Educating Accounting Students On Computer Crime And Ethics

Eddie Metrejean, (Email: eddiemet@txstate.edu), Texas State University, San Marcos
Howard G. Smith, Texas State University, San Marcos
Dennis Elam, (Email: kfdle01@tamuk.edu), Texas A & M University, Kingsville

ABSTRACT

Accounting fraud has been prevalent in the popular press for the past several years. The accounting profession has begun to stress the importance of ethics because of this negative press. Some state boards of accountancy have begun requiring ethics courses as part of continuing education to maintain certification and licensing. Many accounting frauds are in the form of computer crime. Accounting students must be made aware of various types of frauds, including computer crimes, how frauds are prevented and detected, and why ethics are important in the accounting profession. This paper describes several categories of computer crimes and technological means of preventing and detecting these crimes. Computer crimes and prevention and detection means are as varied as the perpetrators who commit these crimes. Finally, this paper suggests using a combination of three courses to educate accounting students on computer crime and ethics for preparation for their accounting careers. These three courses are a traditional Accounting Information Systems (AIS) course, a fraud prevention and detection or forensic accounting course, and an accounting or business ethics course. These three courses, used in concert, will provide accounting students with the tools they need when they are faced with incidents of fraud or ethics decisions during their accounting careers.

INTRODUCTION

Accounting fraud has been a prevalent topic in the popular press for several years. Because of negative press, the accounting profession has begun to stress the importance of ethics in all forms of public practice and in other fields within the accounting profession. The American Institute of Certified Public Accountants (AICPA) has become increasingly interested in educating the accounting profession about fraud and ethics. The AICPA's website contains links to many resources on fraud and ethics for CPAs in public practice, industry, and even education. (See http://www.aicpa.org/antifraud/homepage.htm) The presence of so many documents on this website indicates the importance that the AICPA places on fraud and ethics.

State boards of public accountancy have also begun requiring ethics courses for CPAs to maintain their licenses. For example, the Louisiana State Board of CPAs requires 3 hours of ethics education as part of its continuing professional education requirement. The Texas State Board of Public Accountancy has implemented a requirement that candidates who wish to take the CPA exam must have a 3-hour ethics course as part of their accounting education. This requirement, once in effect, will force accounting programs at Texas universities to begin offering an ethics course as part of their curricula. Undoubtedly, other CPA licensing bodies have also instituted similar ethics course requirements or will do so in the near future.

Accounting programs at many universities stress ethics in their curricula. Almost every accounting textbook has some discussion on ethics; however, it must be asked whether this limited amount of coverage in an accounting curriculum is enough. Accounting educators have begun to perform much needed research on ethics in the accounting classroom. In fact, the entire February 2004 issue of *Issues in Accounting Education* is devoted to ethics in accounting education. Accounting academe has called for increased teaching of ethics in accounting courses.

In order to understand why personal responsibility and accountability are important, accounting students must be made aware of the frauds that have lead to the increased emphasis on ethics in accounting curricula. One particular area of accounting fraud that receives much attention is computer crime and fraud. Computer crime or fraud has been defined in many different ways. One belief is that a computer crime is a crime that takes place within a computer or that is directed at a computer. Another belief includes a broader view of computer crime and asserts that a computer crime is one in which the computer is used in any capacity. (Romney and Steinbart 2003) No matter what the definition of computer crime, the effects of computer crimes have been and can be increasingly devastating to an organization. Society has become dependent on computer systems to provide vast amounts of information. As people demand more information, the computer systems become more complex and, in many cases, harder to protect.

