Information Security Journal: A Global Perspective
Publication details, including instructions for authors and subscription information:
http://www.tandfonline.com/loi/uiss20

Information Security Awareness Status of Business College: Undergraduate Students

Eyong B. Kim [a]
[a] Barney School of Business, University of Hartford , West Hartford , Connecticut , USA
Published online: 18 Nov 2013.

To cite this article: Eyong B. Kim (2013) Information Security Awareness Status of Business College: Undergraduate Students, Information Security Journal: A Global Perspective, 22:4, 171-179, DOI: 10.1080/19393555.2013.828803

To link to this article: http://dx.doi.org/10.1080/19393555.2013.828803

Information Security Journal: A Global Perspective, 22:171–179, 2013

ISSN: 1939-3555 print / 1939-3547 online
DOI: 10.1080/19393555.2013.828803

Taylor & Francis
Taylor & Francis Group

Information Security Awareness Status of Business College: Undergraduate Students

Eyong B. Kim
Barney School of Business, University of Hartford, West Hartford, Connecticut, USA

ABSTRACT Because end users are often the weakest link in a security chain, students need to practice security controls properly to improve information security on campus. This study surveyed undergraduate students in a business college to investigate their understanding and attitudes toward information security. Survey findings show that college students understand most information security topics suggested by National Institute of Standards and Technology (NIST) Special Report 800-50. Universities should provide easily accessible security training programs for students. Practical suggestions are provided to encourage students to participate in security training to enhance their security awareness level.

KEYWORDS college students' information security awareness, information security, information security training

INTRODUCTION

The Internet Crime Complaint Center (IC3) reported that the number of complaints related to crimes committed using the Internet in 2011 was more than 300,000. That is more than six times greater than a decade earlier. The adjusted dollar loss of complaints in 2011 was $485.3 million (IC3, 2011). Because of these thriving cyber crimes, major corporations are currently focused more on information security. For example, information security is moving from a functional information technology (IT) area to strategic importance at the highest levels of corporations, because the number and sophistication of hacker attacks on major corporations continues to increase (Schectman, 2013).

Since college students use information systems and the Internet heavily for their school work and personal use, they may experience information security threats quite often. Based on an EDUCAUSE member institution survey (Ingerman & Yang, 2011), information security continues to be an issue of "strategic importance" and ranked as the fourth most important issue. Higher educational institutions consider information security as the leading computing issue to address (Green, 2009). Moreover, because of end users' noncompliance with information security policies, it is a key problem for any organization and its information security (CSI/FBI Survey, 2007).

Address correspondence to Eyong B. Kim, PhD, Associate Professor of Management Information Systems, Barney School of Business, University of Hartford, 200 Bloomfield Avenue, West Hartford, CT 06117, USA.
E-mail: ekim@hartford.edu

Even though an organization has published an information security policy, many users are often not aware of its content or have not received any training in how to implement it properly (Wood, 2002). The top obstacle in implementing an effective information security policy in an organization is users not being aware of such a policy (Ernst & Young, 2004). If users do not follow the security policy, they may be exposed to security threats because most security attacks target the users who show signs of vulnerability instead of intentionally select targets to attack (DBIR, 2011). It implies that users hardly become victims of security threats if they are well prepared for these security threats. To protect college students from information security threats, universities need to establish good security awareness programs and educate students to follow what they learned because information security is not an intuitive or obvious process. The important issue is that students understand the importance of information security and security awareness topics.

In educating students to improve their information security awareness, one effective method is information security training for users. This paper investigates the status of the information security awareness level of undergraduate students in a business college and the impact of information security training on their security awareness. The basic hypothesis tested is that there is no significant relationship between information security training and students' understanding of what they need to do to protect their systems and information. In this study, the term "training" is used in a broad sense that meets a common definition of training such as "the provision of knowledge and skills" or "the enhancement of learners' knowledge and skills" (Antonacopoulou, 2006; King, King, & Rothwell, 2001, p. 2). Thus, in this study, training includes workshops and class sessions.

CYBER CRIMES

The Bureau of Justice Statistics categorized cyber crimes as cyber attacks, cyber theft, and computer security incidents and provides definitions and examples.

