

AUDITNEWS

Volume XXXI

Fall 2001

Inside this Issue

1

From the Editor....

1

Top Twenty Computer Security Vulnerabilities

2

Are Checks Really as Safe as You Think

3

A Refresher Course in the Use of Procurement Cards

3

Writing in Plain English

Produced by the Boston College
Internal Audit Department

FROM THE EDITOR....

In these stressful times, it is important to maintain a sense of humor. Internal auditors, of course, are known for their keen sense of humor and convivial personalities. Being audited is just a bundle of laughs. Wouldn't you agree? Yes, I thought so! To demonstrate our humorous profession, I submit the following letter to Dear Abby as evidence:

DEAR ABBY:

I am getting married in the near future. However, I have some relatives who have questionable backgrounds, and I am not sure whether I should tell my fiancé about them.

My cousin was arrested for shoplifting. My brother is a bank robber. My father is an embezzler. My niece was arrested for assault and battery. My nephew was indicted for insider trading violations, and my second cousin is an internal auditor.

My question, Abby, is whether I should tell my fiancé that my second cousin is an internal auditor?

It's important when times of stress are upon us to not take everything so seriously – especially receiving a visit from your internal audit department. So, spread the word in your organization. Tell everyone that **INTERNAL AUDITORS ARE A BUNDLE OF LAUGHS!**



TOP TWENTY COMPUTER SECURITY VULNERABILITIES

by: *Pamela Jersey*

In our Spring 2001 Newsletter, we delineated top Internet and cybercrime threats. In keeping with this theme, we wanted to let you know about the top twenty computer security vulnerabilities issued by the FBI along with the Systems Administration, Networking and Security (SANS) Institute, which was published in October 2001. The list includes seven security problems that affect all systems, six vulnerabilities specific to Microsoft servers, and seven flaws that affect various flavors of Unix, including Linux and Solaris. The list also includes many common-sense steps that system administrators can take to secure their networks. Hackers use the easiest and most convenient way to exploit well-known computer and Internet flaws. They use widely available Internet tools. They count on organizations to not fix problems and scan networks for vulnerable systems.

General Vulnerabilities that Affect All Systems:

- **Default installs of operating systems and applications.**

Most software is written with install scripts to get the system implemented quickly. Usually more components are installed than are necessary. Typically users do not actively maintain and patch software they don't use. Attackers can take over computers through these unpatched services. Turn off unnecessary services, close irrelevant ports, and remove any software that you do not use.

- **Accounts with no, weak, or default passwords.**

Passwords are used as the first line of security over your system. Easy to guess passwords (typically those found in a dictionary) are significant problems. Additionally, many systems have built-in or default passwords so various vendors can perform maintenance on systems worldwide. Hackers commonly look for default accounts because they are well known and published on the Internet. Change passwords on default accounts. Remove all accounts from your system with weak or no passwords.

- **Non-existent or incomplete backups.**

Recovery from system problems requires up-to-date backups and knowledge of restoring the data. Another problem involving backups is inadequate physical protection of the backups. An inventory of all critical systems should be identified. Depending on the importance of your data and time required to re-input it in the event of an interruption, backups should be made daily and properly stored.

- **Large number of open ports.**

Systems maintain open ports so users can connect to utilize applications. More open ports provide more possibilities that someone can connect to your system. The system administrator should understand what is running on each port and provide justification to leave that port open. Extraneous ports should be closed.

- **Not filtering packets for correct incoming and outgoing addresses.**

IP spoofing is commonly used by attackers to conceal their malicious activity. Spoofed packets are sent to the victim's computer that results in shutting down the computer or the network. Filtering incoming traffic on your network delivers a higher level of security.

- **Non-existent or incomplete logging.**

In the event that your system is attacked, audit logs provide detail records that can be reviewed to discover what the attackers did. By reviewing the logs, you can decide to patch the current system or restore the original operating system and reload your backed up data. Logging should be done on a regular basis and the logs should be reviewed, backed up and appropriately stored.

- **Vulnerable CGI programs.**

Common Gateway Interface (CGI) programs are web-based applications that are similar to databases. They collect and verify data. Hackers can exploit vulnerable CGI programs to deface web pages and set up areas where they can later enter the system. Remove sample CGI programs from your web server and make sure that all current CGI-related patches are applied.

Details on the above general security concerns and top Windows and Unix system vulnerabilities can be found at: <http://66.129.1.101/top20.htm>



ARE CHECKS REALLY AS SAFE AS YOU THINK?

By: Bill Chadwick

Most people believe that because checks are used instead of cash in financial transactions, that the transactions are safe, secure and fraud proof. **Think Again!** In the United States 65 billion checks are written annually. It is estimated that fraudulent checks will

cost the economy \$10 billion this year. Illegal activity involving checks increased by 25% from 1999 to 2000, a huge increase for one year. Even more disturbing is the fact that banks will only bear about one-tenth of the losses, with customers absorbing the rest.

One major misconception we have is that because a check is made out to the payee we intend to send it to, that it is safe. How can a check made out to Boston College be cashed by anyone other than the University? Aren't banks checking deposits to identify checks that are addressed to someone other than the depositor? The simple (and surprising) answer is **No!**

For example, Meta-Sure Health thought they were secure in processing checks until they discovered that an employee intercepted 60 checks totaling \$92,000 made out to Meta-Sure Health and sent them with her credit card payment slips. Without exception, the credit card companies credited them to her account. In turn, the checks were paid by the bank they were drawn on even though they were payable to someone else.