Each year, the Computer Security Institute (CSI) and the Federal Bureau of Investigation (FBI) conduct a Computer Crime and Security Survey (heretofore called the CSI/FBI survey). The CSI/FBI survey encompasses respondents from many organizations from many different industries. This report shows the types of computer crimes, the technologies used to prevent the crimes, the number of attacks, and the dollar amount of losses by type of attacks. The 2003 report shows that the number of attacks was about the same in 2001 and 2002, but the financial losses caused by the attacks declined by approximately 56% from 2001 to 2002. The report showed that losses declined in areas such as theft of proprietary information and viruses, but increased in areas such as denial of service attacks, unauthorized access, and sabotage. (Computer Security Institute 2003) Estimates of losses from computer crimes range from $300 million to over $9 billion per year. However, the FBI also estimates than only one percent of computer crimes are detected. Many computer crimes go undetected or unreported; therefore, the actual amount lost to computer crime each year may never be known. (Casabona and Yu 1998)

The next section of this paper examines several types of common computer crimes. The following section examines several technologies that are being used to prevent and detect computer crimes. Finally, course offerings to be used to educate accounting students on computer crime, ethics, and fraud detection and possible content in those courses are suggested.

TYPES OF COMPUTER CRIMES

Computer crimes come in many different forms. Some methods of committing a computer crime are unbelievably simple. Other methods are so complex that only computer experts and forensic accountants can wade through the myriad of details to find out exactly what crime was committed and how that crime was committed. In many cases, a computer crime is similar to a non-computer crime, but the crime is perpetrated using electronic means rather than traditional means.

This section examines several categories of computer crimes that are often committed by individuals within the organization. Organizations have no control over individuals who commit many crimes from outside of the organization, such as denial of service attacks or e-mail scams, so a discussion of such computer crimes is not warranted in this paper. Several of the computer crimes discussed are often committed by external individuals, but these crimes may also be committed by an organization's employees.

While computer crimes are divided into six separate categories for purposes of this paper, one should keep in mind that many computer crimes may be classified into several categories, and many computer crimes are known by various names and definitions.

Destructive Or Malicious Programs

Destructive programs come in many forms and from many places. Perhaps the most common forms are computer viruses and worms. In most cases, such destructive or malicious programs are developed and unleashed by individuals external to the organizations affected. However, employees can certainly unleash these programs on their own organizations.

Many definitions exist for computer virus and worm, and many people use the terms interchangeably. Generally, a computer virus is defined as a program or a section of a program that attaches itself to other programs and is easily spread. (Hall 2004; Romney and Steinbart 2003) In many cases, the virus is destructive; however, viruses are sometimes more of an annoyance than a danger to the computer or a network.

A worm is generally defined as a program that embeds itself into a legitimate program. (Hall 2004; Romney and Steinbart 2003) As with viruses, some worms are destructive, while others are not. Worms are often spread via email messages that the worm initiates.

One variation of a virus that is common is a logic bomb. A logic bomb is code inserted into an operating system or other legitimate program and is triggered by some predetermined event. Logic bombs are usually destructive in nature. One famous example of a logic bomb was the Michelangelo virus that was supposed to be triggered on March 6 (the artist's birthday) of each year. In 1992, the virus received a vast amount of publicity but had very little impact worldwide. (vmyths.com 2004)

Any of these destructive programs can be costly to an organization. For example, the CSI/FBI survey showed that 82 percent of organizations surveyed reported virus attacks in 2003. The total cost of those virus attacks was over $27 million. (CSI/FBI 2004) Computer worm attacks are often classified as virus attacks in many such surveys.

Unauthorized Access Into Information Systems

Information systems can generally be accessed in many ways, either internally or externally. Individuals who perpetrate this type of computer crime are commonly called hackers. In the past, hackers would intercept and steal data during transmission. Organizations began encrypting or scrambling the data, so hackers turned to other methods of gaining access to data. In essence, hackers are now breaking and entering, but they are doing so with a computer. Unauthorized individuals typically gain access through password sniffing or piggybacking. Password sniffing involves the use of a program that electronically guesses user IDs and password until the correct one is found. Piggybacking involves following a legitimate user through security into the system. (Luehlfing et al. 2003)

Individuals gain unauthorized access to information systems for many reasons. Some of these individuals gain unauthorized access for personal gain or to steal sensitive data, such as social security numbers, credit card numbers, or bank account numbers. Other individuals gain access to interrupt legitimate access into the computer system, and some simply vandalize websites or delete data from databases. In many cases, external hackers are simply trying to have fun, or they enjoy the challenge of seeing whether they can hack into organizations' computer systems. Whether obtained internally or externally, unauthorized access into information systems can be costly and damaging to any organization.

