Perceptions of Information Systems Security Compliance: An Empirical Study in Higher Education Setting

Lei Li
College of Computing and Software Engineering
Kennesaw State University
lli@kennesaw.edu

Yide Shen
Rohrer College of Business
Rowan University
shen@rowan.edu

Meng Han
College of Computing and Software Engineering
Kennesaw State University
mhan9@kennesaw.edu

Abstract

Ensuring information systems security policy compliance is an integral part of the security program of any organization. This paper investigated the perceptions of different stakeholder groups towards information security policy compliance constructs of the Unified Model of Information Security Compliance (UMISPC) [1] in a higher education environment. The research findings showed that faculty/staff generally has higher tendency towards security policy compliance comparing to students in a higher education institution. In addition, students with security knowledge are more incline to have security policy compliance activities. Our finding not only added to the knowledge base of information systems security compliance research, but also offers practical implications.

1. Introduction

The widespread usage of technology has powered the economic growth and innovations in the world for the past decades. A side effect of technology advancements is the exponential increase of cybercrimes. Hacks and data breaches have become daily news and the damages caused by those attacks have risen dramatically. It was estimated that the global loss of cybercrime for 2017 to be around $600 billion and the figure would be increased to $6 trillion per year by 2021 [2]. In addition to monetary losses, cybercrimes could cause severe sociological issues to our society, such as customers' confidence, social trust, and personal safety [3].

It has become increasingly important to protect organizations' digital assets from cyber threats and attacks [4]. Technological approaches themselves are not sufficient in securing information in organizations; more and more studies call attention to the behavioral and social aspects of security solutions [5] [6]. One important component of an organization's security program is the development of information security policies which define a list of guidelines and rules an employee who work with information assets should follow in order to ensure information security in an organization [7] [8] [9]. While effective information security policies are essential to prevent information security attacks and ensure compliance, many studies show that employees generally don't take appropriate actions prescribed in the information security policies and often become the weakest link in information security [8] [10]. Understanding why individuals in organizations engaging in insecure behavior has become a major area in information security research [1] [11]. This also applies to organizations in higher education sector.

However, limited research on information security compliance has been conducted in higher education domain [12]. This body of literature suggests that higher education institutions struggle to apply effective information security management practices and that employees in higher education institution are "the least concerned, motivated, and aware of the potential threats that can harm their personal and work computing environment" [12, p. 209].

In this study, we used the Unified Model of Information Security Compliance (UMISPC) [1] as a guiding model and investigated the different perceptions on information system security compliance related constructs between two pairs of stakeholder groups: (1) university faculty/staff versus students and (2) students with security knowledge versus students without security knowledge.

The rest of the paper is organized as follows. Section two summarizes related studies in information security compliance area. The research design and findings are presented in section three and four, respectively. The contribution and implication of this research are discussed in section five.

URI: https://hdl.handle.net/10125/71371
978-0-9981331-4-0

2. Related Studies

2.1. Information Security Compliance Theories

There is a wealth of literature that investigated information security policy compliance. Drawing theories from related disciplines such as criminology, psychology, social psychology and health psychology, security researchers proposed many different approaches to explain employees' non-compliance behaviors and improve information security policy compliance in the organizations [1] [11].

However, the number of competing theoretical models and inconsistences in reported findings have made it difficult not only for the security scholars to advance their theory-building efforts but also for practitioners to seek guidelines in managing their security policy compliance initiatives [1] [11]. To address this challenge, two recent studies have attempted to synthesize the information security policy compliance research and deliver some clarity to the domain.

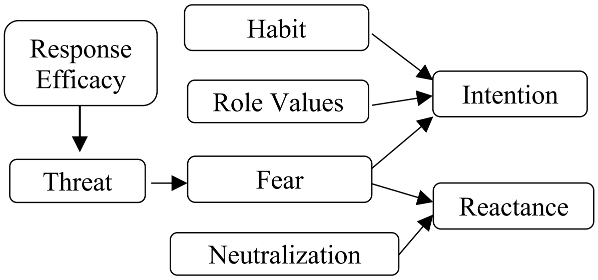

Figure 1. A Unified Model of Information Security Compliance (UMISPC, adopted from Moody et al. [1]).

