ACCOUNTING STUDENT PERCEPTIONS OF ETHICAL BEHAVIOR: INSIGHT INTO FUTURE ACCOUNTING PROFESSIONALS

Teresa K. Lang, Columbus State University
Dianne Hall, Auburn University
Rita C. Jones, Columbus State University

ABSTRACT

Governmental and organizational directives often mandate ethical behavior. Much of the research into ethics relies on whether the participant believes a situation is ethical or not. This study extends ethics research by examining accounting students' perceptions of ethical situations on a continuous scale. Our results suggest that an individual's perception may be influenced by his or her position in the scenario or by his or her gender. We find that perception of ethical behavior is affected by the threat of consequences. These findings can be used to improve ethics training in both organizations and business schools.

INTRODUCTION

The Public Accounting Reform and Investor Protection Act of 2002, better known as the Sarbanes-Oxley (SOX) Act, was developed in response to corporate scandals such as those involving Enron, Tyco International, and WorldCom. WorldCom's earnings management techniques overstated income by hiding bad debt, understating expenses, and backdating contracts. Tyco International executives sold company stock without proper reporting to the United States Securities and Exchange Commission (SEC), gave unapproved bonuses to buy silence within the organization, and gave themselves interest-free or low interest loans for personal use. Enron executives made false statements to banks and auditors and participated in insider trading, bribery, irregular accounting practices, bank fraud, securities fraud, wire fraud, money laundering, and conspiracy. These three scandals ended in bankruptcy and caused significant financial loss to employees and investors.

The United States Congress responded to the scandals by passing SOX, which has effectively changed the business environment in which both accountants and business managers operate. The Sarbanes-Oxley Act attempts to regulate and reinforce ethical behavior within companies in the United States. Corporate chief executive officers and chief financial officers must attest to the accuracy of the company's financial statements. Corporations cannot make personal loans to

executives or directors, and top-level management must attest that the company has effective internal controls in place to prevent or detect misstatements and improprieties.

Section 404 of the Sarbanes-Oxley Act (H.R. 3763) requires that an organization's external auditor assess the internal controls and issue an opinion on the management's report regarding internal controls over financial reporting. The 1992 report of the Committee of Sponsoring Organizations of the Treadway Commission (Committee of Sponsoring Organizations of the Treadway Commission, 1994), The *Internal Control- Integrated Framework*, is the standard used by auditors and managers to evaluate controls. The report outlines the key components of a good internal control structure. The first component is the organization's control environment. The framework outlines that the control environment sets the tone of an organization and influences the control consciousness of its people. The control environment includes the integrity, ethical values and competencies of the entity's people, management's philosophy and operating style, the process used by management to assign authority and responsibility and to organize and develop its people; and the attention and direction provided by the board of directors. An ethical corporate governance system requires an ethical, underlying internal control structure.

External auditors and managers are expected to evaluate whether an organization sufficiently incorporates ethics into the control environment. If they recognize an action is unethical but at the same time perceive the action is commonly accepted or less unethical than another, couldn't this affect the evaluation of risk? This study is part of an ongoing effort to identify factors that influence future managers' and accountants' opinions relating to what is ethically acceptable and unacceptable. This study extends prior research by using a continuous scale instead of the typical dichotomous scale (Kreie & Cronan, 1998; McMahon & Harvey, 2005). The degree to which participants believe the situation is ethical/acceptable or unethical/unacceptable is revealed. The results provide supervisors and academics insight into the ethical perception of future professionals.

MANDATED BUSINESS ETHICS

The need to influence ethical behavior in the business community is not new. Questionable corporate political campaign finance practices and corrupt foreign practices in the 1970s prompted the SEC and the United States Congress to enact campaign finance law reforms. The 1977 Foreign Corrupt Practices Act (FCPA) made it illegal to extend bribes to foreign government officials in order to obtain or retain business within that country, and required evidence of compliance from organizations doing business abroad. In response, a private-sector initiative, the National Commission on Fraudulent Financial Reporting (commonly known as the Treadway Commission), was formed in October 1985. The Treadway Commission issued its initial report in 1987, and among other items, recommended that the organizations sponsoring the Commission work together to develop integrated guidance on internal control.

As a result of this initial report, the Committee of Sponsoring Organizations (COSO) was formed and retained Coopers & Lybrand, a major CPA firm, to study the issues and author a report regarding an integrated framework of internal control. The report titled "Internal Control - Integrated Framework" was issued in 1992 and re-published with minor amendments in 1994. This report presented a common definition of internal control and provides a framework against which internal control systems can be assessed and improved. This report is the standard that U.S. companies use to evaluate compliance with FCPA (1998) and SOX. In 1998, the FCPA was updated; one of the changes was to include employees or officers of public international organizations, including, among others, the Red Cross and the World Health Organization. As a result, many organizations were forced to revisit their compliance policies. SOX further necessitated reviews of ethical behavior in organizations.

