https://doi.org/10.48009/1_iis_2009_191-197

THE IMPACT OF COMPUTER AND INTERNET SECURITY TRAINING FOR UNDERGRADUATE STUDENTS: ATTITUDINAL CHANGES

Queen E. Booker, Minnesota State University, Mankato, queen.booker@mnsu.edu
Carl Rebman, University of San Diego, carlr@sandiego.edu
Fred L. Kitchens, Ball State University, fkitchens@bsu.edu

ABSTRACT

This study compares changes in attitudes of students towards organizational security policies and procedures at various institutions that have implemented information security policy training as part of the orientation and on-going training for students. The results indicate that those institutions that provide multiple venues to discuss security policies and procedures during the student careers have greater improvements in attitudes than institutions with orientation only training for the general student body.

Keywords: Education, Security and Education, Security Literacy

INTRODUCTION AND THEORETICAL FOUNDATIONS

Security, as defined by websters.com, is "the state of being free from danger or injury." Managers of the modern organization, thanks to the growth of Internet based technologies and the growth in workplace violence, find themselves constantly focusing on security measures to increase the safety of workers and data alike. They do so through the declaration of policies and the implementation of security devices such as monitoring systems. The literature suggests that barriers to acceptance of security devices can be grouped into the following categories: organizational commitment, physical invasiveness, information invasiveness, ease of use, privacy, and the perceived level of benefit from the device [1, 2,].

Security policies and technologies, and the people who manage them, have received increased accountability for the security of data regardless if employees actually follow or use organizational security tools. Unfortunately, security policies and technologies often conflicts with personal privacy and perceived risk concerns. Privacy advocates claim security often invades individual's privacy by providing means to capture and monitory information on individuals. Yet, with the need for greater accountability for movements and actions across information systems, organizations employ a variety of technologies to support organizational policies including but not limited to biometric devices, badge systems, password systems, video surveillance, email monitoring, computer usage monitoring, and Internet usage monitoring. Password systems, computer monitoring, email monitoring, Internet usage monitoring and video surveillance are tools with which most are familiar. Biometric devices and active badge systems are less common but are being implemented at a fairly rapid speed.

Organizations implement policies and technologies designed to protect employee, the digital assets as well as the customer. Employees are unable to choose whether they want to use or have the technology used for their benefit. For example, many organizations force users to use passwords to access confidential systems and to change their passwords at least annually, and in doing so ask for a password of a certain length as well as have a combination of letters and numbers. Organizations use tools to monitor email traffic, email content, Internet traffic and Internet behavior. They may also use video surveillance equipment active badges, and digitally coded access keys that track an employee's movement or attempted movement into certain parts of the organization's campus.

Researchers have found that some employees dislike policies and distrust monitoring systems, and some even actively thwart their organization's use of these systems by altering monitoring equipment/software or by avoiding monitored areas [1,3, 4, 5, 6]). Others simply do not comply with company policies or they may unintentionally find themselves creating an opportunity to expose the organizational systems through visiting a bogus website that captures passwords and other personal information, responding to an email that looks as if it is from a trusted source, or simply clicking on a pop-up that turns out to be a worm.

Another serious problem can arise when employees succeed in circumventing systems, then the security technology and policies provide little of its intended value. The effectiveness of organizational monitoring techniques, and policies, then, depends on employees' willingness to comply with their use. Insights into employees' intentions to comply with policies or circumvent monitoring tools

are helpful in promoting effective use of these technologies.