Cram et al. [11] conducted a meta-analysis of 95 empirical papers in the antecedents to the information security policy compliance. They classified 401 independent variables into 17 distinct categories and analyzed each category's relationship with security policy compliance. Their findings suggested that much of the security policy literature is plagued by suboptimal theoretical framing. Moody et al. [1] took the initiative on developing a unified model for information security compliance. As illustrated in figure one, Moody et al. [1] proposed and tested a unified model of information security compliance (UMISPC), based on their review of 11 established theoretical models on information security policy compliance. The UMISPC [1] is an important step forward in security policy compliance research. However, the generalizability of the model is still to be tested due to its limited empirical validation. Thus, the authors encourage future research to examine whether some of the constructs in the UMISPC are relevant in certain information systems security contexts [1].

2.2. Information Security Compliance in Higher Education

Although there is a rich body of literature on employee information security compliance in general, limited research has been conducted in higher education domain. In their review of information security policy compliance literature, Hina and Dominic [12] found that only a few studies have focused on higher education institutions. Findings from these studies suggest that higher education institutions struggle to apply effective information security management practices and that employees in higher education institutions are "the least concerned, motivated, and aware of the potential threats that can harm their personal and work computing environment" [12, p. 209]. Chan and Mubarak [13] found that information security awareness level among employees of a South Australian higher education institution is generally lacking. IT department respondents from Ismail et al.'s [14] study of four Malaysian higher education institutions also reported that faculties and students were the least informed of information systems policies in their organizations

We argue that when studying information security compliance in higher education domain, researchers need to take into consideration two different stakeholder groups: faculty/staff and students. Faculty and staff are employees of higher education institutions and they share very different characteristics with students, who are often considered "customers" of higher education institutions. As employees of higher education institutions, faculty and staff are more committed to their institutions than students. Research has shown that higher levels of organizational commitment are reported to be positively associated with productive technology security behaviors and negatively associated with counterproductive technology security behaviors [15]. In addition, although both faculty/staff and students use information technologies frequently in their daily lives on and off campus, students generally lack formal information systems security trainings [16] [17]. Research found that college students are most vulnerable to phishing attacks [18] and young adults are more likely to share passwords with others and use weak passwords, as compared with other age groups [19].

Within the student population, we believe that students with information systems security knowledge will differ from students with no security knowledge, in terms of information system security compliance related perceptions. It is reported that people with various levels of information security knowledge have different mental models of cyber security and experienced people are expected to make better cyber security related decisions than inexperienced ones [20]. Ben-Asher and Gonzalez [21] also found that cyber security knowledge helps in detecting malicious events.

To answer the call of more information security compliance research in higher education domain [12] and more research in the applicability of UMISPC constructs in various information systems security context [1], this study aims to examine the different perceptions of information system security compliance related constructs between two pairs of stakeholder groups. More specifically, we use the UMISPC [1] as a guiding model and investigate the two research questions below:

Research question 1: will faculty/staff and students differ in their perceptions of information system security compliance related constructs?
Research question 2: will students with security knowledge versus students without security knowledge differ in their perceptions of information system security compliance related constructs?

3. Research Design

We designed an empirical study to investigate the two research questions. A web-based survey was developed to collect data which includes three segments: 1) demographic information; 2) role of the participant (faculty/staff/student); 3) a security policy scenario in which the participants were asked to assume a role and answer a list of related questions.

Adopting Siponen and Vance [22]'s approach, we used the scenario approach instead of self-reporting to capture participants' secure or insecure acts. To ensure the scenario's applicability and authenticity to higher education domain, it was developed by the authors and two security professionals who work at the cybersecurity office of the participating university. We also made sure that the scenario is easy to understand for all participants and the action in the scenario is reasonable. The scenario used in the survey is listed as follows.

