INFORMATION TECHNOLOGY SECURITY AWARENESS IN ACADEMIA: AN INITIAL ASSESSMENT

Miguel Perez & Ronald Berry, Department of Computer Information Systems
Christine T. Hollman, Department of Economics and Finance
University of Louisiana at Monroe
700 University Avenue, Monroe LA 71209
perez@ulm.edu, rberry@ulm.edu, hollman@ulm.edu

ABSTRACT

After recent events, many organizations are enhancing their efforts to improve information technology security awareness. Security awareness involves simple issues such as maintaining confidential passwords, logging off computer systems, and data backup. It also involves complex issues such as having strong passwords, encryption, and maintaining virus protection. The National Security Agency identifies three levels for information assurance: 1) Awareness, training, and education; 2) policy and practices; and 3) technology (3). The purpose of this study is to identify the current awareness level of security issues in an academic environment. Results should provide direction and guidance for development of a security awareness program for what is commonly known to be one of the least secure environments.

Keywords: Information Systems Security, Risk, Security Awareness, Academic Perceptions

INTRODUCTION AND PURPOSE OF STUDY

Risk exists in almost everything humans do, but it is especially prevalent in new endeavors such as the use of modern technologies. In recent years, the concern that businesses are either not aware of the technology risks they face or are not properly prepared to handle technology risks has been expressed throughout business literature (2) (8). Phrases like "network security", "cyber-threats", "cyber-terrorism", and "e-risks" are commonly associated with words like "unknown", "misunderstood" and "unexplored" (4)(6).

Most business professionals agree that risk management should be an important component of any organization's operations. But when an organization is embracing a new exposure with so many inherent and misunderstood risks, risk management becomes critical. Risk management is the process of identifying and analyzing risks and selecting appropriate methods to treat those risks. The goal of risk management is to enable an organization to meet its overall goals without being hindered by deviations from expectations or by uncertainty. Once risks have been identified and analyzed in terms of probabilities and severities, an appropriate treatment method should be selected among retention, transfer, control and avoidance.

To simplify this discussion, we will assume that each treatment method is mutually exclusive. If retention is chosen as the risk treatment method, funds are either set aside to pay for future losses or no additional action is taken. This would generally not be a viable choice for technology risks as the probable severity of loss is unknown. Risk transfer is a second possibility. Typically this

means transferring the risk of financial loss to another entity, e.g., an insurance company. While this method may have some value, it is highly limited for several reasons. A standard property or liability insurance policy does not cover most technology risks (e.g., network security liability, business interruption, information asset coverage). Even if the organization has sought out the unique coverages that protect against these risks, insurers are generally not willing to provide the coverage to high-risk exposures. Still yet, many technology risks are difficult to measure (e.g., loss in reputation, lost productivity) and are therefore difficult to insure. Finally, risk avoidance is an unrealistic solution, as it would require an organization to abandon the technology exposing them to risk. In most cases, the organization would cease to be competitive if they chose avoidance as the risk treatment method.

The most promising risk treatment option for technology risks is risk control. But it is not without complications. As is often true of implementing risk control, controlling technology risks is really a two-part process. Once risks have been identified and analyzed and risk control mechanisms have been put into place, technology managers and users must play their part in managing the risk. For the process to be successful, all involved individuals must: 1) be aware that the risk exists; 2) be aware of the tools available to manage the risk; 3) be comfortable using the tools; and 4) actually put the risk control tools into practice. In an initial assessment of the current level of awareness of security issues, Smith (7) suggests that people are the weakest link. Even if the tools are available, employees of the organization and other users (clients, consultants, etc.) do not meet the criteria listed above, the risk management process will fail.

The association between risk management and information technology security is clearly mentioned by the Computer Security Institute (5). The Institute concludes that the goal of information protection risk management is not to secure all processes one hundred percent, but to create a secure enough environment so that information can be transferred in a safe manner, thereby allowing decision makers to meet their responsibilities.

