Faculty and Staff Information Security Awareness and Behavior

Johnathan Yerby
Johnathan.Yerby@mga.edu

Kevin Floyd
Kevin.Floyd@mga.edu

Middle Georgia State University
School of Information Technology
100 University Parkway, Macon, GA 31206

Abstract - The purpose of this study was to determine the information security awareness and behaviors that faculty and staff report. A sample of 321 participants consisting of 164 faculty and 157 staff members from a public, state university located in the Southeastern United States. The results indicate that overall, faculty and staff had high to moderate levels of information security awareness and behaviors. An independent samples t-test found that there was no significant difference in security awareness, but there were four behaviors differences between faculty and staff. Participants that reported higher levels of security policy awareness demonstrated significantly more secure behaviors in ten of the 18 items measured. Given these findings, comprehensive security awareness training will be essential for institutions of higher education as a means of minimizing threats to information technology resources.

Keywords

Security, awareness, behavior, policy, training

1 INTRODUCTION

The purpose of this research was to study security awareness and behaviors amongst faculty and staff in a university. Generally, people think of financial institutions, healthcare, services, retail, and credit card processors as the most attractive targets for hackers. Colleges and universities are a less obvious, but very data-rich targets. Universities gather vast amounts of personally identifiable information that is replenished frequently and many institutions store pieces of information in multiple silos which end up being managed by multiple departments. The volume of data, the access to many different sources of data by many staff, faculty, part-time employees, student workers, and contractors creates a huge threat to securing information. The decentralization of access, usage, and storage of data creates chaos, duplication, lax security controls, and opportunities for potential attackers.

On a college campus, the technology infrastructure is made up of many different computer systems and applications. It is common for users to have access to many different systems and users do not always follow positive security protocols. These different platforms have potential to be exploited or have information sharing that may lead to a violation of compliance policies such as the Family Educational Rights and Privacy Act of 1974 (FERPA), which protects the privacy of student records [16]. FERPA requires that students are notified of their rights to their educational records, but does not mandate any annual or regular training requirements for the custodians of the educational records. Several higher education institutions fall under multiple compliance and security requirements which increases the burden of the type of information that they are responsible for as well as adhering to the laws and requirements [45]. Most American education institutions have not started to prepare for global regulations such as the General Data Protection Regulation (GDPR). The complex European privacy law creates yet another issue of chaos, confusion, and information security challenges.

Faculty and staff transition between special committees and different roles within the organization. Data security permissions are assigned based on roles, rules, groups, and users. The nature of work results in security exceptions, which lead to permissions beyond what is required for an employee's responsibilities. Educational institutions are facing the same hackers that are attempting to break into the FBI, Google, or Equifax, but they often have a much smaller budget and staff to manage the myriad of systems, users, group, roles, and rules [6]. Following a string of breaches on a single institution, the University of Maryland, President, testified before the Senate Commerce, Science & Transportation Committee, to proclaim "Security in a university is very different than the private sector because we are an open institution. There are many points of access because it is all about the free exchange of information" [7]. Information security training, awareness, and behavior monitoring are not always the top priority for education institutions. The faculty and staff that facilitate the business of the institution are often focused on their role within the institution and security is perceived as the job of the IT people. The IT staff are working on security to the extent that they have support to do so.

2 LITERATURE REVIEW

2.1 Security Awareness

Security awareness is a broad term that has been widely defined by the research literature [3]. Security awareness is an important element of every organization since the employee human factor is often the weakest link [35]. Siponen (2000) described security awareness as one's knowledge of security threats and the countermeasures that can be used to prevent such threats [41]. More specifically, Siponen (2000) further explained that security awareness is a "state where users in an organization are aware of and ideally committed to their security mission (often expressed as in end-user security guidelines" (p. 31) [43]. Dinev and Hu (2007) later defined security awareness as an increased consciousness of security related issues that threaten important technology assets [15]. Security awareness is essential and should be considered a primary pillar of security for any technology driven organization to prevent major security breaches [12].

