ISSN: 2167-1435
v29 n1904

Information Security Education Relationships on Incidents and Preventions: Cyber Assurance Literacy Needs

Garry L. White
gw06@txstate.edu
Department of CIS & QM
Texas State University – San Marcos
San Marcos, Tx 78666

Abstract

Educational institutions are the step for defense through training and educating (Mensch & Wilkie, 2011). The role of education in information security is to reduce risk, reduce incidents, and increase preventive actions. But does education decrease security incidents of being a victim and increase preventive actions? Nothing was found in the literature that shows education will lower the number of security incidents of being a victim. The purpose of this paper is to determine if security incidents can be lowered by education. Findings showed that education does increase preventative behavior and is unrelated to the number of security incidents. An interesting find was the more preventative behavior, the more security incidents occurred. The discussion section explores the possible whys. Since this study used college students, a\future study is needed to use a general population.

Keywords: Security education, security incidents, preventive behavior, security literacy.

1. INTRODUCTION

Criminals are moving faster than the development of technology that ensures security (Luo & Liao, 2007). These criminals target people (i.e. phishing, Trojan Horse, social engineering) and technology (i.e. digital files, systems, hardware through malware and denial of service attacks). Today, there is no perimeter to protect, and it is difficult to know where the hacker is (White, 2010). Firewalls have become less effective over the years. Hackers have learned how to by-pass firewalls (i.e. e-mail with malicious attachments).

Countries and businesses require information security and assurance in order to operate (Ku et. al., 2009). This is a global issue. Many countries recognize this. Taiwan has a national information security policy (Ku et. al., 2009) The United Arab Emirates recognized the need for security awareness in higher education (Rezuli & Marks, 2008). A research paper from South Africa argues that education is critical for information security (Futcher et. al., 2010). Romania, Qatar and the United Kingdom see a need for education on phishing (Al-Hamar, et. al., 2011; Lungu & Tabusca, 2010). How can this global issue be addressed? Education?

The focus must be on the whole global system that crosses national boundaries. New strategies, policies, regulations, and techniques need to be developed and implemented by corporations, governments, and private multi-national organizations, to provide global assurance – the confidence the global computer systems are secure (White, 2010).

However, the problem with assuring a secure Internet system is globalization; different laws, different cultures, and different law enforcement effectiveness. The Internet does not recognize judicial boundaries. Technologies, corporations,

law enforcement, and governments may be impractical due to these differences.

The best technical solution is physical security; be detached from the Internet/Cloud. Yet, this approach would destroy the globalization of our economies. Technology is not enough (Okenyi & Owens, 2007). To have secure global information system requires more than just technology and international laws.

Security is a people issue (Rezui & Marks, 2008). These global issues are people issues. And people are the weakest link in security (Kirkpatrick, 2006; Mitnick, 2002). The best solution maybe to make people the strongest link in global information security/assurance. But how can this be accomplished? Global education? The purpose of this study is to determine the value of education towards security incidents and preventions so users will have the confidence the system is secure.

2. LITERATURE REVIEW

In our society, there is a need for better information security awareness (Mensch & Wilkie, 2011; Okenyi & Owens, 2007). As pointed out earlier, the United Arab Emirates recognized the need for security awareness in higher education (Rezuli & Marks, 2008). South Africa considers education as critical for information security (Futcher et. al., 2010). Romania, Qatar and the United Kingdom see a need for education on phishing (Al-Hamar, et. al., 2011; Lungu & Tabusca, 2010). This need is global.

However, many colleges and universities lack such training in the curriculum (Rotvoid & Landry, 2007). And they have the second highest rate of security incidents (Siegel, 2008). College students have poor security behaviors and use of computer security tools (Mensch & Wilkie, 2011), and have poor awareness of information security issues (McQuade, 2007). Information security awareness is needed in higher education (Rezui & Marks, 2008) as well in school grades K-12.

User security education, awareness, and training are important to organizations (Dodge, et al., 2007; Schultz, 2004). This "need" has been stressed over the years since 1984 (Gage, 1996; Grau, 1984). At first, there was a lack of enforcement of policy and standards involving security education, awareness and training in companies (Gage, 1996). In the 1990's, education and training increased fraud prevention (Brown, 1990). By 2000, corporations recognized the need to get people motivated in the area of information security (Siponen, 2000). Today, most business organizations do conduct security awareness training to address policy, procedures, and tools (Peltier, 2005; Rotvoid & Landry, 2007; Ku et. al., 2009).

