Issues in Information Systems
Volume 24, Issue 1, pp. 159-169, 2023

DOI: https://doi.org/10.48009/1_iis_2023_114

Cybersecurity awareness in higher education: a comparative analysis of faculty and staff

Jonathan Hobbs, *Georgia Southwestern State University, jonathan.hobbs@gsw.edu*

Abstract

Cybersecurity protection remains at the forefront of many organizations' information and communication technology strategies and investments. Higher education has become a profitable target for cyber-attacks which has many institutions reevaluating their cybersecurity awareness programs. The purpose of this research was to determine the cybersecurity awareness of faculty and staff at a small institution in the United States to determine if a standard, mandatory security awareness training was effective amongst both groups. The findings of this study can assist leadership in the development of their security awareness programs to effectively educate their employees.

Keywords: cybersecurity awareness, information security, higher education, information security awareness

Introduction

Cybersecurity threats are ever-increasing as rates of data usage and internet consumption continue to increase. In the context of cybersecurity, social engineering has emerged as one of the most difficult threats to combat as it focuses on humans as the weakest security link (Conteh & Schmick, 2016). Social engineering has led to calls for raising security awareness among users to reduce the number of cybersecurity incidents. Effective cyber security awareness training and campaigns burden small universities with their ever-growing costs and time to accomplish the goals of reducing these cyber security incidents.

Higher education has become a profitable target for cyber-attacks with many institutions already suffering from high-impact incidents (Ulven & Wangen, 2021). Education on these attacks through cybersecurity awareness training has shown to be one of the most effective defenses an organization can deploy to combat these advancements in social engineering. Scholars notice that measuring the effectiveness of these programs is becoming more prominent with new research focused on custom delivery of these programs based on employee's position, knowledge of technology, age, etc. (Dash & Ansari, 2022).

The purpose of this study was to examine cybersecurity awareness at a small to medium sized universities in the United States. Can a general "one size fits all" type approach to cybersecurity awareness training be effective for all employees at institutions of this size? As the general costs for these cybersecurity programs grow, how can smaller institutions meet the demand without finding cost-effective solutions? This research aimed to fill in a gap of knowledge of the current effect of cybersecurity awareness programs for social engineering at small institutions based on employee factors, i.e., gender, age, job designation, and education level. This research answered the following research question:

RQ: *To what extent do the levels of each independent variable (Gender, Job Designation, Age, Education Level) relate to variations in the dependent variable (cybersecurity awareness level)?*

Literature Review

The Need for Effective Information Security Awareness

Information security awareness is often overlooked in information security programs. While organizations continually expand and add sophistication to their security technology, very few resources are used to increase the overall security awareness of their normal users. Thus, making them the weakest link in the organization (Aloul, F. A., 2012). Cybercriminals today are putting significant efforts into developing advanced hacking methods to steal information and money from the general public. Limited security awareness training among users makes them an easy target to infiltrate a wide variety of organizations like universities, hospitals, private companies, and government agencies (Aloul, F. A., 2012). Higher educational institutions have many types of sensitive data that lead to them being at higher risk (Yerby & Floyd, 2018). The data housed by the institution can include student records, employee records, university policies, research data, payroll information, along with intellectual property rights by their research departments (Hina & Dominic, 2018). Unlike many other organizations, higher education is organized around a culture of openness, collaboration, transparency, and information sharing. This culture is a key contributor to the sector's security challenges since they contradict typical security frameworks consisting of rigid architecture and centralized governance (Fouad, 2021). The combination of culture, sensitive data, and the complexity of effectively securing this data has led attackers to attack education institutions with ransomware that is capable of exfiltrating data and encrypting users' critical files and data stored on their systems (FBI, 2021).