SOX outlines the need for internal controls and calls for both financial and criminal penalties for unethical behavior specific to financial reporting. Section 404 requires that companies "provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use, or disposition of (its) assets that could have a material effect on the financial statements" (Securities and Exchange Commission, 2003, p. 11). Section 409 requires all data about financial changes be brought forth and disclosed rapidly and currently. This may include anything that affects the company's financial situation such as stock price and intellectual property. Some issues that may fall into this reportable area include virus attacks, large systems outages, important data loss, and security violations (Cunningham, 2005). Section 802 requires that companies maintain records relating to audits and reviews for five years. The maintenance of this and similar information increases storage requirements and further increases the risk of unintentional information leaks, thus requiring more diligence on the part of the organization along with a focus on appropriately secure technology. Table 1 summarizes some the technology related requirements of the Sarbanes-Oxley Act (Pasley, 2006).

Table 1: Some Technology-related Requirements of the Sarbanes-Oxley Act

Statute	Summary	Threat
Section 302 - Corporate Responsibility for Financial Reports	Requires executives to certify the accuracy of corporate financial reports.	Unauthorized modification of data; data fraud.
Section 404 - Management Assessment of Internal Controls	Requires executives and auditors to confirm the effectiveness of internal controls for financial reporting.	Unauthorized access to data, data deletion.
Section 409 - Real Time Issuers Disclosures	Requires any material changes to financial state of issuer be communicated quickly and with supporting data to public.	Non-availability of data, data recoverability issues, backup, and restore.

A study conducted by Oracle indicated that 42% of the information technology professionals surveyed did not believe their company could adequately protect their information. In addition, 45% of those surveyed did not think their company could appropriately notify their customers in the event of a breach. These professionals cited a need for automated audit and security controls to combat privacy and security risks (Oracle, 2007). Clearly, the intent of SOX and the reality facing most organizations differs, underscoring the need for adequate risk assessment during audits.

The post SOX financial audit requires that auditors expand their concept of risk to include technology issues, and perhaps evaluate their own perceptions of risk related to technology. Prior research indicates that individuals do not regard digital piracy as important or unethical (Al-Rafeem & Cronan, 2006; Im & Van Epps, 1991; Reid & Thompson, 1992). Auditors and managers must identify and evaluate the risks affecting an organization in order to understand, implement, and test the controls operating in the organization in order to provide reasonable assurance that transactions are properly recorded, assets protected, and SOX requirements are met. If individuals do not regard data piracy as important or unethical, they may not assign an appropriate level of risk to technology issues when implementing and evaluating controls.

BUSINESS ETHICS AMONG ACCOUNTING STUDENTS

New accounting graduates have a foundation in business, accounting, and auditing. The context of SOX has been taught; some schools offer classes in business ethics. However, few studies exist to indicate how the average accounting student views ethics in a business environment. Extant studies generally use a dichotomous (ethical, not ethical) scale (Kreie & Cronan, 1998; McMahon & Harvey, 2005). Our study uses a continuous scale to investigate the degree to which business students perceive the unethical/unacceptability of technology scenarios versus a typical unacceptable accounting scenario. This measure may better indicate the level of risk young professionals would assign when evaluating control systems, and provide managers and academics insight for practical application.

This study was conducted in sophomore level core accounting classes at a large southeastern university. There were 174 respondents; 53% were female. Two respondents were freshman, 94 were sophomores, 44 juniors, 27 seniors, and seven did not complete the question. A total of 159 participants were between 19 and 23, seven were 24-30, one was 36-40, and seven did not complete the question. Participants were awarded ten bonus points for completing the survey. Those that did not wish to complete the survey were offered extra homework to earn ten bonus points. Approximately 20% of the students chose this option, for a response rate of 80%.

The survey included three scenarios, two current IT related scenarios, and one accounting related scenario. Scenario one relates to inappropriate use and potential damage of employer resources. Scenario two relates to data privacy, and scenario three relates to earnings management. The scenarios and questions were amended to represent issues common to general business and

accounting disciplines from the scenarios used in a previous study using students in computing classes (Leonard & Cronan, 2005) and are shown below

Scenario 1: "While surfing the web at work, and employee unknowingly downloads a file containing a virus. The person opens the file and a message appears informing the person that the virus has been released on the computer. The computer is connected to the company network and is shared by several users. The computer appears to be operating normally, and when rebooted shows no sign of trouble. The person tells no one about the virus."

