, and keep a written listing of account numbers, expiration dates, and customer service telephone numbers to report a stolen card or to close the bank account. However, one note: do not carry the list with you! Keep it in a secure, safe place. In addition, if you log credit card or account numbers on your personal digital assistant (PDA) device (for example, Palm or PocketPC), invoke password protection so would-be thieves cannot readily access this information.
- Review your credit card and cellular phone statements carefully for unauthorized charges, and sign up for access to this information through the Internet so you can review account activity.
- When using an ATM or calling card in a public place, always cover the number pad so onlookers cannot see your personal identification number or access code. Do not store a written personal identification number or password in your wallet.
- Never use the last four digits of your SSN when creating a personal identification number.
- Always shred credit card applications, slips, medical statements, and any other documents that may have account numbers and personal information when you are throwing them out. Crosscut shredders are recommended to grind paper into pulp. Remember, however, that you should not leave documents to be shredded in plain view in your office; a night janitorial staff can easily steal your information in a matter of moments, and you will never realize it happened because the paper was designed to be eliminated right away.

- When completing online forms, do not fill out any information that is not absolutely required (the required information often has a red asterisk indicating its necessity), and consider using Not Applicable or incorrect information for information fields with which you are not comfortable.

MINIMIZE YOUR INTERNET EXPOSURE

When surfing the Internet, your browser can provide information to Web sites about who you are, your computer setup, and information stored in "auto-complete" fields. To ensure privacy, it is important to reduce this exposure by *locking down your browser.* Within Microsoft Internet Explorer, this information can be eliminated by clearing the auto-complete, forms, and passwords buttons on the Content tab (under Tools, Internet Options).

Your browser also can collect information as "cookies," data stored on your computer you created when visiting a Web site. These cookies can make it easier for individuals to re-visit a Web site, but this information also can be used to provide information *to* the Web site, such as other locations visited. Today, a variety of tools can be used to view and eliminate this information, such as Cookie Crusher (www.thelimitsoft.com) and Cookie Pal (www.kburra.com), available for download from the Internet, as well as Cookie Dog (http://mitglied.lycos.de/atmani) designed specifically for the Mac.

In addition to minimizing your exposure to cookies and information provided by your browser, it also is possible to use anonymous remailers and relay Web sites to "strip" off any information about individual surfing. These sites act as a proxy to transfer information. Several Web sites that provide this service include Anonymizer (www.anonymizer.com), ReWebber (www.reWebber.com), and Zero Knowledge (www.zeroknowledge.com).

Finally, to minimize SPAM (unrequested e-mail) to your business e-mail address, use a public e-mail account such as Juno (www.juno.com) or Yahoo! (www.yahoo.com) when completing forms online or posting information. If you *must* receive business e-mail in this fashion, insert a character or wording so the address is obvious, but cannot be picked up by automated "Webbots" that capture such information (for example, Wayne(at)Anyco.com).

ORGANIZATIONAL PRIVACY

Organizations must also take privacy seriously and do all that is possible to minimize the risks, which can include damage to the entities' reputation, legal liability for damage, and in the end, a loss of business when customers and related parties lose confidence. Although the legal requirements for organization privacy are beyond the scope of this publication, it is important to be aware of adopted legislation with regard to privacy in domestic and international venues where the organization may conduct business. Listed here are some of the more notable privacy acts and legislation:

- The Privacy Act of 1974 applies to federal government entities, and allows personal information to be released only to law enforcement and census agencies without the individual's consent.
- The European Union Privacy Directive went into effect in 1998 with safe harbor provisions, including the United States taking effect in July 2000. This directive "reflects the principles of generally recognized Fair Information Practices that form the basis of the OECD Guidelines and most other recognized personal information protection codes."
- Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) took effect in 2001 and "establishes new rules for privacy recognizing the rights of individuals with respect to the collection, use, disclosure, and retention of their personal information. The rules also recognize the obligations of organizations to protect that privacy in a manner that a reasonable person would consider appropriate in the circumstances."
- The Graham-Leach-Bliley Act of 2001 requires all financial institutions or those engaged in financial activities to provide a privacy notice to their customers.
- The Health Insurance Portability and Accountability Act (HIPAA) takes effect in April 2003, and requires that health care providers have appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information.

