

# The Effect of a University Information Security Survey on Instruction Methods in Information Security

Frank H. Katz  
Armstrong Atlantic State University  
Department of Information Technology  
11935 Abercorn Street, Savannah, GA 31419  
912-921-5608  
katzfran@mail.armstrong.edu

## ABSTRACT

This paper reports on the need for Information Security Awareness educational programs to supplement teaching in Information Security. The need for such a program is demonstrated by findings resulting from a survey of university faculty and staff at Armstrong Atlantic State University conducted from February through April 2005 regarding the information security behaviors of such employees.

## Categories and Subject Descriptors

C.2.0 [Computer Communications Networks]: General – Security and protection

D.4.6 [Operating Systems]: Security and Protection - Access controls – Authentication, Cryptographic controls, Information flow controls, Invasive software.

K.3.2 [Computers And Education] - Computer and Information Science Education – Curriculum, Information systems education.

K.4.1, .2 & .4 [Computers And Society] - .1 Public Policy Issues - Abuse and crime involving computers, Computer-related health issues, Ethics, Intellectual property rights, Privacy. .2 - Social Issues - Abuse and crime involving computers. .4 Electronic Commerce - Security

K.6.5 [Management Of Computing And Information Systems] - Security and Protection – Authentication, Invasive software, Unauthorized access.

## General Terms

Management, Security, Human Factors, Standardization, Legal Aspects.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

Information Security Curriculum Development (InfoSecCD) Conference '05, September 23-24, 2005, Kennesaw, GA, USA.  
Copyright 2005 ACM 1-59593-261-5/05/0009...\$5.00.

## Keywords

Information Security, Information Assurance, Information Security Curriculum, Information Assurance Curriculum, Curriculum Development, Curriculum Instruction.

## 1. INTRODUCTION

On March 11, 2005, the names of 98,000 graduate students and applicants to the University of California, Berkeley disappeared. No one hacked into the University of California's system. The names and their associated social security numbers were stored in a laptop that was left unattended in a restricted area of the graduate division offices. The laptop was located in an office off a corridor normally locked when the receptionist is away, but the corridor wasn't locked the day of the theft. The laptop was left unattended for only 30 to 60 minutes.

A user receives a Web postcard in e-mail, and inadvertently installs a Trojan horse onto his system, becoming a victim of a clever social engineering attack. The card contains a spoofed sender address and appears to come from bluemountain.com. But a link in each e-mail claims to go to Blue Mountain's card pickup Web page, where recipients are asked to enter a unique card ID number provided in the e-mail. Victims who click on the link

pass through a number of sites that may have installed mal-ware, or malicious software.

A student living in a university dormitory installs file-sharing peer-to-peer (P2P) software on her PC to download music from the Internet. Although clearly against university policy, she does it anyway, downloading files that may contain viruses, worms, Trojan horses, or spyware onto her PC. In her university's networked environment, she may have opened up a port on the school's firewall, giving the attacker the capability to attack the system by taking advantage of any vulnerabilities that exist in the P2P application. Besides engaging in what may be copyright violations, putting her university in legal jeopardy, she has unintentionally compromised her own confidential information, the secure data belonging to others using the network, and the integrity of the network itself.

More and more persons are afraid of on-line identity theft, even though many identity thieves are not profiting on-line. Instead, they're diving through garbage and stealing from readily accessible paper files. According to James Van Dyke, principal analyst at Javelin Strategy and Research in Pleasanton, California, friends, family members and neighbors account for half of all known thieves, and on an average cost the victim \$15,607, compared to \$2,320 for an online thief. "It's still so much easier to grab something from a desk or from the trash," said Van Dyke.

Over 2,400 years ago, Chinese General Sun Tzu said that "If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy or yourself, you will succumb in every battle." Here in the 21<sup>st</sup> century, his observation has great relevance to information security today.

