

**The Newest Technology Tools: (Un)Limited Access??**

A version of this article appears in *The CPA Journal*, January 2000.

Julia B. Earp, Ph.D.  
Assistant Professor of Management Information Systems  
College of Management, NCSU  
Department of Business Management  
Raleigh, NC 27695  
(919)513-1707  
julia\_earp@ncsu.edu

Laura R. Ingraham, Ph.D., CPA  
Assistant Professor of Accounting  
College of Management, NCSU  
Department of Accounting  
Raleigh, NC 27695  
(919)513-1436  
laura\_ingraham@ncsu.edu

J. Gregory Jenkins, Ph.D., CPA  
Assistant Professor of Accounting  
College of Management, NCSU  
Department of Accounting  
Raleigh, NC 27695  
(919)513-2476  
greg\_jenkins@ncsu.edu

*...today there are more than 150 million Internet users, Internet traffic growth doubles every 100 days, there are 67,000 new Internet users every day and 70,000 new web sites every hour. But the real growth on the Internet is business to business.*

Selby Wellman, Sr. Vice President, CISCO System, March 24, 1999

In the past, the widespread adoption of e-commerce has been stifled by concerns over the security and integrity of the transactions, but obviously that no longer seems to be the case. The U.S. Department of Commerce reported that Internet sales in 1998 reached \$9 billion, while IDC Research reported that global e-commerce reached almost \$29 billion (up approximately \$18 billion from 1997). The omnipresence, facility and economy of electronic data interchange make EDI increasingly important to businesses today. However, the growth of e-commerce has important implications when taken in conjunction with growing concerns over Internet fraud and computer security. For instance, consider that one-third of the information technology (IT) professionals recently surveyed said their company's information systems had been compromised in the past year and financial losses from these break-ins had exceeded more than \$120 million. While the benefits of engaging in e-commerce may be significant, there are substantial risks as well. What technological innovations have occurred that may influence the future of e-commerce and a company's ability to benefit from this explosive area? What additional security concerns and risks do these innovations pose to your firm and its ability to audit clients engaged in e-commerce? How will these innovations impact your firm's ability to understand client information systems and potential risks surrounding financial data?

## **TECHNOLOGICAL INNOVATIONS**

The latest addition to Intel's family of microprocessors is the Pentium III – a microprocessor with slightly better performance (no more than 8% for most business applications) and vastly improved capabilities for 3-D applications and graphics that are increasingly found on the Internet. Perhaps the most interesting characteristic of the PIII is the inclusion of a unique Processor Serial Number (PSN). Touted by Intel as an advanced security feature, the PSN provides a new method of identity authentication. Intel claims that Internet security is enhanced by allowing certain websites to "read" the user's PSN by running a program on the user's computer, thus "authenticating" the user's identity. Users retain the right, however, to prohibit the PSN to be read by these websites should they be concerned about the use of their PSN. The PSN may also serve to enhance the security of a company's internal information system. While passwords are commonly used security tools, the PSN affords companies an additional tool in the effort to combat misallocation or misappropriation of company funds and/or physical assets.

The PSN is not without its problems. Although the processor number is unique, it is read and recorded by other computers and it will only be a matter of time until IP-type spoofing programs are available to duplicate the PSN – allowing a user to appear as someone else. This raises obvious concerns for businesses in their role as both

consumers and suppliers. By using a fake PSN, a hacker can potentially make purchases in the company's name, sending the bill to the company's address but the goods to another location. Alternatively, a hacker could pose as a vendor submitting fictitious invoices to the company.

Since its release last year, Microsoft 98 has been beset with many obstacles. The most recent, however, concerns a discovery made by a programmer in Massachusetts (Richard M. Smith, president of Phar Lap Software). Smith discovered that the computer's Ethernet address was transmitted directly to Microsoft during the Windows 98 registration process. Information linking a computer owner and the computer's Ethernet address can certainly facilitate the job of an unauthorized individual attempting to access a company's confidential data.