Is education the best solution for this global problem? Many believe education will lower security breaches and incidents (Ballard, 2010; Brown, Jan 1990; Kieke, 2006). Education was found to deter information systems misuse (D'Arcy et al., 2009). But does education prevent being a victim of an attack by a hacker?

Here is another example that supports education. A new problem was ransomware. It encrypts user files and then demands payment (Luo & Liao, 2007). Most ransomware infections came from a user's lack of attention on unknown e-mail attachment, or careless browsing and download from a malware embedded Web page. The best countermeasure for this malware is awareness education (Luo & Liao, 2007).

Good policy/procedure/regulations on education and awareness countermeasures will "prevent" rasomware (Luo & Liao, 2007). So the solution to lower security breaches is to create security education policies for users (Kieke, 2006). However, users must constantly be reminded to be aware of security issues (Peltier, 2005). An educational program must continually keep users aware; be proactive.

Education for users is more prevention as described above with rasomware; do not open e-mail attachments. Awareness training develops a state of mine and culture to be alert. Such activates provides the assurance we are secured. Educational institutions around the globe need to provide information security awareness, training, and education (Piazza, 2006). Or should they?

Education does change behavior towards preventive or avoid misuse (Albrechtsen & Hovden, 2010; D'Arcy et al, 2009; Kruger et. al., 2010). Educated and aware users can minimize risks and result in a safer environment because of these changes in behavior (Greenberg, 1986; Kirkpatrick, 2006). But does

ISSN: 2167-1435
v29 n1904

this lower the number of security incidents; be a victim of an attack by a hacker?

Educational institutions are the step for defense through training and educating (Mensch & Wilkie, 2011). Does education from educational institutions decrease security incidents and increase preventive actions? Unfortunately, higher education ranked second with security instances in 2007, just behind government entities (Siegel, 2008). Literature did show education did increase preventive actions and decreased misuse. But nothing was found in the literature that shows education will lower the number of being a victim of a hacker.

The purpose of this paper is to determine if security incidents can be lowered by education. Incident is defined as being a victim of a hacker. For example, exposure to a phishing e-mail is considered an incident if the user acts on it. The following seven hypotheses were developed:

Hypothesis:

Incident

H1: There is an inverse relationship between the number of general computer information courses and user security incidents.

H2: There is an inverse relationship between the number of security information courses and user security incidents.

H3 There is an inverse relationship between the number of security information presentations and user security incidents.

Prevent

H4: There is a positive relationship between the number of computer information education and user protective actions.

H5: There is a positive relationship between the number of security information courses and user protective actions.

H6: There is a positive relationship between the number of security information presentations and user protective actions

Incident & Prevent

H7: There is an inverse relationship between incidents and preventive actions.

3. METHOD

A survey was distributed to 96 undergraduate business students at a central Texas university. The survey composed of 3 questions of education background, 6 questions for incidents experienced by the subject, and 6 questions for preventive behavior by the subject. See Appendix A. SPSS was used to determine data reliability and correlations between the variables.

An incident score was created by adding the choice values from the incident items. Choice values of an incident item were increased frequencies of an incident. A preventive score was created by adding the choice values from the preventive items. Choice values of a preventive item were increased frequencies of an action. The exception was the last preventive item dealing with passwords. Choice values were based on increased complexity of the password.

Validation and Reliability of survey:

The Cronbach's Alpha shows if the survey respondents have different opinions rather than being confused or have multiple interpretations. There is internal consistency. The Alphas were .683 for Preventive and .631 for Incidents. Although the reliabilities of respondents having different opinions are questionable (<.700), the Friedman's Tests showed the responses were not random (Incident Chi-Square 170.804, $p < .001$, and Preventive Chi-Square 122.631, $p < .001$).

To determine if factor analyses were to be used, Kaiser-Meyer-Olkin Measure of Sampling Adequacy and Bartlett's Test of Sphericity were performed. Since both KMOs were greater than .5 (Incident: KMO .645, Chi-Square 70.483; Preventive: KMO .712, Chi-Square 100.602) and both Bartlett's Tests were significant ($p < .001$), a strong relationship among variables existed supporting the use of a factor analysis.

Factor analyses were used to determine if the Incident and Preventive items were related to a single or multiple components. In doing the factor analysis, the Varimax method was used to ensure factors were uncorrelated. The Scree Plot and Rotated Component Matrix indicated two components for each score; the Incident score and the Preventive score. The two components for each score, accounted for the majority of the score's variance (54% Incident & 58% Preventive). See Appendix B.