- **Cyber attacks** are crimes in which the computer system is the target. Cyber attacks consist of computer viruses (including worms and Trojan horses), denial of service attacks, and electronic vandalism or sabotage.
- **Cyber theft** comprises crimes in which a computer is used to steal money or other things of value. Cyber theft includes embezzlement, fraud, theft of intellectual property, and theft of personal or financial data.
- **Other computer security incidents** encompass spyware, adware, hacking, phishing, spoofing, pinging, port scanning, and theft of other information, regardless of whether the breach was successful.

As described, cyber crimes are diversified and broad-reaching. For example, computer viruses are only one type of computer attack. About 17.7 million virus definitions were listed in Norton/Symantec's security system, with 106,946 additional definitions added in the eight days leading up to April 15, 2012. Viruses or malware attacks historically have been listed at the top or near the top in the CSI reports followed by phishing, laptop or mobile device loss, zombies inside organization, and users' abuse of the system (CSI, 2011). These top five security threats can be effectively prevented if users follow the proper security actions. Due to the wide use of computer hardware and software today, it is not easy to protect users' information effectively by solely utilizing technology. Because technology alone is not sufficient to ensure information security, users should understand the importance of information security and do their share (Ruighaver & Chang, 2007; Workman, Bommer, & Straub, 2008).

Identity theft has been a concern for many end users in the last several years. ID theft is defined as stealing an individual's personal information and illegally using stolen data for financial or nonfinancial gain. Different from other types of cyber attacks, sometimes it may not require any computer or computer network. In earlier days of ID theft, a person illegally accessed victims' information written in documents or credit cards. Now, social networks are a great resource for fraudsters because consumers are still sharing a significant amount of personal information that is frequently used to authenticate a consumer's identity. More than 11.6 million adults became victims of identity theft in the United States, losing approximately $18 billion in 2011 (Javelin Strategy & Research, 2012). The majority of victims were in one of the following age brackets: 40–49 (25%), 18–29 (20%), and 50–60 (20%) in 2009 (ITRC, 2010).

With more people using smartphones, ID theft using a smartphone is increasing. The same survey found 7% of smartphone owners were victims of identity fraud and that is a one-third higher incidence rate compared with the general public. Part of this increase can be attributable to

consumer behavior. Javelin Strategy & Research points out that 32% of smartphone owners do not update to a new operating system when it becomes available; 62% do not use a password on their home screen, which enables anyone to access their information if the phone is lost; and 32% save log-in information on their device (Javelin Strategy & Research, 2012).

INFORMATION SECURITY AWARENESS PROGRAM

A variety of information security threats and attacks have been reported and new ones keep coming as technology progresses and everyone is using more of IT or information security. Based on previous publications and interviews, Whitman (2003) categorized a dozen categories of threats to information security: human error, compromises to intellectual property, espionage or trespass, information extortion, sabotage or vandalism, theft, software attacks, forces of nature, quality of service deviations from service providers, hardware failures or errors, software failures or errors, and technological obsolescence.

Among these threats, users may be one of the most important elements in information security. Users should take on the personal responsibility of protecting their own systems in situations such as social engineering (Sherif, Ayers, & Dearmond, 2003). User-related security threats may include human error, compromises to intellectual property, information extortion, sabotage or vandalism, and others. Since employees can access information systems legitimately and may make careless mistakes or errors, they can cause security breaches unintentionally that can damage an organization's data and security systems.

Users often become victims of social engineering attacks because attackers use persuasive techniques to gain the confidence of an individual by collecting small bit of seemingly harmless information until the attacker can get enough information to access his or her system (Mitnick & Simon, 2002). Social engineering attacks have been used by attackers for years and remain a popular hacking method. Successful social engineering attacks result not only from duplicity but also from a willingness to surrender sensitive information despite awareness of pervasive threats (Calluzzo & Cante, 2004). Social engineering attacks are primarily motivated by financial gain (51% of attacks). They are costly to organizations (15% of large companies cite the loss of more than $2.5 million annually), and new employees are most susceptible to social engineering attacks (Dimensional Research, 2011). A reason that new employees are most susceptible might be the lack of information security training. Training is considered an important component in dealing with social engineering because training mitigates employees' duplicity and develops coping behaviors (Workman, 2007).

