Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2006 Proceedings

Americas Conference on Information Systems (AMCIS)

December 2006

Do Universities and Students Perceive the Necessity of Security Courses?

David Farrar
Southern Illinois University Edwardsville

Anne Powell
Southern Illinois University Edwardsville

Do Universities and Students Perceive the Necessity of Security Courses?

David Farrar
Southern Illinois University Edwardsville
dfarrar@siue.edu

Anne Powell
Southern Illinois University Edwardsville
apowell@siue.edu

ABSTRACT

As the world of technology continues to move forward, one is now able to accomplish more using a personal computer (PC) than ever before; unfortunately, security risks are also growing exponentially. With risks and use increasing, PC users must learn ways to keep data safe. This study examines whether IT departments are offering PC security classes, and whether students perceive a need for such classes. About half the departments examined have security topics covered within a course, but only a quarter offer security as a stand-alone course. While half of business school students think a PC security course is necessary, most would prefer asking a friend for information. Neither perceptions of severity of loss nor the probability of loss are related to intent to take a university course on PC security; however, belief that the individual can make a difference in keeping the Internet secure is related to course intent.

Keywords

Security, Education, Home computer user

INTRODUCTION

As the world of technology continues to move forward, one is now able to accomplish more using a personal computer (PC) than ever before. The Internet in particular has progressed exponentially in terms of its capabilities in the past several years. More and more Internet users are using the web for activities such as online shopping, bill paying, and banking. Today, 84.4% of Internet users shop online; 58% bank online, and 45.5% pay bills online (Zhang, 2005). Unfortunately, security risks such as viruses, spyware, and theft of information are also growing exponentially. Eighteen months ago it took, on average, 45 – 55 minutes before a PC was attacked by something. Today, it takes just four to five minutes (Consumer Reports, 2005).

Considerable effort is being taken by companies today to eliminate security threats to their computer systems. At the same time, these companies recognize that one of the biggest threats to their computer systems is the unintentional actions of their own employees (Keller et al., 2004). Unsafe security practices on home PCs can result in the loss of not only personal information, but also corporate data as more people conduct work at home. While researchers have proposed additional security training (Peltier, 2000; Tuesday, 2001), one study found most users felt comfortable in their own ability to protect themselves from security violations despite little or no formal training (Aytes and Connolly, 2004). This leads to our primary research question, "Can we determine what will motivate users to take educational courses on security issues?" A secondary research question is "Are security courses being offered to university students?"

RESEARCH MODEL AND HYPOTHESES

Need for Security Education

By 2003, 55% of Americans had access to the Internet, triple the number from 1997 (Day, Janus, and Davis, 2005). With growing access to the Internet, security threats also increase. Studies have shown that individuals do not have sufficient knowledge about security, privacy, and threats such as spyware and viruses (Zhang, 2005). Help for security violations is being provided by industry leaders such as AOL, Earthlink, and Microsoft by providing anti-virus and other protection before problems reach the individual. Many security fixes can now be automatically downloaded, and the latest versions of Windows will check PCs for security vulnerabilities (Consumer Reports, 2005). However, despite the best intentions of ISPs and software providers, additional precautions must be taken by individuals to keep their data secure. Because hardware solutions can only do so much, individuals must be educated on how best to keep their PCs secure. One step in doing this would seem to be determining if university courses on PC security are offered. Students represent a population who has used computers from a young age. Most college-age students are very comfortable using computers. Given their age, they may

not have embraced the PC fully for banking or bill-paying yet, but will likely do so in the future. Given the likelihood of their increased use of the PC, and that Internet access in households increases with educational attainment (Day et al., 2005), students seem an ideal population for security education. The best and easiest place for them to take a course on PC security would be at their university. But are universities offering these classes to students?

Factors Motivating an Individual to Take a Security Course

The Individual Security Motivation Model examined antecedents to behavioral intent to protect PCs (Anderson, 2005). Portions of this model are used to measure an individual's perceived necessity of security courses.

Both the perceived severity and perceived probability of security violations have been found to be related to concern regarding security threats. To persuade individuals of the need for additional education on security, we need to understand whether or not they perceive an Internet security violation as something that might happen to them, and how severe they perceive the problem might be (Anderson, 2005).

H1: Greater perceived severity of a security violation will be positively related to perceived necessity of security courses.

H2: Greater perceived probability of security violations will be positively related to perceived necessity of security courses.

Both response efficacy and citizen efficacy are related to whether an individual believes he/she can make a difference by securing his/her computer. Response efficacy measures whether an individual believes individual action is essential to keep the Internet safe, citizen efficacy measures the belief that an individual's action can make a difference in keeping the Internet secure (Anderson, 2005). In order for an individual to believe education will have an effect on security issues, he/she must believe that learning strategies to minimize risk will be effective.

H3: Greater response efficacy will be positively related to perceived necessity of security courses.

H4: Greater citizen efficacy will be positively related to perceived necessity of security courses.

