Save the Date.....

Wednesday, November 29th, 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

<table>
<thead>
<tr>
<th>Safety and Security</th>
<th>In the News</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tips for Preventing Identity Theft</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>Internal Control</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>Ask the Auditor</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>Tips</td>
<td>4</td>
<td></td>
</tr>
</tbody>
</table>

Global Security Week 2006

September 4th to 10th 2006

The theme for Global Security Week 2006 is identity theft: Find out about the truth behind the headlines. Is “phishing” a genuine threat? What can ordinary members of the public do about it? Participate in Global Security Week to help spread the word about identity theft and encourage ordinary law-abiding citizens to be on their guard.

To view a security awareness video on “drive-by downloads” that explains step-by-step how merely visiting a malicious web page with an unpatched PC can result in your machine being silently infected in an instant with spyware and viruses, go to:

http://video.google.com/videoplay?docid=-3351512772400238297&hl=en

The worst operating system and browser flaws can leave your machine wide-open to attack, although properly configured and up-to-date anti-virus/anti-everything software does help to some extent.

Safety and Security in the News......

September is National Campus Safety Awareness Month.
This initiative focuses on security and safety of students, raising awareness of issues such as stalking, alcohol and drug abuse. Visit http://www.campussafetymonth.org/ to find out more.

October is CyberSecurity Awareness Month.
Read more about:

- Protecting your personal information. It's valuable.
- Knowing who you are dealing with online.
- Using anti-virus software, a firewall, and anti-spyware software to help keep your computer safe and secure.
- Being sure to set up your operating system and Web browser software properly, and updating them regularly.
- Using strong passwords or strong authentication technology to help protect your personal information.
- Backing up important files.
- Learning what to do if something goes wrong.
- Protecting your children online.

http://www.staysafeonline.info/

Tips for Preventing Identity Theft

- The next time you order checks, have only your initials (instead of first name) and last name put on them. If anyone takes your check book they will not know if you sign your checks with just your initials or your first name but your bank will know how you sign your checks.

- When you are writing checks to pay on your credit card accounts, DO NOT put the complete account number on the "For" line. Instead, just put the last four numbers. The credit card company knows the rest of the number and anyone who might be handling your check as it passes through all the check processing channels won’t have access to it.

- Put your work phone # on your checks instead of your home phone.

- Never have your SS# printed on your checks. You can add it if it is necessary. But if you have it printed, anyone can get it.

- Place the contents of your wallet on a photocopy machine and copy both sides of each license, credit card, etc. You will know what you had in your wallet and all of the account numbers and phone numbers to call and cancel if your wallet is stolen. If traveling, copy your passport. Keep all photocopies in a safe place.

- 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.
Internal Controls

Assurance that the internal control system is effective can be provided through evaluation of the control system. Evaluations may take the form of self-assessments, where responsible individuals from a particular unit or function will determine the effectiveness of controls for their activities.

Internal Audit's mission is to independently evaluate the adequacy of existing University internal control systems by analyzing and testing controls. Internal Audit makes recommendations to management to improve controls based on system testing and control analysis. Internal auditors also normally perform internal control evaluations as part of their regular duties, or upon special request of the board of directors, senior management or subsidiary/divisional executives.

Similarly, University Management is responsible for maintaining an adequate system of internal control. Department managers should ensure that controls within their organizations are adequate. University Management may use the work of external auditors in considering the effectiveness of internal control. Often a combination of parties will be used in conducting whatever evaluative procedures management deems necessary.

Internal Control comprises five interrelated components:

- **Control Environment:** The core of any business is its people - their individual attributes, including integrity, ethical values and competence - and the environment in which they operate. They are the engine that drives the entity and the foundation on which everything rests.

- **Risk Assessment:** The entity must be aware of and deal with the risks it faces. It must set objectives, integrated with revenues, production, marketing, financial and other activities so that the organization is operating in concert. It also must establish mechanisms to identify, analyze and manage the related risks.

- **Control Activities:** Control policies and procedures must be established and executed to help ensure that the actions identified by management as necessary to address risks to achievements of the entity's objectives are effectively carried out. BC's policies and procedures should be reviewed on a periodic basis.

- **Information and Communication:** Surrounding these activities are information and communication systems. These enable the entity's people to capture and exchange the information needed to conduct, manage and control its operations.

- **Monitoring:** The entire process must be monitored, and modifications made as necessary. In this way, the system can react dynamically, changing as conditions warrant.

