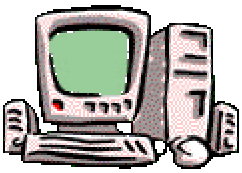
AUDITNEWS

Volume XXXII **Spring 2002**

FROM THE EDITOR…..



Did you know that defragging your computer might help it run better? Files and applications on your computer's hard disk drive are not always stored together as one unit, but are often divided into smaller units and scattered around the hard disk. This is caused by normal use.

Files on your computer are made up of tiny bits of data. Each time a file is saved, these bits of data are distributed to different parts of your hard drive. When a file is requested, the computer gathers all the bits together. Every time a file is saved, the bits of data are more widely dispersed and the computer needs to work harder to reassemble the file.

When you run "defrag" on your computer, it locates all the disseminated bits of information and repositions them so that all the bits are situated closer to each other. The more you use a computer, the more frequently you need to defrag. You will find the defrag tools by clicking on **Start, Programs,**

continued on page 2

INSIDE THIS ISSUE

1	From the Editor
1	Office of Student Services Receives Boston College 2002 Internal Control Best Practices Award
2	Internal Control Concepts to Prevent Fraud
3	The Enron Crisis: The Public Accounting Profession & The Public Interest
3	Building Business Relationships in the E-Marketplace
4	Security Vs. Privacy

OFFICE OF STUDENT SERVICES RECEIVES BOSTON COLLEGE 2002 INTERNAL CONTROL BEST PRACTICES AWARD

By: Bill Chadwick

B. Chadwick, L. Lonabocker, C. Cordella, P. Hayes

The Office of Student Services was recently awarded the eleventh annual Boston College Internal Control Best Practices Award by the Internal Audit Department. Student Services dramatically enhanced parking permit processing accuracy during the past year. Audit exceptions were reduced by 92% from the previous audit engagement.

Effective audit trails were established and parking permit stock safeguards were instituted. This great effort required the cooperation and support of all Student Services staff. Congratulations to Chris Cordella and all Office of Student Services staff for their great efforts in making this award possible. The Internal Control Best Practices Award is granted annually to the individual or department that demonstrates the greatest appreciation for controls during the past year.

continued from page 1

Accessories, System Tools, Disk Defragmenter. Keep in mind that this process usually takes a considerable amount of time, so you may want to start it before you leave your office in the evening.

INTERNAL CONTROL CONCEPTS TO PREVENT FRAUD

by: Bill Chadwick

This article will discuss some of the more important internal controls that reduce the risk of fraud. Although we all believe that a fraud could never occur in our departments, historical evidence exists to the contrary. When a fraud does occur, it is embarrassing to department management, and it can bring into question the adequacy of management's supervision of its employees. It is also important to remember that management is responsible for maintaining an adequate system of internal control. Therefore, a degree of culpability or perceived culpability usually results.

SEPARATION OF DUTIES

When it comes to fraud prevention, separation of duties is often the most important line of defense. In addition, it is usually more efficient to assign tasks to specific independent individuals, provided the volume of activity is sufficient. For example, it is usually better for one individual to process cash receipts through cash registers, and another person to independently count the cash and prepare paperwork for recording register sales in the university accounting system. Therefore, when comparing costs versus benefits of separating responsibilities, management should consider that benefits often include operating efficiencies, in addition to improved internal control.

If different individuals process two elements of a transaction, each person provides a check over the other. Separation of duties also acts as a deterrent to fraud or concealment, because collusion with another individual is required to complete the fraudulent act. Separating responsibility for physical security of assets from related record keeping, is a critical control.

In some instances, it may be impractical to institute effective separation of duties because the department has few employees. In these cases, management should institute more practical alternative controls including: (1) closely supervising administrative staff; and (2) comparing actual amounts to anticipated/budgeted amounts and investigating the causes of significant differences.

PHYSICAL SAFEGUARDS

To prevent theft or unauthorized processing of transactions in the University's Financial Accounting System, unnecessary access to University assets and financial records should be restricted. Negotiable assets such as cash, inventory, equipment and other items easily convertible to cash or personal use require adequate protection from improper use. Physical safeguards also apply to University financial records, and the means to alter record keeping including: unused forms, unissued checks, check signature plates, files, computer tapes, ledgers, etc. Confidential reports and documents should be stored in locked drawers and disposed of via shredding machines.

Physical arrangements should be designed to prevent unauthorized access to University assets and accounting records. Examples of physical security mechanisms include: a safe, vault, locked doors/desk drawers (with properly safeguarded keys), Boston College Police Department guards, computer passwords, and card key systems.