Sabotage And Vandalism

Sabotage and vandalism are not new and can be perpetrated by employees of an organization or by individuals external to the organization. Damage to an organization's physical computer system can be devastating if proper recovery plans are not in place. Most organizations have learned to put their computer systems in areas that are not easily accessible to unauthorized personnel. Many examples of disgruntled employees damaging computer hardware have been documented. By limiting physical access to the main computer systems, an organization can limit the physical damage done to computers by employees.

Rather than physically damaging computer hardware, some perpetrators sabotage or vandalize organizations' databases or websites. A perpetrator must be able to access the website files or the database to damage the files. Controlling access into the computer system is the first line of defense in such a case. Several examples of vandalism of web sites exist. For example, government websites are vandalized quite often by hackers. The U.S. Air Force, Central Intelligence Agency, and NASA have all had their websites vandalized. In addition, several Canadian government websites were vandalized in 1999. (Silverthorn 1997; McGullivray 2000)

In some cases, an organization's website is changed, and the hackers place their own messages in place of the organization's information or the organization's website is used for a disinformation campaign. For example, disgruntled employees or hackers can break into an organization's website and post false information, such as false financial information or mergers, about the organization. Such misinformation can be costly or catastrophic to the victim and can lead to irreparable damage to the organization's reputation. Repairing the resulting damage can take many months and in some cases requires lawsuits. (McGillivray 2000) While these cases may not have been perpetrated by insiders, they are still important computer crimes because of the potential for losses.

Theft Of Proprietary Information

One form of proprietary information theft is the equivalent of industrial espionage, which is the theft of sensitive information or trade secrets from an organization. In many cases, the theft of the information is perpetrated by a trusted employee who has access to the information. Such a crime can encompass complex techniques, such as hacking into databases or software and wiretapping, to simple techniques such as dumpster diving, i.e., rummaging through trash bins for discarded computer printouts or storage media. The loss of proprietary information can be devastating to an organization. Often, sensitive information is used on bids for jobs, and exposure of such information can lead to lost revenues. Alternatively, some employees or hackers attempt to steal trade secrets, which, if divulged, would lead to decreased competitiveness of the organization. In some cases, the proprietary information has been used to blackmail the organization (Whitman 2003)

The theft of intellectual property and software piracy is also considered to be the theft of proprietary information. The theft of intellectual property and software piracy are found in many forms and can be as simple as illegally copying a program to hacking into an organization's computer system and stealing the code for various programs. The Business Software Alliance estimates that 23 percent of all pieces of software in use were illegally obtained. Estimates of economic losses due to copyright infringement range from $1.8 billion to $9.2 billion per year. Losses include loss of revenue, lost jobs, wages, and tax revenue. (Harris 2003) Recently the software and other related industries, particularly the music industry, have been fighting back with lawsuits. However, in many cases, stealing the fruits of the work of others is considered easier and less expensive.

Data Manipulation And Financial Fraud

One form of data manipulation, called data diddling, involves changing data within a database. Data manipulation includes adding, deleting, or altering data within the database. Generally, such manipulation is perpetrated by an employee of the organization and is aimed at changing the financial data. Changing financial data results in incorrect financial statements or other financial reports that many individuals, both internal and external, use to make important decisions.

Another common form of data manipulation is fraudulent data input. An accounting information system's input procedures are regarded as critical because once erroneous or fraudulent data enters the information system the output becomes suspect. Input fraud consists of submitting false data into the accounting information system, often in the form of unauthorized or forged source documents. This crime requires little, if any, computer skills. All that is necessary is an understanding of how transactions are entered into the computer system.

Several infamous cases of accounting frauds have included data manipulation to perpetrate the fraudulent financial statements. For example, WorldCom's fraud consisted partly of individuals within the company capitalizing line costs as prepaid capacity thus reducing expenses and increasing overall financial performance. (Zekany et al. 2004) Fraudulent entries that manipulated the accounting data resulted in a portion of the $11 billion fraud perpetrated by executives within WorldCom. This example is extreme, but it is an example of the damage that may be done by manipulating accounting data to commit financial fraud.