### Specific Controls:

<table>
<thead>
<tr>
<th>Audit Trails</th>
<th>A system of logging transactions processed, who processed them, and the date they were processed.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access/ Authorization</td>
<td>Only authorized personnel should have access to sensitive data. Access levels should be restricted in accordance with job function.</td>
</tr>
<tr>
<td>Data Integrity</td>
<td>Management should review monthly financial reports for unusual items. All unusual items should be investigated and resolved timely.</td>
</tr>
<tr>
<td>Policy/ Documentation</td>
<td>System, operational, and user procedures should be documented to ensure that an effective control environment exists.</td>
</tr>
<tr>
<td>Reconciliations</td>
<td>Data from a subsystem should be compared to the Financial Accounting system. Differences should be analyzed and adjustments should be made and documented.</td>
</tr>
<tr>
<td>Separation of Duties</td>
<td>The same person should not initiate, authorize, and process a transaction. Recordkeeping and custodianship of assets should be segregated.</td>
</tr>
<tr>
<td>System Security</td>
<td>The server/system should (1) be scanned for security vulnerabilities, (2) run anti-virus software, and (3) reside behind a firewall.</td>
</tr>
</tbody>
</table>
Ask the Auditor!

What do I do when a University Asset or Confidential Information is Compromised?

Security over University assets includes physical and data/informational (such as social security numbers, addresses, grades, medical, financial, or personal information). Sound business conduct requires that each employee, as a basic condition of employment, assume responsibility for safeguarding and preserving the assets and resources of the University. In conjunction with policy guidelines, each University employee is expected to report any instance of suspected fraud or compromised data to the Director of Internal Audit. If an instance of suspected fraud or compromised data is reported instead to a supervisor, chairperson, director, dean, vice president, or other responsible person, that person is to report the instance to the Director of Internal Audit. The Director of Internal Audit will conduct an audit to analyze the control environment.

What is my Responsibility for the Protection of Confidential Data?

All users of technological and information resources are responsible for the protection of University assets and for the accuracy, integrity, and confidentiality of the information to which they have access. Resources are not to be abused or employed in such a way as to interfere with, or cause harm or damage to, another person, institution, or company within or outside the Boston College community. While the University encourages the exploration of educational and scholarly interests through the use of its technological resources, respect for the rights and privacy of others must be observed. Community members and their guests may not access the files or communications of others without authorization. Those who are authorized to access confidential files must respect the privacy rights of others and use data only for legitimate academic or administrative purposes.

For more information, see the University Policy and Procedures Manual at:

http://www.bc.edu/offices/policies/manual/toc/

TIPS.....

Securing Wireless PDAs

Blackberries and PDA-enabled devices are becoming more and more popular. The processing power of these hand-held devices equates to desktop systems of a few years ago. Wireless capabilities, along with large file storage, and small physical size, present unique challenges for users to secure their sensitive data. Most PDAs have Microsoft-like operating systems. Therefore, like PCs, a virus can corrupt your data or spread within the organization. Antivirus software should be installed on your PDA and should be periodically run. Both McAfee and Norton make versions of their antivirus software for the Palm and Windows Mobile operating systems. Users should password-protect their PDA so that confidential data is protected if the device is lost or falls into the wrong hands. Additionally, use a third party program such as PGP Mobile or KeyCrypt to encrypt sensitive data. Turn off or disable any Bluetooth or IR services if they aren't being used. Their interfaces could allow outsiders to access the device via a hacking process known as blue-snarfing.

Top Vulnerabilities in Cross-Platform Applications (from www.sans.org)

Read more at http://www.sans.org/top20/#top20-cross-platform. Included are vulnerabilities found in:

Backup Software: popular backup software packages are known to be affected by vulnerabilities.
Anti-Virus Software: vulnerabilities in anti-virus software are not limited to desktop and server platforms. Gateway solutions could also be affected.
PHP-based Applications: PHP is the most widely used scripting language for the web. Problems have been reported in some software using PHP.
Database Software: Databases are complex applications and a collection of a number of programs that results in a large number of attack vectors.
File Sharing applications: Most P2P programs use a set of default ports but can automatically or manually be set to use different ports to circumvent detection, firewalls, or egress filters.
DNS Software: DNS is prone to many types of transaction attacks that take advantage of trust, including domain hijacking.
Media Players: Vulnerabilities allow a malicious webpage or a media file to compromise a user's system without requiring much user interaction.
Instant Messaging: Most IM applications have the capability of transferring files that could be exploited by many IM worms.
Mozilla/ Firebox browsers: Many flaws discovered are critical and allow a malicious web page to completely compromise a client system.