Incident score:

The factor analysis for the Incident score was appropriate (Bartlett's Test, $p < .001$). This very low Bartlett's p value result shows the robust and the profound effect with only 6 Incident items. The factors extracted accounted for a fare/middling amount of variance (54%).

Prevent score:

The factor analysis for the Prevent score was appropriate (Bartlett's Test, $p < .001$). This very low Bartlett's p value result shows the robust and the profound effect with only 6 Preventive items. The factors extracted accounted for a fare/middling amount of variance (58%).

4. RESULTS

Even though the data had questionable reliability, there were significant correlations between all three education items and preventive score. The computer education and preventive score were significant at $p< .05$. The security education items (courses or presentations) and preventive score were significant at $p<.01$, much more pronounced than the computer education. Hypotheses #4, #5, and #6 are supported; there is a relationship between education and preventive behavior. There were no relationships between education and incidents. The null hypotheses of #1, #2, and #3 were not rejected; education has no relationship with security incidents.

There was a strong correlation between the number of security courses and security presentations ($r=.551$, $p < .001$). This was expected since both involved security learning. A surprise was the relationship between preventive and incidents; the more preventive behavior, the more security incidents ($r=.202$, $p<.048$).

5. DISCUSSION

Kabay (2005) made suggestions for enhancing security education; develop a social culture of information security through education. Educated and aware users can minimize the risks (Kirkpatrick, 2006). But will this lower incidents? The common belief is that education can address security issues, hence, lower security incidents and increase confidence in the system. Research has shown that education does change user behavior; more preventative behavior. However, the literature, as well as this study, shows no relationship between education and security incidents. Why? And this study showed the more preventive behavior of a user, the more security incidents experienced by the user. Study suggests risks increases due to preventive behavior. Why?

Here are four post-hoc explanations, as to why education does nothing to lower security incidents and why preventative behavior increases security incidents. 1) Education can overcome security fears (Lungu & Tabusca, 2010), therefore, be less vigilant. 2) Education can increase confidence in dealing with security, therefore, willingness to take more risks with the computer. 3) With more education, the user is more able to detect/recognize an attack. 4) The more time spent on the computer results with more opportunities for a zero-day attack. These explanations serve as the bases for control variables in future research.

Security is a people issue (Rezui & Marks, 2008). People cause the problem. Can technology be the cure? Maybe technology needs to focus on prevention to lower incidents and education needs to focus on backup, detect, incident response, recovery, and contingency planning. Users need to know what to do when attacked. The user is the last layer of defense.

Implications for information technology educators

Generally, education focused on users follow preventive activities with system administrators focused on detection and response through technology (firewalls, IDS, and operating system's registry adjustments). It is the system administrator that deals with such attacks as a denial-of-service attack. Because this study showed that education did nothing to decrease security incidents and preventive behavior increased security incidents, a change in policies and practices maybe in order; reverse what the focuses are. Users become more educated with detection and response, while system administrators use technology to prevent attacks.

There is now evidence of needs and benefits as to what to stress in assurance literacy. State legislators are encouraged to mandate cyber/information security literacy in the schools' curriculum as to how to deal with incidents. Detection, incident response,

recovery, and continuity planning must be the focus.

Information security needs to be a critical cross-field outcome in curriculum due to globalization (Futcher et. al., 2010). Information security needs to be a core competency for the broader IT student since information is part of everyday life (Futcher et. al., 2010). All organizations (schools, corporations, government, and military) need to be proactive (Allison & DeBlois, 2008) on this issue of global assurance. Policies are needed that require awareness, training, and education in cyber assurance, especially with incidents. Worldwide acceptance of these suggestions will provide a global culture of preventive, detect, respond, and recover actions.

Limitations and future research

College students were used. They had greater exposure to education and new technologies. Continued research of this topic will need a more generic sample of users from the general population. A larger sample may show better reliability and/or detect a significant small negative relationship between education and incidents. The four post-hoc explanations serve as the bases for control variables in future research to better explain findings of this research paper.

6. CONCLUSION

Global assurance can only be accomplished by people. After all, security is a management/people issue. However, governments and laws are not the solution to lowering incidents. Education leads to more protective behaviors. At the same time, there is increased ability to identify an attack, but unfortunately, an increased exposure to zero-day attacks. Technology needs to be used to lower incidents with education used to detect, respond, and recover.

One of the author's graduate student indicated there is a need to anticipate attacks and defend from attack. And it is not clear where the enemy is. Security is a strategic issue (White, 2010). Although people are the weakest link in security, people are best solution to global assurance.

