AUDITNEWS

Volume XXXIII **Fall 2002**

DID YOU KNOW?.....

A BusinessWeek article recently reported that your desktop is 400 times dirtier than a toilet seat. YUCK! Chuck Gerba, a professor of microbiology at the University of Arizona, sampled several hundred workstations and reported that a phone receiver has an average of 25,000 bacteria per square inch, your desktop has 21,000 bacteria per square inch, and your keyboard has 3,000 bacteria per square inch. How does that compare to the average office toilet seat? Just 50. The average desktop is rarely cleaned. What's the remedy? Stock yourself with disinfectent wipes and get to work!

INSIDE THIS ISSUE

WORKSTATION SECURITY

by: Pamela Jerskey

Many of you are or will be getting new computers through BC's Desktop 2003 Computer Replacement project. We thought this would be a good time to remind everyone about workstation security. The increased use of technology to streamline operations has also increased network security vulnerabilities. Because all systems are networked, one compromised system can lead to other compromised systems. Security threats have escalated over recent years and include **software bugs, configuration errors, implementation mistakes,** and **social engineering**.

Software can have defects that allow an attacker to get information from your computer. Users can minimize exposure to this type of vulnerability by installing patches from vendors as soon as possible. The **configuration** of your system can affect security. Some features or settings can be activated by default and expose your system to network vulnerabilities. It is important to review and understand all settings on your computer that affect security. **Implementing** custom programs may create vulnerabilities that can be exploited. When implementing programs, it is important to consider all security implications.

Social engineering is a hacker's use of psychological tricks on legitimate users of computer systems in order to gain information (usernames and passwords) needed to gain access to the system. These messages typically offer the opportunity to download software of some value to the user, including improved music downloads or anti-virus protection. Once the user downloads and executes the software, a Trojan horse or backdoor programs could be installed. Here is an example of a message:

> You are infected with a virus that lets hackers get into your machine and read your files, etc. I suggest you download *[malicious url]* and clean your infected machine. Otherwise you will be banned from *[IRC network]*.

continued from page 1

This is purely a social engineering attack since the user's decision to download and run the software is the deciding factor in whether or not the attack is successful.

Data stored in databases and file systems has become increasingly valuable and mission critical to the University. Electronic data should be protected through a series of security measures. Word, Excel, Access, and PowerPoint provide various features to protect documents from changes and unauthorized access. Security practices include:

- controlling access to sensitive documents using file access protection through a password in order to open or modify a document.

- using passwords that meet minimum basic standards. Default passwords shipped with servers, operating system software, or applications should always be changed when the hardware or application is installed or implemented. Some basic password guidelines include configuration of (1) 5-8 characters in length, (2) alpha and numeric characters, (3) a word not listed in the dictionary, and (4) a word not easily associated with you, especially your first or last name. In addition, passwords should not be shared, displayed or written down, or given to another employee.

- using virus protection. Automated virus protection software should periodically scan your workstation for potential virus, worms, and other infections as well as provide regular updates. Most viruses today, as well as other threats, try to enter your system via email, in the form of email attachments. These viruses may appear to be documents sent by someone you know or don't know who happened to have your address on their computer. Don't open suspicious email attachments, even if they seem to come from friends or colleagues.

- defining user-level security for shared files and folders. User-level security should be applied so that only authorized users may view, access, or modify selected information.

- delete accounts on departmental workstations quickly after the termination or transfer of an employee.

- using "Guest" access sparingly.

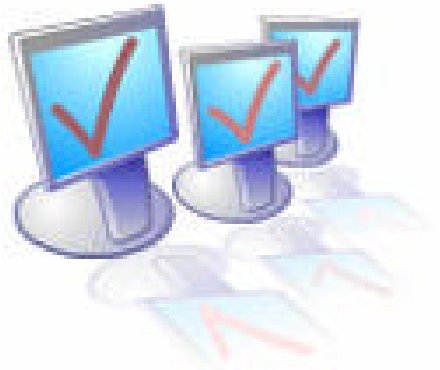
- limiting access to the system registry. The system registry should be limited to administrators or authorized users. The integrity of your workstation can be compromised by changing registry entries.