The FBI and the Computer Science Institute have indicated a need for increased security awareness levels among firms with emphasis placed on statistics illustrating financial losses suffered by firms. Our focus is on academic environments, which has been overlooked by past research. Even though firms could quantify more easily the loss of data caused by security breaches, academic environments should also pay close attention to security issues because of the intellectual value of data held by universities and also because of the amount of physical equipment made available to students and faculty/staff.

While technology risk management by itself poses unique challenges, it is particularly difficult in a setting where upper management has very little control of technology users. A University setting is an excellent example of such an environment, where users of technology include students, who experience few if any direct consequences if technology security fails, and faculty who experience little punitive action for failure to follow policies or financial gain for putting those policies into practice. Our study focuses on the problems associated with managing technology security risk in an academic setting.

Security awareness programs are part of many organizations training programs. For our study, we define security awareness as both a familiarity level about security issues and the level of

comfort dealing with potential security issues. While it is important that users be familiar with security measures, it is also important that they feel comfortable implementing measures to address the risks. Familiarity alone will not mitigate the risks associated with technology security issues.

SURVEY METHODOLOGY

Sample Selection

Faculty, staff and students at a southern regional university participated in this study. The survey was distributed to a wide variety of classes and faculty and staff across campus. Because of their interest in the survey and the results, the University computing center assisted in questionnaire development and distribution. A total of 220 questionnaires were distributed. Of those, 208 were usable.

Survey Instrument

The research instrument consisted of five sections. The questionnaire included sections to measure respondents' risk tolerance, their awareness of security issues, their ability or comfort level with completing tasks related to security and their use of security measures. All of these should provide an overall view of security awareness. A similar methodology was used to study awareness and comfort level with Internet-related technologies and tasks (1).

Section one asked respondents to indicate their risk tolerance with their personal finances, their hobbies, their driving, and finally with technology. For example, respondents were asked "I take risks with my personal finances." The scale used for these four questions was "never", "rarely", "sometimes", "often", and "always."

Section two of the questionnaire was used to identify the respondents' familiarity with certain security-related tasks and measures. Semantic differential scaling was used with "unfamiliar" and "very familiar" as the anchors. For example, respondents were asked to indicate their familiarity level with antivirus software, encryption, firewalls, and smart cards. For each statement, respondents chose a number between 1 and 5, with 1 being near "unfamiliar" and 5 being near "very familiar". A complete list of items can be found in Table 2.

Section three of the questionnaire asked respondents how comfortable they felt completing certain security-related tasks. A similar semantic differential scale was used with "uncomfortable" and "very comfortable" as the anchors. Sample statements from this section included changing your password, updating your antivirus software, encrypting your files, and sharing files. A complete list of statements can be found in Table 3.

Section four of the questionnaire focused on passwords and attempted to determine if the respondents use strong passwords. All questions could be answered with a "yes", "no" or "unsure" response. Sample questions include "my password has at least 7 characters", "my password has a mix of lower and upper case letters", "my password is written down" and "I usually change my password on a monthly basis." All of the statements can be found in Table 4.

Finally, demographic questions were included in section six. Respondents were asked whether they were a student, faculty member, or staff member. Students were asked their classification and major while faculty members were asked their primary field of study. All respondents were asked their age and gender.

Pretest

After careful review for content and face validity, the survey instrument was administered in a low-level class that we assumed would have a low awareness of security issues. These respondents provided several suggestions for improvements that led to rewording and removal of certain items from the questionnaire. Afterwards, the questionnaire was taken to professionals in the University computing center for further development. Additional changes were made because of the pretest process to help provide content validity. Data collected from respondents during the pretest was excluded from final analysis of the results.

SURVEY RESULTS

Two hundred and eight completed questionnaires were used for this project. Approximately 75% of the respondents were students and 25% were faculty and staff. Sixty percent were female and 40% male. A majority of the respondents (76%) were younger than 35 years old. Of the student respondents, 10% were freshmen, 22% sophomores, 26% juniors, and 35% seniors.