Self-efficacy is concerned with an individual's perception of how well he/she can perform the security actions needed to deal with potential security threats. An efficacy expectation is the conviction that one can successfully execute the behavior required to produce the outcomes needed. If someone believes they are capable of securing their PC against threats, they may not believe they need a formal course on security. Therefore, self-efficacy should be considered a moderator of the above four variables and the need for security courses.

H5: Self-efficacy will moderate the relationships between each of the four variables above with perceived necessity of security courses.

The model for this study is shown below in Figure 1.

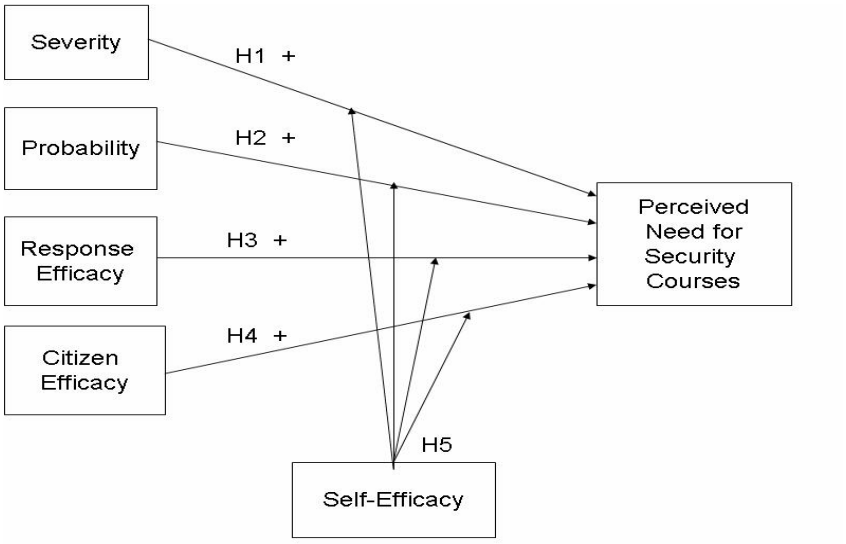

Figure 1: Security Necessity Model

METHODOLOGY

Subjects

Two different methodologies were utilized for the pilot study.

For the first part of the study, assessing students' perceptions of the necessity of security courses, we surveyed junior level students taking an introductory MIS course. As part of the pilot study for this research, we surveyed 62 students. Students were, on average, 21.6 years of age, and were evenly split between males and females.

For the second part of the study, identifying security courses offered in IT departments, a web search was done. We searched departmental web sites for security courses in a large Midwestern state. Specifically, we examined the web sites in the computer science department as well as in the School of Business Information Systems major. We searched all four-year universities for course titles and content to find evidence of security education. All courses shown on the web provided a list of topics covered in that course. If a course did not have Security in the title of the course, we looked for security as a topic covered in the course. While we noted whether the security training offered was specifically for a corporation or for individual security, we looked for both. While our primary goal is to investigate individual PC security education, many of the listed courses did not specify whether the security aspects examined just corporate security, individual home PC security, or both. While we assume much of the course content that did not specify dealt more with corporate security, we also believe that learning something about corporate security will carry-over to individual-PC security awareness.

Instruments

For the first research question, constructs were measured using validated instruments (Anderson, 2005). Severity was measured using four items (e.g., I believe the productivity of individuals is threatened by security violations, I believe the reliability of the Internet is threatened by security violations). Probability was measured using three items (e.g., How likely is it that you will lose personal data due to a security violation?, How likely is it that a security violation will cause a significant outage to the Internet that results in individuals having to spend time to recover their personal data or in some way fix their computer?). Response efficacy was measured with five items. Response efficacy asked students how effective they thought their actions (such as using a firewall, installing anti-virus software, opening email-attachments, etc.) as an individual would be in helping to protect the security of other computers connected to the Internet. Citizen efficacy was measure using four items (e.g., If I adopt security measures on my home computer, I can make a difference in helping to secure the Internet, The efforts of one person are useless in helping secure the Internet (RC)). Finally, self-efficacy was measured using eight items (e.g., How confident are you that you could select the appropriate security software for a home computer?, I have the resources and the knowledge to take the necessary security measures). Items were measured using a 7-point Likert scale.

RESULTS

Data Analysis

Factor analysis and reliability tests were done. Reliability tests ranged from .798 to .908 for the constructs of severity, probability, response efficacy, citizen efficacy, and self-efficacy. Items loaded as expected, although one item from response efficacy was dropped for non-loading, and one item from citizen efficacy loaded on more than one item (it was retained for analysis in the citizen efficacy construct). A full factor analysis table showing all items with their loadings will be presented at the conference.

Preliminary Results

For the first part of the study, we examined factors that might motivate an individual to take a security course. With just 62 responses from the pilot study, preliminary results must be interpreted carefully.

Our model was significant, with adjusted R^2 showing the four independent variables explaining 24.1% of the variance of need for a PC security course. Of the four independent variables, only perceived citizen efficacy was significant (p=.003). Response efficacy is significant at the .10 level (p=.085).