What the average user is unaware of, however, is Smith's other discovery. This was not the first time Microsoft utilized a computer's Ethernet address in its applications. Microsoft's Office 97, a software suite that is present in many companies and organizations, has the ability to create sophisticated documents with embedded spreadsheets, presentations and databases. Office 97 accomplishes this in most small computer networks by linking each file using the computer's Ethernet address which is then electronically inserted into the document. Since Office 97 also documents author information, an author's name and Ethernet address can, therefore, be linked. In addition, a link would then be created to any other vital data (e.g., employee names, social security numbers, passwords, vendor and customer information) stored on that author's computer. To combat these concerns and potential risks, Microsoft has announced plans to make available a Unique Identifier Patch and Unique Identifier Removal Tool for users of its office suite. In addition, the company has announced that its new suite, Office 2000, will not include the ability to insert these numbers in documents.

Jini™, Sun Microsystem's newest networking technology software, is designed to simplify the addition of new hardware and software onto a network. The new software tracks all electronic devices, from computers to cellular telephones to digital cameras, that are connected to the network and provides a protocol for all hardware and software attached to the network. Jini makes it possible to add and execute new services effortlessly. However, the effortlessness with which they work also makes Jini-enabled devices vulnerable to unscrupulous persons. When a Jini-enabled device is connected to the network, it automatically broadcasts its presence and sends information about itself to any party with authorized or unauthorized access to the network.

***A Frightening Scenario:*** Assume for a moment that a cybercriminal is engaging in financial espionage, selling his information to the highest bidder. Since the cybercriminal is an experienced and thorough hacker known for providing very reliable information, he has obtained a database containing the PSN's of millions of PIII computers. Having heard that the black market has bid up the price for information in a particular industry, the hacker has singled out the industry leader, XYZ Corporation, as his next target. While lurking on the Internet, he intercepts an innocuous Office 97 document from Joe, a high-level executive in XYZ Corporation. While the document itself provides no valuable

information, the hacker can obtain the author's name and Ethernet number from the document. Once he circumvents the firewall, the hacker can go directly to Joe's computer, peruse his files, gain the Ethernet numbers of other high level executives from documents sent to Joe, and proceed directly to their computers.

## **SECURITY MEASURES**

When taken individually, it would not appear that any one of these new technologies poses a significant threat. However, they collectively exemplify the need for increasing awareness of the threats to an organization's data. It is important to recognize that new security measures are merely one step ahead of the computer hackers. As soon as a new security technique is developed, computer criminals begin looking for holes in the technique. A business with insufficient protection from the Internet can inadvertently provide an additional means for computer criminals to access proprietary information stored in the business' server or mainframe. The following is a partial listing of security measures that companies should consider.

*Firewalls:* A firewall is used to limit access to a computer network by electronically screening all network traffic, both internal and external, that passes through the network. Firewalls can be in the form of software, hardware, or a combination of the two. Recently, businesses have started installing firewalls onto internal servers within the intranet, an Internet-like network within the organization, to increase internal security of critical computer files.

[Insert Figure 1 about here]

Many organizations erroneously feel that, because they have installed a firewall, their data is impervious to attacks. While they are certainly a vital part of network security, any weakness in the network's security can be exploited by an experienced hacker. For example, hacker tools systematically scan hundreds of corporate networks and computer systems for vulnerability to various attack methods in as little as an hour. However, firewalls should not be dismissed simply because they can be circumvented. Organizations need to be aware of the true capabilities and limitations of firewalls to prevent being lulled into a false sense of security.

*Encryption:* Encryption is essentially the mutation of any form of information, whether it is text, video, animation, or graphics, so that it can only be readable by persons holding the decryption key. Encryption techniques are used to protect sensitive data and are a primary element of electronic commerce. These techniques protect information travelling across the Internet by making it more difficult for a hacker who obtains the encrypted message to recover the original data. Encryption techniques rely on encryption keys to transform the data into an unrecognizable form and then back again. Encryption keys which consist of a string of random bits must be stored somewhere, usually on a computer's hard drive. Everything else on the hard drive is filed in a logical, ordered fashion. Therefore, the chunks of randomness stand out. In response to the increasing

use of encryption, a new strain of computer viruses is being tailored to scan a hard drive for these chunks of randomness.