PRIVACY POLICIES

Many organizations today have developed formal privacy policies listed on their Web sites that state specifically how the information will be used. These policies should be reviewed by the organization's legal counsel before implementation. Sample policies can be obtained from Better Business Bureau OnLine (www.bbbonline.org/privacy/sample_privacy.asp), CIO Magazine (www.cio.com/archive/040100/privacypol_content.html), and the Federal Trade Commission (www.ftc.gov/os/2000/05/privacyanthonyattach.htm).

EXHIBIT 10-1: RESOURCES

- CPA2Biz Privacy Resource Center (www.cpa2biz.com/ResourceCenters/Information+Security/Privacy/default.htm) is a resource center providing information about enterprise privacy and privacy services that can be provided by CPAs. Also available is "20 Questions Businesses Need to Ask About Privacy," a publication from CPA2Biz (order number 056591HI).
- Electronic Privacy Information Center—EPIC (www.epic.org) is a public interest research center in Washington, D.C. It was established in 1994 to focus public attention on emerging civil liberties issues, and to protect privacy, the First Amendment, and constitutional values.
- Identity Theft Reporting Center (www.idtheftcenter.org) is a nationwide nonprofit organization dedicated to developing and implementing a comprehensive program against identity theft by supporting victims of identity theft, broadening public awareness and understanding of identity theft, and decreasing the potential victim population.
- Privacy Foundation (www.privacyfoundation.org) exists to educate the public, in part by conducting research into communications technologies and services that may pose a threat to personal privacy.
- Privacy Rights Clearinghouse (www.privacyrights.org) is a nonprofit consumer information and advocacy program offering consumers a unique opportunity to learn how to protect their personal privacy.
- Privacy.Org (www.privacy.org) offers daily news, information, and initiatives on privacy. This Web page is a joint project of the Electronic Privacy Information Center (EPIC) and Privacy International.

Emerging Technologies Watch List and a Look Ahead

chapter 11

Each year, the Top 10 Technologies Task Force creates a set of emerging technologies for consideration. Sometimes, several of these technologies may already be available in the marketplace but may not be widely used by CPAs in their daily work and service deliverables.

■■■

EMERGING TECHNOLOGIES WATCH LIST

The 2003 Watch List includes ID/Authentication, M-Commerce, Tablet PC, and 3G Wireless.

ID/Authentication

This emerging technology is an addendum to information security (see Chapter 1, "Information Security") but is considered too important and too new to include it only as part of current information security practices and technologies.

ID/authentication focuses on current and evolving technologies for verifying the identity of a user who is logging onto a computer system or verifying the integrity of a transmitted message. Examples include password scenarios, digital signatures, biometrics, and dealing with issues such as IP spoofing.

As systems become even more sophisticated and security continues to be an ever-growing problem with regard to protecting sensitive information, verifying an identity and knowing *who*, for example, accesses a system, also will become paramount to the process. Although passwords, digital signatures, and biometrics are not new, they are not being used widely by the CPA community.

M-Commerce

Mobile commerce (m-commerce) uses smart phones and handheld computers with wireless connections to place orders and transact business over the Web. Even though widely accepted in Europe and the Far East, m-commerce has had slow adoption in North America.

There is quite a bit of information already on the Internet that focuses on m-commerce. A simple search on Google produced many pages, including the M-Commerce Times (www.mcommercetimes.com), a site with many articles and feature stories about American and European m-commerce initiatives.

Tablet PC

Tablet PCs include the next evolution of the personal computer in a tablet format that allows both handwritten and voice input to interact with the applications found on a computer. The system uses a pen-based stylus, in addition to the traditional keyboard (not required). Tablet PCs provide expanded portability because they can be used in a wireless environment.

