https://doi.org/10.48009/3_iis_2020_217-226

Issues in Information Systems
Volume 21, Issue 3, pp. 217-226, 2020

IMPACT OF HABITS ON INFORMATION SECURITY POLICY COMPLIANCE

Jeretta Horn Nord, Oklahoma State University, jeretta.nord@okstate.edu
Alex Koohang, Middle Georgia State University, alex.koohang@mga.edu
Kevin Floyd, Middle Georgia State University, kevin.floyd@mga.edu
Joanna Paliszkiewicz, Warsaw University of Life Sciences, joanna_paliszkiewicz@sggw.pl

ABSTRACT

Information systems are an integral part of an organization. In recent years, security threats or malicious acts that aim to corrupt or steal data or disrupt an organization's systems have become a major concern for organizational leadership. Information security policy provides a means for protecting information system resources. While creating information policy is an essential starting point, it is not enough to ensure employees' compliance as employees are often the weakest link in information security. When developing security policy, organizational leadership needs to understand the impact of employees' habits on information security policy compliance (ISPC) giving attention to factors such as information security policy (ISP) awareness, gender, age, and IT knowledge. This research sought to determine if there were significant differences between employee ISP awareness, gender, age, and IT knowledge and the impact of employees' habits on ISPC. Using a survey adapted from previous research, 153 faculty and staff from a medium-sized university in the Southeast region of the USA were asked to respond to 8 items that define habit, regular tendency, or practice toward complying with the ISPC that does not require individuals' awareness. Univariate Analysis of Variances (ANOVA) was used to analyze the data. Significant differences were found between each of the independent variables of awareness, gender, age, and IT knowledge and the impact of employee's habits on information systems policy compliance. The results of this research will be useful to leadership as they develop policy and work to ensure security compliance within organizations.

Keywords: Habits, information security policy compliance, age, gender, awareness, IT knowledge

INTRODUCTION

Information security policy is defined as the "… aggregate of directives, regulations, rules, and practices that prescribes how an organization manages, protects, and distributes information." (Nieles et al., 2017, p. 26). Information security policy within an organization should be the basis for all information security plans, designs, and deployments (Yung et al., 2020). Organizations' reliance on information systems requires managing the risk associated with those systems (Bulgurcu et al., 2010). Organizations often rely on technical security solutions to protect themselves against information security threats. However, technology-based solutions alone cannot reduce security risks. Success in information security can be achieved when organizations invest in both technical and socio-organizational resources (Bulgurcu et al., 2010).

NIST SP800-14, (National Institute of Standards and Technology, 1996) identified three levels of information security policy:

- The lower-level information security policy that is a systems-specific security policy (SysSP). This level is a standard or process used when configuring or maintaining a system, and is divided into two categories: (1) management operation specifications; and (2) technical operation specifications;
- The middle-level information security policy that is an issue-specific security policy (ISSP) that guides employees to correctly use various technologies and processes when the organization implements them to support routine operations;
- The upper-level information security policy that is an enterprise information security policy (EISP) that is the overall enterprise security policy, organizational security policy, IT security policy, or information security policy. It is based on the mission, vision, and direction of an organization. (NIST, 1996)

Risks related to information security are a major challenge, since these risks may have dire consequences, including loss of credibility, corporate liability, and monetary damage (Cavusoglu et al., 2004a, 2004b, Vance et al., 2012; Posey et al., 2015). Compliance with information security policy within organizations can reduce these risks (Furnell and Rajendran, 2012).

While creating information security guidelines and policies is an essential starting point, it is not enough to ensure employees' compliance with them. Employees are often the weakest link in information security (Mitnick and Simon 2002; Warkentin and Willison 2009). Therefore, an understanding of what motivates employees to comply with their organizations' information security policies is imperative.

Alhogail (2015) described four dimensions of the human factors concerning information security. They are preparedness (awareness and competency aspects); responsibility (monitoring and control aspects); management (policies and practices aspects); and society and regulation (social, cultural, and regulation aspects).