CONCLUSION

Preventing fraud is part of your responsibility as a member of Boston College administrative management. In addition, from a practical point of view, having a fraud occur in your department will infringe on the reputation of your department members and yourself. Therefore, it is best to implement the internal control concepts discussed earlier to avoid fraudulent acts from taking place.

SOURCE: *Evaluating Internal Control.* Johnson, Kenneth P., and Jaenicke, Henry. New York: John Wiley & Sons, Inc. Copyright Coopers & Lybrand. 1980.

THE ENRON CRISIS:
The Public Accounting Profession & The Public Interest

by: John Soto

By now, many people have heard about the Enron scandal, and are extremely concerned about their personal savings and retirement plans. Enron's collapse coupled with the downward spiral of the financial markets during the past year, have had a tremendous impact on the economy, and the personal investments of thousands of employees. Investors and the general public are particularly upset at Arthur Andersen & Company, Enron's public accounting firm. They feel that Anderson failed to sound the alarm, and warn the public about Enron's shady financial dealings and accounting irregularities. Hence, the unethical and possibly illegal behavior of a few renegade accountants, in one of over 45,000 public accounting firms, has tainted the public accounting profession. The American Institute of Certified Public Accountants (AICPA) recently made the following statement, in an effort to reassure the public:

"The AICPA is dedicated to taking the necessary steps to restore public confidence in the capital market system and accounting profession that may have been shaken by the Enron collapse. We represent more than 340,000 CPAs employed by businesses of all sizes and in all industries, by governmental bodies or by one of the over 45,000 public practice firms. These CPAs provide a wide range of valuable services and great advice to their clients and employers, large and small, across the United States and worldwide.

"The CPA profession has a successful, 100-year history serving the public interest through the core service of financial statement audits. We believe that the independent audit has contributed greatly to the issuance of reliable financial statements, which help attract the capital that finances American business. Close to 17,000 public company audits are completed successfully every year without restatement or allegations of impropriety. The AICPA provides invaluable guidance and tools to auditors to assist them in the conduct of audit engagements.

"The AICPA also plays a central role in establishing accounting and auditing standards. Our profession has zero tolerance for CPAs who do not adhere to the rules. In enforcing those rules, the self-regulatory process has generally been effective. However, the profession recognizes the need for improvements in oversight. Therefore, we have pledged to cooperate fully with SEC's proposal to change the regulation of the accounting profession. The proposal, as outlined by SEC Chairman Harvey Pitt on January 17, 2002, focuses chiefly on changes to the disciplinary and quality monitoring processes."

Hopefully, the regulatory measures being taken by the SEC, in cooperation with the AICPA, will restore public confidence in the capital market system and accounting profession. After all, employees want to rest assured that their personal savings and retirement plans will be in tact when they retire.

BUILDING BUSINESS RELATIONSHIPS IN THE E-MARKETPLACE

by: Frank Amara

The new online economy has mired a company's ability to decipher whether or not something is trustworthy. The Internet enables instant communication among businesses across the world. Who can you trust? Trust is a difficult concept to understand and yet it is one of the most significant aspects of building business relationships. There are currently over 250 countries in the e-marketplace. Most experts agree that virtual relationships have increased the potential for fraud. Swindlers rely on the trust of others to execute their crimes. Losses associated with computer fraud continue to increase every year. It is difficult to detect computer crime, and many computer-related frauds are not reported to law enforcement.

The Organization for Economic Cooperation and Development (OECD) has assembled 30 member countries who share a commitment to democratic government and the market economy. OECD's work covers economic and social issues including macroeconomics, trade, education, development, science, and innovation. OECD also produces internationally agreed instruments, decisions and recommendations to promote rules in areas where multilateral agreement is necessary for individual countries to make progress in a globalized economy. In addition, OECD attempts to deter international corruption. In a global economy, what constitutes a corrupt act in one culture may be consider legitimate in another culture.

In the global marketplace, sellers and buyers may not have the same sense of what are acceptable business practices. By not attaching personal harm to their acts, most cyber criminals are able to diminish the consequences of their acts. Also, the e-marketplace's anonymity enables potential cyber criminals to rationalize and justify destructive and fraudulent actions. Corporate cultures can guide employees to the right behavior. When a company decides to conduct business on the Internet, developing risk management initiatives into the corporate culture should be high priority. To prevent e-business fraud consider the following:

- Protect sensitive and confidential information.
- Know who you are dealing with over the Internet
- Use firewall technology to protect networks against viruses, hackers, and other malicious acts
- Use secure passwords, antivirus software, and encryption for sensitive data
- Maintain an awareness program to enlighten employees about ethical dilemmas

Source: Whom Do You Trust? Doing Business and Deterring Fraud in a Global e-Marketplace, Douglas M. Watson, Ph.D., CFE, "The White Paper" (a publication of the Association of Certified Fraud Examiners), Vol. 16, No.2, March/April 2002.