- logging off your computer when leaving your office. Someone could walk up to your PC and access the information stored on it or on your server. Also, if you are still logged onto your e-mail account, someone could send an e-mail message under your user ID. Remember to close and sign-out of your e-mail account when you leave your office.

- disposing your confidential material in a responsible manner.

- keeping back up copies of important documents.

- securing physical equipment. Even with the best software technologies, equipment can be stolen.



INTERNAL CONTROL CONCEPTS

by: Bill Chadwick

I thought this might be a good time to provide a refresher concerning internal control concepts. I will discuss *authorizations, validation, and accuracy and completeness of data*. There are, of course, other elements of internal control. However, I will discuss them in future articles.

AUTHORIZATIONS:

Authorizations may be ***general*** or ***specific***. Giving a department permission to expend funds against a budgeted amount is an example of a ***general*** authorization. ***Specific*** authorizations relate to individual transactions and require formal approval signatures by University personnel having proper approval responsibility. It is important to remember that the Boston College employee approving the transaction is assuming responsibility for authentication of the transaction. Approvers should understand what information is required on the document to justify the document's correctness before they sign it. For example, approving an expense report requires that the approver examine supporting documentation (hotel bills, restaurant receipts, etc.), checking the math on the expense report, and determining that the expenditures are in accordance with the Boston College Travel Policy. You should be familiar with the travel policy in order to complete your task.

For a transaction to be properly authorized, it must be approved by a person having (1) proper authority to approve, and (2) competence to do so under the conditions specified by the system. The key control element of the approval process is the ***independent*** approval evaluation provided by the approver. Ideally, the individual initiating the transaction should receive approval from a BC employee at a higher professional level (step-up approval). Approval authority may also be linked to specific dollar approval levels. Transactions that exceed the specified dollar approval level would require additional approval by a higher level professional.

VALIDATION:

Validation of transactions requires establishing controls to ensure that only valid transactions are recorded, i.e., entered on a document or into a computer file that can later be compared with accounting records, reports or other documents. For example, matching vendor invoices to receiving reports and purchase orders prior to payment provides assurance that the University is only paying for items actually received, and in accordance with terms and prices determined by the Purchasing Department.

ACCURACY AND COMPLETENESS:

Numbering all transactions as soon as they originate (or using pre-numbered documents) and accounting for the documents as being processed is a standard control practice. The control procedure is the act of checking to see that all numbered documents complete the expected processing. This control can be accomplished via a log maintained in number sequence. Many BC systems are currently in a batch mode although this methodology is changing to on-line input of data. Data input into the computer system via the batch mode should be agreed to computer-generated data output to ensure completeness and accuracy of processing. Differences that arise should be investigated and appropriate corrections processed. Reconciliations are critical controls that ensure completeness and accuracy of transactions. They are particularly important where stand-alone subsystems exist. For example, a stand-alone subsystem used to process revenue transactions should be reconciled to deposit slip totals and the Financial Accounting System to ensure that amounts received are properly deposited in University bank accounts and recorded accurately in the financial records. Reconciliations should be formal documents. They should also be reviewed and approved by department management.

If you have further questions concerning the concepts discussed in this article, or if you would like additional information, please email me at bill.chadwick@bc.edu or give me a call (2-3294).

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

COPYRIGHT LAW PROTECTION VS. THE PUBLIC DOMAIN

by: John Soto

INTRODUCTION

During their current term (October 2002 to June 2003), the United States Supreme Court will decide a landmark copyright case (Eldred v. Ashcroft, No. 01-618). The Court's ruling will undoubtedly have a great impact on colleges and universities, and anyone who utilizes the public domain (e.g. scholars, educators, librarians, archivists, historians, authors, publishers, artists, musicians, and theatrical performers). Specifically, the Court will decide on the constitutionality of the Sony Bono Copyright Term Extension Act (CTEA) of 1998. The plaintiffs argue that the CTEA copyright term extensions are unreasonable, and violate the Constitution.

HISTORICAL BACKGROUND

The U. S. Constitution (Article I., Section 8, Clause 8) provides that Congress has the power "to promote the progress of science and useful arts, by securing for limited times to authors and inventors the exclusive right to their respective writings and discoveries."