"Bob, a staff member in a large public university, needs to access to data for his work that are classified as confidential (Social Security Numbers and Dates of Birth), while traveling. He realizes that storing on OneDrive or some other cloud service (Box, Dropbox, etc.) is explicitly against policy. The easiest way to facilitate this would be to use a USB thumb drive. Bob plan to store the confidential data in a USB drive and will keep the USB with him all the time".

After reading the scenario, participants were asked to answer a list of questions related to UMISPC constructs (Table 1), which were adopted from Woody et al. [1]. For each question, participants were asked to indicate their opinion on the statements associated with the scenario using a 7-point scale: strongly disagree - 1, disagree - 2, somewhat disagree - 3, neither agree or disagree - 4, somewhat agree - 5, agree – 6, strongly agree – 7.

Table 1. Questions to Measure UMISPC Constructs

UMISPC Construct	Survey Statement
Response Efficacy	If I were to do the opposite of what Bob did, IS security breaches would be minimal.
Threat	An information security breach in my organization would be a serious problem for me.
Fear	Any problems that result from acting like Bob did will go away with time.
Habit	Complying with Information Security policies is something I do frequently.
Role Value	What Bob did can be justified due to the nature of Bob's work.
Neutralization	It is not as wrong to violate company information security procedures that require too much time to comply with.
Reactance	Problems resulting from acting like bob did are overly exaggerated.
Intention	I would act in the same way as the scenario describes.

The survey participants were recruited from a large public university in the southeast of United States. The web-based survey was distributed to the university community through daily university newsletter to faculty, staff and students in a two-week period. The survey link was included in the newsletter once in week one, and then reappeared in the newsletter on week two as reminder. The survey is totally voluntary and anonymous. To encourage participation, the participants will be entered into a random drawing a $10 Starbucks gift card (40 available). Participants who wish to enter the gift card drawing can click a link at the end of the survey and enter their contact information in a separate survey.

To analyze the data, we run t-test on the faculty/staff versus students, students with security knowledge versus students without security knowledge.

4. Research Findings

The survey instrument was distributed to all faculty, staff, and students in the participating university. 339 responses were received, and 133 responses were removed from analysis for either incomplete or completed within 3 minutes or less. Thus, we have 206 valid responses.

Among all valid responses, 32 were faculty/staff and 174 were students. For faculty/staff, 68.75% were 35 years or older. For students, 71.26% were 24 year or younger. The age distribution is consistent with the demographic distribution of the participating university. We run two-sample assuming unequal variances T-test to determine if there is statistical difference between two comparing groups, i.e., faculty/staff versus students and students with security knowledge versus students without security knowledge.

4.1. Faculty/staff versus Students

As shown in Table 2, faculty/staff's perceptions are significantly different from student's perceptions on 6 out of 8 UMISPC model constructs at α = 0.05 level. Among all 6 significant constructs, faculty/staff have indicated higher level of policy compliance tendency. For habit construct, higher value means higher tendency towards security policy compliance. For fear, role value, neutralization, intention and reactance, lower value means higher tendency toward compliance. While there is no significant difference between faculty/staff and student groups for threats and response efficacy, it's worth noting that both faculty/staff and student group recognize the seriousness of security policy violation (threat construct) and understand the complexity in mitigating security breaches with recommended actions (response efficacy construct).

In term of research question 1, faculty/staff's perceptions on information system security compliance related constructs are quite different from those from students. Moreover, faculty/staff generally has indicated higher level of tendency toward policy compliance. Our findings provided a mostly positive answer to our research question 1.

4.2. Students with Security Knowledge versus Students without Security Knowledge

Our second research question is concerned with whether students' information security knowledge level would influence their perceptions on security policy related constructs. In our survey, student who have taken information security related classes are considered as participants with information security knowledge. Table 3 shows the summary of the t-test between the two student groups.

The two comparing groups are significantly different in all UMISPC constructs at α = 0.05 level, except for threat construct. And student with information security knowledge indicated perception of higher level of tendency towards security policy compliance than student without security knowledge. Our findings provided a mostly positive answer to our research question 2.