All too often when IT managers look to secure their organization, their focus turns to firewalls, routers, intrusion detection software, proxy servers, and the like. However, they may be overlooking the most obvious problem in their organization, one that cannot be cured by the most modern software and hardware. They neglect their end users. As General Tzu would say, these managers don't know themselves – their own organizations. People are part of the system, and failure to recognize this and address the training of end users can result in disaster. It is certain that "employees constitute one of the greatest threats to information security." Indeed, the 2004 Ernst & Young Global Information Security Survey "revealed that end-user security training was the No. 1 problem inside large organizations. Yet less than half of the respondents said their companies had a formal training program to meet the threat."

On November 18, 2004 a conference of Chief Information Officers of various companies and organizations in the Savannah area was held at Savannah Technical Institute. Participants were asked to list and then rank the problems facing their organizations. Nearly every attendee ranked information security at the top of his or her list. A corollary to the problem of keeping information secure was the perceived lack of employee training in this discipline. Discussions among the attendees emphasized the need to train employees not just in technological security solutions, but on how to mitigate and prevent those threats caused by people.

Universities, with a considerable amount of confidential information being handled at any given time, are particularly prone to many of the purely human threats to information security. Some of these include compromises to intellectual property; deliberate acts of theft; deliberate acts of information extortion; deliberate acts of sabotage and vandalism; and deliberate acts of espionage and trespass. Armstrong Atlantic State University (AASU) is no different than any other university. Professors and staff are responsible for securing private information, ranging from student grades to faculty evaluations. It is important that not only are faculty and staff trained in the proper behaviors necessary to secure information, but that Information Technology students are taught these as well so that they will be able to participate in the development of information security programs upon graduation.

Consequently, it is necessary to determine if university faculty and staff are engaging in proper information security practices, and if not, how we can make recommendations to correct any

flaws in our practices, best train our users, and include these best practices in the pedagogy of our information technology courses as well as in employee training.

## **2. METHODOLOGY TO DETERMINE CURRENT PRACTICES**

From February through April 2005, I conducted a survey about information security practices and behaviors among faculty and staff at Armstrong Atlantic State University. The questions in the survey assessed whether the faculty and staff of AASU have been performing the simple everyday practices and behaviors necessary to avert the threats to information security described above. The survey contained statements about various information security practices, and users were asked to state whether they perform them on a range of strongly agree to strongly disagree. The questions are listed in the Appendix.

In administering the survey to the Armstrong Atlantic State University community, it was important to determine who would be participating. Ideally, it would be preferable for every employee, whether faculty or staff, to do so. Realistically, this would not be possible. On a campus with over 600 such employees, it would be unlikely that I would get every employee to cooperate. I attempted to obtain a cross-section of the employees on campus, ranging from academic departments in all colleges and schools to functional departments such as the Registrar and Financial Aid. My initial plan was to send the surveys to the various heads of the departments I selected, and then have them distribute the surveys to their employees. In order to maintain anonymity for both the employees and departments, I requested that the surveys be returned to me by each respondent. In this way, no one department or individual would feel "singled out" because of potentially poor information security behaviors. As time progressed, however, I decided to send out the surveys to individual employees in departments that had not initially received them. Again, the response sheet not containing the name of the respondents guaranteed them anonymity.

210 surveys were sent out, representing approximately one-third of the faculty and staff of AASU. Out of these, just over 33%, or 73, were returned, of which 50 were faculty and 23 were staff. In addition, 58 respondents have their own office, 6 share an office, and 9 sit in a cubicle or open area.

## **3. FINDINGS**

### **3.1 Positive Results**

Overall, the responses to the survey indicate that faculty and staff take the most basic preventative information security practices seriously. One hundred percent of those surveyed who have their own office or share an office always lock it at night. Over 91% of the respondents strongly agreed or agreed to the statement that they never open an attachment to an e-mail unless it comes from a trusted source. In addition, 87.6% of the respondents agreed or strongly agreed with the statement that they turn off their PCs at night when they leave, and 86.3% agreed or strongly agreed with the statement that they close confidential web pages when they are done viewing them.

When asked questions about revealing their AASU computer passwords, indicating susceptibility to social engineering, nearly all the respondents indicated that they disagreed or strongly

disagreed with statements that on occasion they had done so. Even so, eight employees out of 73 have on occasion revealed their passwords to employees or co-workers prior to going on vacation, which may be a cause for concern. However, taken as a whole, these responses seem to indicate that users are properly performing the most fundamental information security behaviors.