SECURITY VS. PRIVACY

by: Pamela Jerskey

The rapid growth of computer technology has made it difficult to maintain and monitor privacy of information. Because computer information flows over the Internet at such high speeds, there is easier manipulation, dissemination and merging with other data that could compromise individual privacy. The right to privacy, in relation to technology, elicits strong and controversial philosophical debate. Most individuals probably expect that privacy is a fundamental right. However, the right to privacy is not explicitly mentioned in the US Constitution. While the Fourth Amendment does not have the word "privacy" in it, common law doctrines, public opinion, and state constitutional provisions have reinforced privacy rights. After the September 11th terrorist attacks, does the right to privacy debate still produce intense deliberation? In order to research this question, privacy issues need to be broken down into two categories: (1) consumer privacy rights and (2) electronic seizure and surveillance practices.

Consumer Privacy Rights Before September 11th

Public opinion has always been a strong factor in influencing government and industry to consider changes to certain nationwide practices, policies, and procedures. Various organizations provide forums for public opinion. One such entity, the Berkman Center for Internet & Society at Harvard University was founded in the 1990s to explore and understand cyberspace, and to discuss standards, laws and sanctions for Internet use. Another organization that provides a public forum for privacy advocates is the Electronic Privacy Information Center, which was established in 1994.

In 1999, a Business Week / Harris poll confirmed that Americans were concerned about their privacy. This concern and mistrust regarding what vendors were doing about protecting and dissemination personal information kept many individuals from using the Internet for commerce. "The poll, published in the March 16, 1999 issue of Business Week, reveals that almost two-thirds of non-Internet users would be more likely to use the Net if the privacy of their personal information and communications were protected."[1] The survey asked consumers if they shop online, were they concerned that a company would use personal information to send unwanted information back to them. In 1998, 31% of consumers replied that they were "very" concerned. When the save question was asked in 2000, 41% of consumers replied that they were "very" concerned. In two years, American consumer concerns about privacy increased thirty-three percent.

Electronic Seizure and Surveillance Practices Before September 11th

The FBI routinely conducts lawful electronic surveillance of telecommunications of criminal suspects. In recent years, the FBI found that the Internet was routinely used for criminals to communicate with each other, which made it more difficult to scrutinize criminal correspondence. In 2000, the FBI created a new diagnostic tool to wiretap the Internet called "Carnivore" because Internet Service Providers could not discriminate between communications. Carnivore works like a sniffer and helps the FBI collect specific electronic communications that may be lawfully intercepted while ignoring others. According to the FBI, the use of Carnivore is subject to intense oversight from internal FBI controls, the U.S. Department of Justice and by the Court. The FBI contends that the system is not subject to abuse because installation and operation requires expertise, and must be performed in close cooperation with ISPs.[2] Privacy groups are concerned about how this new system could be used, and what constitutes a reasonable search. They are also concerned about how the Fourth Amendment and federal wiretap laws will be applied to the Internet.

In July 2001, Andrew Schulman, Chief Researcher for the Privacy Foundation, conducted a workplace surveillance project. This study endeavored to estimate workplace monitoring with a focus on continuous, systematic monitoring of employees, rather than random spot-checks. The study found that approximately one-third of online workers in the United States have their Internet or e-mail use under continuous surveillance at work. According to the survey, employers monitored Internet use and e-mail to scrutinize productivity and to limit liability for sexual harassment or other employee online misbehavior.

---

[1] "Survey Information: Americans Care Deeply About Their Privacy," Center for Democracy and Technology, http://www.cdt.org/privacy/guide/introduction/surveyinfo.html.

[2] FBI Programs and Initiatives, Carnivore Diagnostic Tool, http://www.fbi.gov/hq/lab/carnivore/carnivor2.htm

Carnivore and workplace surveillance software are two examples of how individual privacy rights could be intrude upon. Some federal laws that have been passed that deal with privacy issues in relation to electronic seizure and surveillance include the Federal Wiretap Act, the Electronic Communications Act of 1986, and the Privacy Act of 1974.