Increase the Effectiveness of Security Awareness Programs

Knowledge and behavior about good practices concerning information security awareness are often weak based on systems and policies that are poorly designed. Answering questions correctly does not mean it will motivate a user to behave according to knowledge obtained from the awareness program. To enhance future security awareness campaigns, certain factors can help increase the overall effectiveness and decrease the chance of failure (Bada, M. et al., 2019). Do not invoke fear as a tactic to achieve compliance but do keep the material professionally prepared and organized. The education needs to be targeted as something doable for the user and it helps to provide feedback. Once users are ready for change, continuous feedback, and varying types of training or necessary to sustain them through this change period (Bada, M. et al., 2019). To increase the effectiveness of an Information Security Awareness (ISA) program, higher education programs must understand the main purpose of the program of making employees aware of information security policies and how to handle information systems securely (Dhakal, 2018). Dhakal (2018) found institutions must assess their position by answering the following types of questions: "Where are we now? What is the status and current situation of the educational institution? What information security-related incidents is the institution facing? What are the plans and strategies to reduce these security incidents?" before implementing any changes to any awareness programs to better understand the awareness program's effectiveness later.

Factors for Internal Efficiency and External Effectiveness

A cybersecurity awareness program's effectiveness can be measured internally and externally for an organization. Measuring internal efficiency for an organization can consist of endpoint awareness, proactive monitoring of threats and vulnerabilities, security architecture, cyber security governance, and legal and regulatory compliance (Dube & Mohanty, 2022). An effective cybersecurity awareness program is not just based on internal factors but also external factors. An organization can measure business continuity, prevention of data and IPR loss, facilitation of digital transformation, cyber intelligence, and general

cybersecurity awareness as factors to measure their external effectiveness (Dube & Mohanty, 2022). Information security executives should closely monitor policy statements, metrics/goals, training, resource allocation, etc. to integrate internal efficiency and external effectiveness. An understanding of the program's starting point is key and can be benchmarked by the SANS Security Awareness Maturity Model, which was developed to help institutions identify how mature or immature their program is and where that can take it (Almomani, et al., 2021). Evaluating internal and external factors can be tied to this strategic roadmap to understand if an institution's overall level of security awareness is in the range of nonexistent or in a state of a robust metrics framework aligned with the institution's mission to track progress and measure impact (Almomani, et al., 2021).

The Covid-19 Pandemic Impact on Higher Education

Higher education institutions were impacted heavily by the Covid-19 pandemic. A shift to distance learning began in March 2020 to continue the education process. Online learning platforms, cloud computing, and video conferencing shifted from accessories to the education process to the main assets of conducting online studies (Alexei & Alexei, 2021). This increase was reflected in the number of risks of cross-site scripting, DoS (denial of service) / DDoS attacks, unauthorized data access, spoofing, and infection with malicious programs. Higher education institutions had to invest heavily in defending against the larger attack surface due to this e-learning environment. The use of cloud computing through Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) brought the basic services of accessing resources and storing information in the academic environment (Alexei & Alexei, 2021). Along with these technologies, Learning Management Systems (LMSs) and Video conferencing applications became the main sources of communication between higher education institutions and their students. Information about these resources for distance learning could then be exploited by bad actors through the act of spoofing and phishing emails. Attempts to pose as the higher education institution's LMS or as a video conferencing solution like Zoom, Microsoft Teams, and GoToWebinar increased tremendously in efforts to gain access to confidential information from students and faculty during this time (Ulven & Wangen, 2021). Cybersecurity awareness training became more important to educate higher education users on the ability to realize when emails were not legitimate (Ulven & Wangen, 2021).

Social Engineering and Awareness Programs

Seeking to exploit a weakness in human nature and take advantage of the naivety of the average person defines the method of social engineering. The goal of social engineering is often either sabotage to disrupt or corrupt data or theft to obtain information, money, or access (Aldawood & Skinner, 2019). Social engineering threats are dynamic and constantly evolving as an attacker's use of confidence and persuasion can lead a person into behaviors of heightened emotions including anger, curiosity, excitement, or fear. Other traits typically revolve around a sense of urgency in time-sensitive opportunities and trust. Phishing attacks are one of the most common methods attackers use as social engineering that utilize these traits. See Table 1 for types of common phishing attacks and their modes of delivery (Nguyen & Bhatia, 2020).

Techniques that act as countermeasures for social engineering can be human-based or computer-based. Computer-based solutions are typically efficient and accurate but have limitations of being expensive, limited by human awareness, and programmed to be very specific. The human-based approach has the advantage of it being easier to train humans and typically leading to a lower number of victims. But limitations are still relative to human decisions, greed, and influence through human emotions (Hu et al., 2019).