It is true that users may not use information security techniques or procedures properly if they do not understand the importance of information security (Ceraolo, 1996; Straub & Welke, 1998). To help users understand what they need to do for information security, a strong awareness and training program is essential (NIST, 1998).

A security awareness program might be the most effective method of maintaining information security in an organization. According to the Information Security Forum (ISF, 2002), security awareness is defined as the degree or extent to which every member understands the importance of information security, the levels of information security appropriate to the organization, their individual security responsibilities, and acts accordingly. Organisation for Economic Co-operation and Development (OECD) guidelines (2002) defined the goal of security awareness as: "Participants should be aware of the need for security of information systems and networks and what they can do to enhance security." In other words, members of an organization should understand the importance of information security and act upon the guidelines provided by the security policy.

A security awareness program keeps users aware of information security in everyday work. Security awareness programs set the stage for training by changing organizational attitudes to realize the importance of security and the adverse consequences of its failure and remind users of the procedures to be followed (NIST, 1995). Through the security awareness program, organizations want to enhance the importance of information systems security and minimize the possible negative effects of a security breach or failure (Hansche, 2001). To keep organizational information safe, Ernst and Young (2008) recommended investing in training and awareness programs to keep people from being the weakest link. One of the best uses of the information security budget is comprehensive user information security awareness programs (von Solms & von Solms, 2004). If users' security awareness is improved, they make fewer mistakes and increase the

efficiency of security techniques and procedures (Siponen, 2000). However, simply passing around well-documented security awareness guidelines among end users may not be an effective approach. If users are not fully aware of information security, information security techniques and procedures can be misused, misinterpreted, or not used at all by end users (Ceraolo, 1996; Straub & Welke, 1998). Therefore, for a security awareness program to be effective, end users need a high level of security awareness, and must comply with the security policy in their everyday computing.

INFORMATION SECURITY TRAINING

A security awareness program is not effective if an organization simply has well-documented security guidelines without implementing the guidelines properly (Siponen, 2000). According to NIST Special Publication 800-16 (1998), user awareness, training, and education are important aspects when addressing human factors and competencies in information security. A successful security awareness program should focus on how users achieve continuously secure behavior because security awareness training reduces the success rate of hacking attacks at the individual and organizational levels (Okenyi & Owens, 2007). One effective approach of achieving this objective is end-user security training (Siponen, 2000), which is intended to persuade end users and stimulate their thinking processes regarding information security. A training program should adopt empirically proven approaches to persuade users to follow what they learned in training (Puhakainen & Siponen, 2010).

An effective training program considers several factors, such as trainee selection, overview briefings to participants, training design and delivery, support from the supervisor immediately after training, and feedback and incentives or consequences (Stolovitch, 2000). If there are no follow-up training actions such as adequate management attention, user performance deteriorates rapidly (Stolovitch, 2000). If the campus information security problem is due to the lack of individual knowledge or skill, training is an appropriate intervention method (King et al., 2001, p. 7). Based on a survey of training transfer studies, it was found that the training content does not always effectively transfer to the work setting (Baldwin & Ford, 1988; Ford & Weissbein, 1997). Therefore, it is important to encourage trainees to actually implement what they learned from the training in everyday work.

METHODOLOGY AND INSTRUMENT DEVELOPMENT

To develop the survey questionnaire, the security awareness topics were compiled from previous studies and NIST SP 800-50 (2003) that has 27 topics. As a result, the questionnaire has 21 items to investigate attitudes toward information security awareness among undergraduate students in a business college. In addition, 14 items were added for the demographic information of respondents (five items) and the students' experience and practices of information security controls (nine items). These 14 items use the categorical variables. The remaining 21 items examine students' attitudes and perceptions toward information security using a 5-item Likert scale. These items are shown in Appendix 1.