Based on that power, the First Congress passed the first Copyright Act in 1790. They modeled the 1790 Act on the 1710 Statute of Anne in England, which was the first copyright protection law in the world. The Act granted 14 years of protection with a provision for a 14-year renewal providing that the author were alive. Once those terms elapsed, the protected works would flow into the public domain. During Congress' prior debates and deliberations, preservation of the public domain was a central issue. Since 20 delegates of the First Congress were among the 55 original Founding Fathers, the First Congress was in position to properly interpret the Constitution's copyright clause. They knew that protection from excessively long copyright monopolies was a fundamental right of the people. Hence, the "limited times" language in the copyright clause makes it clear that the constitutional Convention did not want Congress to have power to grant perpetual copyright.

Several copyright laws enacted between 1790 and 1909 encouraged an expansion of the public domain, and the term extensions were few and modest. Copyright laws since have dramatically suppressed the growth rate of the public domain. The Sony Bono CETA of 1998 has been the most aggressive extension to date. It grants exclusive rights for the life of the author plus 70 years. If the life of the author cannot be ascertained, it then provides rights for 95 years after publication or 120 years after the creation of the work, whichever is shorter.

CHRONOLOGY OF CASE

The class action, headed by plaintiff Eric Eldred, was originally filed against Janet Reno in the U. S. District Court for the District of Columbia. The judge upheld the constitutionality of the CTEA (74 F.Supp 2d 1, 1999). Eldred appealed via a Writ of Certiorari to the U.S. Appeals Court for the District of Columbia. The Appeals Court also upheld the constitutionality of the CTEA (255 F.3d 849, 2001). The case is now before the U. S. Supreme Court, who will rule on it during their current term (October 2002 to June 2003). In fact, the Court heard oral arguments in this case on October 9, 2002.

THE ISSUE BEFORE THE U. S. SUPREME COURT

The plaintiffs seek the U. S. Supreme Court's reversal of the lower court decisions. They contend that under those decisions, Congress may at or before the end of each such "limited period" enact a new extension, apparently without limitation. This they feel is unconstitutional, in that it exceeds the power conferred to Congress by the Copyright Clause. Moreover, they argue that such extensions do not "promote the progress of science and useful arts," which was the intent of the Founding Fathers. The defendant argues that determining "limited times" is within the discretion of Congress.

Although the plaintiffs lost in the lower courts, their position has since been strongly reinforced by new arguments. These arguments are contained in several *amici curiae* briefs filed with the Supreme Court. In my opinion, the most thorough and convincing brief (2001 U.S. Briefs 618, 2001) was submitted by a coalition of several professional organizations (e.g. Society of American Archivists, American Library Association, American Association of Law Libraries, and Medical Library Association,

and Digital Future Coalition), whose members are adversely affected by restrictive copyright laws. They submitted the brief to assist the Court's understanding of the practical consequences of this unique case for large segments of the public.

IMPACT OF THE CTEA ON COLLEGES AND UNIVERSITIES

The CTEA inhibits educators' efforts to provide students with texts in electronic form. As we know, electronic teaching tools have become an important resource for educators. The creation of such pedagogical tools becomes difficult or impossible if the information needed remains under copyright protection. The CTEA also greatly affects educational enterprises by adding to the cost of books that are commonly assigned for class use. Moreover, copyright term extensions create huge burdens for scholarship, documentary filmmakers and authors, and severely limit the publication of scholarly works.

Many colleges and universities have libraries that possess large holdings of original unpublished manuscript and photographic materials, which they could freely disseminate if the materials were in the public domain. Once the materials are in the public domain, scholars could use them without having to worry about "fair use doctrine" concerns. Nor would they have to worry about tracking down, getting consent from, and paying licensing fees to the owners of the copyright. Educators, archivists, librarians and their organizations serve the public without commercial gain. They seek only to benefit users through promoting accessible information, exposure to arts and sciences, and cultural enrichment, drawing in part on the public domain. Their goal is precisely what the Framers of our Constitution intended with the Copyright clause wording "to promote the progress of science and useful arts."

For additional information, see BC Library's website for information on copyright and fair use http://www.bc.edu/libraries/resources/ejournals/copyright/

Source: Federal case law and briefs filed in the U. S. Supreme Court