Students' Perceived Ethical Severity of e-Learning Security Attacks

Yair Levy
Nova Southeastern University
levyy@nova.edu

Michelle M. Ramim
Nova Southeastern University
ramim@nova.edu

Abstract

Over the past 15 years there has been a sharp increase in the use of e-learning systems both in education for degree delivery as well as corporate environment for training and certification purposes. Information systems security has been an important concern for most organizations. However, very little attention has been given to information security in the context of e-learning systems. In this study, we conducted an investigation into students' perceptions of ethical severity related to five common information security attacks in the context of e-learning. We have concentrated our investigation specifically in testing for differences over these five e-learning security attacks based on gender, age, and academic rank (undergraduate/graduate). Our findings indicate that majority of the students appears to self-report their perceptions as ethically driven across all five e-learning security attacks. However, we were somewhat alarmed to find that, although a small percentage, indeed some students reported these security attacks to be ethical. Our results indicated that overall males find these security attacks less severe than females. We also found that undergraduate students appear to perceive these attacks only slightly less severe than graduate. Age wise, our results indicated that there is an increase trend where the older the student is, the more severe s/he ranks the attacks. The paper concludes with a summary of the results and implication of this study for practice and research.

Keywords: Students' ethical perceptions, e-learning security attacks, e-learning system attacks, perception of ethical security, perceived ethical severity of security attacks.

Introduction

In 2007, more than 3.94 million U.S. students enrolled in at least one online course as reported by the Sloan Consortium. E-learning enrollment trend has proliferated steadily by about 13% annually or 758,000 students annually over the past few years (Johnson, 2009). Additionally, according to one study, e-learning has captured about 32% of the adult education market (Means, Toyama, Murphy, Bakia, & Jones, 2009). E-learning has expanded beyond higher education to career technical education, medical education, corporate and military training, as well as K-12 education. At the same time, higher education institutions have supported this trend by offering more e-learning courses (Geri & Gefen, 2007). In fact, 96% of 2-year and 4-year public higher education institutions provide some form of e-learning courses ("U.S. Department of education", 2009). Following these statistics affirming the trend in e-learning, higher education institutions are faced with the challenge of providing a secured and accountable e-learning environment. Within this established environment, where learning is conducted over the Web, learners and instructors interact via the e-learning system. Though there is a limited body of research about security strategies for any Web-based system, cyber-security does pose a real concern (Kritzinger, 2006), so much that the U.S. government has appointed a czar to help coordinate strategic efforts to reduce cyber-security treats (i.e. malware,

spoofing, phishing, and botnets to name a few) ("Obama calls for cyber czar", 2009). Cyber-security attacks were also found to have a profound crippling impact on the e-learning systems of higher educational institutions (Ramim & Levy, 2006).

Given the recent reporting in the news media about the downturn in the global economy, some employees face intense pressure to meet expectations from their organizations and various stakeholders. Additionally, literature previously noted that corporate social responsibility appears to be a façade rather than a sincere practice in most business organizations (Geva, 2006). Indeed, a surge in incidents of unethical behavior has been reported in the U.S. news media, for example, the Barney Madoff Ponzi scam, the 2008 Singapore Grand Prix crash, and the ACORN scandal, to name a few. Following legal investigation of these incidents revealed that employees acted unethically and illegally under pressure to reap personal gains. Similar unethical scandals have been reported in higher education, for example, the student Loan Xpress fraud, the admissions scandal at the University of Illinois, and the 2007 Duke Business School cheating scandal among other incidents. Similarly, students have engaged in unethical behavior in order to gain an advantage. Despite the public attention to these scandals, it appears that unethical behavior still occurs in alarming ways including in higher education.