Scholars have studied many factors based on behavioral theories i.e., protection and motivation theory (Herath and Rao, 2009; Johnston and Warkentin, 2010; Vance et al., 2012) and general deterrence theory (Lee et al., 2004; D'Arcy and Devaraj 2012) among others. These factors can affect employees' behavior toward ISP compliance or non-compliance. For example, normative beliefs, threat appraisal, self-efficacy, and visibility (Siponen et al., 2010); individual's thoughts, actions, feelings, attitudes, and behaviors (Ifinedo, 2013); security awareness and training (D'Arcy et al., 2009; Jenkins et al., 2013 da Veiga and Martins, 2014; Tsohou et al., 2015; Bélanger et al., 2017; Chul et al., 2018); sanctions (Herath and Rao, 2009; Hu et al., 2012; Cheng et al., 2013) rewards (Hu et al., 2012; Posey et al., 2015; Moody et al., 2018); compliance cost and benefits (Bulgurcu et al., 2010); culture (da Veiga and Martins, 2015); attitude and perceptions (Bulgurcu et al., 2010; Guo et al., 2011; Safa et al., 2016; Han et al., 2017); users' competences (i.e. skills and knowledge to maintain security controls) Padayachee (2012); and norms (Yazdanmehr and Wang, 2016).

Of interest to the present study is the variable of habit as a factor influencing ISPC rooted in the theory of interpersonal behavior advanced by Triandis (1977). This theory's basic principle describes individuals' intentions as immediate precursors of behavior, but includes other affective components, social factors, etc. that could predict behaviors such as habits. Habits are considered to be "… learned sequences of acts that become automatic responses to specific situations, which may be functional in obtaining certain goals or end states" (Verplanken and Aarts, 1999, p. 14).

Habits are defined as automatic responses to specific situations (Bamberg, Schmidt, 2003); a certain amount of repetition or practice (Limayem, et al., 2007); and automatic behavior tendencies (Limayem & Hirt, 2003). Habits can also predict an individual's future behavior (Bamberg, Ajzen, & Schmidt, 2003).

Employees' habits have found to have a significant impact on information security in organizations (Cheng, et al., 2016). The literature in the area of habit and its impact to ISPC, though limited, has shown that individuals' habits have a significant effect on the intention to comply with information security policies within organizations (e.g., Pahnila et al.,2007; Vance et al., 2012). In particular, Moody et al. (2018) concluded that habit is a significant predictor of ISPC.

The purpose of this study is to find out the impact of employee's habits on ISPC giving attention to several factors, i.e., ISP awareness, gender, age, and IT knowledge. The motivation for this study stemmed from the fact that these factors had not previously been studied. Therefore, we sought to answer the following research question (RQ):

RQ: Are there significant mean differences between the levels of each independent variable (ISP Awareness, Gender, Age, and IT Knowledge) and the dependent variable (impact of employee's habits on ISPC)?

METHOD

Instrument

We used an instrument that was originally developed by Verplanken and Orbell (2003) and revised later by Moody et al. (2018). The instrument included 8 items that define habit, a regular tendency, or practice toward complying with the ISP that does not require individuals' awareness. The items of the instrument were as follows:

Complying with information security policy is something:

1. I do frequently
2. I do automatically
3. I do without having to consciously remember
4. I do without thinking
5. that belongs to my (daily, weekly, monthly) routine
6. I start doing before I realize I'm doing it
7. that's typically "me"
8. I have been doing for a long time

The Likert-type instrument used a seven-point scale from completely agree (7) to completely disagree (1).