A key component of security awareness is the human element or the employees within an organization [14]. The security of technology resources within the work place is largely dependent on employee behavior and it is imperative that organizations take steps to enhance users' perceptions of practicing security best practices [35]. Abawajy (2014) stated that many security breaches are the result of user ignorance and careless behaviors when sharing passwords and opening unknown email attachments. Employees are typically not aware of the consequences to themselves or the organization when security breaches occur. A primary goal of security awareness within the organization is to heighten the importance of security best practices and make users aware of the consequences associated with security infractions failures [19]. While employees can be considered the weakness link in information security, those who follow and comply with security polices, rules, regulations, and best practices are the key to strengthening the organization's information security infrastructure [8]. The lack of security awareness leads to ignorance, negligence, apathy, mischief, and resistance which are the root of user behaviors that lead to IT security related vulnerabilities and loss [37].

2.2 Security Behaviors

While technology solutions are available to detect and prevent security vulnerabilities, software and hardware solutions alone are not enough since employee behaviors represent the greatest threat to effective security [20]. According to an IBM report, 55% of all security breaches were due to employee related actions and 95% of those incidents were due to human error [25]. Similarly, a 2014 UK report indicated that 31% of the worst security breaches were the result of human error and 20% were caused by deliberate employee misuse of technology systems [1]. End user security behaviors have become a topic of increasing research as a means of protecting organizational assets since technology-based deterrents are often not enough to protect against malicious attacks [4].

Many factors influence cyber security behaviors. Research conducted by Herath and Rao (2009) [21] found that security behaviors can be influenced by both intrinsic and extrinsic motivators. Peer and environmental pressures influence employee security behaviors. Intrinsic motivation of employee perceived effectiveness of their actions was also found to play an important role in security policy compliance intentions. Chan, Woon, and Kankanhalli (2014) [10] reported that management practices, supervisory practices, and co-worker's socialization were found to be positively related to employees' perception of information security climate in the organization. Perception of security climate and self-efficacy had positive impacts on compliant behavior. McCormac et al. (2017) [32] concluded that conscientiousness, agreeableness, emotional stability, and risk-taking propensity significantly explained differences in end user's security behaviors. Drawing from Social Bond Theory [22], Safar et al. (2015) [37] reported that knowledge sharing, collaboration, intervention, and experience had a significant impact on users' attitudes toward compliance with information security policies.

2.3 Security Incidents in Higher Education

In recent years, security breaches have become commonplace at institutions of higher education. In 2014 the University of Maryland had a breach of over 309,000 records which included social security numbers, dates of birth, and university ID numbers [49]. In 2015 the University of Maryland notified 288,000 students, faculty, and staff that their personal information was breached, then a month later they were breached again [36].

A 2017 report found that a prominent Russian hacker recently breached 63 high profile government agencies including 24 U.S. universities, listed in Table 1, ten universities in the U.K. and one in India [47]. The University of Maryland was amongst the new list of the Russian hacker's latest exploits. In the Identity Theft Resource Center's 2017 report there were multiple companies or colleges that had more than one single breach in the past year [26].

In 2014 the Identity Theft Resource Center reported 57 incidents and in 2017 they cataloged 127 breaches accounting for 1,418,258 records affected [26]. In March of 2018 the U.S. government charged nine Iranian hackers with a massive

31 terabytes breach of 144 U.S. universities and more than $3 billion in stolen intellectual property [18]. Clearly, academic institutions are attractive targets with a great deal of potential threats. According to Roman (2015), experts recommend ramping up cyber security education for faculty, staff, and students, implementing stronger defenses, and instituting security behaviors such as destructing sensitive data [13]. The people interacting with, storing, transmitting, and generating student educational records can be a weak point in security. The human component plays an important role in reducing security risks by increasing their information security awareness and taking responsibility for their behaviors [30].

Information security training and awareness takes resources of some type. At a minimum, it takes the time for the end users to be trained since focusing solely on creating a security or acceptable use policy does not solve training, awareness, or behavior issues [50].

Table 1
U.S. University Victims

Cornell University	University of the Cumberlands
Virginia Tech	Oregon College of Oriental Medicine
University of Maryland	Humboldt State University
University of Pittsburgh	University of N. Carolina Greensboro
New York University	University of Mount Olive
Rice University	Michigan State University

Table 1
U.S. University Victims

University of CA, Los Angeles	Rochester Institute of Technology
Eden Theological Seminary	St. Cloud State University
NC State University	University of Arizona
Purdue University	University at Buffalo
Atlantic Cape Community College	University of Washington

Colleges and universities have large amounts of personally identifiable data that would be an attractive target for hackers. Information is used by faculty and staff from several different systems to complete the work on the institution. Information security training has been shown to decrease the chance and cost of a data breach [34]. This research sought out to understand the information security awareness and behaviors at a university in the Southeastern United States by administering a survey. The results of the study will provide a mean score for security awareness for both faculty and staff, as well as individual items that could be classified as awareness or behavior. The results of the study provided an understanding of security awareness and behaviors. Implications of the findings are presented in this paper. The research questions that this study answered were:

RQ1: What information security awareness and behaviors do faculty and staff report?