The Tablet PC is a cross-breed that has the same physical characteristics as a laptop because it has a monitor, keyboard, and connectors. The added key feature is the capability of capturing text and diagrams written on the screen with a special stylus. Traditional business applications can be installed and used just like any other laptop or desktop. If you want to include Microsoft Word and Excel, a special Office Edition for the tablet is available. Tablet PCs represent a continuation in the evolving line of mobile computers, but there are a few drawbacks: Reliability will be questionable for a few years; built-in wireless features are not present; and handwriting recognition is imperfect.[1]

3G Wireless

Third-generation (3G) wireless systems are designed for high-speed multimedia data and voice with the goal of producing high-quality audio and video, and advanced global roaming—the ability to go anywhere and automatically be handed off to whatever wireless system is available (in-house phone system, cellular, satellite).

3G systems will provide access, by means of one or more radio links, to a wide range of telecommunication services supported by the fixed telecommunication networks and to other services that are specific to mobile users. A range of mobile terminal types will be encompassed, linking to terrestrial or satellite-based networks, and the terminals may be designed for mobile or fixed use.

There will be much more information about 3G in the near future. One online source includes Wireless NewsFactor (www.wirelessnewsfactor.com/perl/section/3gw).

[1]Richard Oppenheim, "Tablet PC—Painkiller OR Pain?," *InfoTech Update* 11, no. 1 (Jan./Feb. 2003), pp. 7–8.

XBRL UPDATE[2]

The Top Technologies 2003 program would not be complete without information on one of the CPA profession's most in-demand components—eXtensible Business Reporting Language (XBRL).

According to XBRL International,[3] XBRL is an XML-based reporting standard that provides a common platform for critical business reporting processes, and improves the reliability and ease of communicating financial data among internal and external users to the reporting enterprise. This royalty-free, open standard is being developed by a consortium of more than 170 companies and agencies to deliver benefits to investors, accountants, regulators, executives, business and financial analysts, and information providers.

Most CPAs and accounting professionals want to know how XBRL will influence their own delivery of services to their clients and customers, and while XBRL International and other countries involved in the project continue to develop new ways to incorporate XBRL into the business marketplace, a number of tasks are in development. In 2003, for example, a number of initiatives are underway, including:

- OneSource, a provider of information on companies from around the world, is now aggregating this information from multiple sources and delivering it as fully XBRL, version 2.0, valid instance documents. OneSource is using the U.S. generally accepted accounting principles (GAAP) draft taxonomy and extensions, and has submitted this information to XBRL-U.S. for consideration in the next release of the U.S. GAAP taxonomy.
- The Tokyo Stock Exchange now accepts company financial summary filings in XBRL, and in late 2003, will release improvements to this system.
- The new call report system from the Federal Deposit Insurance Corporation (FDIC) is entirely XBRL-based, resulting in more than 10,000 banks operating in the United States submitting quarterly financial status and performance

[2]Source: AICPA, "Progress Report—April 2003."
[3]See www.xbrl.org.

data in XBRL. In addition, other agencies, including the Federal Reserve and the Office of Thrift Supervision, are working closely with the FDIC to streamline data gathering and minimize compliance cost and flexibility.

In addition to these and other activities, formally established XBRL jurisdictions include the United States, Australia, Canada, Germany, the International Accounting Standards Board, Japan, the Netherlands, New Zealand, and the United Kingdom. In the United States, a special pilot program was launched in early 2003 to explore XBRL-formatted filings to be used by lending institutions for credit analysis or loans to small and midsize companies.

A number of vendors are currently in the process of developing XBRL-enabled tools and applications, which should stimulate increased adoption and use of XBRL. A number of these tools are scheduled to be released in 2003. For more information, regularly visit www.xbrl.org.

A LOOK AHEAD

If there is one certainty about technology, that is it *will* change, and often sooner rather than later, but like any crystal ball, knowing what lies ahead is a guessing game that at its best is uncertain.

This publication is filled with tips, tools, and resources, but the best use of technology within your own firm or business depends on your own situation and how comfortable you are incorporating any of these technologies into your business plan. The real key to this is to plan, plan, plan—and understand that you cannot change an entire system or even anyone's mindset overnight. Be patient, conduct your own research, and network with peers at national conferences or local gatherings.

The 2004 Top Technologies program is just beginning to take shape, and we encourage you to become an active participant. For more information, contact the AICPA at (212) 596-6211.