Theft Of Computer Hardware

Another form of computer crime is the theft of computer hardware. Naturally, if computer hardware is stolen, the data within the computer is also stolen and may be used for any number of fraudulent schemes. While computer hardware is usually stolen by people external to the organization, employees often "borrow" computer hardware.

Theft of hardware is often in the form of laptop computer theft. The CSI/FBI survey shows that laptop theft was the second most common form of computer fraud in 2003, with over 47 percent of respondents indicating that their organization had been the victim of laptop theft. (Computer Security Institute 2003) While replacing a laptop can be expensive in some circumstances, the major danger with laptop theft is that the person who steals the laptop may now be able to access the organization's internal networks, and he or she may be able to perform any number of fraudulent or destructive activities and cause problems within the organization.

Laptops are not the only type of computer hardware that is stolen. Central processing units (CPU), personal digital assistants (PDA), flash memory devices, and other types of computer hardware are often easy targets. Any portable computer devices or computer hardware that is somewhat easy to move are easy targets for hardware theft. In any case in which computer hardware is stolen, sensitive data or access to networks may be compromised, either of which could prove to be costly to the organization.

USING TECHNOLOGY TO PREVENT AND DETECT COMPUTER CRIME

Computer crimes and fraud can be prevented and detected in many ways. Physical controls, such as locks and controlled access to computer centers, hardware, and documents related to accounting transactions can prevent perpetrators from gaining access into the accounting information system. Most organizations have some level of physical controls in place, but many organizations also use technology to help prevent and detect computer crimes and intrusions. Computerized crime prevention can range from simple controls, such as passwords, to complex software that scans an information system for unusual occurrences or changes made to the system. Accounting students should be knowledgeable about using technology, both simple and complex, to prevent and detect computer crime because nearly all organizations have computerized accounting information systems, and these systems invariably use some forms of technology to prevent and detect computer crimes. Without knowledge of these techniques, an accounting student is at a disadvantage.

This section examines several techniques that are commonly used to prevent access into an information system and detect intrusion if or when it does occur. This list of computerized prevention and detection techniques is not all-inclusive. Instead this list is meant to give an idea of the types of controls that are used to prevent computer crimes and fraud.

Controlling Access Into A Computer System

As mentioned above, the preference is to prevent computer crimes before they occur. The first line of defense is preventing access into a computer system is to prevent physical access to the computer system. However, once a perpetrator gains physical access, another line of defense must be in place to prohibit entry into the computer system. Examples of techniques that are commonly used to control access into a computer system are passwords, biometrics, and firewalls. Perhaps the most common type of access control is the password. Individuals are required to have passwords, typically in combination with a user ID, to gain access into a computer system. Passwords provide some assurance against unauthorized access, but they are by no means foolproof. Many passwords are easy to guess and provide little, if any, protection to an organization. Therefore, passwords should not be used alone for complete control of unauthorized access.

Another method that is used to control access into a computer system is biometrics, which involves the use of some physical characteristic of a person to allow or deny access into a computer system or some secure area of a facility. Examples of biometric devices are systems that use scanners that recognize fingerprints, voice prints, retina

patterns, and even signatures or keyboarding patterns. (Hall 2004) The use of biometrics for controlling access is becoming more common because of decreases in the costs of the technology. Organizations may use biometrics in combinations because, as with passwords, these devices are not foolproof.

Firewalls are commonly used to prevent unauthorized access into the information system by outsiders. Firewalls are typically a combination of hardware and software that acts as a buffer between an organization and the outside world, usually the Internet or a value added network (VAN). (Romney and Steinbart 2003; Hall 2004) In effect, the firewall acts as a filter to keep out unwanted communications, both incoming and outgoing. Some organizations also place information that they want to shield from outsiders on a separate Internet server that is placed behind a firewall. This server acts as another buffer between the outside world and the organization's information system. If a hacker gains access to the Internet server, only public information can be corrupted or stolen because the proprietary or sensitive information is stored on a separate server that is further protected from the outside world by another firewall. Many organizations use concepts, such as this one, that are based on redundancy to protect themselves from undesirable events.

