AuditNews

Produced by: Internal Audit (617) 552-8689 **Spring 2006** Volume XXXX

Save the Date.....

Wednesday, April 5th, 10-11:30
Business Ethics and Controls Workshop
(McElroy Conference Room)

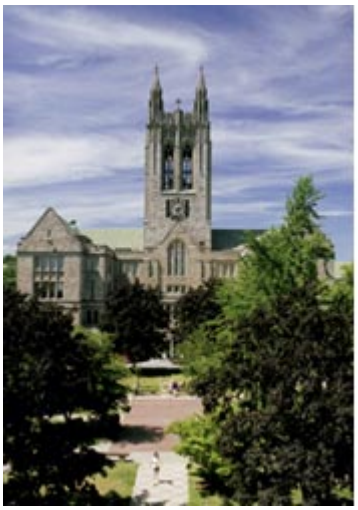
"Ethics is a "hot" topic in today's business world. How can we be proactive to prevent theft or fraud? In this interactive session, you will learn (1) ways to identify risks, (2) how to implement procedures to improve your controls, and (3) appropriate actions to resolve ethical issues and maintain the University's integrity.

Who Should Attend?
Anyone who wants to learn more to maintain high professional and ethical standards in their work environment.

To register, email employee.development@bc.edu or call x28532.

The purpose of this newsletter is to provide the BC community with articles on good business practices, internal controls and responsibilities. Each issue will provide insights to internal control techniques. We have also included an "Ask the Auditor" section to give you an opportunity to obtain answers to specific questions. Additionally, we will provide information on recent items in the news.

We hope that by providing this array of information, we can help you implement effective controls in your area of operations.



Contents

Did you Know That.....

When customers offer their bankcard at a point of sale, over the Internet, on the phone, or through the mail, they want assurance that their account information is safe. In 2004, Visa and MasterCard instituted an industry standard known as **Payment Card Industry (PCI)** Data Security Standard to create common industry security requirements for credit cards. This standard is intended to protect credit card data–wherever it resides–ensuring that members, merchants, and service providers maintain the highest information security standard.

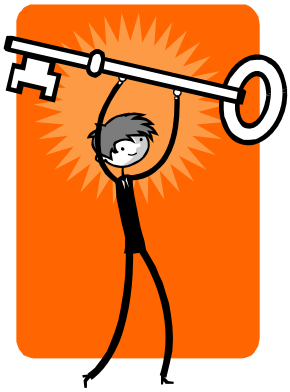
Boston College is currently undergoing a detailed process to ensure that all credit card data is secured in compliance with this program. The PCI data security standard includes:

- ⇒ Building and Maintaining a Secure Network
- ⇒ Protecting Cardholder Data
- ⇒ Maintaining a Vulnerability Management Program
- ⇒ Implementing Strong Access Control Measures
- ⇒ Regularly Monitoring and Testing Networks
- ⇒ Maintaining an Information Security Policy

By complying with the PCI Data Security Standard, merchants, and service providers not only meet their obligations to the payment system, but also build a culture of security that benefits everyone.

For more information, see: http://usa.visa.com/business/accepting_visa/ops_risk_management/

Confidential Data Security Threats



Why should we protect our computers? What will happen if we do not guard our computer systems? In today's world, we are faced with various security threats. Making sure that our computers are as secure as possible can save you and the University unnecessary anguish. Security threats can be categorized into two categories – **malicious** and **non-malicious**.

Malicious threats are well-known. These include:

- Viruses
- Worms
- Trojan Horses
- External hacking
- Denial of service attacks

Non-malicious threats usually occur internally, and might be unintended but can cause serious damage. These include:

- Improperly patched software
- Peer to peer file transfers
- Unauthorized instant messaging
- Outdated firewall rules
- Allowing children to use your work computer
- Downloading email from an unknown sender

By understanding certain concepts of confidentiality, integrity, and availability of data, the risk of malicious and non-malicious threats can be minimized.