Studies have been conducted that examined employee compliance or resistance to such monitoring systems. Two recent studies that focus primarily on security related concerns include the study by James et al [2] that investigated the intention to use biometric devices and the study by Spitzmuller and Stanton [1] that investigated the intention to thwart monitoring systems related to email. However, these studies focused more on user acceptance and did not consider risk. The objective of this study is to examine and compare attitudinal antecedents of compliance and resistance with organizationally-imposed policies and monitoring systems given perceived risk. The ability to predict employees' compliance and resistance behaviors can help managers devise programs and techniques to minimize the behaviors on the security of the company's information assets. The study utilizes a Likert-type scale survey designed to study the user behavior toward security policies and technologies, the intention to use these devices, and the perception of risk to the user, providing insight into possible barriers to adoption of general security technologies. And, a study by Booker and Kitchens [7] that investigated user policy acceptance based on perceived risk showed that intentions to comply decreased when people perceived the use to bring harm such as a threat to their personal safety. All of these studies investigated intentions and found that most people attitudes toward security policies and procedures are to follow them.

The common theme in all of these studies is to understand what motivates people to comply with security systems helps to improve their willingness to comply. Part of that understanding comes from education, training and experience. While most information technology research focuses on building software that prohibits actions from occurring there are others such as hackers and other people intent on using ignorance for their purposes spending their time finding holes and ways around said software applications. As such it is imperative that educators understand how much training would minimize the "experiences" that lead to vulnerabilities in systems that would also help improve compliance. This understanding of how education and training affects and improves the attitudes for compliance can be quite useful, moving beyond simply knowing a person's intent.

This paper compares and contrasts the changes in attitudes of students towards university organizational security policies and procedures at various institutions that have implemented formal or information security policy training as part of the orientation and on-going training for students over their academic careers. The contribution of this paper is to ascertain the level and intensity of security training for non-computer science/information technology students necessary to improve their understanding and attitudes toward security and reduce the risk of successful intrusion through user non compliance with policies and procedures or unintentional mistakes. Further, it is the expectation that students leaving the college or university setting with a more positive attitude towards security policies and procedures would be better employees, eventually reducing the number of unintentional mistakes that might leave a corporate system vulnerable to outside attacks or that might open the individual to identity theft.

The research was conducted in the 2004-2008 academic years through surveys at six public regional colleges and universities with a freshman class of no more than 2000. Two of the institutions had no form of information systems security training for new students. Four of the selected universities provided a minimum of security training as part of the new student orientation. For comparison, two of the institutions had on-going communications via the university's website, newspaper, or other campaigns about protecting computers and digital information while 2 others had no intentional ongoing campaigns. Two surveys were conducted each academic year: one survey was taken for students at the beginning of the academic year and a second one towards the end of the academic year. But for the purpose of this paper, only the 2004-2005 freshmen and 2007-2008 senior survey results are analyzed. Data on transfer students were not used.

THE STUDY

To examine student attitudes toward organizational policies and procedures, and the intent to abide by those policies and procedures, institutions used a survey with fifteen questions not including demographic data. Each institution used a paper survey for the freshman survey and an online survey for the senior year. The answers were measured using a 5-point Likert scale ranging from "strongly disagree" to "strongly agree" for all questions except if students felt the university was a caring or a rules organization. "Strongly caring" was at one extreme of the scale and "strong rules based" on the other with neutral as the middle choice.

The purpose of the study was to determine if the various levels of information security training and campaigns made a difference on student attitudes towards organizational policies and procedures for systems protection at the respective colleges and universities. The expectation was on average, students at the beginning of their academic careers would have neutral attitudes towards information systems policies and procedures as

well as their intent to comply. The expectation was that at the end of their academic careers, those institutions with some form of training would experience positive improvements in attitudes and intentions, and the more frequent the communications about security, the more positive the improvements.

DATA ANALYSIS AND RESULTS

The questions for the study were developed according to the strategy described by Ajzen and Fishbein [8]. Item content was derived previous studies on technology adoption and acceptance based on research from Stanton and Weiss [6,9], Bennett & Robinson [10], Hope & Pate [11], and Hodson [12]. These sources provided input regarding which items were important regarding intentions. After developing a list of forty questions for the survey, an exploratory study was conducted with a group of 100 students to identify those questions that matter most to them. The result was the 15 question survey that simply asked students their intent to comply with or avoid certain security policies and procedures. The survey included 6 questions that were specific to information technology and security and 3 that were more general in nature.