Table 2. Faculty/Staff and Student Comparison

UMISPC Construct	Faculty/staff	Student	P Value
Response Efficacy	3.63	3.39	0.556
Threat	6.34	5.98	0.143
Fear	1.69	2.47	0.001
Habit	6.66	5.75	0.000
Role Value	2.84	3.70	0.018
Neutralization	1.53	1.97	0.048
Intention	2.84	3.66	0.038
Reactance	2.13	2.68	0.035

Note: the participant of survey will give 1-7 perception value on the statement represents a corresponding construct. The numbers in the "Faculty/staff" and "student" columns are the average values of the group.

Table 3. Student with and without Security Knowledge Comparison

UMISPC Construct	Students with Security Knowledge	Students without Security Knowledge	P Value
Response Efficacy	3.95	3.22	0.04
Threat	6.05	5.96	0.72
Fear	1.95	2.69	0.01
Habit	6.23	5.61	0.00
Role Value	3.00	3.91	0.01
Neutralization	1.53	2.10	0.00
Intention	2.88	3.89	0.00
Reactance	2.53	2.73	0.40

Note: the participant of survey will give 1-7 perception value on the statement represents a corresponding construct. The numbers in the "students with security knowledge" and "students without security knowledge" columns are the average values of the group.

5. Discussion

In this paper, we conducted an empirical research to investigate the perceptions of different stakeholder groups towards information security policy compliance constructs in a higher education environment. Our research answers the call of more information security compliance research in higher education domain [12] and more research in the applicability of UMISPC constructs in various information systems security context [1] This research also offers practical implications for information systems security compliance practitioners.

Based on our study, faculty/staff generally has higher tendency towards security policy compliance, comparing to students in a higher education institution. This is consistent with existing literature that people with higher levels of organizational commitment are more likely to have productive technology security behaviors and less likely to have counterproductive technology security behaviors [15]. In addition, students with security knowledge are more inclined to security policy compliance activities. This is also consistent with prior research that people with technology security knowledge are expected to make better security related decisions [20].

Our finding not only added to the knowledge base of information systems security compliance research, but also offers practical implications. For universities that strive to improve security policy compliance across their campus community, they should put special emphasis to the student population. And educating students more on information security will help with this endeavor.

There are some limitations to this paper. Frist, we use the scenario-based technique to measure participants' security policy compliance perceptions. While the scenario method is widely used by security policy researchers and has been proven to be appropriate [1], such a method only measures the prospective perception of the participants, not their actual behavior. Secondly, a large number of survey responses were removed due to incompleteness or not taking the survey seriously. The number of faculty/staff respondents are relatively small comparing to students. More work needs to be done on the design and administration of the survey.

This research can be expanded in two directions: 1) the study could be repeated in an industry setting to study the perceptions of different stakeholder groups. 2) The study could be re-designed to validate the UMISPC model in a higher education domain. We also can test how the UMISPC model hold up for both faculty/staff and students.

6. Acknowledgement

This research is sponsored by a SunTrust Fellowship grant from the Institute of Cyber Workforce Development from Kennesaw State University.

7. Reference

[1]. Moody, G. D., Siponen, M., & Pahnila, S. (2018). "Toward A Unified Model of Information Security Policy Compliance, " MIS Quarterly, 42(1). (doi: 10.25300/misq/2018/13853)

[2]. Security First. (2019) Why is Cyber Security Important in 2019? Retrieved from https://securityfirstcorp.com/why-is-cyber-security-important/.

[3]. Liu, L., Han, M., Wang, Y., & Zhou, Y. (2018). "Understanding data breach: A visualization aspect," In International Conference on Wireless Algorithms, Systems, and Applications (pp. 883-892). Springer, Cham. (doi: 10.1007/978-3-319-94268-1_81)

[4]. Peltier, T. R. (2016). Information Security Policies, Procedures, And Standards: Guidelines for Effective Information Security Management. Auerbach Publications.