We next looked at self-efficacy as a moderator. However, self-efficacy did not moderate any of the relationships, and also did not have a significant direct effect on need for security education. Table 1 provides a summary of the preliminary findings.

Variable	t	Significance
Severity	.584	.562
Probability	.361	.719
Response Efficacy	1.761	.085
Citizen Efficacy	3.344	.002
Self-efficacy (as direct relationship)	-.745	.460

Table 1: Construct Significance

For the second part of the study, we examined prevalence of university courses. We recognize that some course descriptions may not have included all topics covered in the class, but believe this method shows us what courses consider security to be a primary topic. We also realize that a course could specialize in corporate security, but believe that being aware of corporate needs for security will raise awareness of individual security needs. We examined the web sites of 30 universities. Of these, 43.3% offered no courses on security topics, *and* no courses listed security issues as a topic in a course. Less than half (46.7%) of the universities listed security as a topic within another course; these were typically in a general "Introduction to MIS" type course or an e-commerce course. Just over ¼ (26.7%) of the universities offered an entire course on security. While it is difficult to determine if individual PC security as a topic is covered in these security courses, two universities offered very specific security courses intended for home users (e.g., Internet Security at Home and at Work). Table 2 summarizes these findings.

No Security courses/topics indicated	Security topics mentioned within course	Security course
43.3%	46.7%	26.7%

Table 2: Prevalence of Security Courses in Universities

(totals > 100% because a university could offer both a course, and cover security topics in a different course).

While 50% of the students indicated a course on PC security was necessary (slightly necessary, necessary, or very necessary), it doesn't mean they want to take the course. Only 35% indicated they would consider, would sign up, or would definitely sign up for such a course if one were offered at their university. In fact, 50% of the students indicate they turn to friends for answers often or all the time, while only 25% of the students go to friends rarely or never. Given that less than half the universities offered courses on security may mean that students do not have the opportunity to learn more about security through courses. Also, without the visibility of security courses on campus, students may not be fully aware of the need to protect their computers. If more courses were offered, the need for security might be made more salient to the student population.

DISCUSSION AND CONCLUSION

With only a pilot study conducted at this time, discussion is limited. While less than half the universities offer security topics within courses, and only ¼ offer security courses, it is possible that new courses are currently being added, and working their (slow) way through the university bureaucracy. One limitation to this pilot study was the methodology used to collect information on security courses offered. Recognizing that course content listed on the web is not sufficient in determining content of courses, we will provide results from alternative methods of data collection from universities.

Finding that just 50% of students realize the need for security classes may be explained by the limited monetary losses this age group has seen over the Internet. While this age group has embraced e-commerce in a limited fashion, they are less likely to have begun using the Internet for banking and paying bills. Therefore, they may not yet be fully aware of the potential severity in not fully securing their computers. Alternatively, since the pilot study examined only business students, we may find different results on the perception of the need for security courses when the survey is broadened to include students outside the School of Business.

Of the four independent variables examined, only one was significant. There was a significant, positive relationship between those believing an individual can make a difference in Internet security and the necessity of taking security courses. For this age group then, it may be necessary to stress that individuals can make a difference in keeping the Internet secure. Students' perceptions of severity, probability, and the effectiveness of certain actions in keeping the Internet safe were not significantly related to students' perceptions of the necessity of taking security classes.

At this time, only a small subset of data has been collected. A second round of data collection has started and these results will be available at the conference. Results from a larger survey of students will be available; in addition, recognizing that security courses may be offered outside the School of Business or Computer Science, other potential departments where security courses might be offered will be addressed. While this study began with an examination of perceptions of Business students, students from other areas also need to be made aware of security risks of using PCs, so their access to security courses must also be addressed.

REFERENCES

1. Anderson, C. (2005) Creating the Conscientious Cybercitizen: An Examination of Home Computer User Attitudes and Intentions Towards Security, *CIST INFORMS Conference Proceedings*, November 12-13, San Francisco, CA, USA.
2. Aytes, K. and Connolly, T. (2004) Computer Security and Risky Computing Practices: A Rational Choice Perspective, *Journal of Organizational and End User Computing*, 16, 3, 22-41.
3. Consumer Reports (2005) Net Threat Rising, *Consumer Reports*, 12-18.
4. Day, J., Janus, A, and Davis, J. (2005) Computer and Internet Use in the US, US Census Bureau, http://www.census.gov/prod/2005pubs/p23-208.pdf.
5. Keller, S., Powell, A., Horstmann, B., Predmore, C., and Crawford, M. (2005) Information Security Threats and Practices in Small Businesses, *Information Systems Management*, 22, 2, 7-19.
6. Peltier, T. (2000) How to Build a Comprehensive Security Awareness Program, *Computer Security Journal*, 16, 2, 23-32.
7. Tuesday, V. (2001) Human Factor Derails Best-Laid Security Plans, *ComputerWorld*, 35, 18, 52-53.
8. Zhang, X. (2005) What Do Consumers Really Know About Spyware?, *Communications of the ACM*, 48, 8, 44-48.