As shown in Table 1, neither group of respondents reported a very high level of risk tolerance. When comparing the two groups, it appears that students have a higher tolerance for risk when it comes to hobbies and driving. It is also interesting to note that faculty have a very low mean value for risks associated with technology.

Table 1
Perceptions of Risk

Statement	Students	Faculty	p-value
When new technology becomes available, I am one of the first to buy it.	2.29	1.89	.12
I take risks with my personal finances.	2.25	2.12	.66
I take risks in my hobbies.	2.78	2.20	.006
I take risks when I drive.	2.65	2.25	.02

Respondents had a high familiarity level with using passwords, as shown in Table 2. Additionally, respondents seemed to be fairly familiar with sharing files, setting file properties, antivirus software, data backup, and viruses. Respondents were not, however, very familiar with the more advanced security topics such as firewalls, encryption, and smart cards. When comparing faculty and students, there are statistical differences between the two groups for the items related to sharing files, setting file properties, and smart cards. In each case, students reported a higher familiarity level.

Table 2
Familiarity Level

Item	Mean Scores			
	All Respondents	Students	Faculty	p-value
Passwords	3.90	3.94	3.74	.28
Sharing files on your computer	3.36	3.54	2.76	.0005
Setting file properties/attributes	3.10	3.23	2.69	.01
Antivirus Software	3.08	3.10	3.02	.69
Data Backup	3.07	3.04	3.08	.87
Viruses	3.05	3.03	3.12	.69
Https/SSL	2.62	2.71	2.33	.06
Firewalls	2.35	2.39	2.26	.51
Encryption	2.12	2.21	1.86	.067
Smart Cards	1.89	2.00	1.55	.02

When asked about their comfort level, respondents seemed to be comfortable with changing passwords, downloading files, backing up data, updating antivirus software, and sharing files (Table 3). As with familiarity level, respondents seemed less aware of the more advanced security topics. For example, encrypting files, installing a personal firewall, providing personal information on the web, and opening attachments had low mean values. When comparing the results between faculty and students, differences were found with sharing files, allowing other people to use your computer, and installing a personal firewall. As with familiarity level, students seemed to have a higher level of comfort in these areas than faculty members.

Table 3
Comfort Level

Item	Mean Scores			
	All Respondents	Students	Faculty	p-value
Changing your password	3.94	3.94	3.96	.91
Downloading files	3.72	3.81	3.48	.07
Backing up your data	3.41	3.35	3.54	.43
Updating your antivirus software	3.25	3.23	3.30	.77
Sharing files	3.25	3.40	2.82	.003
Allowing other people to use your pc	2.92	3.08	2.50	.006
Using a credit card on the Internet	2.72	2.68	2.92	.28
Restoring a backup	2.64	2.65	2.60	.82
Removing viruses from your computer	2.55	2.57	2.52	.82
Opening Attachments in e-mails	2.48	3.47	3.56	.65
Providing personal information online	2.46	2.45	2.56	.59
Installing a personal firewall	2.25	2.37	1.90	.04
Encrypting your files	2.19	2.17	2.29	.58

To investigate the implementation of security measures, a set of questions related to passwords was included on the instrument. Analysis of the results indicated that most respondents do not have what are considered to be strong passwords. Only 11% use both lower and upper case letters while only 10% change their password on monthly basis. It was encouraging to find that only 10% of the respondents indicated that they have written down their passwords and that only

4% reported having a password that is the same as their username. Interestingly, only 12% of the respondents have a password on their screen saver and 34% indicated they leave their computer unattended while logged in.

Table 4
Passwords *

Item	YES	NO	UNSURE
My password has at least 7 characters.	65	30	5
My password has a mix of lower and upper case letters.	11	85	4
My password has at least one special character.	13	82	5
I have never changed my password.	25	73	2
I usually change my password on a monthly basis.	10	87	3
I usually change by password on a weekly basis.	2	94	4
My password contains alphanumeric characters.	49	49	2
My password is written down.	10	86	4
My password is part of my or a family member's name.	28	70	2
I often leave my computer unattended while logged in.	34	63	3
My screen saver has a password.	12	86	2
My password is the same as my username.	4	94	2
I have multiple accounts with the same password.	50	46	4

* Figures are percentages. Percentages may not equal 100% because of rounding or non-responses.