The survey questionnaire was conducted on 196 undergraduate students in a business college of a mid-sized university in New England. The survey questionnaires were sent to students as e-mail attachments and posted on Blackboard. A reminder e-mail was sent one week after the initial e-mail notification of the survey. As a result, total of 87 students out of 196 returned the survey yielding a 44.9% return rate. A reason for the high return rate might be due to the acquaintanceship between students and the author. Survey participation was voluntary and made anonymous by the collection of survey questionnaires by a third party. The principal investigator received responses without any identification. Among the 87 responses, two responses were deleted because they were unacceptable (one did not specify training participation, and the other responded to only demographic questions). The remaining 85 responses were analyzed using SPSS.

SAMPLE CHARACTERISTICS

Respondents consisted of 3 freshmen (3.5%), 21 sophomores (24.7%), 23 juniors (27.1%), 37 seniors (43.5%), and 1 student did not specify. Nine students (10.6%) are working full time, 34 students (40.0%) work part time, and the remaining 42 students (49.4%) do not work at all. More than half (51 students, 60%) are male students, and 33 students (38.8%) are female students (one student did not specify). Age distribution of the sample is as follows: the majority (76 students, 89.4%) are between 18 and 23 years old, 5 students (5.9%) are between 24 and 30 years old, 3 students (3.5%) are older than 30, and 1 student did not specify. Out of 85 responses, about

one-third (27 students, 31.8%) had received information security training while the remaining 58 students did not.

RELIABILITY AND VALIDITY OF THE INSTRUMENT

To test the reliability of these questionnaire items, Cronbach's alpha test, which is a model of internal consistency based on the average inter-item correlation and is one of the established techniques for reliability testing, was conducted. The alpha coefficient of these questionnaire items is .775, which is considered a reliable measure of a construct for exploratory studies (Nunnally, 1978). Concerning validity, the questionnaire items were developed based on the NIST Special Publication 800-50 and previous studies.

The raw matrix of 86 responses was analyzed by the principal components analysis with varimax rotation (Kaiser's Varimax method) with the latent root criterion (eigenvalue 1 criterion) applied to obtain the eight factors (factor loadings greater than .40). Only those factors with eigenvalues (the column sum of squares for a factor) greater than 1 are considered as significant. Kaiser's Varimax method (Kaiser, 1958), one of the most widely used methods to obtain an orthogonal rotation, maximizes the sum of variances of squared loadings in the columns of the factor matrix.

Results revealed that 64.4% of the variance could be explained by the first five factors with eigenvalues of 1.0 or more. Twenty-seven percent of the variance is explained by a first factor; 12.5%, by a second factor; 10.8%, by a third factor; 7.9%, by a fourth factor; and 6%, by a fifth factor. After analyzing loaded items on each factor, the author considers the factor 1 as Web and e-mail security, factor 2 as cyber-attack prevention, factor 3 as document safety, factor 4 as mobile security, and factor 5 as password security. These five dimensions of information security seem to represent the security issues the current college students are experiencing.

RESULTS AND DISCUSSIONS

The hypothesis was tested using the Mann-Whitney Test because the normality assumption of the training group is not guaranteed (sample size of training group is 27). Among 21 security awareness topics, only one, installing patches whenever available ($p = .010$), has a significant relationship with the information security training. The remaining 20 information security topics are not significantly related to information security training. It may be because students are familiar with these topics from a variety of other sources. Students responded that they learned information security through taking classes (61.2%), the work place (11.9%), friends (10.4%), media (9.0%), and other sources. This variety of sources for information security may have contributed to the improvement of students' information security awareness for most security topics in general. Even though only one issue, installing software patches whenever available, has a significant relationship with security training statistically, students need comprehensive security training because a student's ignorance of any one security issue can still have serious consequences.

About 40% of students (34 out of 85) believe their information in the university system is effectively protected and 7 students (8.3%) think it is not effectively protected; the remaining students (44 out of 85, 51.8%) think the university provides average protection for their information. About 65.9% of students (56 out of 85) claim they protect their information, computers, and storage devices sufficiently. Surprisingly, there was no significant relationships between information security training and students' belief in protecting their personal information and systems sufficiently ($p = .076$). It seems that most students believe they know what to do to protect their systems even though it is not necessarily true based on the results of this study, for example, the issue of timely installation of software patches. If a security training program does not thoroughly cover most of the important security controls, participants may feel confident even though they are in a vulnerable position.