There were six institutions involved in the study. The number of freshmen and senior surveys completed and were usable for each institution is shown in Table 1: Institutional Data.

Table 1. Institutional Data

Class	1	2	3	4	5	6
Freshman	1119	1204	1196	1240	1120	1006
Senior	763	756	812	739	719	632

The first analysis performed investigated the mean attitude of freshmen for each institution. As suspected, the average attitude for the freshman class for each institution was fairly neutral. The results for each institution are shown in Table 2.

Table 2. Means and Standard Deviations for Freshmen at all Institutions

	Institution 1		Institution 2		Institution 3		Institution 4		Institution 5		Institution 6	
	Mean	Std. Dev.	Mean	Std. Dev.	Mean	Std. Dev.	Mean	Std. Dev.	Mean	Std. Dev.	Mean	Std. Dev.
Intent to comply with password use policies	3.03	1.39	3.01	1.41	3.00	1.41	2.96	1.42	3.01	1.42	2.95	1.39
Intent to comply with email use policies	2.98	1.44	3.01	1.43	2.98	1.42	3.03	1.41	2.95	1.40	2.94	1.44
Intent to comply with Internet use policies	3.06	1.45	2.95	1.43	3.01	1.40	2.99	1.42	2.98	1.41	3.03	1.41
Comfort with public policies on security	2.95	1.42	3.06	1.42	3.04	1.39	2.94	1.41	2.95	1.39	2.96	1.40
Attitude towards organizational security policies	3.12	1.38	2.99	1.42	2.93	1.40	3.07	1.40	2.93	1.39	3.07	1.39
Attitude towards security technologies	3.06	1.41	2.97	1.41	3.01	1.43	3.03	1.42	2.96	1.40	3.03	1.28
Accept Organizational Policies	3.02	1.43	2.99	1.42	2.96	1.40	2.94	1.41	2.94	1.41	3.06	1.40
Accept Organizational Technologies	3.00	1.42	2.99	1.41	2.94	1.42	3.05	1.39	3.00	1.42	3.00	1.41
Rules Culture	3.03	1.82	3.00	1.81	2.98	1.82	2.97	1.81	3.03	1.81	3.00	1.82

Institutions 1 and 2 discussed security including information systems security during orientation. Institutions 3 and 4 discussed security during orientation and continued on-going campaigns. For example, institution 3 had a website that was updated regularly with potential threats that also allowed students to post threats they found or heard of through their social networks. Institution 4 had a "campus tech" section in the campus paper where they discussed various computer issues particularly how to recognize when something was amiss. For example, one student went to what he thought was a Microsoft data warehouse site. The site downloaded a keylogger to his computer and rebooted it. Once the computer was rebooted, a message popped up saying *"Windows has detected a malicious spyware. Please click here to pervent damage to your computer."* The campus tech article used the example as an opportunity to teach students to look for typos in pop-ups and emails, stating that the typos are a general indication that the email or the popup was not from a reliable source. Institutions 5 and 6 were the control group and thus had no specific information security training for students beyond what is covered in the introduction to MIS course unless the student was a computer science or management information systems major.

Students completing the survey at each institution used the entire Likert Scale (e.g., 1 through 5). The results for each question centered around 3 which are essentially neutral attitudes. This was true for the three policies in question – email, passwords, and Internet use. The standard deviations also were fairly evenly distributed across the campuses ranging from 1.39 to 3.07. A breakdown of students by intended major, gender, or ethnicity or age showed that there were no significant differences across intended majors, gender, ethnicity or age.

The next analysis was to analyze the senior class attitudes. There were fewer usable senior surveys collected. Part of the reason for this may have been the lack of structured environment to discuss the importance of the surveys as was used for the freshmen. Another reason may be that the seniors were involved with internships or other senior activities that would have taken them off campus. For this reason, the results of the post senior analysis may have some bias but since the survey results are a larger sample size than needed for significant results, no attempt was made to increase the number of usable surveys. The results for the seniors are shown in Table 3.