Levy and Ramim (2009), as well as Molnar, Kletke, and Chongwatpol (2008) reported that students' misconduct is more likely to involve the use of Information Technology (IT) resources. Furthermore, students perceived that cheating using IT is more acceptable than cheating without the use of IT. Rogers (2006), Cronan, Foltz, and Jones (2006), and Harris (2004) found that students are using advanced IT tools to engage in unethical behavior. Furthermore, these studies indicated that it is also alarming that in some courses students are learning about specific IT breaching techniques (i.e. hacking skills, approaches for installing sniffing software and approaches for the identification of passwords, developing Denial of Service (DoS) attacks, and learning how to manipulate weaknesses with a Transmission Control Protocol (TCP) connection). The number of cyber-security incidents have climbed sharply over the past decade, though only small percentage of such attacks is reported to the public (Harris, 2004). Subsequently, Harris (2004) reported that the majority of computer hackers are below the age of 30, pointing the need to investigate users in that age group and their perceptions about unethical behaviors, specifically security attacks.

Students' motivation to engage in unethical behavior can be accounted to temptation to speed graduation (Lawson, 2004), availability of convenient IT tools (Molnar et al., 2008), a sense of entitlements and lack of consequences, peer pressure, as well as lack of understanding of the purpose of their education (Nguyen & Biderman, 2008). Lawson (2004) found that students engaging in misconduct in their academic career are more likely to engage in unethical behavior during their professional career compared with students that are ethical. Thus, the focus of this work was to investigate students' perceptions about the severity level of key e-learning security attacks, and to create awareness about e-learning security. The nucleus idea behind this investigation was that if students perceive the severity of key e-learning security attacks to be low, then they might be more likely to engage or seek help in engaging on their behalf in such unethical behavior.

Theoretical Background

According to Shaw (2008), "ethics deals with individual characters and moral rules that govern and limit our conduct" (p. 5). He also added that ethics "investigates questions of right and wrong, fairness and unfairness, good and bad, duties and obligation, justice and injustice, as well as responsibility and the value that should guide us" (Show, 2008, p. 5). Researchers such

as Cronan et al. (2006), Dorantes, Hewitt, and Goles (2006), as well as Kreie and Cronan (1998) noted that ethical behavior is gender dependent, indicating significant differences between males and females in their ethical perceptions as well as their behaviors. They indicated that in general, males appear to be less ethically driven, whereas females appear to be more ethically driven. Moreover, age and academic rank was also found to show differences related to perceptions about ethical behaviors. Kreie and Cronan (1998) noted that "a person's characteristics, such as gender, age, and education may also affect one's view of what is ethical" (p. 72). Although such investigations appear to indicate gender, age, and academic rank differences with ethical perceptions, very little research has been done about such differences in the context of cyber-security attacks, especially in the growing Web-based environments such as e-learning systems.

Methodology and Instrument

The aim of this study was to investigate students' perceptions of e-learning security attacks. With some evidence from literature (Cronan et al., 2006; Ramim, 2007) indicating that gender, age, and academic rank may have implications on ethical severity, this study investigated the following four research questions:

RQ1: How severe do students perceive e-learning security attacks?
RQ2: Are there significant differences between males and females on their perceived ethical severity of e-learning security attacks?
RQ3: Are there significant differences between undergraduate and graduate students on their perceived ethical severity of e-learning security attacks?
RQ4: Are there significant differences between students' age groups on their perceived ethical severity of e-learning security attacks?

As the key part of this study was to try to simplify the data collection, only five key security attacks were investigated. The five were set to include the common components of security attacks of any type of a system including: attack to the server, intercepting e-mails, unauthorized file sharing, unauthorized access, and spoofing attack. As the context of this work is in e-learning security, the five security attacks were communicated to the study participants specifically in the context e-learning systems use. The five e-learning security attacks (note as eLSA) that this study investigated are indicated in Table 1. The instrument included these five items with a scale assessing their perceived ethical severity on a five point Likert scale (1= 'ethical', 2 = 'somewhat ethical', 3='slightly unethical', 4='unethical', and 5='very unethical') regarding the five e-learning security attacks.