Controlling Data Input

As stated above, the input process is the most critical process in an information system. Data that enters the information system is what gets processed and output. Computer-based information systems usually use some type of input validation routines to examine data being input. These validation routines can be as simple as checking the types of characters being input into certain fields or as complex as routines that check the reasonableness of data entered into fields. Other examples of validation routines include validity checks, sign checks, completeness checks, sequence checks, and consistency checks, to name a few. (Moscove et al. 2003; Hall 2004)

If the perpetrator is the person who is entering the data, input controls may not be very effective. As mentioned earlier, access controls also act as input controls. If a perpetrator can get to the input devices, then he or she may be able to obtain unauthorized access to the input routines of the information system. Access controls and input validation routines provide protection against such frauds, but as with most controls, they are not foolproof.

Controlling Output From The Computer System

The purpose of an accounting information system is to be able to obtain useful information that is relevant and necessary to make decisions. While the input process may be the most critical process in an information system, the output must also be controlled. Many computer criminals scavenge trash bins to find sensitive or proprietary information that they can use to commit their crimes. Although theft of hard copy documents may not technically be a computer crime, the output that is being stolen comes from a computer information system. Methods of controlling hard copy computer output include shredding all documents that are no longer needed, control lists that indicate who should and should not receive certain reports, and document retention polices.

Interception of electronic communications is another method that perpetrators use to steal computer output. This form of computer crime is similar to wiretapping. The most common method of preventing the theft of electronically transmitted data is encryption. Encryption is the scrambling of data that is transmitted over communications lines. (Moscove et al. 2003; Hall 2004) If the data is stolen, the perpetrator gets only garbled data that cannot be used. The legitimate recipient of the encrypted data must have an encryption key to unscramble the data. Without the encryption key, the data is practically useless. Encryption is also used to scramble the data that is stored in an organization's database to protect that data from hackers. (Hall 2004)

Preventing And Detection Destructive Programs

The CSI/FBI survey indicates that 82 percent of organizations surveyed reported some type of attack from destructive programs. Viruses can be prevented in many ways. Two ways to prevent computer virus infections are antivirus control procedures and antivirus software. Antivirus control procedures include items such as:

- Buying software only from reputable vendors,
- Avoiding copying software,
- Prohibiting the downloading of files from the Internet,
- Deleting e-mail messages from unknown sources without opening them,
- Discouraging the exchange of computer disks,
- Periodically performing virus scans with antivirus software. (Moscove et al. 2003)

Although many organizations have antivirus procedures in place, viruses and worms invariable do enter computer systems. A good protection against such intrusion is antivirus software. Antivirus software scans input and computer or network files for computer code that resembles the code of known viruses. Antivirus programs generally have an antivirus feature that detects viruses as they are downloaded via e-mail or other means. In this case, antivirus software acts as a preventive control. Preventing viruses is the best method of protecting an information system from damage; however, realistically, computers do get viruses. In that case, the antivirus software can detect and usually destroy or quarantine the virus.

Antivirus control procedures are often better preventive controls than antivirus software. New viruses are created daily, and many antivirus software vendors have trouble keeping their software updated. In this case, some viruses or worms can go undetected until the software is updated. Also, many organizations shift the responsibility to scanning for viruses up to individual computer users. These users often do not take the time to perform the scans, which increases the likelihood that the organization's network will become infected. The potential damage caused by a destructive program can be crippling to even the largest organizations.