Some students (11.8%) claimed they were victims of phishing while about one-third (35.3%) did not know if they have been a phishing victims, and the remaining students (50.6%) said they never experienced a phishing attack. There is a significant relationship between the experience of phishing victims and security training ($df = 2$, $p = .016$). Ten students (11.8%) reported that they were victims of identity theft in this survey. That shows no significant relationship with security training statistically. However, identity theft victims among college students in this survey (11.8%) were more than double the U.S. average (4.9%) in 2011 (Javelin Strategy & Research, 2012). At the same time, a similar number of students were victims of phishing (11.8%). The reason may be that college-age adults tend to be not as careful with their

TABLE 1 Response for Each Security Topic*

Topic	Not Important	Neutral	Important
Need of information security training	11 (12.9%)	13 (15.3%)	61 (71.8%)
Need of an anti-virus program	6 (7.1%)	5 (5.9%)	74 (87.0%)
Needs to update virus definitions	3 (3.6%)	10 (11.9%)	71 (84.5%)
Regularly scan computer(s) and storage device(s)	19 (22.6%)	18 (21.4%)	47 (55.9%)
Installing and enabling a personal firewall	6 (7.1%)	16 (18.8%)	63 (74.1%)
Installing software patches whenever available	0 (0%)	42 (51.2%)	40 (48.8%)
Encrypting important files	49 (57.6%)	18 (21.2%)	18 (21.2%)
Change default password when installing a router	26 (30.6%)	12 (14.1%)	47 (55.3%)
Use browser-enabled pop-up blockers	7 (8.2%)	14 (16.5%)	64 (75.3%)
Risk of peer-to-peer file sharing	11 (10.6%)	14 (16.5%)	60 (70.6%)
Risk of downloading programs or files	4 (4.7%)	5 (5.9%)	76 (89.4%)
Risk of clicking on unknown e-mail links	2 (2.4%)	5 (6.0%)	77 (91.6%)
Risk of e-mailing passwords	2 (2.4%)	1 (1.2%)	81 (96.5%)
Regularly backup important files	22 (26.2%)	20 (23.8%)	42 (50.0%)
Risk of e-mail attachments	26 (30.6%)	24 (28.2%)	35 (41.2%)
Smartphone viruses	12 (14.3%)	27 (32.1%)	45 (53.6%)
Need of an anti-virus program for smart phones	26 (29.4%)	40 (47.1%)	18 (21.2%)
Knowledge of strong password characteristics	3 (3.5%)	10 (11.8%)	72 (84.7%)
Use different passwords	18 (21.2%)	14 (16.5%)	53 (62.4%)
Change passwords regularly	35 (41.1%)	22 (25.9%)	28 (33.0%)

*Number of responses may not add to 85 because of no responses on some items.

personal information because they come to school, live social lives in shared housing without appropriate security measures (Better Business Bureau, 2012). As a result, college students are susceptible to friendly fraud which means fraud perpetrated by people known to the victim such as a roommate who may steal credit card information, credit card statements, or negligently thrown away credit card offers.

Also, it seems students do not change passwords regularly unless they are required to do so. About 71% of students have up to five passwords (mode is three passwords), and about half (58.1%) memorize their passwords. Students with up to five passwords most likely memorize their passwords while students with more than five passwords tend to write down their passwords ($\chi^2 = 11.293$, df $= 2$, $p = .023$). This finding confirms the previous study (Adams & Sasse, 1999) that if users have more than five passwords, they cannot remember their passwords effectively. Many students (61.7%) memorized their passwords while 36% of students recall their passwords by memorization and write them down somewhere. Writing down passwords could compromise their secrecy (Paans & Herschberg, 1987), and people tend to keep their written passwords in an insecure location (Corbitt, 1997). Thus, it is good practice for students to reduce the number of passwords or use meaningful passwords so that they can memorize them instead of writing them down. A meaningful password means a password that has special meaning to the person but not to others, such as a combination of family members' name and date of birth.