Table 1. The five e-learning security attacks

Item #	Item Description
eLSA1	Initiating a cyber-attack on the e-learning server via the Internet and causing it to be unavailable
eLSA2	Intercepting e-mails (reading and/or altering e-mails sent to someone else)
eLSA3	Unauthorized file sharing during e-learning exams
eLSA4	Unauthorized access to e-learning network resources
eLSA5	Spoofing attacks by students who impersonate their peers to falsify data

Analysis and Results

Sample and Descriptive Statistics

The sample used for this research included about 1,100 students attending online courses both at the undergraduate and graduate level during fall 2006 to fall 2009. Students received an email message closer to the end of the term explaining about the growing issues with e-learning security and seeking their consent to take part in the study. Then, a link to the survey was provided where they were first introduced to concepts assessed. A set of 519 responses were received, which represents about 47% response rate. Responses included 268 females (51.6%) and 251 males (48.4%). Academic rank based on undergraduate and graduate level was about half with 261 participants (50.3%) undergraduate and 258 (49.7%) graduate students. Additionally, majority of the students, 434 (83.6%), were under the age of 34. Table 2 depicts the descriptive statistics of the study participants.

Table 2. Descriptive Statistics of Study Participants (N=519)

Item	Frequency	Percentage (%)
Gender		
Male	251	48.4%
Female	268	51.6%
Age		
18 or under	2	0.4%
19-24	221	42.6%
25-29	150	28.9%
30-34	61	11.8%
35-39	24	4.6%
40-44	26	5.0%
45-54	30	5.8%
55-59	4	0.8%
60 or older	1	0.2%
What degree program are you currently enrolled in?		
Undergraduate	261	50.3%
Graduate	258	49.7%

Analyses

In order to test for students' perceived ethical severity of the five e-learning security attacks, we started by conducting an overall frequency assessment across all five items. We have found that majority of the students appears to self-report their perceptions as ethically driven across all five e-learning security attacks. Specifically, we found that the overall percentage of students reported, either '4' (unethical) and '5' (very unethical) when asked to rate their ethical severity about the five e-learning security attacks, was very high (eLSA1: 452 or 87.1%; eLSA2: 492 or 94.8%; eLSA3: 439 or 84.5%; eLSA4: 465 or 89.6%; eLSA5: 490 or 94.4%). Such results indicates that majority of the students appear to understand the severity of these e-learning security attacks. However, what have alarmed us was that, although a small percentage, indeed we had students who reported either '1' (ethical) and '2' (somewhat ethical) when asked to rate their ethical severity about the five e-learning security attacks. Specifically for eLSA3, we found 34 students who self-reported that unauthorized file sharing during e-learning exams is

ethical. We anticipated that none of the study participants would score '1' or '2'. However, it appears that not all students recognized the severity of such attacks. Here, attacking the e-learning server is the equivalent of shutting down the university's e-learning program. This is comparable to activating the fire alarm at the university campus so that the class will be cancelled, exam will not be conducted, assignments will not be collected, etc.

In order to test for differences between males and females on their perceived ethical severity of e-learning security attacks, we conducted a nonparametric test using Mann-Whitney U Test. The reason for using a nonparametric test is due to the ordinal data used in the rankings of the students' perceptions of ethical severity. Results of the gender Mann-Whitney U Test analysis are presented in Table 3. We found that significant gender differences exist only for eLSA3 ($p<0.005$). Overall across all five items (eLSA1- eLSA5), the results indicated that in regards to perceived ethical severity of e-learning security attacks males find these attacks less severe than females.