Detecting Intrusions Into Computer Systems

Organizations naturally want to prevent intrusions into their information systems, but hackers can get past many of the preventive controls that organizations implement. In such a case, the organization must be able to detect the intrusion to stop it. Several methods can be used to detect an intrusion into a computerized information system. Examples of detection technologies that are used are trip wires, honey pot lures, and anomaly detection systems. Once the intrusion has been detected by any of theses methods, the organization can begin to determine what was accessed and by whom, when the unauthorized access occurred, and whether any damage was done, among other things. The organization can then develop preventive measures that can be put in place to prevent such intrusions in the future. One method of developing new controls is the use of vulnerability checking tools. These tools are used to examine computer systems for areas that may be potential security risks. While vulnerability checking tools are generally considered preventive measures, but they are often used to monitor and detect suspicious patterns of usage or changes in configurations that may be the result of a hacker. (Luehlfing et al. 2003)

Trip wires take snapshots of key system characteristics at periodic intervals. When hackers enter a computer system, they often unknowingly alter files and directories. The trip wire devices detect these changes and alert the organization that unauthorized changes have been made.

Anomaly detection systems are similar to trip wires. These systems examine the information system for deviations in expected activity. These deviations provide clues that a computer crime may have been committed. (Luehlfing et al. 2003)

Honey pot lures are used to trap a hacker long enough for the hacker to be identified and possibly apprehended. This method of intrusion detection also stores some evidence of the intrusion that can be used in prosecuting the hacker if apprehended. (Luehlfing et al. 2003)

Although these methods can be quite effective for detecting intrusions, none are foolproof. As with any software, these programs may not work exactly as planned. In some cases, a single intrusion detection system may not be enough. Legitimate changes may be mistaken for unauthorized intrusions. Also, experienced hackers may be able to evade the detection techniques. (Luehlfing et al. 2003) In spite of their limitations, these are better than having no intrusion detection systems at all.

SUGGESTIONS FOR EDUCATING ACCOUNTING STUDENTS ON COMPUTER CRIME AND ETHICS

Accounting students need a good working knowledge of fraud, including frauds committed using computers, and ethics. Students should be aware of the types of computer crimes that are committed, the agencies or people who investigate computer crimes, and how to detect computer crimes, especially if a student plans to work in the area of technology. No single accounting course can provide students with all of this knowledge. Calhoun et al. (1999) suggest that business ethics courses should be a part of the core curriculum in colleges and universities. Accounting students should have more than an ethics course to prepare them for their careers. This paper suggests using three courses to educate accounting students about computer crimes and fraud, detecting fraud, and ethics. These three courses are a traditional accounting information systems course, a fraud detection and/or forensic accounting course, and an accounting or business ethics course. Of course, traditional auditing course also include coverage of fraud and internal controls, especially in the wake of the infamous accounting fraud scandals in recent years, such as Enron, WorldCom, Adelphia, and Tyco. Therefore, auditing courses also add to an accounting student's education on ethics.

Almost all accounting curricula include an accounting information systems (AIS) course, either as a required course or as an elective. The coverage of AIS courses, whether taught using an AIS textbook or instructor notes, generally includes a discussion of fraud, including computer crimes, and internal controls. These courses also include discussion of ethics in accounting and information systems in general. AIS courses are a good starting point in an accounting student's ethics education; however, because of the number of topics that are covered in most AIS courses, the coverage of ethics in computer environments is typically not comprehensive. For example, many AIS textbooks devote at least a chapter to fraud and internal controls used to prevent and detect fraud, but only a portion of one chapter is typically devoted to the issue of ethics in business. Further, textbooks seldom cover ethics related to accounting systems and computers in sufficient detail. Therefore, accounting curricula should include other courses that will allow students to obtain more knowledge on fraud and ethics. Accounting programs that offer graduate degrees have the ability to offer graduate level AIS course in which more ethics can be covered. However, many graduate AIS courses cover advanced technology topics rather than more ethics.

Another suggested course is a fraud detection or forensic accounting course. For an individual to understand the details of frauds that are committed, he or she must understand the different types of frauds and how they are perpetrated. This course should include discussion of not only the types of frauds that are commonly committed, but also of the agencies or people who investigate these crimes. A fraud detection course is the logical place in which to teach these topics.

The fraud detection course should include an in-depth study of how and why frauds are committed. Computer crimes and frauds perpetrated using the computer should be included in the discussion since virtually all organizations have computerized information systems. Such coverage should give students insight into how the perpetrators come to the decision of why and how they commit their crimes.