RQ2: What differences are there between faculty and staff reported security awareness and behavior?

RQ3: What differences are there between users that are aware and unaware of security policies?

3 METHODS

The purpose of this study was to gain an understanding of security awareness, behavior and determine differences between faculty and staff. Respondents were not given instructions or primers prior to participating in the study, which helped the study to measure existing security awareness and behavior before any treatment. All faculty and staff in a teaching university in Southeastern United States were invited to participate in the 20-question survey. Questions 1-2 collected demographic data and questions 3-20 used a 5-point Likert scale to measure awareness and behaviors. The survey was adapted using a previously published study examining university security awareness and behaviors [29]. On question 18 participants indicated if they had read and understood policies regarding computing. The group that answered agree of strongly agree were considered the "aware group" and the respondents that answered disagree or strongly disagree were classified as unaware of security policies and considered the "unaware group". The Cronbach's alpha level was calculated using questions 3-20 to test the reliability of the single-items in the instrument [17]. Four items (Questions 14-17) on the survey were reverse scored. The reverse scored items were presented together and all focused on revealing passwords.

Two invitations to participate were sent to 604 staff e-mail addresses and 748 faculty (including adjuncts) e-mail addresses. The survey was administered by sending a link to an online survey [48]. Data collection lasted for two weeks. There were 351 total responses. Data was screened and any results missing one or more responses was deleted, using the SPSS N-missing function, resulting in a sample size of n=321. Faculty accounted for 164 (51.09%) respondents and staff accounted for 157 (48.91%) responses. The "aware group" accounted for 201 (53.41%) and unaware accounted for 116 (36.6%) responses.

The responses on the survey included strongly agree, agree, disagree, strongly disagree, and not applicable. Surveys with not applicable as a potential response can be analyzed using hot deck imputation, a tendency score, or treating N/A responses as missing data per response [23]. For this study the researchers determined that responses where individuals selected not applicable were transformed and treated as missing for statistical analysis so that it did not affect the results. One item resulted in as few as 89 responses and some items with the full 321 responses. The N/A responses did not conflate the results or mean score for individual items or the overall security and awareness score.

The researchers used SPSS to calculate descriptive statistics. In addition to descriptive statistics, researchers compared two different groups, faculty and staff, plus "policy aware" and "policy unaware" users, as grouping variables to conduct independent samples t-tests for 18 individual items (Q3-Q20) and a means comparison for each group. The overall security awareness and behavior scores were calculated using the means function. Results are presented in the following section.

4 RESULTS

The responses consisted of 164 faculty and 157 staff members. Most participants (257) worked in an office with a door that could be locked, 42 worked in a shared office, and 22 participants worked in a cubicle. The Cronbach's alpha for the 18 items related to security behavior was .794 and a .799 based on standardized items. No items needed to be deleted. Table 2 summarizes the nine items that participants scored highly in, six that had moderate levels of secure behaviors and two with lower levels.

	Question		N	Mean	Sig. 2-tail		N	Mean	Sig. 2-tail
3	I work in my own office, and lock it during the workday, even when leaving for just a few minutes.	Aware	167	3.31	0.429	Faculty	149	3.65	*0.000
		Unaware	107	3.17		Staff	128	2.80	
4	I work in my own office, and always lock it when I leave at the end of the workday.	Aware	174	4.61	0.819	Faculty	148	4.85	*0.000
		Unaware	107	4.58		Staff	136	4.33	
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.	Aware	57	3.40	0.780	Faculty	29	3.59	0.324
		Unaware	27	3.30		Staff	56	3.21	
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.	Aware	62	4.13	0.111	Faculty	28	4.18	0.393
		Unaware	26	3.54		Staff	61	3.87	