Table 3. Gender Analysis using Mann-Whitney U Test (N=519)

e-Learning Security Attack	Males (n=251)		Female (n=268)		Noparametric (Mann-Whitney U Test)	
	M	SD	M	SD	Z	Sig. (2-t)
eLSA1	4.51	0.83	4.46	0.82	-1.050	0.294
eLSA2	4.66	0.67	4.62	0.66	-1.064	0.287
eLSA3	4.15	1.03	4.44	0.78	***-2.986*** **	***0.003***
eLSA4	4.36	0.86	4.51	0.75	-1.947	0.052
eLSA5	4.59	0.72	4.62	0.66	-0.449	0.653

** - p< 0.05*

*** - p< 0.01*

In order to test for differences between undergraduate and graduate students on their perceived ethical severity of e-learning security attacks, we also conducted similar test using Mann-Whitney U Test based on academic rank (undergraduate and graduate). Table 4 depicts the results of the academic rank analysis. We found a significant age level differences exist only for eLSA1 ($p<0.001$). Overall across all five items (eLSA1- eLSA5), the results indicated that graduate students appear to report these e-learning security attacks slightly higher than undergraduate students.

Table 4. Academic Rank (Undergraduate/Graduate) Analysis using Mann-Whitney U Test (N=519)

e-Learning Security Attack	Undergraduate (n=261)		Graduate (n=258)		Noparametric (Mann-Whitney U Test)	
	M	SD	M	SD	Z	Sig. (2-t)
eLSA1	4.36	0.91	4.62	0.71	***-3.504*** **	***0.000***
eLSA2	4.62	0.65	4.66	0.68	-1.066	0.286
eLSA3	4.23	0.97	4.37	0.87	-1.515	0.130
eLSA4	4.38	0.84	4.49	0.77	-1.482	0.138
eLSA5	4.55	0.74	4.66	0.62	-1.730	0.084

** - p< 0.05*

*** - p< 0.01*

In an attempt to test for differences between students' age groups on their perceived ethical severity of e-learning security attacks, we conducted another non-parametric test using Kruskal-Wallis H Test of multiple groups based on age groups. The results of the age-group analysis are presented in Table 5. We found that there were significant age level differences for all items with eLSA1, eLSA3, eLSA5 ($p<0.001$), eLSA2 ($p<0.01$), and eLSA5 ($p=0.01$). Overall across all five items (eLSA1- eLSA5), the results indicated in regards to perceived ethical severity of e-learning security attacks, there is an increase trend where the older the student is, the more severe s/he ranks the attacks.

Table 5. Age Analysis using Kruskal-Wallis H. Test (N=519)

e-Learning Security Attack	Noparametric (Mann-Whitney U Test)	
	Z	Sig. (2-t)
eLSA1	***33.037*** **	***0.000***
eLSA2	***20.353*** **	***0.009***
eLSA3	***30.261*** **	***0.000***
eLSA4	***25.569*** **	***0.001***
eLSA5	***29.751*** **	***0.000***

** - p< 0.05*

*** - p< 0.01*

Conclusions and Discussion

The main goal of this study was to conduct an investigation about students' perceptions of ethical severity related to five common information security attacks in the context of e-learning. The focus of our work was about testing for differences over the five e-learning security attacks based on gender, age, and academic rank (undergraduate/graduate). This research included a sample of 519 students attending e-learning courses in the U.S. Results of our investigation revealed that majority of the students appear to self-report their perceptions as ethically driven across all the five e-learning security attacks. Moreover, we found from our results that majority of the students appear to understand the severity of these e-learning security attacks. However, we were somewhat alarmed to find that, although a small percentage, indeed some students reported these security attacks to be ethical. Specifically, we found that file sharing during e-learning sessions is less technically challenging then other security attacks such as spoofing, thus students appears to perceive such attack more acceptable. Our results indicated that overall males find these security attacks less severe than females. We found that males are more risk takers, while females tend to be risk averse than males. We also found that overall undergraduate students appear to perceive these attacks only slightly less severe than graduate students, however, these are not directly correlating to age distribution as some of the undergraduate students in this study were adult learners that are a bit older. As such, we also conducted an analysis based on age. Our results indicated that in terms of age, there is an increase trend where the older the student is, the more severe s/he ranks the attacks. These results indicate that younger students, in particular young male students, appear to find the e-learning security attacks significantly less ethically severe or not severe at all. These results are alarming especially as younger students entering technical educational programs (information technology, computer engineering, computer science, information security, etc) where they also learn how to conduct some of these exact security attacks. Future research may attempt to investigate students' engagements in these e-learning security attacks. An interesting comparison may result between assessing the results of our study here and the results of such

potential study to see if there are any discrepancies between the students' perceived ethical severity and the relationship to their actual engagement in unethical behavior such as initiating security attacks on an e-learning system. Also, future research may wish to investigate these results with different majors, specifically in subject areas such as computer science, computer and/or electrical engineering, information systems/technology, and information security to uncover if there are any differences among these students and non technical majors.