Table 3. Means and Standard Deviations for Seniors at all Institutions

	Institution 1		Institution 2		Institution 3		Institution 4		Institution 5		Institution 6	
	Mean	Std. Dev.	Mean	Std. Dev.	Mean	Std. Dev.	Mean	Std. Dev.	Mean	Std. Dev.	Mean	Std. Dev.
Intent to comply with password use policies	3.57	1.29	3.59	1.26	3.97	1.28	4.02	1.28	3.09	1.32	2.98	1.29
Intent to comply with email use policies	3.65	1.24	3.66	1.26	3.98	1.31	4.11	1.31	3.15	1.30	3.04	1.42
Intent to comply with Internet use policies	3.61	1.28	3.56	1.27	3.95	1.25	4.15	1.30	3.08	1.28	3.07	1.42
Comfort with public policies on security	3.62	1.28	3.56	1.28	3.96	1.26	3.90	1.27	3.05	1.41	3.06	1.40
Attitude towards organizational security policies	3.54	1.32	3.58	1.28	3.95	1.22	4.12	1.26	3.03	1.32	3.07	1.33
Attitude towards security technologies	3.63	1.25	3.65	1.30	3.91	1.31	4.22	1.25	3.03	1.40	3.03	1.28
Accept Organizational Policies	3.52	1.29	3.67	1.21	3.92	1.28	4.11	1.29	3.02	1.31	3.06	1.41
Accept	3.58	1.28	3.58	1.25	3.96	1.30	4.11	1.25	3.01	1.28	3.05	1.41

Organizational Technologies												
Rules Culture	3.06	1.43	3.02	1.39	3.04	1.44	3.02	1.40	3.03	1.81	3.08	1.28

As shown in the Table 3, institutions 3 and 4 showed the greatest improvement in moving student attitudes towards a more positive view of information security policies. None of the attempts changed student attitudes towards the university towards a more caring or more rules based culture.

Further, a chi square test for each institution was performed to compare the before and after analyses and found that all the institutions' improvements except institutions 5 and 6 were significant between the freshmen year and the senior year for attitudes.

When comparing the improvements between groups for the senior year data, institutions 1 and 2 showed no significant difference at or below .05 between their outcomes but institutions 1 and 3, 1 and 4, 2 and 3, 2 and 4, and 3 and 4 all showed significant differences between their outcomes indicating the on-going campaigns can improve student attitudes better than just an orientation.

As shown in Table 3, even institutions 5 and 6 showed minor improvements of attitudes which suggested a deeper analysis to understand further underlying factors. For that purpose the data was subdivided for each institution. Analyses by gender, ethnicity, and major were conducted.

The study showed that overall, freshman males had more negative attitudes towards compliance whereas freshman females and transgendered students were slightly more geared towards positive attitudes even without the training. The senior males made some improvements with a chi-square significance .047 for compliance with Internet, .049 for compliance with email and .051 for passwords. Females however showed a more significant improvement with chi square significances of .03, .00, and .02 for compliance with Internet, email, and passwords respectively. Transgendered students, though, showed significant improvements at .00 for the three.

When comparing ethnicities, freshman whites were more neutral than non minorities on compliance attitudes. But the senior results are a bit more interesting. While the white seniors showed some movement towards compliance, the non white students showed significantly higher movements. This could be partially explained by a number of factors including the number of whites that had more than 1 year of computer experience prior to enrolling in college (78%) as opposed to the number of non whites with the same level of experience (43%). The lack of knowledge of the technologies could have biased answers on the initial survey as many of the non whites did not have prior experiences with the use of passwords, email or the Internet.

The last comparison was for major. The analysis for this paper was between business and non business majors, and technology and non technology majors. Technology majors were eliminated from the study on business and non business majors. On the business and non business majors, at institutions 5 and 6, business students had improvements from freshman to senior year where as non business students did not. The business majors could explain part of the slight improvements enjoyed by those two institutions. For the technology and non technology comparisons, technology students entered the institutions with a significantly higher intent to comply than non technology majors. The senior data showed they maintained that level of intent and did not show any major increase or decrease.