	Question		N	Mean	Sig. 2-tail		N	Mean	Sig. 2-tail
7	I always lock my computer during the workday when I leave my workstation for more than 5 minutes.	Aware	185	3.51	*0.000	Faculty	153	3.02	0.115
		Unaware	113	2.61		Staff	148	3.30	
8	I always turn off or lock my computer when I leave my workstation at the end of the workday.	Aware	188	4.29	*0.003	Faculty	155	3.91	*0.022
		Unaware	113	3.79		Staff	150	4.29	
9	I always close confidential web pages or files as soon as I am done working or viewing them.	Aware	190	4.52	*0.000	Faculty	161	4.34	0.998
		Unaware	114	4.04		Staff	146	4.34	
10	Using the anti-virus program loaded on my PC, I execute an anti-virus scan of my	Aware	177	2.59	*0.000	Faculty	152	2.24	0.816
		Unaware	107	1.73		Staff	135	2.28	

	Question		N	Mean	Sig. 2-tail		N	Mean	Sig. 2-tail
	computer at least once per week.								
11	I never open an attachment to an e-mail unless it comes from a trusted source.	Aware	200	4.61	*0.000	Faculty	164	4.54	0.691
		Unaware	116	4.40		Staff	156	4.51	
12	The date on my PC is backed up at least once per week	Aware	179	2.97	*0.000	Faculty	152	2.55	0.232
		Unaware	106	2.11		Staff	135	2.76	
13	I understand what a strong password is, and always employ one when accessing any of MGA's secure web-sites (Banner, One USG Connect)	Aware	201	4.68	*0.000	Faculty	164	4.54	0.859
		Unaware	115	4.32		Staff	156	4.56	
14		Aware	194	4.50	0.337	Faculty	156	4.54	0.160

	Question		N	Mean	Sig. 2-tail		N	Mean	Sig. 2-tail
	On occasion (e.g. when going on vacation), I have revealed my computer password(s) to an MGA site to my supervisor or co-workers.	Unaware	112	4.38		Staff	154	4.38	
15	On occasion I have revealed my computer password(s) to an MGA site in an e-mail message.	Aware	199	4.77	0.111	Faculty	161	4.72	0.873
		Unaware	115	4.64		Staff	157	4.73	
16	On occasion, I have revealed my computer password(s) to an MGA site on a survey or questionnaire.	Aware	198	4.86	0.140	Faculty	160	4.81	0.527
		Unaware	115	4.77		Staff	157	4.85	
17		Aware	198	4.82	0.681	Faculty	161	4.82	0.765

	Question		N	Mean	Sig. 2-tail		N	Mean	Sig. 2-tail
	On occasion I have revealed my computer password(s) to an MGA site to someone who has contacted me telephonically and asked for my password.	Unaware	115	4.79		Staff	156	4.80	
18	I understand what a password - protected screen saver is.	Aware	199	4.20	*0.000	Faculty	163	4.02	0.447
		Unaware	115	3.59		Staff	156	3.91	
19	I always use a password - protected screen - saver on my PC.	Aware	185	3.43	*0.000	Faculty	150	2.97	0.266
		Unaware	107	2.46		Staff	145	3.17	
20	I have read and understand the various policies regarding computing at MGA as posted	Aware	201	4.35	*0.000	Faculty	162	3.19	*0.012
		Unaware	116	1.70		Staff	155	3.57	

	Question		**N**	**Mean**	**Sig. 2-tail**		**N**	**Mean**	**Sig. 2-tail**
	by The Office of Technology Resources on their website.								
	Overall Security Behavior		321	3.08		Faculty	164	3.08	0.977
						Staff	157	3.08	

Table 2 - Means, Awarness t-test, and Faculty Staff t-test

Items 4, 8, 9, 11, and 13-17 reported positive security behaviors with overall mean score above 4. Survey items 14-17 were good to discover highly secure behaviors since these dealt with revealing passwords, although items 14 and 15 had nine individuals that either agreed or strongly agreed and 3 respondents for items 16 and 17. Items 3, 5, 6, 7, 18, and 19 had an overall mean between 3 and 4, which would indicate moderately secure behavior. Items 10 and 12 dealt with executing antivirus weekly and backing up the machine weekly, these two items had means of 2.26 and 2.65. The two lower security behaviors were not overly concerning since these procedures are not typically managed by end-users.