References

Cronan, T. P., Foltz, C. B., & Jones, T. W. (2006). Piracy, IS misuse at the university. *Communication of the ACM, 49*(6), 85-90.

Dorantes, C. A., Hewitt, B., & Goles, T. (2006). Ethical decision-making in an IT context: The roles of personal moral philosophies and moral intensity. *Proceeding of the Hawaii International Conference on System Sciences,* Big Island, HI, pp. 1-10.

Geri, N. & Gefen, D. (2007). Is there a value paradox of e-learning in MBA programs? *Issues in Informing Science and Information Technology, 4*, 163-174.

Geva, A. (2006). Three models of corporate social responsibility: Interrelationships between theory, research, and practice. *Business and Society Review, 113*(1), 1–41.

Harris, J. (2004). Maintaining ethical standards for a computer security curriculum. *Proceeding of the Proceedings of the 1st annual conference on Information security curriculum development,* Kennesaw, Georgia, pp. 46-48.

Johnson, A. R. (2009). Distance learning in higher education. *Review of higher education, 32*, 542-545.

Kreie, J. & Cronan, T. P. (1998). How men and women view ethics. *Association for Computing Machinery. Communications of the ACM, 41*(9), 70-78.

Kritzinger, E. (2006). Information security in an e-learning environment. In T. D. Kumar (Ed.), *International federation for information processing, education for the 21st centiuy - impact of ict and digital resources* (Vol. 210, pp. 345-349). Boston: Springer.

Lawson, R. A. (2004). Is classroom cheating related to business students' propensity to cheat in the real world. *Journal of Business Ethics, 49*(2), 189-199.

Levy, Y. & Ramim, M. M. (2009). Initial development of a learners' ratified acceptance of multibiometrics intentions model (RAMIM). *Interdisciplinary Journal of E-Learning and Learning Objects, 5*, 379-397.

Means, B. Toyama, Y., Murphy, R., Bakia, M., & Jones, K. (2009). Evaluation of evidence-based practices in online learning: A meta-analysis and review of online learning studies., from www.ed.gov/rschstat/eval/tech/evidence-based-practices/finalrepott.pdf

Molnar, K. K. Kletke, M. G., & Chongwatpol, J. (2008). Ethics vs. IT ethics: Do undergraduate students perceive a difference? *Journal of Business Ethics, 83*, 657-671.

Nguyen, N. T. & Biderman, M. D. (2008). Studying ethical judgments and behavioral intentions using structural equations: Evidence from the multidimensional ethics scale. *Journal of Business Ethics, 83*(627–640).

Obama calls for cyber czar. (2009). *Information Management Journal, 43*(5), 16.

Ramim, M. M. (2007). An examination of factors associated with students' ethical decision making in post-secondary e-learning programs. *Dissertation Abstracts International, 68*(12), 1-123. (UMI No. AAT 3290937).

Ramim, M. & Levy, Y. (2006). Securing e-learning systems: A case of insider cyber attacks and novice IT management in a small university. *Journal of Cases on Information Technology, 8*(4), 24-34.

Rogers, C. F. (2006). Faculty perceptions about e-cheating during online testing. *Journal of Computing Sciences in Colleges, 22*(2), 206-212.

Show, W. H. (2008). *Business ethics* (6th ed.). Belmont: Thompson-Wadsworth.

U.S. Department of education. (2009). *National Center for Education Statistics (NCES): Distance education at degree-granting postsecondary institutions*.