- **Confidentiality** is protecting information from unauthorized individuals. Access controls, user accounts and passwords, encryption, intrusion detection, and firewalls can help protect confidentiality.
- **Integrity** ensures that data is accurate and has not been inappropriately changed. Mechanisms for confidentiality are the same for integrity, but additional attention is paid to monitoring audit and transaction logs. Unauthorized changes can be found in logs.
- **Availability** ensures that data can be accessed at all times. Email, voicemail, financial systems, etc. cannot afford to be compromised and unexpectedly become unavailable.

Since new risks and threats continue to develop, it is important that users understand the importance of securing their computer systems. All levels of personnel are responsible for keeping their data safe.

Source: ISSA Journal, February 2006, "Calculating IT Security Risk" Ron Lepofsky

Guidelines for Protecting Confidential Data (from Visa.com)

- **Empty the mailbox.** Never leave outgoing or incoming mail in pick-up boxes overnight. This is your best defense against possible off-hour mail snoops.
- **Watch the fax.** A document sitting on the fax waiting for pick-up is an open invitation for prying eyes. Try to stand by the fax machine to receive sensitive information as soon as it comes in.
- **Send email sparingly.** When sending sensitive information via email, encrypt it first—or don't send it at all. There's always the possibility of cyber-thief interception or an accidental electronic distribution.
- **Make copies carefully.** Private matters can go public fast when juicy stuff gets left behind. When making copies of sensitive documents, remember to grab your originals off the copy machine.
- **Use the shredder.** Always shred sensitive information before dumping it in the trash bin. If you can't shred, use receptacles designed for sensitive paper disposal.
- **Leave discrete voicemail messages.** You never know who's standing within earshot of someone's work area, so avoid leaving a detailed voice-mail message if it involves sensitive information.
- **Protect your onsite ID.** Play it safe with your ID badges, office keys, and building-entry codes. Protect them as you would your own credit cards and cash.
- **Keep things private in public.** When you're in a public place, think twice before discussing proprietary information or any details about sensitive projects. You never know who's listening.
- **Identify strangers.** Don't make it easy for an outsider to pull an inside job. If you see an unfamiliar face roaming around your office, step up and ask if you can assist. Make your presence known.
- **Be careful with your documents.** Remove all sensitive materials from your work area when you're not using them or at the end of the day. Be sure to lock them in the appropriate file cabinets, desk drawers, etc.
- **Note what's on your screen.** Those account numbers and financial details on your computer screen are intended for your eyes only! To keep it that way, use a glare screen to minimize easy information access.
- **Limit cell phone conversations.** Anyone can listen in on your cellular conversations. All it takes is a good ear and a decent scanner. Avoid sharing any sensitive information over a cell phone.

In the News.....

Beware of Email Tax Scam

If you receive an email from "taxrefunds@irs.gov," delete that email immediately. According to the IRS, this is a scam designed to trick consumers into revealing their personal and financial information. The IRS does not email taxpayers about refunds or other confidential tax information. Additionally, you can call the IRS to discuss missing tax refunds and other matters. The IRS' toll-free number is **1-800-829-1040**.

Spyware, SPAM & Phishing

--Tool Kits Boost Number of Phishing Sites
(February 27, 2006)

The Anti-Phishing Working Group (APWG) says the number of phishing web sites increased from 4630 to 7179 between November and December of 2005.

The number of phishing emails dropped in that same period. The increase in the number of sites is thought to be due to the availability of easy to use phishing tool kits.

http://www.zdnet.com.au/news/security/print.htm?TYPE=story&AT=39240328-2000061744t-10000005c

Cybercrime on the Rise

By Amanda Cantrell,
CNNMoney.com staff writer
(March 7, 2006)

Criminal attacks online are on the upswing, and they are getting stealthier, according to Symantec.

Cybercrime consists of criminal acts performed using a computer or the Internet. Symantec also found a rise in the use of "crimeware," or software used to conduct cybercrime.

"Phishing" threats, which are attempts to steal financial and personal data from computer users via e-mail, accounted for one in every 119 e-mail messages processed during the last half of 2005. These e-mails often appear to have come from a user's financial institution and urge the victim to update their account information on the firm's Web site.