After analyzing the descriptive statistics, the researchers conducted an independent samples t-test to address research question two, examining differences between faculty and staff.

Overall, the total average security awareness and behavior scores were not significantly different between faculty (M = 3.081, SD =.501) and staff (M=3.083, SD = .517), p = .977. Table 2 shows that four of the 18 items did significantly differ between faculty and staff. First, when leaving the office for just a few minutes, faculty were significantly more likely to lock the door (M = 3.65, SD =1.39) than staff (M=2.80, SD = 1.43), t (275) = 5.00, p < .01.

Second, when leaving at the end of the work day, faculty were significantly more likely to lock the door (M= 4.85, SD=0.64) than staff (M=4.33, SD=1.32), t (282) = 4.29, p < .01. Next, when leaving at the end of the work day, staff were significantly more likely to turn off or lock their computer (M=4.29, SD = 1.30) than faculty (M=3.91, SD=1.54), t (303) = -2.31, p<.05. Finally, staff were significantly more likely to read computing policies posted on the institution's website (M=3.57, SD=1.25) than faculty (M=3.19, SD=1.44), t (315) = -2.52, p <.01.

Lastly, to answer the third research question, an independent samples t-test uncovered ten of the 18 items were significantly different between groups that were aware of security policies versus those that reported disagreeing or strongly disagreeing that they had read and understood policies. The results shown in Table 2, revealed that the "aware group," which indicated that they were aware of the security policies, demonstrated more desirable security behaviors than the group that was classified as "unaware". Differences in security behaviors included locking their computer when stepping away or at the end of the day, closing confidential information as soon as they have finished using systems, not opening unknown emails, backing up data, understanding strong passwords, and use of password protected screen saver.

5 CONCLUSION

The purpose of this study was to determine what information security awareness and behaviors that faculty and staff report. While overall, there was no significant difference in security awareness and behavior between faculty and staff, there were nine areas in which participants scored highly in, six that had moderate levels of secure behaviors and two with lower levels. Faculty and staff demonstrated different security behaviors as two different groups. Neither of the groups were mandated to complete an information security awareness training. Both groups had access to the university's security policies, but staff were more likely than faculty to read the policies. Those staff who responded as more aware of security policies demonstrated more desirable security behaviors. Institutions cannot simply advise staff to be aware of security policies and practices. Effective awareness training is a result of engagement through training in which the end users' awareness is increased and users across the organization realize that security is everyone's responsibility [20].

Security awareness training will be essential for institutions of higher education as a means of minimizing threats to information technology resources. Comprehensive training must go beyond simply making policies and best practices available on the institution's website [39]. Having information or policies available, but not investing time to train, support, and inform the users is only slightly better than not having a policy. Institutions must commit to creating, purchasing, or subscribing to training resources. To ensure security of the many systems accessed by people across the university requires an investment in time. There are free resources tailored specifically to higher education such as the higher education information security council (HEISC) supported by EDUCAUSE [5]. Other institutions have reported success with security training through creating courses [28]. If training is not meaningful, it is essentially a ruse to protect an organization from legal action. [24]. If training is truly an institutional concern or priority, the institution must insure that the information is understandable, memorable, and that it is followed [45]. Given the human factor associated with security awareness and behaviors, Human Resources must take a lead role in rolling out training programs [37]. To remain effective, programs must undergo periodic evaluation and should be updated to address new and emerging security threats [19].

This study found an opportunity to increase security awareness which should hopefully lead to more secure behaviors. Limitations of this study include behaviors and awareness being self-reported from a convenience sample at a single institution in the Southeastern United States. The generalizability may vary, especially depending on the culture of placing importance on information security. Future research should include applying some sort of treatment, training, or increased awareness and then comparing the changes based on types of treatments to make users behave more securely to protect the many information systems that they have access to. Future work will seek to develop a solution to improve security behaviors amongst faculty and staff. Some behaviors such as not running your own backup may be tolerable, but revealing passwords or opening untrusted e-mail attachments could be detrimental if even one person exhibits poor security behavior. The instrument in this survey was based on a previously published study that defined desirable secure behaviors. Future research may also seek to revise this instrument to ensure that the measured behaviors are truly the most important behaviors for faculty and staff of educational institutions. As new policies and investments in training are made, the institutions should evaluate the findings of this study, prioritize information security behaviors, and tailor a solution to meet their needs. There are many similarities amongst higher education institutions such as the type of data managed, the software and systems, and the roles of individuals accessing the valuable information. Universities will continue to be an attractive target for hackers, one method to deter and mitigate threats involves increasing awareness and encouraging secure behaviors.