*Other Measures:* There are other inexpensive security procedures and practices a company might consider. For example, the business should take an “inventory” of its data to determine what needs protection and place the sensitive data on a server that has limited access or is physically isolated from those computers connected to the outside world. In addition, businesses can institute policies that require computers to be turned off during non-business hours – this reduces the opportunities outside parties have to communicate with the business’ computer system. Finally, business managers need to stay abreast of the changing technological landscape. For instance, managers should be aware of potential risks posed by new software, such as the popular *pcAnywhere*, which enables a user to remotely access their office computer.

And, when all else fails, there is insurance. Protection against loss is now being offered by a number of large insurance companies (e.g., Lloyd's of London, St. Paul, Cigna, Reliance National and AIG), but claims must be substantiated by proving that losses were caused by hacking and not by a computer glitch. Given that hackers can destroy any evidence of their presence using log modification tools by imitating a disk crash, such claims may be difficult to substantiate.

## **IMPLICATIONS FOR FINANCIAL DATA**

CPAs face a business landscape significantly different from that encountered just a few years ago and the pace of innovation promises to continually change that landscape into the foreseeable future. One of the greatest concerns centers around the core of financial reporting – the reliability of underlying financial data when data are created and stored electronically. Because such data may be more vulnerable to manipulation, auditors should direct significant efforts towards understanding a company’s IT function. Auditors must look first to management’s policies and procedures regarding computer security. Security is a policy issue, not a technology void. The technology exists to keep data secure but the use of technology must be backed by sound management policies and procedures.

SAS 80 explicitly recognizes the increased potential for improper initiation or alteration of financial data when data are produced, maintained and accessed only in an electronic format. Moreover, as some information exists only in electronic form, CPAs must carefully consider the nature, timing, and extent of their planned auditing procedures to ensure that the information is subjected to examination.

According to SAS 78, an additional consideration in the audit of electronic data is the internal control structure. Because many of a company’s controls may be of an electronic nature, CPAs need to be more knowledgeable about the operations of information systems. They may be required to evaluate controls either through observation or computer-assisted audit techniques. If they do not have the appropriate knowledge, then they must either obtain the necessary knowledge or employ the services

of another auditor who has the requisite expertise. In short, CPAs will need to be even more sophisticated in their use and understanding of IT.

CPAs should also assess a company's disaster recovery plan with emphasis on a company's ability to authenticate transactions, utilize data back-ups, and avoid business interruptions. Auditors should understand that outside parties can often emulate and circumvent the authorization process established by a company. In the event that such unauthorized access occurs, other parties could be harmed resulting in legal action against the company. Auditors should be aware of this possibility and should inquire about such claims as part of the normal process of obtaining a legal representation letter (SAS 12). In addition, auditors should recognize that the feature used to enable encryption also now aids in exposing it to viruses.

Many companies do not possess the resources or expertise of IT departments in larger organizations – such companies present auditors with additional problems. At the most basic level, CPAs should exercise special care in their evaluation of such company's information system and electronic data. Moreover, as these companies are frequently the targets of mergers and acquisitions, CPAs should be aware of the risks posed by the integration of information systems. Often times, in the heat of the merger or acquisition, companies are so focused on trying to achieve a smooth transition that they overlook any gaps or weaknesses that might exist in the information system of the target company.

Finally, the advent of the Internet has allowed many small startup companies to begin business with little more than a good idea. As it takes relatively little time to set up a web site and start transacting business, CPAs should exercise great care in evaluating the internal control structure and the financial records of such Internet-based companies.

## **SUMMARY**

There is no question that, as e-commerce continues to explode, cybercrime will continue to increase. In response, there will be a call for increased law enforcement and regulations, but the wheels of bureaucracy move infinitely slower than the wheels of progress. Management cannot afford to bide its time, awaiting the day when "cyberbusiness" becomes safe. CPAs need to work side-by-side with information technology departments to ensure the reliability of financial data and to assist businesses in taking every precaution necessary to thwart the efforts of cybercrooks. Although today's new technologies bring challenges and risks to business, many CPAs possess the knowledge which uniquely positions them to help companies turn these challenges and risks into opportunities.

**Figure 1. Firewall**