Because of the significant improvements at institutions 3 and 4, further analysis into the campaigns at those institutions were analyzed for possible best practices. Institution 4 shared several practices that are worth sharing. For example, phishing emails were quite common so the institution ran several articles on some of the more common phishing scams, sent emails regarding what to look for in scam emails, and ran an article about how websites use your email address. They ran a story about how a faculty member visited a popular higher education journal website, posted a comment and then received an email that his comment had been deleted. The site was hacked and comment email addresses were used to direct users to a porn site when the link inside the email was clicked. Again, the email contained typographical errors. The technology team at institution 4 also provided a sample of an information technology quiz they give students as part of the orientation and at the end of their academic careers.

The quiz contains examples similar to those shown in Figures 1 – 4. Figures 1 – 3 are used to ask students if the message or email is valid or invalid. Figure 4 is an example asking students whether or not it is appropriate to open the emails shown in the Figure 4 while using the university's computer systems. These tests are used to help students, particularly freshmen who have never used computers or computers with some key important messages what is valid and what is not valid and what to do should they encounter these messages.

Figure 1. Quiz Example 1

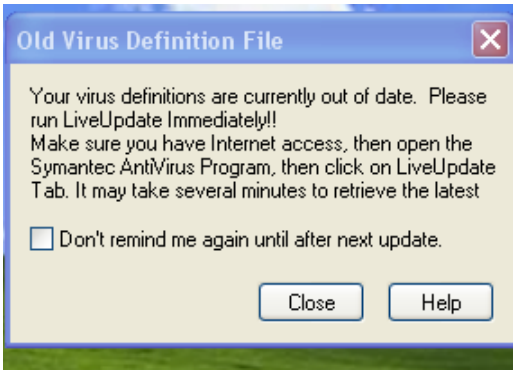
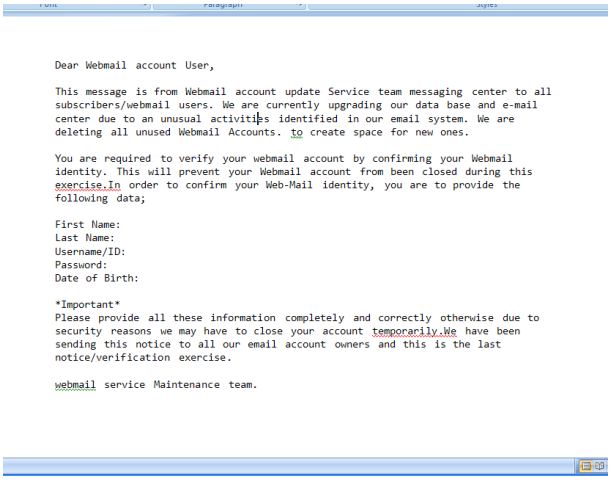


Figure 2. Quiz Example 2



Dear Webmail account User,

This message is from Webmail account update Service team messaging center to all subscribers/webmail users. We are currently upgrading our data base and e-mail center due to an unusual activities identified in our email system. We are deleting all unused Webmail Accounts. to create space for new ones.

You are required to verify your webmail account by confirming your Webmail identity. This will prevent your Webmail account from been closed during this exercise.In order to confirm your Web-Mail identity, you are to provide the following data;

First Name:
Last Name:
Username/ID:
Password:
Date of Birth:

Important
Please provide all these information completely and correctly otherwise due to security reasons we may have to close your account temporarily.We have been sending this notice to all our email account owners and this is the last notice/verification exercise.

webmail service Maintenance team.