Deterring fraud should also be included in a fraud detection or forensic accounting course. All things being equal, preventing fraud from occurring is preferred to detecting the fraud after it has happened. The traditional auditing and AIS courses typically include coverage of internal controls and prevention of fraud, but an understanding of fraud prevention techniques may help students understand how the crimes are committed.

Finally, the fraud detection course should include discussion of how frauds are investigated and resolved. If possible, discussion of the organizations that typically investigate computer crimes should also be included in the course. Case studies are appropriate for a course on detecting fraud because of the vast amount of information on fraud in academic articles and in the popular press at any given time. Guest speakers can be integrated into the course to share their experiences in the field of fraud detection so the students understand how important this field is to the accounting profession. Supplementing the professor's knowledge with guest speakers can usually add valuable material to almost any fraud prevention course. Also, many practitioner and academic articles have been written on preventing and detecting fraud. Such articles typically make excellent outside sources for supplementing any textbook used in the fraud detection or forensic accounting course.

Examples of specific topics that might be included in a fraud prevention and detection course are:

- General fraud categories, i.e., financial statement fraud, misappropriation, tax fraud, etc. and the specific frauds that fall into each category, including computer crimes when applicable;
- Perpetrators of fraud and their motivations;
- Control frameworks, particularly COBIT;
- Fraud detection tools and methods of detecting fraud, particularly in computerized environments;
- Interviewing in fraud investigations or examinations; and
- Organizations that investigate frauds

These topics are not all-inclusive nor in any particular order of coverage, nor must they all be included in a fraud prevention and detection course the course to be effective.

Some accounting programs already offer fraud detection or forensic accounting courses. Others may have plans to create such a course to be offered in the near future. Many accounting academics have some experience with fraud detection since many were auditors before turning to academe. Auditors are often exposed to detecting and investigating fraud in the work that they perform for their clients. Therefore, accounting professors are often well suited to teach a fraud detection course. As an alternative to the accounting department offering a fraud detection course, many criminal justice departments offer similar courses on fraud, although such courses do not typically focus on accounting frauds and may not focus on computer crime. For accounting programs that do not have professors who are experienced in fraud detection or that are looking for a different perspective on the topic, using a criminal justice course to supplement an accounting education may be an acceptable alternative.

Another course that will help to educate accounting students is a business or accounting ethics course. As mentioned earlier, almost all accounting courses include some discussion of ethics. However, in many cases, these discussions are limited and may not enough to persuade students that ethics are critically important to the accounting profession and in the business world. In the wake of the recent accounting scandals, states have begun requiring that accounting students take an ethics course as part of their preparation for an accounting career, so many accounting programs have no choice but to offer an ethics course.

The ethics course should preferably be taught by an accounting professor, and the course should focus on accounting and business ethics rather than ethics in general. Philosophy departments at many colleges and universities offer courses on ethics that examine the concepts of ethics being determining right from wrong. However, an accounting or business ethics course narrows the focus to the accounting or business environment so that students can relate ethical issues to the preparation for their careers in accounting.

The ethics course should include as many current events as possible. Current fraud investigations and trials of individuals or organizations that have been accused of committing frauds are quite common in the popular press. Many recent academic and practitioner articles have been written on ethics in the accounting profession and educating accounting students on ethics. In addition, many books, videos, documentaries, and movies include fraud or the investigation of fraud. These media, especially popular movies, usually stimulate the interest of students and can be used to examine the ethical choices that were made by the perpetrators. Current events and teaching media other than textbooks often keep the attention of students better than lectures, so as many alternative formats should be used in the ethics course since so many worthwhile examples exist.

Examples of specific topics that might be included in an accounting ethics case are:

- Professional and corporate codes of ethics;
- The significance of a public accounting firm's culture in promoting ethics;
- Laws, regulations, and standards that pertain to ethics;
- Oversight bodies that are responsible for "legislating" ethical standards;
- An examination of the differences in ethics among groups, i.e, new professionals versus older professionals, professionals versus non-professionals, etc. and the erosion of ethical standards in recent times;

- Responsibility of the CPA to clients, the public, and the profession;
- Challenges to CPAs in keeping the public trust.