Table 1: Phishing Attacks

Attack	Characteristic/Mode of Delivery
Email phishing	Email with web links, malware attachments, and phone numbers urging user to reply or follow up by other means.
Voice phishing (vishing)	Automated message system or live person speaking with user to increase trust and urgency.
SMS phishing (smishing)	Mobile app or text messages that can include a prompt or web link to follow up via a fraudulent phone number or email.
Angler phishing	Attacker imitates a company's customer service team on social media to intercept communications with the brand and divert the conversation into private messages to advance the attack.
Search engine phishing	Attempts to place links to fake websites high on search engine results using paid ads or legitimate optimization methods of search ranking manipulation.
URL phishing	Links to tempt users into traveling into phishing websites using hidden hyperlinked text, buttons, or deceptively spelled URLs.
In-session phishing	The appearance of an interruption of normal web browsing for a user with fake login pop-ups or FBI threats on pages being currently visited

Many factors can contribute to overcoming the posed challenges of implementing cybersecurity awareness programs against the threats of social engineering. Companies must invest large amounts of money into resources that are both human and computer-based moving forward to combat the ever-growing number of attacks but as these solutions mature and cyber security awareness programs for employees develop a need to educate K-12 students at an early age will become more necessary to minimize the number of victims in the future (Salahdine & Kaabouch, 2019).

Methodology

Subjects and Procedures

A convenient sample consisting of all faculty and staff, who were currently employed at a small university in the southeastern United States was utilized as a part of this study. The university consists of a student body of fewer than 3,500 students with fewer than 400 faculty and staff employees. The sample contains faculty and staff from the University's 4 academic units: College of Arts and Sciences, College of Business and Computing, College of Education, and College of Nursing and Health Sciences. A total of 147 usable surveys were completed including 68 faculty (N=68) and 78 staff (N=78) with a response rate of 54.5%. The anonymous survey was administered via Qualtrics™ upon approval from the university's IRB (Institutional Research Board) and the links to the survey were sent via email.

Instrument

The instrument for this study was adapted from a study by Ng, et al (2009). Questions 1-4 collected demographic data of the employees. This instrument included 10 items, questions 6-15, that define employee behavior that illustrate the use and compliance of security awareness and compliance with the training administered by the institution. A seven-point Likert scale ranging from completely disagree (1) to completely agree (7) was used and the items of the instrument can be found in Appendix A.

Data Analysis

The data were imported into SPSS for processing. The Univariate Analysis of Variances (ANOVA) procedure was conducted to answer the research question. This procedure was used because there are multiple independent variables (i.e., Gender, Job Designation, Age, and Education Level) with one dependent variable (cybersecurity awareness level). The means and standard deviation of the dependent variable are demonstrated with each independent variable using descriptive analyses.

Results

Demographic data was collected and is presented in Table 2. Most of the participants were female with an average age between ages 35-54 (N=75). Having a master's degree or higher represented the largest group based on education level.

Table 2: Demographic Data for Survey Respondents

Characteristic	n	%
Gender		
Male	64	43.8%
Female	82	56.2%
Job		
Faculty	68	46.6%
Staff	78	53.4%
Age		
25-34	29	19.9%
35-44	37	25.3%
45-54	37	25.3%
55-65+	43	29.5%
Education		
Highschool Diploma/GED	12	8.2%
Bachelor's Degree	38	26.0%
Master's Degree or Higher	96	65.8%

Descriptive Analysis

The 10 Likert-style questions were used to measure the overall awareness levels of faculty and staff. The Cronbach's alpha coefficient was calculated to test the reliability of the 10 questions. The items were found to be reliable ($\alpha = .957$) (Sürücü & Maslakci, 2020). Figure 1 shows the descriptive analysis comparing the means of each question for the dependent variable of employee behavior that illustrates the use and compliance of security awareness and compliance with the training administered by the institution. The dependent variable indicated an above-average mean score for all 10 questions.

- Q1 = Before reading an email, I will first check if the subject and the sender make sense (μ=6.27).
- Q2 = Before opening an email attachment, I will first check if the filename of the attachment makes sense (μ=6.25).