CONCLUSIONS AND IMPLICATIONS

This initial assessment of security awareness in academia provides a foundation upon which to develop a risk management program. The results also provide a benchmark for future studies and analysis regarding security issues. As noted by the National Security Agency, the three levels of information assurance include 1) awareness, training and education, 2) policy and practices, and 3) technology (3). Our study assesses the first component of this assurance plan. The results from the study unfortunately do not provide support that the respondents were very aware of security issues or very comfortable performing certain tasks related to technology security.

As stated earlier, for any risk control process to be successful, all individuals involved in the process must: 1) be aware that the risk exists; 2) be aware of the tools available to manage the risk; 3) be comfortable using the tools; and 4) actually put the risk control tools into practice. The results of this study indicate the potential for failure of security risk controls in an academic setting. It is encouraging that students and faculty are both familiar with and comfortable taking basic security measures. However, both students and faculty do not appear to be familiar with or comfortable practicing advanced security measures. Certainly in at least in one typical academic setting, technology security may be vulnerable.

These results give credence to specific and ongoing training of both students and faculty on the topic of technology security. But training by itself will only be as effective as the technology users' commitment to technology security. While training should improve awareness and

comfort with advanced security controls, it will not work if users do not actually practice security measures. Risk managers in academic settings should consider additional risk control tools such as "locking out" those who do not practice appropriate risk control measures or requiring the technique to be executed for the user to proceed with the technology. Additional risk controls are especially critical when users are less likely to practice risk control measures because of their high level of risk tolerance. There is some evidence from our study that, while students are more familiar with and comfortable practicing security measures than faculty, students have a higher level of risk tolerance. Further research should be done in this area to determine whether student's attitude towards risk influences their willingness to practice risk control procedures.

LIMITATIONS AND FUTURE RESEARCH

Since this study is an initial study, the reliability and validity of the research instrument cannot be assured. Additional research should be conducted using the same instrument to test for reliability and validity. Additionally, the results of this study may not be generalizable to academia since a random sample from academia was not used. A broader sample could be used in future studies to ensure generalizable results. The results presented in this paper do, however, provide a strong baseline from which to base future studies. Future research should also be conducted to determine if there are relationships between individual risk tolerance levels and information technology security risk tolerance. This study provides a starting point; however, additional scale development should provide reliable and valid measures for risk tolerance. Additionally, these findings should be compared to security awareness in businesses.

REFERENCES

1. Berry, Ronald L. and Mary C. Jones. (1998). The Internet: An Assessment of Student Perceptions, Journal of Information Systems Education, 9(1 & 2), 39-43.
2. Carr, Nicholas (2003). IT Doesn't Matter, Harvard Business Review, 81(5), 41-49.
3. Jacobs, Mike. (1999). Information Assurance in the 21st Century: A Critical Role for Academia, www.infosec.jmu.edu/ncisse/Conference99: 3rd National Colloquium for I.S. Security Education, May, 25-27.
4. MacSweeney, Greg (2001). Technology Risk still not Understood, Insurance and Technology, 26(7), 21.
5. Peltier, Thomas (1998). Information Protection Fundamentals, Computer Security Institute, accessed via web at www.gocsi.com/ip.htm, May, 2003.
6. Salierno, D. (2001). Managers Fail to Address E-Risk, The Internal Auditor, 58(2), 13.
7. Smith, Kenton (2001). Security Awareness: Help the Users Understand, SANS Infosec Reading Room, accessed via http://www.sans.org/rr/aware/help.php, April 15, 2003.
8. Veysey, Sarah (2001). Industry not Ready for E-risks: Study, Business Insurance, 35(6), 1,29.