Sample and Data Collection

The subjects for the present study included 153 faculty (N = 83) and staff (N = 70) from a medium-sized university in the Southeast region of the USA. Upon approval from the university's IRB (Institutional Research Board) where this study took place, the instrument was administered to the subjects via SurveyMonkey™. The subjects were chosen from a large dataset conducted in six weeks. We used the data from weeks 3 and 4 for this study, which included 158 responses. Two responses were eliminated because of incomplete data, and 3 responses were eliminated as a result of outlier test. All subjects were over 30 years of age. They were assured confidentiality and anonymity.

Data Analysis

Univariate Analysis of Variances (ANOVA) procedure was conducted to answer the research question. Univariate ANOVA procedure is used where there are multiple independent variables with one dependent variable. The independent variables for this study were *ISP Awareness, Gender, Age,* and *IT Knowledge*. The dependent variable was the *impact of employee's habits on ISPC*, which is a regular tendency or practice toward complying with the ISP that does not require individuals' awareness. According to Mertler & Vannatta (2010), to correctly interpret the results of the univariate ANOVA procedure, the data must be assessed to meet the criteria that the dependent variable is continuous, each independent variable includes two or more levels, there is no relationship between the observations in each group or between the groups, the outliers in the data are removed, and data should be tested for homogeneity of variance to indicate a non-significant value from the Levene's test.

The univariate ANOVA table yields the calculated F value for each independent variable, which establishes the significance or non-significance of the groups on the dependent variable. Next, descriptive analyses show the means and standard deviation of the levels of each independent variable with the dependent variable. Finally, multiple comparison Post hoc analyses for groups of more than two levels (ISP Awareness, Age, and IT Knowledge) are conducted to ascertain significant group comparisons. A predetermined significant level of .05 was chosen.

RESULTS

Descriptive Analysis

Figure 1 shows the descriptive analysis comparing the means of each item for the dependent variable of Habit which indicated above average and near high mean scores for all eight items, i.e., Habit_1 = Complying with ISP frequently (μ = 6.37), Habit_2 = Complying with ISP automatically (μ = 6.20), Habit_3 = Complying with ISP without consciously remembering (μ = 6.04), Habit_4 = Complying with ISP without thinking (μ = 5.92), Habit_5 = Complying with ISP routinely (μ = 6.12), Habit_6 = Complying with ISP before realizing doing it (μ = 5.84), Habit_7 = Complying with ISP is typically "me" (μ = 6.04)), and Habit_8 = Complying with ISP for a long time (μ = 6.18).

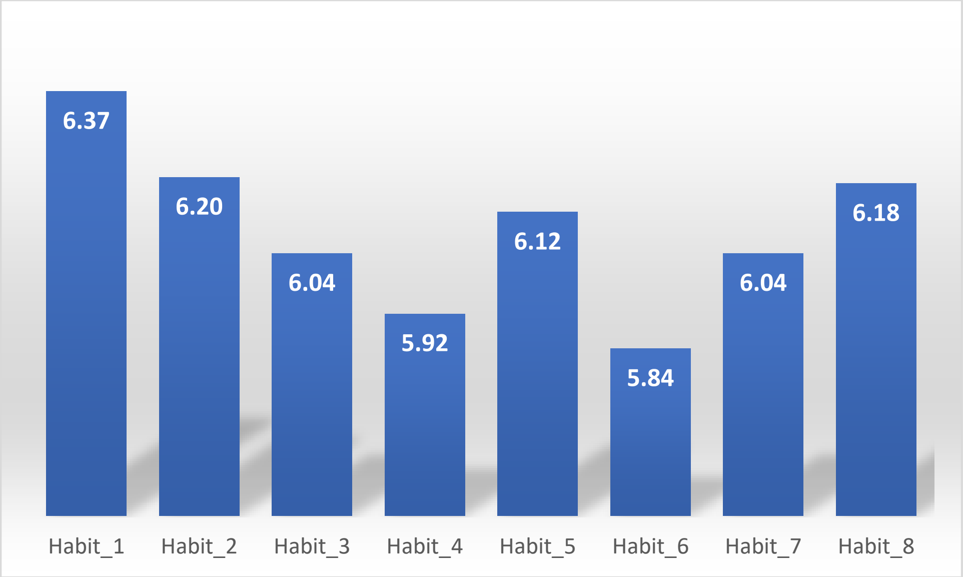

Figure 1: Means of the Dependent Variable (The impact of employee's habits on ISPC)