Descriptive statistics of the survey results of students' attitudes and perceptions toward the information security topics are listed in Table 1. In the questionnaire, these topics used a 5-item Likert scale converted into three categories of agree, neutral, and disagree for reporting purposes. As expected, most students are well aware of the importance of anti-virus programs, updating virus definitions, personal firewalls, pop-up blockers, and strong password characteristics. They are also well aware of the dangers of P2P file sharing, downloading programs or files, clicking on e-mail links, and e-mailing passwords.

As Table 1 shows, regardless of training participation, students do not consider some security topics important. Those are, in order of high percentage, encrypting important files (88.8%), anti-virus program for smartphones (76.5%), changing passwords regularly (67%), risk of e-mail attachments (58.8%), installing patches when

available (51.2%), and regularly backing up important files (50%). Surprisingly, students do not fully understand the risk of opening e-mail attachments such as 33.6% of them consider it is safe even though it is well known that e-mail attachments may cause serious damage to computer systems and flies. Students seemed apprehensive about downloading files but not opening e-mail attachments, possibly because students usually receive e-mail attachments only from reliable sources such as instructors or school officials. Even though most of these topics do not have a significant relationship with security training statistically, it is important that a university understands what topics students need to learn more about to reach an acceptable level of security awareness. For example, currently students are fully understand the importance of some security topics such as the risk of e-mailing passwords (96.5%) or the risk of clicking on unknown e-mail links (91.6%) even though they do not consider some issues important such as encrypting important files (21.2%) or changing password regularly (33.0%). It is recommended that a university assess students understanding of information security awareness regularly to develop more effective security training specifically designed for students.

One interesting finding is the majority of the students (62 out of 85, 71.8%) understand the importance and need for information security training, but about two-thirds (68.2%) did not have security training at the university or at work. Among students who claimed they had information security training (27 students out of 85, 31.8%), more than half took classes (14 out of 27), 4 students said they had information security training workshop (other than class) at the university, and 9 students had training at work. Since many students learn security in class, it is desirable to offer a course (i.e., MIS course) or one class session in a required course for first-year students because knowing security topics in junior or senior years may be too late to protect students' systems effectively. If an information security course cannot be offered in the first year, a university could offer a security workshop instead. It seemed that not many students realized that the university offers security training for students, or they were reluctant to participate for several reasons such as overlapped classes. Whatever the reason, if security training for students is offered, a university should provide easy-to-access training sessions and make it mandatory training for all students by requiring it when registering for other courses because simply offering a security program is not worth anything at all.

CONCLUSIONS

Technology has advanced to protect users from cyber threats, but technology alone cannot protect end users' information and systems effectively (Okenyi & Owens, 2007). End users need to learn security concepts and controls to maintain a safe environment. It seems that students learn information security in multiple sources including classes, work, friends, and others. As a result, regardless of training participation, undergraduate students in a business college have similar attitudes toward information security. Because a security awareness program is a critical element to creating and maintaining security-positive behavior (Kruger & Kearney, 2006), universities should provide students with more opportunities for security training or courses that cover security controls. Courses that discuss information security should include practical how-to information security details to protect students' systems and information, instead of simply covering theoretical concepts. Learning theories and concepts of information security without knowing useful practical details does not work effectively against real world cyber threats.

It is recommended that information security training be offered during the students' first semester in college. It may be a workshop during the incoming students' orientation or one class session of a required course for all first-year students. To develop the contents of training to fit students' needs, a university should assess students' understanding of information security awareness topics. Without having an assessment, training could be a one-size-fits-all approach, but that may not be effective and may be less attractive to students.

Security training could be offered online as video clips or in other virtual formats. However, universities need to carefully monitor if students actually implement and follow what they learn. To monitor students' information security activities, a university can regularly survey its students or analyze hard data such as an information security incident reports, a help desk log file, hardware repair reports, or others.

This study was limited to the undergraduate students in a business college in New England. It would be desirable to expand it for a bigger student population to minimize the geographical limitations. This study focused on the information security issues in everyday computer use. If a student encounters a specific situation, for example, e-business transactions, there could be additional security issues to consider.

REFERENCES

Adams, A., and Sasse, M. A. (1999). Users are not the enemy. Communications of the ACM, 42(12), 41–46.