All organizations (schools, corporations, government, and military) need to be proactive (Allison & DeBlois, 2008) on this issue of global assurance. Policies are needed that require awareness, training, and education in cyber security. Along with preventive education, cyber security education needs to stress backup, incident response, recovery, and contingency planning. The user will experience an attack no matter how much security education the user has.

7. REFERENCES

Albrechtsen, E. & Hovden, J. (2010). Improving information security awareness and behavior through dialogue, participation and collective reflection. An intervention study. Computers & Security, 29(4), 432.

Al-Hamar, M. & Dawson, R. & Al-Hamar, J. (2011). The need for education on phishing: a survey comparison of the UK and Qatar. Campus-Wide Information Systems, 28(5), 308-319.

Allison, D. H., & DeBlois, P.B. (2008). Top 10 IT issues 2008. Education Review, 43(3), 1622-1629.

Brown, C.P. (Jan 1990). Crimes of the Vault. Security Management 34(1), 31.

Chen, C. C. & Shaw, R. S. & Yang, S.C. (2006). Mitigating information security risks by increasing user security awareness: A case study of an information security awareness system. Information Technology, Learning, and Performance Journal; 24(1), 1-14.

Chen, C. C. & Medlin, B. D. & Shaw, R. S. (2008). A cross-cultural investigation of situational information security awareness programs. Information Management & Computer Security, 16(4), 360-376.

D'Arcy, J. & Hovav, A. & Galletta, D. (Mar 2009). User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach. Information Systems Research 20(1), 79-98, 155, 157.

Dodge, R. C. & Carver, C. & Ferguson, A. (2007). Phishing for user security awareness. Computers & Security, 26(1), 73.

Futcher, L. & Schroder, C. & Rossouw S. (2010). Information security education in South

Africa. Information Management & Computer Security, 18(5), 366-374.

Gage, D. (1996). Companies need more security training programs, study finds. Info World Canada, 21(3), 24-25.

Grau, J. (1984). Security Education: Something to Think About. Security Management, 28(10), 24.

Greenberg, M. (1986). Security Awareness + Effective Training = Safer Schools. Security Management, 30(8), 47.

Kabay, M.E. (2005). Improving Information Assurance Education Key to Improving Security Management. Journal of Network and Systems Management, 13(3), 247-251.

Kieke, R. L. (2006). Survey shows high number of organizations suffered security breach in past year. Journal of Health Care Compliance, 8(5), 49-50, 67-68.

Kirkpatrick, J. (2006). Protect your business against dangerous information leaks. Machine Design, 78(3), 66.

Kruger, H. & Drevin, L. & Steyn, T. (2010). A vocabulary test to assess information security awareness. Information Management & Computer Security, 18(5), 316-327.

Ku, C.Y. & Chang, Y.W. & Yen, D. D, (2009). National Information Security Policy and its Implementation: A case study in Taiwan. Telecommunications Policy, 33(7), 371.

Lungu, I. & Tabusca, A. (2010). Optimizing anti-phishing solutions based on user awareness, education and the use of the latest web security solutions. Infromatica Economica, 14(2), 27-36.

Luo, X. & Liao, Q. (2007). Awareness Education as the key to Ransomware Prevention. Information Security Journal, 16(4), 195-202.

McQuade, S. C., (2007). We must educate young people about cybercrime before they start college. Chronicle of Higher Education, 53(18), B29-B31.

Mensch, S. & Wilkie, L. (2011). Information security activities of college students: an exploratory study. Academy of Information and Management Sciences Journal, 14(2), 91-116.

Mitnick, K. (2002). The Art of Deception. John Wiley & sons, Hoboken, NJ. (p. 3).

Okenyi, P.O. & Owens, T. J., (2007). On the anatomy of human hacking. Information Systems Secuirty, 16, 302-314.

Peltier, T. (2005). Implementing an information security awareness program. EDPACS, 33(1), 1-18.

Piazza, P. (2006). Security goes to school. Security Management, 50(12), 46.

Rezui, Y. & Marks, A. (2008). Information security awareness in higher education: An exploratory study. Computers & Security, 27(7/8), 241.

Rose, L. (2004). Information Security: A Difficult Balance. EDUCASE Review, 39(5), 10-11.

Rotvoid, G. & Landry, R. (2007). Status of security awareness in business organizations and colleges of business: an alnaysis of training and education, policies, and social engineering testing. Dissertation, Univeristy of North Dakota.

Schultz, E. (2004). Security training and awareness – fitting a square peg in a round hole. Computers & Security, 23, 1-2.

Siegel, P.M. (2008). Data breaches in higher education: from concern to action. EDUCAUSE Review, 43(1), 72.