Question Regarding Password Security	Percent Disagreeing or Strongly Disagreeing
On occasion, I have revealed my computer password(s) to AASU site to my supervisor or coworkers	84.9%
On occasion, I have revealed my computer password(s) to an AASU site in an e-mail message	93.1%
On occasion, I have revealed my computer password(s) to an AASU site on a survey or questionnaire	94.5%
On occasion, I have revealed my computer password(s) to an AASU site to someone who has contacted me telephonically and asked for my password	93.1%

### 3.2 Some Causes for Concern

Despite the positive findings described above, when further reviewing the data, there are some causes for concern. Questions addressing technical aspects of information security indicated that respondents are not as likely to regularly perform these behaviors. These practices are not so technical as to require programming skills, but it is possible that the respondents are not fully trained in them, are not aware that they are being automatically performed unbeknownst to them, or are not even aware that they exist.

These more technical aspects of information security include: the use of anti-virus software; the backup of the users' data; the use of strong passwords; and the use of password protected screensavers to prevent "shoulder surfing," which is an espionage technique whereby an individual is able to view the contents of a screen after the user has walked away for a short period of time.

Only 27% of those surveyed agreed or strongly agreed with the statement "using the anti-virus program loaded on my PC, I always execute an anti-virus scan of my computer at least once a week." All of our users outside of AASU's School of Computing are connected to the AASU Novell network, and AASU's Computer and Information Services (CIS) runs McAfee's Netshield for Novell to protect the servers from viruses. However, instructions are provided to users on the CIS website describing how to ensure that the user's version of McAfee Virus Shield is up-to-date. Users should be made aware of these instructions and encouraged to perform this check periodically. This still will not detect viruses on a users' hard drive, and users must take a more proactive approach to routinely and frequently scanning their own PCs' hard drive to ensure that their PC is not infected.

Just over 63% of our survey disagreed or strongly disagreed with the statement that "the data on my PC is backed up at least once

per week." Unbeknownst to the user, if he or she has arranged with CIS to place their files on a network drive, they will be backed up on a network drive for them. But if the user has not made such an arrangement, backing up his or her data becomes the user's responsibility. According to the Coordinator of Central Systems Networking and Network Administrator for Armstrong's CIS, the users are not routinely trained on how to place their data on a network drive. Many users may not place their data on the network server, perhaps for fear of the data becoming lost, corrupted, or even read by CIS personnel. In some cases, academic department heads determine whether personal data is placed on the network servers. Armstrong's CIS department does provide guidance on backing up sensitive data on their website.

52% of those surveyed agreed or strongly agreed with the statement that they "understand what a strong password is, and always employ one when accessing any of AASU's secure websites." Strong passwords, which are character strings that include numerals, upper and lower case characters, and are not obvious or not real words help prevent passwords from being compromised. While it was welcome that 52% of the respondents understood this concept, it would be important that more employees did so.

Only 47% of those surveyed agreed or strongly agreed with the statement that they "understand what a password-protected screen-saver is and additionally, only 22% agreed or strongly agreed with the statement that they always use one. The screen-saver can be programmed to execute after a specified time interval has passed (perhaps five to ten minutes), during which time the mouse has not been moved and/or the keyboard has not been touched. Once activated, the screen-saver can only be disengaged by the password being entered. Password-protected screen-savers are a very effective method of protecting users from having information on their screen viewed by others and potentially stolen, and users should be encouraged to employ them.

The last cause for concern does not relate to a technical security solution. Rather, it has to do with a very simple element of information security: reading and understanding organizational security policies. In response to the final question in the survey, 53% disagreed or strongly disagreed with the statement "I have read and understand the various policies regarding computing at AASU as promulgated by CIS on their website <http://www.cis.armstrong.edu/cispolicies/index.html> . Each employee of the university should be encouraged to read and follow the points in the policy's webpages.

