

Save the Date.....

Thursday, November 29th, 10-11:30
Identity Theft and Fraud: A Guide to
Protecting Yourself and Boston College
(McElroy Conference Room)

Identity theft and fraud are "hot" topics in today's world, and they are not likely to fade any time soon. The challenge for us, as Boston College employees, as well as in our personal life, is taking preventative action so that they don't happen. In this interactive session, we address types of identity theft, fraud, and ethical issues.

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

Nat'l Cyber Security Awareness Month	1
Who Audits the Auditors?	2
Conflict of Interest	3
Bluetooth Security	3
Ask the Auditor	4
In the News	4

October is National Cyber Security Awareness Month

The National Cyber Security Alliance (NCSA), is a consortium of government agencies and private industry sponsors. National Cyber Security Awareness Month is a national campaign designed to increase awareness of cyber security and cyber crime so that users can take precautions to avoid these threats on the Internet. The National Cyber Security Alliance's Top Eight Cyber Security Practices are steps you can take to stay safe online and avoid becoming a victim of fraud, identity theft, or cyber crime.

- Protect your personal information. If you're asked for your personal information learn how it's going to be used, and how it will be protected, before you share it.
- Know who you're dealing with online. A legitimate business or individual seller should give you a physical address and a working telephone number at which they can be contacted in case you have problems.
- Use anti-virus software, a firewall, and anti-spyware software to help keep your computer safe and secure.
- Be sure to set up your operating system and Web browser software properly, and update them regularly. Decrease your risk by changing the settings in your browser or operating system to increase your online security.

Continue on Page 2...





- Use strong passwords or strong authentication technology to help protect your personal information. Keep your passwords in a secure place, and out of plain view. Don't share your passwords on the Internet, over email, or on the phone. Your Internet Service Provider (ISP) should never ask for your password.
- Back up important files. No system is completely secure. If you have important files stored on your computer, copy them onto a removable disc, and store them in a secure place, preferably away from your computer.
- Learn what to do if something goes wrong. Be aware of any unusual or unexpected behaviors.
- Protect your children online.

Read the full story at: <http://www.staysafeonline.org/practices/index.html>



Who Audits the Auditors?

The *International Standards for the Professional Practice of Internal Auditing (Standards)* provides guidance for the conduct of internal auditing at both the organizational and individual auditor levels.

The purpose of the *Standards* are to:

1. Delineate basic principles that represent the practice of internal auditing as it should be.
2. Provide a framework for performing and promoting a broad range of value-added internal audit activities.
3. Establish the basis for the evaluation of internal audit performance.
4. Foster improved organizational processes and operations.

The Standards define the following areas:

Purpose, Authority, and Responsibility

The purpose, authority, and responsibility of the internal audit activity is formally defined in a charter, consistent with the *Standards*, and approved by the board.

Independence and Objectivity

The internal audit activity is independent, and internal auditors are objective in performing their work.

Proficiency and Due Professional Care

Engagements are performed with proficiency and due professional care. Internal auditors possess the knowledge, skills, and other competencies needed to perform their individual responsibilities. Internal auditors enhance their knowledge, skills, and other competencies through continuing professional development.

Quality Assurance and Improvement Program

Internal Audit has developed and maintains a quality assurance and improvement program that covers all aspects of internal audit activity and continuously monitors its effectiveness.

Managing the Internal Audit Activity

The internal audit activity is effectively managed to ensure it adds value to the organization. Internal Audit has established risk-based plans to determine the priorities of the internal audit activity, consistent with Boston College goals.

Nature of Work

The internal audit activity evaluates and contributes to the improvement of risk management, control, and governance processes using a systematic and disciplined approach.

Performing the Engagement

Internal auditors identify, analyze, evaluate, and record sufficient information to achieve the engagement's objectives.

Communicating Results

Communications include the engagement's objectives and scope as well as applicable conclusions, recommendations, and action plans.

Monitoring Progress

Internal Audit has established and maintain a system to monitor the disposition of results communicated to management.

Resolution of Management's Acceptance of Risks

If Internal Audit believes that management has accepted a level of residual risk that may be unacceptable to the organization, the matter is discussed with senior management.

In April 2007, The Boston College Internal Audit Department completed a quality assurance peer review. As a result, Boston College Internal Audit fully complies with the *Institute of Internal Auditors (IIA) International Standards for the Professional Practice of Internal Auditing*. Compliance means that policies, procedures, and practices are in place to implement the *Standards* and requirements necessary to ensure the independence, objectivity, and proficiency of the internal audit function.

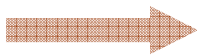
Assessments are conducted at least once every five years by a qualified, independent reviewer or review team from outside the organization.

Conflict-Of-Interest, What Does It Mean?

