Save the Date.....

Thursday, December 11th, 10-11:30
Identity Theft: A Guide to Protecting Yourself and Boston College
(Walsh Hall)

Identity theft is a “hot” topic in today’s world, and it is 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 identity theft won’t happen. In this interactive session, we address types of identity theft and fraud. Topics discuss include common types and warning signs of identity theft, and ways in which you can identify risks that may result in identity theft.

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
Data Privacy And Security 2
Reconciliations... Why Should I Care? 3
Security Tips 3
Ask the Auditor 4

October is National Cyber Security Awareness Month

October is National Cyber Security Awareness Month. Microsoft and the National Cyber Security Alliance (NCSA) have teamed up to help increase awareness about Internet security issues. The Top Eight Cyber Security Practices you can take to stay safe online and avoid becoming a victim of fraud, identity theft, or cyber crime can be found at: http://staysafeonline.org/practices/index.html

Cyber Security: Make it a Habit.
Start with the Basics: Three Core Practices
- Install anti-virus and anti-spyware programs and keep them up to date.
- Install a firewall and keep it properly configured.
- Regularly install updates for your computer’s operating system.

Read more at: http://www.dhs.gov/xprevprot/programs/gc_120274648575.shtm
Data Privacy and Security

In recent years, you have read more and more about how hard it is for institutions to contain the loss of sensitive data. Incident rates are rising, operational liability is high, and the risk of identify theft is far-reaching. Everyone at BC is responsible for safeguarding confidential and sensitive data.

The first step in locking down sensitive data is to be aware of the importance of how to handle data in a secure fashion. Data, like a living entity, has a lifecycle. Each phase of its lifecycle has different security risks and needs.

The first phase of a data lifecycle is **collection**. Data enters the University in a myriad of ways: on-line tuition payments, donations, student applications, athletic ticket sales, employment, etc. All data is not created equal. A common cause for inappropriate use of data is a lack of understanding about the data’s significance or overall sensitivity.

In the second phase of a data lifecycle, one needs to determine a **classification level**. The Data Security Policy at BC has three classification levels:

- **Confidential information** includes sensitive personal and institutional information, and must be given the highest level of protection against unauthorized access, modification or destruction.
- **Internal Use Only** information includes data that is less sensitive than Confidential information, but that, if exposed to unauthorized parties, may have an indirect or possible adverse impact on Boston College.
- **Public Information** is information that is generally available to the public, or that, if it was to become available to the public, would have no material adverse effect on Boston College.

Phase three is to determine how we **handle and store data**. For instance, confidential information should not be stored on your desktop computer, but rather stored in a server that is protected by a hardware firewall. Additionally, confidential data that must reside on your laptop should be encrypted. Some security hints to keep that sensitive data confidential include:

- logging out of your computer when you leave your office.
- not writing down passwords.
- not sharing passwords.
- not leaving paper documents that contain sensitive information unattended, or within view of others.
- not emailing confidential data to someone else. See related article on page 3, Security Tips.
- not storing sensitive data on a USB Flash Memory Data Storage Device.
- not leaving sensitive documents in the copier, on printers, or on fax machines.
- not leaving sensitive information on white boards or flip charts in meeting rooms.

Phase four of a data lifecycle is **retention**. Confidential data becomes more vulnerable to mishandling the longer it sits around. Data retention policies are useful documents that deal with complex issues of maintaining information for a pre-determined length of time. Different types of data require different lengths of retention and computer systems and applications have added increased complexity to the issue. The University is working on a data retention policy. However, in the meantime, make sure that desk drawers and filing cabinets that store sensitive documents are locked.

Phase five constitutes **destruction** of data. Be aware of where you throw away confidential paper documents. All sensitive data should be shredded or thrown away in appropriate locked “burn bins”. Electronic information can be destroyed in several ways including (1) overwriting (also know as wiping), (2) low-level formatting, (3) physical destruction of hard drives, and (4) degaussing. Contact ITS Security if you need help destroying electronic information.
Reconciliations....Why Should I Care?