Scenario 2: "A fellow employee asks the database administrator working for a large health care organization to give them a copy of the data stored on the database. The information stored in the database comes from a questionnaire filled out on the company website. In exchange for completing the questionnaire (containing specific questions about prescription use and medical conditions), visitors to the website are provided access to a medical encyclopedia and drug interaction program. The database administrator copies the information and gives it to the employee."

Scenario 3: "A manager at a large, international corporation is reviewing the monthly financial reports. The manager finds that his division will fall short of his projected net income by $20,000. The manager was promised a bonus if the net income projection was met. He remembers he increased the estimated loss on accounts receivable for the month by $24,000 (an acceptable accounting practice). This resulted in a decrease in net income for the month of $24,000. He contacts the accounting department and tells them he overestimated the loss by $20,000. Since the estimate is based on the manager's calculation, accounting makes the change; the manager receives the bonus, and next month the manager increases the estimated loss back to $24,000."

Participants were asked whether they believed the behavior described in each scenario was ethical/acceptable or not ethical/not acceptable. The question was repeated several times asking the participants to put themselves in the position of the employee, the supervisor of the employee, or the friend of the employee. The participants were also asked their opinion when there would be consequences if the behaviors were reported.

ANOVAs were completed using scenarios as the factor and ethics/acceptability on the continuous scale as the response variable. The scale is zero (acceptable) to thirteen (unacceptable). There is a significant difference between the scenarios (Table 2).

Scenario two relates to data privacy. Participants felt less strongly about the unacceptability of sharing private data than about the release of a virus on the employer's computer system or about earnings management. This held true for questions one through three. Question one refers to a theoretical employee's behavior. Question two indicates the participant is the employee, and question three indicates the participant is the supervisor in-charge of the employee. The lower mean indicates participants believed less strongly that the behavior was unacceptable in scenario two than scenario one or three.

Questions three and four ask the respondent the acceptability of the behavior from the perspective of being the supervisor or the friend of the employee. Again the data sharing is perceived as less unacceptable than the other two scenarios. Question 5 indicates that the individual would be caught. Only in this instance is data piracy more unacceptable than virus reporting.

Table 2: ANOVA Analysis Results

Scenario 1	Mean	Scenario 2	Mean	Scenario 3	Mean	df	P-value
1. The employee did not report the virus.	9.905	1. The administrator providing the employee a copy of the information.	7.683	1. The manager changing the estimate.	9.709	2	.000
2. If I were the employee, not reporting the virus would be	10.112	2. If I were the administrator, copying the information would be	8.182	2. If I were the manager, changing the estimate would be:	9.598	2	.000
3. If I were the supervisor, I would find the employee's behavior:	10.208	3. If I were the supervisor, I would find the administrator's behavior	8.504	3. If I were the supervisor, I would find the manager's behavior:	10.298	2	.000
4. As a friend of the employee, I would advise my friend to: 0 not report the virus; 13.2 report the virus.	10.283	4. As a friend of the administrator, I would advise my friend to: 0 copy the information; 13.2 not copy the information	8.736	4. As a friend of the manager, I would advise my friend to: 0 change the estimate; 13.2 not change the estimate	9.482	2	.000
5. If the employee knew that, if discovered, he (she) would be reprimanded, he(she) should:	9.423	5. If the administrator knew that, if discovered, he(she) would be reprimanded, he(she) should	10.61	5. If the manager knew that, if discovered, he (she) would be reprimanded, he(she) should	10.56	2	.000

Pairwise comparisons confirmed the differences between scenario 2 and the other two scenarios (Table 3). All results were confirmed using non-parametric measures.

Table 3: Pairwise Comparisons				
Question	Scenario	Scenario	Significance	Second Comparison
1	2	1 and 3	.000	1 to 3 not significant
2	2	1 and 3	.000	1 to 3 not significant
3	2	1 and 3	.000	1 to 3 not significant
4	1	2 and 3	.000 and .028	2 to 3 not significant
5	1	2 and 3	.000 and .001	2 to 3 not significant

DISCUSSION

Question one for each scenario describes the situation and asks the respondent in general whether the behavior is acceptable or not. Respondents rated scenario one, not reporting the introduction of a virus to the employer's computer network, and scenario three, changing an accounting estimate for personal gain, similarly with means of 9.7 – 9.9. The higher the mean, the more unacceptable the respondent perceives the behavior. However, scenario two, the database administrator providing private data to an employee, averaged 7.7. Respondents viewed scenario two as less unacceptable than the other two scenarios. The pairwise comparison indicates there is a statistically significant difference between scenario two and the other two scenarios, but not between scenarios one and three. Clearly, as a general behavior, data piracy is less important to accounting students than reporting a virus or changing estimates. Given that data piracy is a major issue both from a government mandate perspective and a consumer trust perspective, this finding is worrisome. Is this a general attitude for accounting students in particular, and potentially the generation about to enter the workforce? Do individuals at this stage simply have less concern because they have fewer items about which to worry (e. g., retirement accounts, credit history)? More investigation into these results may shed light on the foundations that facilitated these responses.