Most people have heard the term "conflict-of-interest". However, often there is confusion about what is meant by the term and whether there are ethical or legal ramifications of such conflicts.

A possible conflict-of-interest exists if an employee (or an employee family member):

- has an existing or potential financial or other interest which impairs, or might impair, that person's independent, unbiased judgment when performing responsibilities to the University.
- has a significant business relationship with a person or firm engaging, or seeking to engage in, business with the University.
- has a significant ownership interest, and may receive a financial or other benefit from knowledge or information confidential to the University.



WHO SHOULD I CALL ABOUT AN ALLEGED FRAUD?

An anonymous Business Ethics Hotline (2-3194) has been established for employees to convey their concerns to the Director of Internal Audit.

<http://www.bc.edu/offices/audit/hotline/>

Individuals have an obligation to avoid conflicts-of-interest or any appearance of conflicts between their personal interests and the interests of the University. Conflicts-of-interest can arise because of circumstances alone (in appearance) without any action on the part of the employee. However, it is also important to recognize that in some cases the risk to all concerned is so small that the University agrees to accept the existence of the conflict.

Conflicts-of-interest often relate to situations where an employee uses influence with the University for personal gain. The following situations are examples of conflicts-of-interest:

- An employee negotiates or approves a contract or purchase on behalf of the University and has an interest in or receives a personal gain from the company providing the goods or services.
- An employee uses University facilities or other assets for personal gain.

- An employee directs other employees to perform tasks for an outside business which the employee has an interest in or receives personal gain.
- An employee sells products or services offered by the University in competition with the University.
- An employee responsible for initiating or approving purchases is given a substantive gift by a vendor used by the University (for example a trip).

If an actual or potential conflict-of-interest is disclosed, the affected employee should refrain from further participation in the matter to which the conflict relates until the question of conflicts has been resolved. The Vice President for Human Resources, in consultation with University Legal Counsel will review all disclosures, and together with the cognizant vice president, will pursue resolution of such conflicts. Annually, the Internal Audit Department performs a conflict-of-interest disclosure statement circularization for selected individuals.

Related useful websites:

Boston College Professional Standards and Business Conduct General Policy
<http://www.bc.edu/offices/policies/meta-elements/doc/policies/1/1-100-010/1-100-010.shtml>

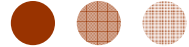
Boston College Research Policies:
<http://www.bc.edu/research/osp/policies.html>

Tips.....

Symantec warns users over Bluetooth security. *From CNET News.com, September 21, 2007.* In this article, a Symantec executive notes that users need to be aware of security vulnerabilities linked to Bluetooth wireless features on mobile devices. Learn more about:

- Bluejacking, a technique used to send anonymous text messages to mobile users via Bluetooth.
- Bluesnarfing, a technique that can allow a hacker to access information stored on a mobile device without its user's knowledge.
- Bluebugging, a technique that allows attackers to access mobile-phone commands without notifying or alerting the device owner.

http://www.news.com/Symantec-warns-users-over-Bluetooth-security/2100-1029_3-6209361.html?tag=cd.lede



Ask the Auditor!

If we didn't have controls, what could happen?

Unauthorized access to highly sensitive data can compromise the confidentiality of student records, salary information, and strategic Boston College financial records. For instance, incorrect information can result in inaccurate financial statements.

Here are a few things that can result from inadequate protection of sensitive or confidential data:

- malicious damage to data files
- deliberate manipulation of application programs
- reprocessing effort due to lost data costing time and money
- misuse of output (i.e., selling information, etc.)

Are there legal reasons for protecting my information?

There are federal and state laws that make Boston College legally responsible to ensure information is correct and used appropriately. The laws:

- protect a person's right to privacy
- prohibit violations of copyright infringements
- protect student records from unauthorized access

How can I protect my sensitive information?

The same principle of locking the door to your office applies to your computer. Lock up your sensitive information by:

- using password software
- choosing a hard-to-guess password
- changing your password periodically
- never posting your password/pin number near your terminal
- keeping your password and pin number confidential
- disposing your confidential material in a responsible manner

In the News.....

Trends show that with increased physical mobility in the workplace, critical and confidential data can reside on portable devices that easily travel where their owners go. As a result, every time a user takes a portable device off-site, that user could be placing sensitive data at risk of being acquired for unauthorized uses and potentially malicious intents. On <http://www.informationweek.com>, E. Zeman, 9/12/2007, notes five simple steps to take to protect your data that include:

- using VPNs to authenticate and connect through secure tunnels to protect data in transit.
- using strong passwords.
- encrypting individual files to make it even harder for people to break in.
- protecting against removable storage. Software is available that prevents even authorized users from downloading files to removable storage.
- being aware of your neighbors. Filters or screen protectors are available that prevents others from seeing what you're doing.