- Q3 = I do not open email attachments if the content of the email looks suspicious (μ=6.55).
- Q4 = I exercise caution when I receive an email attachment as it may contain a virus (μ=6.33).
- Q5 = I would never give my personal identification information over email (μ=6.25).
- Q6 = I am concerned about security incidents and try to take action to prevent them (μ=6.21).
- Q7 = I am interested in information about computer security (μ=5.49).
- Q8 = I am constantly mindful of computer security (μ=5.99).
- Q9 = I am confident of recognizing a suspicious email (μ=5.83).
- Q10 = I can recognize a suspicious email attachment even if there is no one around to help me (μ=5.82).

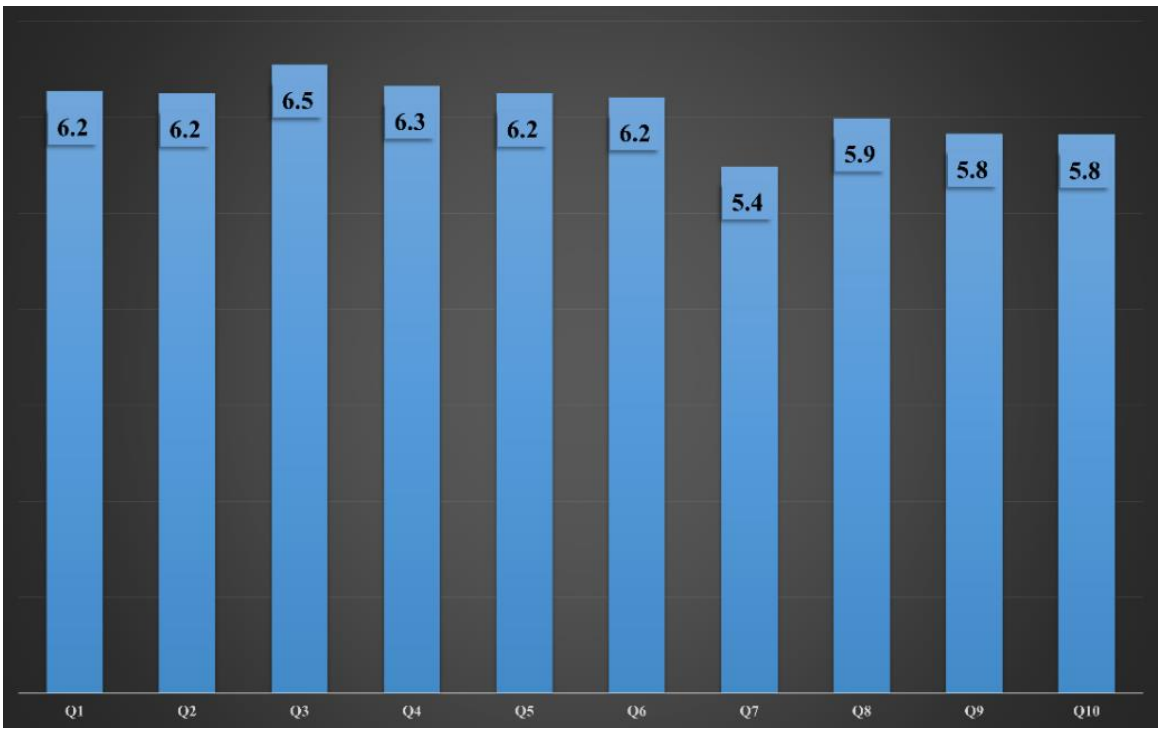

Figure 1: Illustration of Means of the Dependent Variable

Univariate ANOVA

The results of the univariate ANOVA for the dependent variable of cybersecurity awareness and the independent variables of Gender, Job Designation, Age, and Education level are shown in Table 2.

Non-significant Variables

As seen in Table 3, the independent variables of sex, age, and education level are not significant in predicting cybersecurity awareness as their p-values are greater than 0.05. This means there is no statistically significant effect on cybersecurity awareness based on the evidence gathered on sex, age, or education level. However, the age independent variable does come close to the significance level with a p-value of 0.080, indicating a possible trend towards significance.

Significant Variables

As observed in Table 4, the independent variable of job designation had a significant difference on the dependent variable of cybersecurity awareness, indicated by its p-value of 0.014. This suggests that there is evidence that job designation has a statistically significant effect on cybersecurity awareness. Individuals in faculty positions are more likely to have a higher level of cybersecurity awareness compared to those in staff positions.