Question two asks the participant to respond assuming the participant is the employee, administrator, or manager performing the behavior. Scenario two is again scored as less unacceptable/unethical than the other two scenarios. Interestingly, the virus and data infractions are scored even more unacceptable than when considered as general behavior, while the accounting change is scored slightly less unacceptable. Although statistically insignificant, these differences are interesting. It would appear that students perceive data piracy and non-report of a virus more troublesome when they take ownership of the scenario, but changing an estimate less so. Nonetheless, data piracy was still statistically less important than either of the other scenarios. There were no significant differences between scenario one, not reporting the computer virus and scenario three, manipulating the accounting information.

Question three puts the participant in the position of supervisor. Scenario two is again scored less unacceptable/unethical than the other two scenarios. All three scenarios are scored more unacceptable/unethical for this question than questions one and two, perhaps indicating that students place a higher ethical standard on supervisors than supervisees. Although not statistically significant, this is an interesting finding. Would this general assertion (that supervisors should be held to a higher standard) be found in a general population? How would this change if working individuals were surveyed? Would there be a difference between supervisors and supervisees in their assumptions of unethical behavior?

Participants' responses to questions one through three all indicate that participants perceive the data privacy scenario differently than the virus or earnings management scenarios. Managers dealing with young professionals should take this possible bias into consideration when establishing controls and may want to reinforce the importance of data privacy and other technology related risks during training. Academics training future professionals should include technology ethical issues when addressing ethics in the classroom.

Question four puts the participant in the position of a friend and advisor to the person involved in the scenario. More participants would advise a friend to report the virus infection than would advise a friend not to copy the data or not to make the accounting change. This is the first question in which the data piracy scenario is not different from the others. There was no significant difference between the data privacy issue and the accounting manipulation, although the emphasis on an accounting change dropped from its position in question three. These results make us wonder why virus reporting is emphasized over data piracy or accounting changes when the participant takes on an advisory role. Is this because reporting a virus is largely non-consequential? The scenario does not state whether the original action (web surfing) was not permitted at the workplace. Assuming that the employee was surfing during a break, contracting a virus is less of a direct ethical issue than either data piracy or accounting changes. Therefore, suggesting that not reporting the virus has, apparently, fewer consequences. The participant's role as advisor allows him or her to maintain an ethical standard without causing issue for his or her friend. It is also important to note, that while participants more strongly recommended virus reporting than either preventing data piracy or accounting changes, the mean of the responses is still in excess of the midpoint, thus more respondents would recommend an ethical behavior.

Question five directly introduces consequences into the scenarios. If a reprimand would result, the mean is lower for reporting the virus than for choosing not to copy the data or not to change the accounting estimate. Clearly, the consequences of the action have a bearing on a participant's choice. The issue of data piracy being unethical is relatively low (mean = 7.683) whereas, once consequences are added, the mean jumps to 10.60 for the other two scenarios. For both data piracy and accounting changes, this question results in the highest level of perception of unethical behavior. Virus reporting, on the other hand, is perceived as the least unethical of all the questions. These results are different from those of question four where the participant is advising

a friend. It appears that, when reprimands are included, participants are more worried about avoiding reprimands (e.g., for data piracy) than for virus reporting.

Consequences seem to provide the most extreme responses for scenarios two and three. Managers should note that introducing consequences seems to have a varied affect on the intensity of the participants' responses. Specifically outlining consequences for undesirable actions may decrease the likelihood of young professionals engaging in certain activities, while providing an anonymous method to report similar activities may offer another way to decrease the risk related to these situations.