REFERENCES

[1] 2015 Information Security Breaches Survey. Retrieved February 26, 2018 from: https://www.pwc.co.uk/assets/pdf/2015-isbs-technical-report-blue-03.pdf

[2] Abawajy, J. (2014). User preference of cyber security awareness delivery methods. *Behaviour & Information Technology*, 33(3), 237-248.

[3] Aloul, F. (2012). The need for effective information security awareness. *Journal of Advances in Information Technology*, 3(3), 176-183.

[4] Australian Standard, ISO/IEC 27002. (2015). *Information technology – security techniques – code of practice for information security controls, (AS ISO/IEC 27002:2015).* Standards Australia.

[5] Awareness Campaigns. (2018). Retrieved from https://www.educause.edu/focus-areas-and-initiatives/policy-and-security/cybersecurity-program/awareness-campaigns

[6] Bishop, M. (2002). Computer security education: training, scholarship, and research. *Computer*, 35(4), 31-30. doi:10.1109/MC.2002.1012429

[7] Bracy, J. (2014). UMaryland President: Breach would have bankrupted many institutions. Retrieved from https://iapp.org/news/a/umaryland-president-breach-would-have-bankrupted-many-institutions/

[8] Bulgurcu, B., Cavusoglu, H., Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security practices. *MIS Quarterly*, 34(3), 523-548.

[9] Campagna, R. (2018). Threats to information security in K-12. Retrieved from https://www.csoonline.com/article/3258797/education/threats-to-information-security-in-k-12.html

[10] Chan, M., Woon, I., & Kankanhalli. (2014). Perceptions of information security in the work place: Linking information security climate to compliant behavior. *Journal of Information Privacy and Security*, 1(3), 18-41.

[11] Dahbur, K., Isleem, M.R. (2012). A study of information security issues and measures in Jordan. *International Management Review Journal*, 8(2), 71-82.

[12] Dahbur, K., Bashabsheh, Z., Bashabsheh, D. (2017). Assessment of security awareness: A qualitative and quantitative study. *International Management Review*, 13(1), 37-55.

[13] Day of Cyber. (2018). Retrieved from www.nsadayofcyber.com

[14] Desman B. M. (2003, Jan-Feb), The ten commandments of information security awareness training. *Information Systems Security*, 39-44

[15] Dinev, T., & Hu, Q. (2007). The centrality of awareness in the formation of user behavioral intention toward protective information technologies. *Journal of the Association for Information Systems*, 8(7), 386-408.

[16] Family Educational Rights and Privacy Act. (2018). Retrieved from https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

[17] Gliem, J. A. G., Rosemary R. (2003). *Calculating, interpreting, and reporting Cronbach's alpha reliability coefficient for Likert-type scales*. Paper presented at the Midwest Research-to-Practice Conference in Adult, Continuing, and Community Education, Columbus, OH.

[18] Graff, G. (March23, 2018). DOJ indicts 9 Iranians for brazen cyberattacks against 144 us universities. Retrieved from https://www.wired.com/story/iran-cyberattacks-us-universities-indictment/

[19] Hanshe, S. (2001, Jan-Feb). Designing a security awareness plan: Part I. *Information Systems Security*, 14-22.

[20] Hanus, B. & Wu, Y. (2016). Impact of users' security awareness on desktop security behavior: A protection motivation theory perspective. *Information Systems Management*, 33(1), 2-16.

[21] Herath, T., & Rao, H. (2009). Protection motivation and deterrence: A framework for security policy compliance in organizations. European *Journal of Information Systems*, 18(2), 106-125.

[22] Hirschi, T. (1969). Causes of Delinquency. Berkeley: University of California Press.

[23] Holman, R., Glas, C. A. W., Lindeboom, R., Zwinderman, A. H., & de Haan, R. J. (2004). Practical methods for dealing with 'not applicable' item responses in the AMC Linear Disability Score project. *Health and Quality of Life Outcomes*, 2(1), 29. doi:10.1186/1477-7525-2-29

[24] Horton, W. (2011). *E-learning by design* (2 ed.). San Francisco, CA: John Wiley and Sons.