[5]. Han, J., Kim, Y. J., & Kim, H. (2017). "An integrative model of information security policy compliance with psychological contract: Examining a bilateral perspective, " Computers & Security, 66, 52-65. (doi: 10.1016/j.cose.2016.12.016)

[6]. Safa, N. S., Von Solms, R., & Furnell, S. (2016). "Information security policy compliance model in organizations, " computers & security, 56, 70-82. (doi: 10.1016/j.cose.2015.10.006)

[7]. Straub, D., Goodman, S., and Baskerville, R. 2008. "Framing the Information Security Process in Modern Society, " in Information Security: Policy, Processes, and Practices, D. W. Straub, S. Goodman, R. Baskerville (edsl), Armonk, NY: M. E. Sharpe Inc., pp. 5-12.

[8]. Puhakainen, P., and Siponen, M. 2010. "Improving Employee's Compliance through IS Security Training: An Action Research Study, " MIS Quarterly (34:4), pp. 757-778. (doi: 10.2307/25750704)

[9]. Cassetto O. (2019). The 8 elements of an information security policy. Retrieved from https://www.exabeam.com/information-security/information-security-policy/

[10]. Bulgurcu, B., Cavusoglu, H., Benbasat, I. (2010). "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness, " MIS Quarterly (34:3), pp. 523-546. (doi: 10.2307/25750690)

[11]. Cram, W. A., D'arcy, J., & Proudfoot, J. G. (2019). "Seeing the forest and the trees: a meta-analysis of the antecedents to information security policy compliance, " MIS Quarterly, 43(2), 525-554. (doi: 10.24251/hicss.2017.489)

[12]. Sadaf Hina & P. Dhanapal Durai Dominic (2020) Information security policies' compliance: a perspective

for higher education institutions, Journal of Computer Information Systems, 60:3, 201-211

[13]. Chan H, Mubarak S. Significance of information security awareness in the higher education sector. Int J Comput Appl. 2012;60 (10):23–31.

[14]. Ismail Z, Masrom M, Sidek Z, Hamzah D. (2010) "Framework to manage information security for Malaysian Academic Environment," Journal of Information Assurance & Cybersecurity, 1–16.

[15]. Stanton, J.M., Mastrangelo, P., Stam, K.R. & Jolton, J. (2004). Behavioral information security: Two end user survey studies of motivation and security practices. In Proceedings of the 10th Americas Conference on Information Systems (Paper 175). Atlanta, GA: AIS

[16]. Bennett, S., Maton, K., Beyond the 'digital natives' debate: Towards a more nuanced understanding of students' technology experiences, Journal of Computer Assisted Learning, 26 (5) (2010), pp. 321-331

[17]. Bennett, S., K. Maton, Kervin, L., The 'digital natives' debate: A critical review of the evidence, British Journal of Educational Technology, 39 (5) (2008), pp. 775-786

[18]. Bailey, J.L., Mitchell, R.B. & Jensen, B.K. (2008). Analysis of student vulnerabilities to phishing. AMCIS 2008 Proceedings, Paper 271.

[19]. Shay, R., Komanduri, S., Kelley, P.G., Leon, P.G., Mazurek, M.L., Bauer, L., … Cranor, L.F. (2010). Encountering stronger password requirements: User attitudes and behaviors. In Proceedings of the Sixth Symposium on Usable Privacy and Security (Paper 2). New York: ACM.

[20]. Asgharpour, F., Liu, D., & Camp, L. J. (2007). Mental models of computer security risks. In Proceedings of the 6th Annual Workshop on The Economic of Information Security (WEIS 2007).

[21]. Ben-Asher, Noam ; Gonzalez, Cleotilde, Effects of cyber security knowledge on attack detection, Computers in Human Behavior, 2015, Vol.48, p.51(11)

[22]. Siponen, M., and Vance, T. 2014. " Examining the Phenomenon of Deliberate IS Security Policy Violations: A Call and Guidelines for Research, " European Journal of Information Systems (23:3), pp. 289-305.

.