As consumers become more educated, the chances that they'll suffer from a cybercrime attack declines and most of the preventative measures haven't changed. Users should make sure they've downloaded the latest security patches for their operating system and software programs, and keep on top of their passwords.

http://money.cnn.com/2006/03/07/technology/symantec_survey/index.htm

CYBERSECURITY-RELATED LEGISLATION

Computer Fraud and Abuse Act (1986): To convict whoever both "knowingly accessed a computer without authorization or exceeding authorized access" and obtained information that the U.S. government deems to "require protection against unauthorized disclosure for reasons of national defense or foreign relations."

Gramm-Leach-Bliley Act (1996): requires financial organizations to protect security and confidentiality of customers' non-public, personal information. Allows customers to opt out of having their nonpublic information disclosed to a third party.

Health Insurance Portability and Accountability Act (1996): Establishes requirements for maintaining the privacy and integrity of personal health data.

USA Patriot Act (2001): To enhance law enforcement investigatory tools. Charged Attorney General to establish regional computer forensics laboratories.

Sarbanes-Oxley Act (2002): Places regulations upon corporations to punish fraud, fraudulent destruction of information and threats to data integrity.

Federal Information Security Management Act (2002): Supports efforts to bring standards and guidelines of national security systems in line with National Institute of Standards and Technology (NIST) standards. Requires agencies to: create security awareness training; conduct periodic testing of infosec policies; ensure that info security is addressed throughout the left cycle of each system; and create procedures for responding to security incidents.

Ask the Auditor!

What are good internal controls? Why should I be concerned?

Good internal controls safeguard or make more efficient and effective use of University assets. They are good business practices that assist you in achieving your objectives. Good internal controls are cost effective, timely, and flexible. Good controls are placed where they are most effective and identify both the problem and its cause.

Senior administrators are responsible for developing a good system of internal controls, but all employees should be concerned about maintaining good internal controls because they are concerned about achieving their objectives.

Why Should I Document What I do?

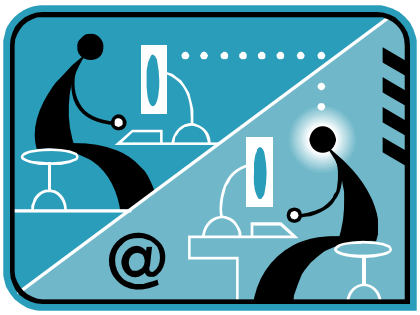
Documentation is essential for communication purposes, approval, analysis, and accountability. For instance, documenting the decisions that are made and agreed upon by management alleviates future misunderstandings and provides endorsement. Documentation also ensures that unauthorized, erroneous, or incomplete transactions are minimized.

I Don't Have Time to Document Procedures in My Office.

Writing procedures is important to any office and serves several purposes. Procedures serve as communication to employees on how to handle a particular process and why. This aids in the consistent application of processing effective transactions and how to address unauthorized, incomplete, or erroneous transactions.

Providing the "why" of information assists employees in identifying what critical information needs to be maintained should a new system or changes within a federal regulation, state statute or University policy occur. Documenting procedures is essential for communication, analysis, accountability and control. Adequate documentation permits correct accounting and helps prevent errors in processing and recording.

TIPS.....



Security of Assets

Securing assets entails protecting key information, property, or resources from physical loss or inappropriate use. This control should be considered when the integrity, condition, or confidentiality of University valuables needs to be protected. Examples include locking office doors when employees are not present, turning computer screens and papers so they cannot be seen by others, emphasizing the importance of confidentiality to employees (including students) who may have access to information, not sharing passwords and keys, and keeping virus-protection and operating systems updated.

Computer Backup and Recovery

Would critical information be lost if your computer were to crash? How long would it take you to re-create that information? Good business practice dictates that critical electronic information be backed up. Backups can be as simple as copying the files to a confidential directory on your department's server, which is then backed up by a system administrator. Server administrators should also consider the need to store server backups in a secure, secondary location. A few minutes spent backing up your computer each week can save you a great deal of time re-creating information later.

Never Provide Your Password to Anyone

Only you should know your password. If anyone requests your password, even if they identify themselves as authorized to know this information, advise them that you are not permitted to provide your password and immediately advise your supervisor of this request.