How is it possible that banks are not catching these simple frauds? The reason is that banks process nearly all checks by machine. Rarely does a person ever actually view the check. It is not practical for banks to process 65 billion checks annually and have someone review each check before processing it for payment. Banks use software to flag exceptionally large amounts, out-of-sequence checks, and checks printed on non-check stock. However, misappropriated checks are not identified.

Banks are very slow to compensate victims. In the case of Meta-Sure Health, only 25% of the \$92,000 has been recovered from the bank for the 60 checks that were diverted. Customers lose out because it is economically impossible for a consumer to sue a bank over a \$5,000 check because the legal fees will exceed the amount of the check.

What can we do to help prevent misappropriation of checks? The most important prevention mechanism is to

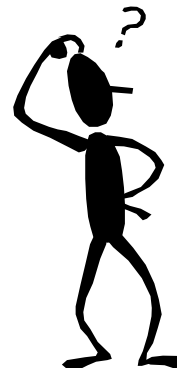
have an effective system of internal control in your department. Specifically, you should ensure that there is proper separation-of-duties for individuals involved in the receipt or disbursement of checks. In terms of outsiders, knowing your customers/vendors is

important in judging risk.

SOURCE: Business Week, August 13, 2001, pp. 70-71, "Good Times for Bad Paper" by Pallavi Gogoi.

Writing in Plain English

by: John Soto



A REFRESHER COURSE IN THE USE OF PROCUREMENT CARDS

By: Frank Amara

The use of procurement cards is an effective method of purchasing goods and services with a value of less than \$1,000. Purchases should relate to University business only. Use of the card for personal purchases is strictly prohibited. The procurement card is issued to individual employees. Department personnel with budget responsibility for a particular General Ledger account designate spending limits for each card issued.

Before purchases can be made, sufficient funds must be transferred to the #320 subcode account. Using the card is similar to using any credit card. Purchases may be made in person at any store that accepts Visa, over the phone, by facsimile, or through a secured Internet connection. Single purchases cannot exceed \$999. In addition, certain commodities, regardless of the amount, are specifically disallowed from Procard use. (These commodities are listed in the Purchasing Card Users Guide.) To maximize efficiency, departments should order from suppliers who are authorized University contract suppliers, wherever possible.

Upon placing an order, the purchaser must inform the vendor that Boston College is tax exempt to ensure the University is not charged a state sales tax. Cardholders are also responsible for following up with merchants for erroneous charges, disputed merchandise, or returns.

Departments are responsible for retaining documentation and will be subject to review by Internal Audit. Documentation must also be maintained and available for audit review by federal, state, or private agencies for externally funded projects. Federal regulations require that supporting documentation, (receipts, etc.) be maintained for three years after submission of the final expenditure report. Proper record retention by the Principal Investigator is essential because the University is required to reimburse the agency for the amount of unsupported transactions.

Finally, each department is required to reconcile Procard transactions. Specifically, original receipts should be matched to the monthly bank statement amounts and to the AMO 90 charges in the #320 subcode.

For more information, go to: http://www.bc.edu/bc_org/fvp/purch/

I sometimes have difficulty clearly expressing my ideas in writing, but I guess I am not alone. Many writers often produce complicated, jargon-filled documents that often mislead, confuse and frustrate readers. Government documents and regulations are notorious for being difficult to understand. If their authors were to write them more clearly, the documents would improve compliance, and increase trust in government. Recognizing this as a major problem, President Clinton, in 1998, issued a presidential memo requiring agencies to use plain language principles.

This memo was in line with his Executive Order #12866 of 1993, which set up a program to reform and make more efficient the regulatory process. Among the Order's many mandates was that "All information provided to the public by the agency shall be in plain, understandable language."

To assist in reaching that goal, the Plain English Network (PEN) emerged. PEN is a government-wide group of volunteers working to improve communications from the federal government to the public. Their website (<http://www.plainlanguage.gov/>) contains a wealth of information that could benefit all writers, including us at Boston College. One of its most useful tools is a guidance manual, *Writing User-Friendly Documents*. The manual can help you write plain language documents that are understandable by

your readers at first reading. Some of the techniques are writing skills--using simple words and phrases instead of unnecessarily complicated and wordy ones. Others are presentation skills--displaying the information in a way that is readable and visually appealing.

The PEN website lists these three guiding principles:

- Use reader-oriented writing. Write for your customers, not for other government employees.
- Use natural expression. To the extent possible, write as you would speak. Write with commonly used words in the way that they are commonly used.
- Make your document visually appealing. Present your text in a way that highlights the main points you want to communicate.

The PEN website also contains links to other plain language sources. One of the sources is a link to *Plain Train*, an online training program developed by the National Literacy Secretariat, Canada. In the tutorial, you board a train, and the conductor takes you on a tour of eight topics. It contains many helpful tips and techniques for improving your communication skills with the use of plain language.

There are many misconceptions about plain English. Plain English is not a simplified style of writing, and does not mean writing in kindergarten language. It involves more than replacing jargon and complex language with shorter sentences and familiar words. Plain English looks at the whole message - from the reader's point of view. This means pitching the language at a level of sophistication that suits the readers. Plain English gives the readers a good chance of understanding the document at first reading, and in the same sense that the writer meant it to be understood.

Here are two more excellent reference tools:

The AskOxford.com website
<http://www.askoxford.com/betterwritin>

[g/plainenglish/](#)) offers tips for keeping your writing user-friendly, and a Quick Reference Plain English Guide.

The Guide to Grammar and Writing website:

<http://ccc.commnet.edu/grammar/>) explains grammar concepts, presents samples of different forms of written communication, and makes available PowerPoint presentations on several grammar topics.