Figure 3. Quiz Example 3

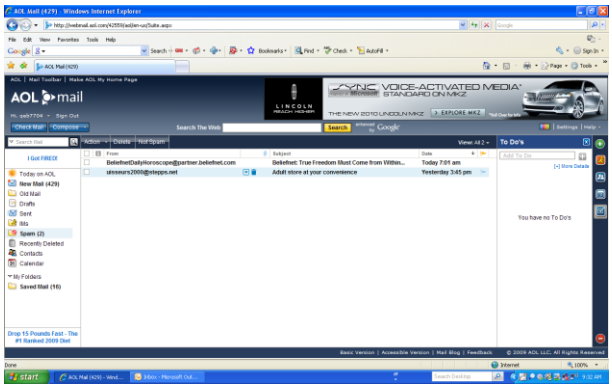


Figure 4. Quiz Example 4

CONCLUSIONS

This study provided some evidence that providing on-going communications with students help to improve their attitudes toward information systems security. The reason the study began with freshmen is that for many freshmen this is their first time actually operating in an organizational networked environment, not just the one in their family home and one that could affect many thousands of individuals instead of two or three. The concept of organizational implications is new to them. Often the younger members of society are attributed to their computer savvy but that savvy has more to do with their personal use than the use in a business environment. Training students early in their careers about how to avoid potentially disastrous activities could save corporations millions in information security risk management in the future while also reducing potential problems on campus. This study is just a beginning and much more work needs to be done to fully understand the role higher education needs to play to improve or mitigate behaviors that can place digital assets at risk. For example one question that should be addressed is what are the overall best practices and can these become part of the training for all higher education institutions? How long is a particular threat relevant? Does it matter what major a student undertakes in shaping their attitude? How does similar training work for the corporation? Are the changes in attitude gradual? Does it matter if the student is a transfer? What is the impact of age on these trainings, campaigns and attitudinal change? Future studies will be necessary to begin to determine just what impact higher education has and can have on improving attitudes and compliance with information systems security.

REFERENCES

1. Spitzmuller, C. & Stanton J. M. (2006). Examining employee compliance with organizational

surveillance and monitoring, Journal of Occupational and Organizational Psychology, 79, 245–272

2. James, T., Pirim, T., Boswell, K., Reithel, B., & Barkhi, R. (2006) Determining the Intention to Use Biometric Devices: An Application and Extension of the Technology Acceptance Model. Journal of Organizational and End User Computing. Hershey: Jul-Sep 2006. 18 (3) 3, 1-24
3. Nussbaum, K., & du Rivage, V. (1986). Computer monitoring: Mismanagement by remote control. Business and Society Review, 56, 16–20.
4. Stanton, J. M. (2000). Reactions to employee performance monitoring: Framework, review, and research directions. Human Performance, 13, 85–113.
5. Stanton, J. M. (2002). Information technology and privacy: A boundary management perspective. In S. Clarke, E. Coakes, G. Hunter, & A. Wenn (Eds.), Socio-technical and human cognition elements of information systems (pp. 79–103). London: Idea Group.
6. Stanton, J. M., & Weiss, E. M. (2000). Electronic monitoring in their own words: An exploratory study of employees' experiences with new types of surveillance. Computers in Human Behavior, 16, 423–440.
7. Booker, Q. E, & Kitchens, F. L. (2007) Predicting Employee Intention to Comply with Organizational Security Policies and Procedures Factoring Risk Perception, Proceedings of the 2007 Security Conference, Las Vegas.
8. Ajzen, I., & Fishbein, M. (1980). Understanding attitudes and predicting social behavior. Englewood Cliffs: Prentice-Hall.
9. Stanton, J. M., & Weiss, E. M. (2003). Organisational databases of personnel information: Contrasting the concerns of human resource managers and employees. Behaviour and Information Technology, 22(5), 291–304.
10. Bennett, R. J., & Robinson, S. L. (2000). Development of a measure of workplace deviance.
11. Hope, J.W., & Pate, L. E. (1988). A cognitive-expectancy analysis of compliance decisions. Human Relations, 41, 739–751.
12. Hodson, R. (1991). The active worker: Compliance and autonomy at the workplace. Journal of Contemporary Ethnography, 20, 47–78.