Every day we read about security breaches where personal information, such as social security and credit card numbers, have been exposed to unauthorized access. Therefore, paying attention to bank account statements, credit reports and credit card statements is becoming more important.

Reconciliation is a control tool that can help protect your personal information and can also help you in your daily business practices. The official definition of “reconciliation” is getting two things to correspond. For instance, by matching your checkbook to your bank statement, you can identify unauthorized purchases. Everyone is eligible for free annual credit reports. See: http://www.ftc.gov/opa/2005/08/freecredreports.shtm. By reviewing your credit report, you can determine if anyone has tried to open an account in your name.

At work, PeopleSoft system accounts should be properly reconciled to detail support, and reconciling items should be cleared in a timely manner. This process ensures that:

- revenues and expenses associated with your department accounts are showing correct balances and are properly accounted for.
- problems or incorrect data that result from daily processing are managed or responded to in a timely manner.
- revenue and/or expenses do not distort financial statements and are recognized in the appropriate month.

Another example of reconciliations involves the procurement card. Receipts for purchases should be reconciled to your monthly procurement card statement.

For reconciliations to function as an internal control tool, separation of duties needs to be in place. Separation of Duties means that the same person does not initiate, authorize, and process a transaction. Additionally, record keeping and custodianship of assets should be segregated.

Security Tips.....

......Protect Your Computer, Your Information, and Your Identity.

Check out the following web site from ITS to learn more about keeping your system updated, links in emails, file-sharing, spyware, and other important information about computer security:

http://www.bc.edu/offices/itwelcome/security.html

......Ensure That Your Department has Established and is Maintaining Good Internal Controls.

An organization must be aware of and deal with the risks it faces. Therefore, it must develop and implement control policies and procedures to effectively handle potential risks. Go to Internal Audit’s web site on Internal Controls at:

http://www.bc.edu/offices/audit/controls.html

......Emailing Confidential Information
Use MyFiles@bc To Transmit Data Securely

When sending confidential data electronically, it is important to ensure it is being transmitted securely. Email is not a secure method of electronic delivery. Go to the following web site from ITS to learn more about transmitting electronic data securely.

Ask the Auditor!

What is the authority of Internal Audit?

The scope of audit coverage is enterprise-wide and no function, activity, or unit of the University is exempt from audit and review. The Audit Director and staff of the internal auditing department are authorized to:

- Have unrestricted access to all functions, records, property, and personnel.
- Have full and free access to the audit committee.
- Allocate resources, set frequencies, select subjects, determine scopes of work, and apply the techniques required to accomplish audit objectives.
- Obtain the necessary assistance of personnel in units of the organization where they perform audits, as well as other specialized services from within or outside the organization.

The Audit Director and staff of the internal auditing department are not authorized to:

- Perform any operational duties for the organization or its affiliates.
- Initiate or approve accounting transactions external to the internal auditing department.
- Direct the activities of any organization employee not employed by the internal auditing department, except to the extent such employees have been appropriately assigned to auditing teams or to otherwise assist the internal auditors.

The internal auditing department is guided by the International Standards for the Professional Practice of Internal Auditing of The Institute of Internal Auditors.

How are Audits Chosen?

The University Audit Plan and University Operations Risk Analysis are prepared annually by the Audit Director.

Reviews are designed to evaluate and test significant accounting, operational, compliance, and information system controls within the University.

The purpose of the Annual Risk Analysis is to prioritize all audit areas for review based on a risk assessment. Internal Audit is utilizing comprehensive risk based software to target resources to areas of greatest exposure.

This process automates the audit planning approach by:

1. defining and weighting risk criteria,
2. providing assurance that high-risk areas are being reviewed on a regular basis, and
3. continuously updating the audit plan to reflect emerging issues. Risk criteria are updated as each audit is performed to provide continuous assessment.

Risk factors include:

- dollar amounts controlled by a department or organizations.
- accuracy, availability, and integrity of the information provided via manual or automated systems.
- sensitivity, exposure, or potential for public embarrassment if controls fail in the department.
- existing control structure, expertise of management or historical problems.
- interval since the last audit and conditions found during the review.

See more information at: http://www.bc.edu/offices/audit/about/planning/audprocess.html