Save the Date.....

Thursday, April 23rd, 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.

Fraud and The Current Economic Downturn

The current economic downturn has affected all sectors of the economy on a global scale including higher education. As a result, the risk of fraud and misappropriation could increase during this disappointing economic period. Fraud research indicates that fraud generally occurs when three factors are present: pressure, opportunity, and rationalization. During a downturn all three factors can increase, particularly the pressure employees may feel such as increased personal debt and the lack of salary increases. It is very important that the University proactively manage their fraud risk especially during this difficult time.

To address the above issues, BC Internal Audit continues to enhance fraud detection auditing techniques. A “Red Flags” approach to auditing is instituted whereby staff members are alerted to increases in the risk of fraud based on changes in human behavior and personal life-style observations.

Continue on Page 2......
Most people who commit fraud against their employers are not career criminals. The vast majority are trusted employees. So the question is what factors cause these otherwise normal, law abiding persons, to commit fraud? To understand why individuals commit fraud, we must understand the fraud triangle.

**Pressure** can be due to personal financial problems, personal vices such as gambling, drugs, etc, or a desire for status symbols.

**Opportunity** is generally provided through weaknesses in internal controls. Some examples include:
- Lack of supervision and review
- No separation of duties
- Inadequate approvals

**Rationalization** occurs when an individual develops a justification for their fraudulent activities. Some examples include:
- “I really need this money and I’ll put it back when I get paid.”
- “I just can’t afford to lose everything—my home, car, everything!”

It is important to recognize that as a Boston College employee, you have stewardship responsibility for safeguarding University assets under your purview. Fraud prevention measures include:
- Strong Internal Controls such as segregation of duties, physical safeguards, independent cross-checking, appropriate authorization on documents and records, and sufficient approvals.
- Fraud and Ethics Training (see page 1 under “Save the Date”).
- Anonymous Fraud Reporting Mechanisms (see Internal Audit’s Business Ethics Hotline at http://www.bc.edu/offices/audit/hotline.html)
- Comprehensive Fraud Policies (see University policy at http://www.bc.edu/offices/policies/meta-elements/pdf/policies/I/1-100-010.pdf)

**Ask the Auditor!**

**What Role and Responsibilities do Internal Auditors have to Identify Fraud?**

The Institute of Internal Auditors has published standards regarding assurance for internal audit engagements. The Standard states: “Internal auditors must have sufficient knowledge to evaluate the risk of fraud and the manner in which it is managed by the organization, but are not expected to have the expertise of a person whose primary responsibility is detecting and investigating fraud.”

Internal auditors are responsible to evaluate the adequacy and effectiveness of the system of internal controls. Internal Audit assists management to evaluate fraud risks, specifically their processes for identifying, assessing, and testing potential fraud and misconduct schemes and scenarios, including those that could involve suppliers, contractors, and other parties.
Managing Risk

One primary activity of the Internal Audit Department is to assist the University by identifying and evaluating significant exposures to risk and recommending controls to mitigate risk.

Managing risk is a key responsibility of University managers. Managers should (1) ensure that adequate and effective processes are in place to control risk exposures and (2) develop ongoing monitoring processes to periodically reassess risk and the effectiveness of controls.

During this time of economic uncertainty, management will be faced with difficult decisions that require them to carefully balance the risk/reward equation. The financial crisis is causing management and boards to assess their assets to determine how to properly protect and develop them in the current economic environment.

Risk assessments should identify the adequacy and effectiveness of controls that encompass:

- reliability and integrity of financial and operational information.
- effectiveness and efficiency of operations.
- safeguarding of assets.
- compliance with laws, regulations, and contracts.

Control Self Assessment (CSA) methodology is a useful and efficient approach for managers in assessing and evaluating control procedures. A self-assessment allows management to:

- identify risks and exposures,
- assess control processes that mitigate or manage those risks,
- develop action plans to reduce risks to acceptable levels, and
- determine the likelihood of achieving business objectives.

Positive outcomes of a self-assessment include (1) staff training to assess and manage risks, and (2) staff taking ownership of control processes in their units and taking responsibility for corrective actions. More information including a questionnaire can be found at:

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

In The News.....

Dave Escalante, ITS Director of Computer Policy & Security at Boston College, notes that it's a bad idea to use your BC username and password for other, non-BC web sites, especially for financial and “throwaway” web sites – that is, sites where there's no particular focus on protecting your credentials. He states that there is documented evidence that hackers will first steal credentials from non-financial sites, and then try them out elsewhere, like at financial sites, or at the e-mail address you provided when registering at the hacked site.

The link below talks about a large-scale theft from a “throwaway” site and states that, "A survey by Sophos, published earlier this week, found a third of users used the same password for every website."

"Nature" Security Breach Prompts Password Reset
http://www.theregister.co.uk/2009/03/12/nature_password_breach/
Protecting Your Data - It Takes a Team

Dave Escalante, ITS Director of Computer Policy & Security at Boston College

Per the Board of Trustees, all BC faculty and staff must become aware of the importance of handling confidential data in a secure fashion. Training is being provided throughout the University to ensure that all faculty and staff who handle confidential data are aware of the importance of protecting personal information, and the proper computing practices they should utilize when dealing with confidential records and other sensitive information.

One thing to bear in mind is that protecting your data is a combination of people, processes, and technology. Many people think that technology such as anti-virus software will completely protect their computers and data, but this is not the case - technology is just one third of it.

Make data security a priority by thinking about the “people” and “process” aspects as well. For example:

- Be aware of being overheard when on the phone.
- Do not leave paper documents that contain sensitive information unattended, or within view of someone walking by.
- Protect any vulnerable information on your desktop when you are not present (lock it in a drawer, lock the office, etc.).
- Lock the screen or log off your computer when you are not nearby.
- Keep laptops, PDAs, and cell phones safe from theft at all times (leaving them visible in cars is a really bad idea, for example).
- When disposing of sensitive information, make sure it’s properly destroyed.

Does your department have written policies on where to save confidential data? Are they up-to-date?

More tips to secure your data include:

- Beware of password savers and auto-completion of forms. The computer is trying to “help” you, but saving passwords and form entries can be a serious security risk.
- Create “strong” (difficult-to-guess) passwords with letters and numbers for important accounts such as BC, your financial institution(s), and online merchants where you save your credit card for repeated use.
- Use different passwords for different systems and web sites, especially the important accounts in the previous bullet.
- Change passwords at least once a year.