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

White, G. (2010). "The Evolution and Implementation of Global Assurance." Issues in Information Systems, 11(1), 35-40. (Also appears in PROCEEDINGS of the International Association for Computer Information Systems, Las Vegas, NV, October 6-9, 2010).

ISSN: 2167-1435
v29 n1904

Appendix A: Survey

A study of Education, Incidents, and Preventions: Computer Information Security

Education -- For the past five (5) years

1. How many semesters of computer courses have you taken? (a high school course of a year counts as two semesters). 1. _____

2. How many semesters of computer/information security have you taken? 2. _____

3. How many presentations (not courses) on computer/information security have you attended? This "can" include training from your employer or attending a session at a conference. 3. _____

Incidents -- For the past five (5) years

4. Victim from ID theft 4. _____
   1) Never 2) At least once
   3) 2 to 3 times 4) or more

5. Computer problems due to viruses 5. _____
   1) Never 2) At least once
   3) 2 to 3 times 4) or more

6. Victim of phishing 6. _____
   1) Never 2) At least once
   3) 2 to 3 times 4) or more

7. Victim of denial of service attack 7. _____
   1) Never 2) At least once
   3) 2 to 3 times 4) or more

8. Fallen to a hoax e-mail 8. _____
   1) Never 2) At least once
   3) 2 to 3 times 4) or more

9. How many times did you have some type of privacy problem with social networks? 9. _____
   1) Never 2) At least once
   3) 2 to 3 times 4) or more

Preventions -- For the past five (5) years

10. How many times did you upgrade your anti-virus software? 10. _____
    1) Never 2) At least once
    3) 2 to 3 times 4) or more

11. How many times did you increase the security settings of your web browser? 11. _____
    1) Never 2) At least once
    3) 2 to 3 times 4) or more

12. How many times did you increase the privacy settings (cookies) of your web browser? 12. _____
    1) Never 2) At least once
    3) 2 to 3 times 4) or more

13. How many times have you re-configured your privacy settings with a social network like Facebook? 13. _____
    1) Never 2) At least once
    3) 2 to 3 times 4) or more

14. How many times did you encrypt your data on your computer? 14. _____
    1) Never 2) At least once
    3) 2 to 3 times 4) or more

15. Which best describes your password. 15. _____
    1) a simple word or number (i.e birthdate)
    2) a word with one or more numbers
    3) a phrase using letters
    4) a phrase using letters and numbers
    5) a phrase using letters and numbers and special characters

Appendix B: Factor Analysis

Incident score: Extraction Method: Principal Component Analysis. Rotation Method: Varimax with Kaiser Normalization

Total Variance Explained for Incident Score

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	2.126	35.428	35.428	2.126	35.428	35.428	1.734	28.900	28.900
2	1.114	18.569	53.997	1.114	18.569	53.997	1.506	25.098	53.997

Rotated Component Matrix[a]

	Component	
	1	2
I-04	.045	**.463**
I-05	**.679**	.300
I-06	.034	**.859**
I-07	**.786**	-.099
I-08	.242	**.641**

ISSN: 2167-1435
v29 n1904

I-09	**.770**	.210

Prevent score: Extraction Method: Principal Component Analysis. Rotation Method: Varimax with Kaiser Normalization. Rotation converged in 3 iterations.

Total Variance Explained for Prevent Score

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	2.398	39.971	39.971	2.398	39.971	39.971	1.824	30.392	30.392
2	1.095	18.249	58.220	1.095	18.249	58.220	1.670	27.828	58.220

Rotated Component Matrix[a]

	Component	
	1	2
P-10	**.762**	.064
P-11	**.616**	.574
P-12	.326	**.744**
P-13	**.513**	.263
P-14	-.127	**.844**
P-15	**.691**	-.038

Appendix C: Correlations

		Sec Sem	Sec Pres	Incident Score	Prevent Score
Com Sem	Pearson Correlation	.045	.151	-.055	.255*
	Sig. (2-tailed)	.663	.142	.594	.012
	N	96	96	96	96
Sec Sem	Pearson Correlation		.551**	.018	.266**
	Sig. (2-tailed)		.000	.863	.009
	N		96	96	96
Sec Pres	Pearson Correlation			-.112	.284**
	Sig. (2-tailed)			.276	.005
	N			96	96
Incident Score	Pearson Correlation				.202*
	Sig. (2-tailed)				.048
	N				96

*. Correlation is significant at the 0.05 level (2-tailed).

ISSN: 2167-1435
v29 n1904

**. Correlation is significant at the 0.01 level (2-tailed).