Antonacopoulou, E. P. (2006). The relationship between individual and organizational learning: New evidence from managerial learning practices. Management Learning, 37(4), 455–473.

Baldwin, T. T., and Ford, J. K. (1988). Transfer of training: A review and directions for future research. Personnel Psychology, 41, 63–105.

Better Business Bureau (BBB). (2012, August). College-age adults at higher risk of falling victim to identity theft. Retrieved from http://upstatesc.bbb.org/article/college-age-adults-at-higher-risk-of-falling-victim-to-identity-theft-36477

Bureau of Justice Statistics. (n.d.). Cybercrime. Retrieved from http://bjs.ojp.usdoj.gov/index.cfm?ty=tp&tid=41

Calluzzo, V. J., and Cante, C. J. (2004). Ethics in information technology and software use. Journal of Business Ethics, 51(3), 301–312.

Ceraolo, J.P. (1996). Penetration testing through social engineering. Information Systems Security, 4(4), 37–48.

Corbitt, T. (1997). Ensure your datafiles are secure even if the Pentagon's are not. Management Services, 41(5), 24–26.

CSI. (2011). 15th annual edition of the CSI computer crime and security survey. New York, NY: Computer Security Institute. Retrieved from https://cours.etsmtl.ca/log619/documents/divers/CSIsurvey2010.pdf

CSI/FBI. (2007). CSI survey 2007: The 12th Annual Computer Crime and Security Survey. New York, NY: Computer Security Institute. Retrieved from http://gocsi.com/sites/default/files/uploads/2007_CSI_Survey_full-color_no%20marks.indd_.pdf

Data Breach Investigation Report (DBIR). 2011. Verizon. Retrieved from http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf

Dimensional Research. (2011). The risk of social engineering on information security: A survey of IT professionals. Retrieved from http://www.checkpoint.com/press/downloads/social-engineering-survey.pdf

Ernst & Young's Global Information Security Survey. (2004). Retrieved from http://trygstad.rice.iit.edu:8000/Articles/2004GlobalInformationSecuritySurvey-Ernst&Young.pdf

Ernst & Young's Global Information Security Survey. (2008). Retrieved from http://www2.eycom.ch/publications/items/giss_2008/2008_EY_GISS.pdf

Ford, J. K., and Weissbein, D. A. (1997). Transfer of training: An updated review and analysis. Performance Improvement Quarterly, 10(2), 22–41.

Gordon, L. A., Loeb, M. P., Lucyshyn, W., and Richardson, R. (2005). CSI/FBI computer crime and security survey. New York, NY: Computer Security Institute. Retrieved from https://gocsi.com/sites/default/files/uploads/FBI2005.pdf

Green, K. C. (2010). Campus computing 2010: The 21st national survey of computing and information technology in U.S. higher education. The Campus Computing Project. Retrieved from http://www.campuscomputing.net\

Hansche, S. (2001, January/February). Designing a security awareness program: Part 1. Information Systems Security, 14–22.

Identity Theft Resource Center (ITRC). (2010). Identity theft: The aftermath 2009. Retrieved from http://www.idtheftcenter.org/artman2/uploads/1/Aftermath_2009_20100520_1.pdf

Information Security Forum. (2002). Effective security awareness workshop report. London, England: Author. Retrieved from https://gocsi.com/sites/default/files/uploads/FBI2005.pdf

Ingerman, B. L., and Yang, C. (2011, May/June). Top 10 IT issues 2011. Educause Review, 26–40.

Internet Crime Complaint Center. (2011). IC3 2011 Internet Crime Report. Retrieved from http://www.ic3.gov/media/annualreport/2011_ic3report.pdf

Javelin Strategy & Research. (2012). 2012 identity fraud industry report: Social media and mobile forming the new fraud frontier. Pleasanton, CA: Author.

Kaiser, H. F. (1958). The Varimax criterion for analytic rotation in factor analysis. Psychometrika, 23(3), 187–200.

King, S. B., King, M., and Rothwell, W. J. (2001). The complete guide to training delivery. New York, NY: AMACOM: A Division of American Management Association.