Consumer Privacy Rights After September 11th

The attacks of September 11th seemingly shifted nationwide concerns from privacy issues to security issues. Anti-terrorism investigations could require corporations to divulge employee records, consumer information and financial records. Bob Evans, Editor-in-Chief of Information Week stated in an editorial, that because of September 11th, privacy issues and questions would continue to be hot topics. "We are a nation that cherishes many types of freedom, including privacy. We are also a nation at war, against a brutal and ruthless enemy whose forces clearly live among us. In such a context, we need to be willing to think long and hard about exactly what privacy is and what it is not."[3]

After September 11th, various news media showed that several of the terrorists were known to US intelligence officials. Technology exists that could have been used to thwart the attacks. For example, potential terrorist names could have been linked to commercial databases such as Visa or MasterCard. Business Week reports that in the future, more technologies will be used to search out terrorists and "it's likely to drive a broad expansion of the use of intrusive security measures. Polls taken since September 11th show that 86% of Americans are in favor of wider use of facial-recognition systems; 81% want closer monitoring of banking and credit-card transactions; and 68% support a national ID card. But the quest for safety is also going to come at an incalculable cost to personal privacy."[4] This is such a contrast to previous mentioned polls in 2000 that showed 41% of consumers were very concerned about their privacy.

Electronic Seizure and Surveillance Practices After September 11th

The single most compelling regulation enacted since September 11th is the USA Patriot Act, which was signed into law on October 26, 2001. This law has many provisions. Several significant provisions that impact privacy are: (1) to allow a trapping device to identify a source (but not content) of a wire or electronic communication; (2) to permit seizure of voice mail messages under a warrant; (3) to allow intercept of electronic communication of a computer trespasser; and (4) to permit service providers to make emergency disclosures to a government entity.[5] The Patriot Act provides investigators with more flexibility and greater access to high-tech tools that includes interception of e-mail messages and monitoring of Web surfing. Privacy advocates feel that personal liberties could be infringed upon by misuse of powers permitted under the Patriot Act.

It is the Electronic Frontier Foundation's opinion that the Patriot Act impinges on the civil liberties of Americans in the area of privacy and on-line communications. EFF's position is that the government did not prove that prior means of investigation were insufficient for the government to expand powers for terrorism. EFF stated that the law is "amplified by the inclusion of so many provisions that, instead of aimed at terrorism, are aimed at nonviolent, domestic computer crime."[6]

Another tool the FBI is developing to eavesdrop and monitor computer use is called "Magic Lantern."[7] Magic Lantern technology would allow investigators to secretly install software via the Internet that records keystrokes on personal computers. The FBI is concerned about being able to read encrypted messages in criminal or terrorist investigations. Several recent news stories on the web show how controversial this software product is. Specifically, it is rumored that McAfee Antivirus Software Company contacted the FBI "to ensure its software wouldn't inadvertently detect the bureau's snooping software and alert a

---

[3] B. Evans, "A New Definition of Privacy", Information Week (October 2001).

[4] "Privacy in an Age of Terror", Business Week (October 2001).

[5] "Provide Appropriate Tools Required to Intercept and Obstruct Terrorism (PATRIOT) Act of 2001", H.R. 2975, (October 2001), http://thomas.loc.gov/cgi-bin/query/D?c107:6:./temp/~c107qmrdAF::

[6] "EFF Analysis Of The Provisions Of The USA PATRIOT Act That Relate To Online Activities", (October 2001), http://www.eff.org

[7] T. Bridis, "FBI Develops Eavesdropping Tools," (November 2001), http://www.washingtonpost.com/wp-dyn/articles/A1436-2001Nov22.html

criminal suspect."[8] Another article highlights how antivirus vendors are debating the pros and cons, and discussing the ethics of putting Magic Lantern on their virus definition lists.[9] Privacy advocates raise questions about the legal aspects of this tool and how it would be incorporated into existing laws.

September 11th certainly changed the scope of privacy considerations for US citizens. We went from a society who was very concerned about privacy to a society who was more concerned about personal security and willing to sacrifice some privacy for security. But how long will this last? As more government intrusions take place, privacy advocates will continue to question the necessity of greater access to information and how to protect privacy. As privacy concerns gain more attention and as technology advances, current laws must be examined and updated. The line between consumer privacy rights and electronic seizure and surveillance practices has narrowed for now, but in the future, as always, the pendulum will swing the other way.

[8] D. McCullagh, "Lantern' Backdoor Flap Rages" (November, 2001), http://www.wired.com/news/conflict/0,2100,48648,00.html

[9] J. Leyden, "AV vendors split over FBI Trojan snoops", (November 2001), http://www.theregister.co.uk/content/55/23057.html