[25] IBM 2015 Cyber Security Intelligence Index. (2015). Retrieved March 1, 2018 from: https://essextec.com/wp-content/uploads/2015/09/IBM-2015-Cyber-Security-Intelligence-Index_FULL-REPORT.pdf

[26] Identity Theft Resource Center and CyberScout. (2018). 2017 *Annual Data Breach Year-End Review*. Retrieved from

https://www.idtheftcenter.org/images/breach/2017Breaches/2017AnnualDataBreachYearEndReview.pdf

[27] Identity Theft Resource Center and IDT911. (2014). *Identity Theft Resource Center Breach Report Hits Record High in 2014*. Retrieved from https://www.idtheftcenter.org/ITRC-Surveys-Studies/2014databreaches.html

[28] Information Security Awareness Training. (2018). Retrieved from http://technology.pitt.edu/security/information-security-awareness-training

[29] Katz, F. H. (2005). *The effect of a university information security survey on instruction methods in information security*. Paper presented at the Proceedings of the 2nd annual conference on Information security curriculum development, Kennesaw, Georgia.

[30] Korovessis, P. (2015). *Establishing an information security awareness and culture*. (Doctoral dissertation), Plymouth Electronic Archive and Research Library. Retrieved from http://hdl.handle.net/10026.1/3836

[31] Lebek, B., Uffen, J., Neumann, M., Hohler, B., Breitner, M.H. (2014). Information security awareness and behavior: a theory-based literature review, *Management Research Review*, 37(12), 1049-1092.

[32] McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2017). Individual differences and information security awareness. *Computers in Human Behavior*, 69, 151-156.

[33] Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers & Security*, 42, 165-176.

[34] Ponemon Institute, L. (2017). *Cost of data breach study: global overview*. Retrieved from https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03130WWEN&

[35] Rantos, K., Fysarakis, K., Manafavis, C. (2012). How effective is your security awareness program? An evaluation methodology, *Information Security Journal: A Global Perspective*, 21(6), 328-345.

[36] Roman, J. (2015). Universities: prime breach targets. Retrieved from https://www.databreachtoday.asia/universities-prime-breach-targets-a-7865

[37] Safar, N.S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N.A., Herawan, T. (2015). Information security conscious care behavior formation in organizations. *Computers & Security*, 53, 65-78.

[38] Security Awareness Training. (2018). Retrieved from http://technology.gsu.edu/technology-services/it-services/security/security-awareness-training/

[39] Security Awareness: Middle Georgia State University. (2018). Retrieved from https://www.mga.edu/technology/security-awareness.php

[40] Semer, L. J. (2012, December). Evaluating the employee security awareness program, *Internal Auditor*, 53-56.

[41] Schneier, B. (2000). *Secrets and Lies: Digital security in a networked world*. Indianapolis, IN: Wiley Publishing, Inc.

[42] Shropshire, J., Warkentin, M., Johnston, A., & Schmidt, M. (2006). *Personality and IT security: An application of the five-factor model*. AMCIS 2006 Proceedings, 415.

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

[44] Sipionen, M. (2001). Five dimensions of information security awareness. *Computers & Society*, 31(2), 24-29.

[45] Solove, D. J. (2016). HIPPA Training Requirements: FAQ. Retrieved from https://teachprivacy.com/hipaa-training-requirements/

[46] Stancia, V., Tinca, A. (2016). Students' awareness on information security between own perception and reality – An empirical study. *Accounting and Management Information Systems*, 15(1), 112-130.

[47] Storm, D. (2017). Hacker breached 63 universities and government agencies. *Computer World*.

[48] SurveyMonkey Inc. (2018). Retrieved from www.surveymonkey.com

[49] Svitek, P., & Anderson, N. (2014, February 19, 2014). University of Maryland computer security breach exposes 300,000 records. *The Washington Post*. Retrieved from https://www.washingtonpost.com/local/college-park-shady-grove-campuses-affected-by-university-of-maryland-security-breach/

[50] Yerby, J. (2013). Legal and ethical issues of employee monitoring. *Online Journal of Applied Knowledge Management*, 1(2), 44-55.