As with the fraud detection course, these suggested topics are not all-inclusive, nor are they required in every ethics course. Many accounting professors have their own ideas about what is important enough to be included in an ethics course. As long as the basics of ethics and ethical behavior in the accounting profession and in business environments in general are covered and the students are made aware that ethics are a critical part of the accounting profession, the coverage in the course need not be set in stone.

These three courses should give accounting students a good start on building an ethical framework. Accounting students must have sufficient knowledge of computer fraud to be an effective accounting professional. The traditional AIS course and a fraud detection or forensic accounting course give students the foundation they need to understand why and how computer crimes and fraud are committed. Although many people feel that ethics cannot be taught, continued exposure to the topic gives accounting students a good foundation for making choices in situations with which they will be faced during their careers.

CONCLUDING COMMENTS

The accounting profession has seen several recent incidents of fraud that have shaken the foundations of the profession. For example, WorldCom and Enron have both been implicated in frauds that have involved their auditor, and HealthSouth and Tyco have been implicated in frauds that involved their upper managements. One-time "Big Five" accounting firm Arthur Andersen basically no longer exists as a result of lapses in ethics and competence that constituted fraud. Accounting students must be made aware that such actions are not acceptable to the profession or to society. Students must be exposed to as much ethics as possible during their years in accounting programs. Most accounting courses include discussions of ethics, but these limited discussions on ethics may not be enough.

This paper examines several types of computer crimes and ways that technology is being used to prevent and detect computer crimes. Three accounting courses that will give accounting students a good foundation regarding fraud and ethics are suggested. These courses are an AIS course, a fraud detection course, and an ethics course. These courses, used in concert with each other, will provide accounting students with knowledge they will need when they are faced with frauds or ethical decisions during their accounting careers.

REFERENCES

1. American Institute of Certified Public Accountants. 2004. Antifraud Resource Center accessed on 3/30/2004 at http://www.aicpa.org/antifraud/homepage.htm.
2. Calhoun, C. H., M. E. Oliverio, and P. Wolitzer. 1999. *Ethics and the CPA: Building Trust and Value-Added Services*. John Wiley & Sons, Inc.: New York, NY.
3. Casabona, P. and S. Yu. 1998. Computer Fraud: Financial and Ethical Implications. *Review of Business*. 20 (1): 22-25.
4. Computer Security Institute. 2003. *CSI/FBI Computer Crime and Security Survey*. Computer Security Institute: San Francisco, CA.
5. Hall, J. A. *Accounting Information Systems*, 4th Edition. South-Western College Publishing: Mason, OH.
6. Harris, S. 2003. Fighting Pirates. *Government Executive*. 35 (15): 68.
7. Luehlfing, M. S., C. M. Daily, T. J. Phillips, Jr., and L. M. Smith. 2003. Cyber Crimes, Intrusion, Detection, and Computer Forensics. *Internal Auditor*. 18 (5): 9-13.
8. McGillivray, G. 2000. Hazards of the Information Superhighway. *Canadian Underwriter*. 67 (4): 34-40.
9. Moscove, S., M. Simkin, and N. Bagranoff. 2003. *Core Concepts of Accounting Information Systems*, 8th Edition. John Wiley & Sons: New York, NY.
10. Romney, M. and P. J. Steinbart. 2003. *Accounting Information Systems*, 9th Edition. Prentice Hall: Upper Saddle River, NJ.
11. vmyths.com. 2000. The Worldwide Michelangelo Virus Scare of 1992. Accessed on 3/30/2004 at http://vmyths.com/fas/fas_inc.inc1.cfm.

12. Whitman, M. E. 2003. Enemy at the Gates: Threats to Information Security. *Communications of the ACM*. 46 (8): 91-95.
13. Zekany, K. E., L. W. Braun, and Z. T. Warder. 2004. Behind Closed Doors at WorldCom: 2001. *Issues in Accounting Education*. 19 (1): 101-117.

NOTES

NOTES