Table 3: Tests of Between-Subjects Effects

Source	Type III Sum of Squares	df	Mean Square	F	Sig.
Corrected Model	17.176	7	2.454	1.805	.091
Intercept	2058.887	1	2058.887	1514.836	.000
Job Designation	8.403	1	8.403	6.182	**.014***
Sex	.038	1	.038	.028	.867
Age	9.372	3	3.124	2.298	.080
Education Level	4.877	2	2.438	1.794	.170
Error	187.562	138	1.359		
Total	5632.520	146			
Corrected Total	204.739	145			

**Significant at .05 level of significance*

Table 4: Means and Standard Deviations

Job Designation	Mean	JN	Std. Deviation
Faculty	6.278	68	0.7553
Staff	5.940	78	1.452
Sex			
	Mean	N	Std. Deviation
Male	6.134	64	1.123
Female	6.068	82	1.243
Age			
	Mean	N	Std. Deviation
25-34	6.103	29	1.004
35-44	6.311	37	0.474
45-54	5.705	37	1.837
55-65+	6.254	43	1.193
Education Level			
	Mean	N	Std. Deviation
Highschool Diploma/GED	5.923	12	1.583
Bachelor's Degree	6.142	38	1.292
Master's Degree or Higher	6.104	96	1.189

Discussion and Conclusion

The aim of this study was to examine cybersecurity awareness at a small university in the United States. Can a general "one size fits all" type approach to cybersecurity awareness training be effective for all employees at the institution? The research revealed substantial variances in cybersecurity awareness among faculty and staff, indicating that a one-size-fits-all cybersecurity awareness training approach may not be suitable for educational institutions where all employees are required to participate. The findings suggest that personalized training programs tailored to specific job designations could be more effective. Although the sample size was small relative to the size of the institution where the survey was conducted, the study's results are consistent with previous research that emphasizes the importance of measuring the effectiveness of cybersecurity awareness programs using metrics that can be updated continuously to address new threats and vulnerabilities (Aldawood & Skinner, 2019).

Personalized training can be more effective than a one-size-fits-all approach to cybersecurity awareness training (Chowdhury & Gkioulos, 2023). Customized training can help mitigate the risk of employee disengagement, which can occur if the employees feel that the training is irrelevant to their roles or if the training is too advanced or too basic for their needs.

Smaller universities with limited budgets could benefit from personalized cybersecurity awareness training since they typically have fewer resources to allocate to cybersecurity initiatives. An individualized approach could help optimize the use of available resources by focusing on the areas the institution believes are most critical (Chowdhury & Gkioulos, 2023). While this approach may require additional effort and resources to implement, the benefits of such an approach are worth considering.

In future research, the definition of employee roles beyond faculty and staff should be extended, allowing for a more targeted approach at a granular level, such as IT staff, accounting staff, business faculty, etc. The survey instrument used in this study should be refined to ensure that the behaviors being measured are the most relevant to faculty and staff based on their job designations. This study can also be conducted at a larger university to see if the results are similar as the size scales up.

As institutions plan new policies and investments in training, they should consider the study's findings to ensure that their solutions are effective and fiscally responsible. As universities continue to be attractive targets for attackers due to the similarities in data management, user roles, and systems used, it is critical to enhance cybersecurity awareness to mitigate potential attacks.

The results of this study suffer from the limitation of a small sample size based on the overall size of the institution in which it was administered. The convenience sample of employees from this single university may not be representative of the larger population of institutions.

References

Alexei, L. A., & Alexei, A. (2021). Cyber security threat analysis in higher education institutions as a result of distance learning. *International Journal of Scientific and Technology Research*, (3), 128-133.

Aldawood, H., & Skinner, G. (2019). Reviewing cyber security social engineering training and awareness programs—Pitfalls and ongoing issues. *Future Internet*, *11*(3), 73.

Almomani I, Ahmed M, Maglaras L. 2021. Cybersecurity maturity assessment framework for higher education institutions in Saudi Arabia. *PeerJ Computer Science* 7:e703 https://doi.org/10.7717/peerj-cs.703

Aloul, F. A. (2012). The need for effective information security awareness. *Journal of advances in information technology*, *3*(3), 176-183.