Kruger, H. A., and Kearney, W. D. (2006). A prototype for assessing information security awareness. Computers & Security, 25(4), 289–296.

Mitnick, K., & Simon, W. L. (2002). The art of deception: Controlling the human element of security. New York, NY: John Wiley & Sons.

National Institute of Standards and Technology (NIST). (1995). An introduction to computer security. The NIST handbook (NIST SP 800-12). Washington, DC: U.S. Department of Commerce.

National Institute of Standards and Technology. (NIST) (1998). Information technology training requirements: A role- and performance-based model (NIST Special Publication 800-16). Washington, DC: U.S. Department of Commerce.

National Institute of Standards and Technology (NIST). (2003). Building an information technology security awareness and training program (NIST SP 800-50). Washington, DC: U.S. Department of Commerce.

Nunnally, J. C. (1978). Psychometric theory, 2nd ed. New York, NY: McGraw-Hill.

OECD. (2002). OECD guidelines for the security of information systems and networks: Towards a culture of security. Paris, France: OECD Publications. Retrieved from http://www.oecd.org/sti/ieconomy/15582260.pdf

Okenyi, P. O., and Owens, T. J. (2007). On the anatomy of human hacking. Information Systems Security, 16, 302–314.

Paans, R., and Herschberg, I. S. (1987). Computer security: The long road ahead. Computers & Security, 6(5), 404–416.

Puhakainen, P., and Siponen, M. T. (2010). Improving employees' compliance through information systems security training: An action research study. MIS Quarterly, 34(4), 757–778.

Ruighaver, A. B., Maynard, S. B., and Chang, S. (2007). Organizational security culture: Extending the end-user perspective. Computers & Security, 26(1), 56–62.

Schectman, J. (2013, January 24). CIOs make tough calls on the cost of cyber security. CIO Journal. The Wall Street Journal. Retrieved from http://online.wsj.com/public/page/cio-journal.html

Sherif, J. S., Ayers, R., and Dearmond, T. G. (2003). Intrusion detection: The art and the practice. Information Management and Computer Security, 11(4), 175–186.

Siponen, M.T. (2000). A conceptual foundation for organizational information security awareness. Information Management and Computer Security, 8(1), 31–41.

Stolovitch, H. D. (2000). Human performance technology; research and theory to practice. Performance Improvement, 39(4), 7–16.

Straub, D. W., and Welke, R. J. (1998). Coping with systems risk: Security planning models for management decision making. MIS Quarterly, 22(4), 441–464.

von Solms, B., and von Solms, R. (2004). The 10 deadly sins of information security management. Computers & Security, 23, 371–376.

Whitman, M. E. (2003). Enemy at the gate: Threats to information security. Communications of the ACM, 46(8), 91–95.

Wood, C. C. (2002). The human firewall manifesto. Computer Security Journal, 18(1), 15–18.

Workman, M. (2007). Gaining access with social engineering: An empirical study of the threat. Information Systems Security, 16, 315–331.

Workman, M., Bommer, W. H., and Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. Computers in Human Behavior, 24(6), 2799–2816.

BIOGRAPHY

Eyong B. Kim is an Associate Professor of Management Information Systems at the Barney School of Business at University of Hartford. His research interests

include information security, e-commerce, and online education. He has published papers in *Communications of the ACM, Decision Sciences, Decision Sciences Journal of Innovative Education, Journal of Operational Research Society, OMEGA: The International Journal of Management Science* and others.

APPENDIX. INFORMATION SECURITY TOPICS IN THE SURVEY QUESTIONNAIRE

Need of information security training
Need of an anti-virus program
Need to update virus definitions
Regularly scan computer(s), storage device(s), and e-mail
Installing and enabling a personal firewall
Installing software patches whenever available
Use browser-enabled pop-up blockers
Risk of peer-to-peer file sharing
Risk of downloading programs or files
Risk of clicking on unknown e-mail links
Risk of e-mailing passwords
Regularly backup important files
Risk of e-mail attachments
Smartphone viruses
Need of an anti-virus program for smart phones
Strong password characteristics
Use different passwords
Change passwords regularly
Change default password when installing devices
Encrypting important files