## 4. RECOMMENDATIONS

My recommendations are directed at two different audiences – faculty/staff, and pedagogical with regard to the curriculum of Armstrong Atlantic State University's School of Computing.

### 4.1 Faculty and Staff

Faculty and staff at AASU are performing the minimal practices necessary to safeguard their information. But they can do more. Each individual must take ownership of the security of their PC and their data. Persons who do not regularly backup the data on their hard drive should contact AASU's CIS to be taught how to securely place their data on the Novell network so that it may be

backed up daily. Those individuals who, as a matter of personal or department preference, will not place their important files on the network server must be provided a means of backing up their most critical files. Because of size limitations of using 1.44MB floppy diskettes for backup, users must either be provided a CD-R or CD-RW capability, or an USB-compatible “thumb drive” or “memory stick.” Unfortunately, not every PC on campus is set up to write to CDs, and installing this hardware/software combination would be expensive for each PC. Since nearly all PCs are set up with USB ports, the use of 128MB or 256MB “thumb drives” may be a more reasonable solution. Instructions should be provided not only for their use, but also as to a methodology for performing regular backups. Those personnel who cannot make their own backups should be forced to move their important data to the Novell network.

In their AASU Campus IT Documents page, CIS provides detailed information on how to create a secure, strong password. While it may be impossible to enforce a strong password policy for websites such as the Pirates Cove e-mail/calendar/news portal, a security awareness publicity campaign should be launched to ensure that each employee has read the instructions and knows how to create and use such a password. It is well known that passwords create a challenge for users. The user is required to create a strong password that is hard to break, but wants to create a password that he or she will remember. The user ends up complaining that he cannot remember a strong password, and hesitates to create one. To encourage users to do so, perhaps they should be encouraged to do something they’re told not to do – write the password down. Then place that password in a secure place, like his wallet. Money and credit cards are placed inside a wallet, so it is presumed that users try to keep their wallet safe.

## 4.2 Pedagogical Implications

Security and privacy issues are addressed in many courses in the AASU Computer Science and Information Technology curricula. As a required course in their curriculum, each student in the AASU School of Computing must take CSCI 2070, Computer Ethics. During the 2004-05 academic year, the Information Technology department has taught a course in Information Security, which initially used the text Principles of Information Security by Whitman and Mattord. Originally taught as a Special Topics course, the topic matter was deemed so important that ITEC 3100, Information Security, was added to the curriculum as a new, required course.

The issues raised in the survey will provide a unique opportunity for our IT students to apply what they learn in the classroom to real-world situations. The syllabus for ITEC 3100 could include various projects that would allow students to put into practice the course material, including:

- Write an “acceptable use policy”.
- Plan and implement, with the cooperation of Armstrong’s CIS, a training seminar that would be conducted for faculty and staff of the various departments of the university. Such a seminar could include training in (but not limited to):
  - The proper use of anti-virus software.
  - The proper use of strong passwords.
  - The use of password-protected screensavers. These could be particularly effective in ensuring that sensitive material on a monitor

screen is secured from view by unauthorized persons.

- Plan and conduct one-on-one training for faculty and staff in information security practices, especially the items listed above. This too would require the cooperation of CIS as well as the individual department heads.
- Plan and conduct a poster or brochure contest among students in the School of Computing. The posters could be part of an information security awareness campaign, with a prize for the winning poster. That poster could be used in a campus-wide campaign to make students, faculty, and staff more aware of proper information security practices.
- Plan and implement a security awareness award program. Students could, with the permission of department heads, visit various departments several times during a semester. If they observe someone practicing proper security behaviors, such as using password-protected screensavers, they could award that person a desk token highlighting IT security.

## 5. CONCLUSIONS

Whether in printed documents or temporary images on a screen, university faculty and staff are responsible for securing many types of confidential information. The survey described in this paper was administered to determine the level of physical and technical information security among the employees of Armstrong Atlantic State University. Its findings indicate that while many employees of the university understand and utilize appropriate physical measures to secure their information, they need to become more aware of and skilled in using technical security methods. An important tool in accomplishing this goal is the development of campus-wide information security awareness programs.