Bada, M., Sasse, A. M., & Nurse, J. R. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour?. https://doi.org/10.48550/arXiv.1901.02672

Chapman, J. (2019). *How Safe is Your Data?: Cyber-security in Higher Education* (Vol. 12, pp. 1-6). Oxford, UK: Higher Education Policy Institute.

Chaudhary, S., Gkioulos, V., & Katsikas, S. (2022). Developing metrics to assess the effectiveness of cybersecurity awareness programs. *Journal of Cybersecurity*, *8*(1), tyac006. https://doi.org/10.1093/cybsec/tyac006

Chowdhury, N., & Gkioulos, V. (2023). A personalized learning theory-based cyber-security training exercise. *International Journal of Information Security*, 1-16.

Conteh, N. Y., & Schmick, P. J. (2016). Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks. *International Journal of Advanced Computer Research*, *6*(23), 31. http://dx.doi.org/ 10.19101/IJACR.2016.623006

Dash, B., & Ansari, M. F. (2022). An Effective Cybersecurity Awareness Training Model: First Defense of an Organizational Security Strategy. *Int. Res. J. Eng. Technol*.(IRJET), 9.

Dhakal, R. (2018). Measuring the effectiveness of an information security training and awareness program. *Charles Sturt University*.

Dube, D. P., & Mohanty, R. P. (2022). Application of grounded theory in construction of factors of internal efficiency and external effectiveness of cyber security and developing impact models. *Organizational Cybersecurity Journal: Practice, Process and People*, (ahead-of-print). https://doi.org/10.1108/OCJ-04-2022-0009

FBI. 2021. "Increase in PYSA Ransomware Targeting Education Institutions." https://www.ic3.gov/Media/News/2021/210316.pdf

Fouad, N. S. (2021). Securing higher education against cyberthreats: from an institutional risk to a national policy challenge. *Journal of Cyber Policy*, *6*(2), 137-154.

Hina, S., & Dominic, P. D. D. (2018). Information security policies' compliance: a perspective for higher education institutions. *Journal of Computer Information Systems.*

Hu, Z., Buriachok, V., & Sokolov, V. (2019). Implementation of social engineering attack at institution of higher education. *Available at SSRN 3679106*.

Ng, B. Y., Kankanhalli, A., & Xu, Y. C. (2009). Studying users' computer security behavior: A health belief perspective. *Decision Support Systems*, *46*(4), 815-825. http://130.18.86.27/faculty/warkentin/securitypapers/Merrill/NgEtAl2009_DS46_4_PMTandSecurity.pdf

Nguyen, T., & Bhatia, S. (2020, December). Higher education social engineering attack scenario, awareness & training model. In *Journal of The Colloquium for Information Systems Security Education* (Vol. 8, No. 1, pp. 8-8).

Salahdine, F., & Kaabouch, N. (2019). Social engineering attacks: A survey. *Future Internet*, *11*(4), 89.

Sürücü, L., & MASLAKÇI, A. (2020). Validity and reliability in quantitative research. *Business & Management Studies: An International Journal*, *8*(3), 2694-2726.

Ulven, J. B., & Wangen, G. (2021). A systematic review of cybersecurity risks in higher education. *Future Internet*, 13(2), 39.

Yerby, J. & Floyd, K. (2018). Faculty and Staff Information Security Awareness and Behavior. *Journal of The Colloquium for Information System Security Education (CISSE) 6*. 138-160.

Appendix A

Effect of Cyber Awareness Training Survey

Demographics

1. What is your sex?
2. What is your job designation?
3. What is your age?
4. What is your ethnicity?
5. What is your educational background?

Cybersecurity Awareness Level

1. Before reading an email, I will first check if the subject and the sender make sense.
2. Before opening an email attachment, I will first check if the filename of the attachment makes sense.
3. I do not open email attachments if the content of the email looks suspicious.
4. I exercise caution when I receive an email attachment as it may contain a virus
5. I would never give my personal identification information over email.
6. I am concerned about security incidents and try to take action to prevent them.
7. I am interested in information about computer security.
8. I am constantly mindful of computer security.
9. I am confident of recognizing a suspicious email.
10. I can recognize a suspicious email attachment even if there is no one around to help me.