This survey was initially developed and used in ethics research in systems classes. Earlier studies of ethics found differences in ethical decisions between gender (Kreie & Cronan, 1998). Therefore, gender differences were analyzed. T-tests reveal a significant difference between means for males and females relative to virus reporting. Males averaged 10.49, while females mean was 9.06 ($df = 156$, $p=.000$). Therefore, males found not reporting the virus more unacceptable than females. Although the gap is closing, this finding may be explained by the gender gap that exists in technology (Bhattacharjee & Shaw, 2001). Overall, there are more men in the technical field; these individuals are more likely to understand the true impact of a virus. Therefore, they see failure to report a problem as being more troublesome. However, men were less likely to encourage a friend to report a virus (men=9.86; women=10.61, $p=.05$) than women. While this seems contrary on the surface, it may simply have to do with women being more collaborative and social, thus engaging in advise giving, whereas men are more solitary and hands-off, therefore less likely to engage in a casual advisory role (Brody, 1997; Carli & Eagly, 1999). No differences were detected for scenarios two and three.

CONCLUSION

In general, the participants in this study did not treat the scenarios the same, although most government and corporate mandates view ethical violations equally. While it would be true that the consequences may vary, each of these scenarios are in direct violation of ethical guidelines for technology use and financial reporting. It may be that organizations and business schools should focus on eliminating unethical behavior of any kind, rather than focus on the level of consequences attached thereto. FCPA, SOX, and other acts developed by the federal government are attempts to dictate acceptable, ethical business behavior. States have attempted to address the need for ethical behavior in the accounting industry by requiring certified public accountants pass ethics exams before renewing their licenses (Burke & D'Aquila, 2004). Accounting is not alone in this endeavor, but it is the industry that draws focus from the two acts discussed here.

This study extends our understanding of the relative degree to which accounting students interpret ethical and unethical behavior by using a continuous rather than dichotomous scale. This provides a better indication of the beliefs of the individuals involved and may provide better insight

into what their behavior might be given different situations. Management and auditors can also use this information to better design, implement, and evaluate the control environment in business today. The better our understanding of ethical behavior of students and employees, the better we can train future professionals to engage in ethical behavior and compliance.

REFERENCES

Al-Rafeem, S., & Cronan, T. P. (2006). Digital Piracy: Factors that Influence Attitude Toward Behavior. *Journal of Business Ethics, 63*, 237-259.

Bhattacharjee, S., & Shaw, L. (2001). Evidence that Independent Research Projects Improve Accounting Students' Technology-related Perceptions and Skills. *Accounting Education, 10*(1), 83-103.

Brody, L. R. (1997). Gender and Emotion: Beyond Stereotypes. *Journal of Social Issues, 53*(2), 369-394.

Burke, J. A., & D'Aquila, J. (2004). A Crucial Test for New CPAs. *The CPA Journal, 74*(1), 58.

Carli, L. L., & Eagly, A. H. (1999). Gender Effects of Social Influence and Emergent Leadership. In G. Powell (Ed.), *Handbook of Gender and Work* (pp. 203-280). Thousand Oaks, CA: Sage.

Casabona, P., & Yu, S. (1998). Computer Fraud: Financial and Ethical Implications. *Review of Business, 20*(1), 22.

Committee of Sponsoring Organizations of the Treadway Commission. (1994). *Internal Control - Integrated Frameworks (2. Vols)*. New York, NY: American Institute of Certified Public Accountants.

Cunningham, M. (2005). *Meeting Sabanes-Oxley Section 409 Requirements*. Retrieved April 4, 2008, from www.s-ox.com/feature/detail.cfm?articleID=1067

Im, J., & Van Epps, P. (1991). Software Piracy and Software Security in Business Schools: An Ethical Perspective. *The DATABASE for Advances in Information Systems, Summer*, 15-21.

Kreie, J., & Cronan, T. P. (1998). How Men and Women View Ethics. *Communications of the ACM, 41*(9), 70-76.

Leonard, L. N. K., & Cronan, T. P. (2005). Attitude toward ethical behavior in computer use: A shifting model. *Industrial Management & Data Systems, 105*(9), 1150-1171.

McMahon, J. M., & Harvey, R. J. (2005). *Psychometric Properties of the Reidenback-Robin (1990) Multidimensional Ethics Scale (MES).* Paper presented at the Society for Industrial and Organizational Psychology, Los Angeles, CA.

Oracle. (2007). *What Worries IT & Compliance Practioners Most about Privacy and Data Security?* : Ponemon Institute LLC.

Pasley, K. (2006). *Sarbanes-Oxley (SOX) - Impact on Security in Software*. Retrieved July 23, 2008, from www.developer.com/security/article.php/3320861

Reid, R., & Thompson, J. (1992). Knowledge and Attitudes of Management Students Toward Software Piracy. *Journal of Computer Information Systems, 33*, 46-51.

Securities and Exchange Commission (2003). *Final Rule: Management's Report on Internal Control Over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports*. Retrieved July 24, 2008, from http://www.sec.gov/rules/final/33-8238.htm