Students receiving instruction in information security would benefit from participating in the development of such programs among the university community. To that end, the recommendations presented above can be incorporated into either an information security course, or included as a module of a general information technology or computer science course.

## 6. REFERENCES

- [1] AASU *Campus IT Documents (Policies)*. Retrieved March 28, 2005, from <http://www.cis.armstrong.edu/cispolicies/index.html>
- [2] Gartenberg, Marc. *Simple steps for raising the security bar at your company*. (2005, March 30) Retrieved April 8, 2005, from <http://www.computerworld.com/printthis/2005/0,4814,100589,00.html>
- [3] Hall, Mark *Secure the People*. (2005, March 21) Retrieved April 8, 2005, from <http://www.computerworld.com/printthis/2005/0,4814,100448,00.html>
- [4] *Risks of File-Sharing Technology*. Retrieved April 8, 2005, from <http://www.us-cert.gov/cas/tips/ST05-007.html>
- [5] Roberts, Paul. *Web postcards hide Trojan horse programs*. (2005, April 5) Retrieved April 8, 2005, from <http://www.computerworld.com/printthis/2005/0,4814,100874,00.html>
- [6] UGA – *Security Awareness, Training and Education (SATE)*. Retrieved April 8, 2005 from <http://www.infosec.uga.edu/sate/>
- [7] Verinder, Matthew. *Study: More identity theft off-line than online*. (2005, January 28) Retrieved April 8, 2005, from <http://www.computerworld.com/printthis/2005/0,4814,9329,00.html>
- [8] Weiss, Todd R. *Laptop with 98,000 names stolen from UC-Berkeley*. (2005, March 29) Retrieved March 30, 2005, from <http://www.computerworld.com/hardwaretopics/hardware/story/0,10801,100712,00.html>
- [9] Whitman, Michael E. & Mattord, Herbert J. *Principles of Information Security* 2003 Boston: Thomson Course Technology, pp. 44-45

## APPENDIX – SURVEY QUESTIONS

This survey was administered to faculty and staff who work in both offices and in open spaces such as cubicles. In order to be used again in the future, it should be modified to meet different situations regarding the physical location of the respondents.

1. Are you:
  - a. Faculty
  - b. Staff
2. I work in:
  - a. My own office with a door that can be locked
  - b. An office that I share with another person
  - c. A cubicle

For questions 3 through 20, the options were:

(a) Strongly agree (b) Agree (c) Disagree (d) Strongly Disagree, or (e) Not Applicable

3. I work in my own office, and always lock it *during the workday*, even when I leave for just a few minutes.
4. I work in my own office, and always lock it when I leave *at the end* of the workday.
5. I share my office, and my office-mate(s) or I always lock our office *during the workday*, when no one is occupying it.
6. I share my office, and my office-mate(s) or I always lock our office when we leave *at the end* of the workday.
7. I always turn off my computer *during the workday* when I leave my workstation for more than 5 minutes.
8. I always turn off my computer when I leave my workstation *at the end* of the workday.
9. I always close confidential web pages or files as soon as I am done working or viewing them.
10. Using the anti-virus program loaded on my PC, I always execute an anti-virus scan of my computer at least once per week.
11. I never open an attachment to an e-mail unless it comes from a trusted source.
12. The data on my PC is backed up at least once per week.
13. I understand what a *strong password* is, and always employ one when accessing any of AASU's secure web-sites (SHIP, WebCT, Pirate's Cove).
14. On occasion (e.g., when going on vacation), I have revealed my computer password(s) to an AASU site to my supervisor or co-workers.
15. On occasion, I have revealed my computer password(s) to an AASU site in an e-mail message.
16. On occasion, I have revealed my computer password(s) to an AASU site on a survey or questionnaire.
17. On occasion, I have revealed my computer password(s) to an AASU site to someone who has contacted me telephonically and asked for my password.
18. I understand what a password-protected screen-saver is.
19. I always use a password-protected screen-saver on my PC.
20. I have read and understand the various policies regarding computing at AASU as promulgated by CIS on their website: <http://www.cis.armstrong.edu/cispolicies/index.html>