Meeting Criteria for conducting Univariate ANOVA Analysis

The assessment of the data concluded that the dependent variable (impact of employee's habits on ISPC) was continuous and that each independent variable (ISP Awareness, Gender, Age, and IT Knowledge) included 2 to 4 levels. There was no relationship between the observations in each group or between the groups. Three outliers were identified and removed from the dataset. Levene's Test of Equality of Error Variances result (F = 1.125, *P* = .304), a non-significant value, revealed homogeneity of variance.

Univariate ANOVA Analysis

Table 1 shows the results of univariate ANOVA between the independent variables of ISP Awareness, Gender, Age, and IT Knowledge and the dependent variable of the impact of employee's habits on ISPC. The results indicate significant mean differences between each independent variable (ISP Awareness, Gender, Age, and IT Knowledge) and the dependent variable (impact of employee's habits on ISPC).

Table 1: Univariate Analysis of Variance (Tests of Between-Subjects Effects)

Source	Type III Sum of Squares	df	Mean Square	F	Sig.
Corrected Model	37.608	8	4.701	6.481	.000
Intercept	2875.031	1	2875.031	3963.893	.000
ISP Awareness	16.150	3	5.383	7.422	**.000**
Gender	4.205	1	4.205	5.797	**.017**
Age	8.374	2	4.187	5.773	**.004**
IT Knowledge	9.143	2	4.571	6.303	**.002**
Error	104.444	144	.725		
Total	5814.766	153			
Corrected Total	142.052	152			

Table 2 shows the means and standard deviations of all independent variables (ISP Awareness, Gender, Age, and IT Knowledge) with the dependent variable (impact of employee's habits on ISPC). Regarding ISP Awareness, the highest mean score belonged to those indicating "completely aware" of ISP within their workplace following by those with "mostly aware" of ISP. Those indicating "somewhat aware" and "completely unaware" of ISP scored the lowest mean scores respectively. This suggests that habits as a regular tendency or practice toward complying with the ISP are reinforced and strengthened by those being more aware of the ISP in their workplace.

Regarding gender, female subjects received a higher mean score than male subjects. In other words, female subjects respond better to their habits as a regular tendency or practice toward complying with the ISP in their workplace.

Regarding age, older subjects received the highest mean score and the youngest subjects received the lowest mean score. This suggests that habits as a regular tendency or practice toward complying with the ISP are better reinforced and strengthened with older subjects.

Regarding IT knowledge, those subjects indicating "very high knowledge" of IT had the highest mean score following by those indicating "moderate" and "low" knowledge respectively. This suggests that habits as a regular tendency or practice toward complying with the ISP are better reinforced and strengthened with subjects with higher IT knowledge.

Table 2: Means and Standard Deviations

Habit * ISP Awareness			
	Mean	N	Std. Deviation
Completely aware	6.6382	19	.69209
Mostly aware	6.3063	60	.72172
Somewhat aware	5.8484	61	1.03986
Completely unaware	5.4135	13	1.28430
Habit * Gender			
	Mean	N	Std. Deviation
Female	6.2058	82	.89027
Male	5.9542	71	1.03816
Habit * Age			
	Mean	N	Std. Deviation
31–40	5.8560	46	1.02401
41–50	6.0285	57	1.00028
Above 50	6.3725	50	.80950
Habit * IT Knowledge			
	Mean	N	Std. Deviation
Very High	6.3702	26	.73099
Moderate	6.2000	85	.85873
Low	5.6905	42	1.17884

Post Hoc (Multiple Comparisons) Analysis

Tables 3, 4, & 5 show the multiple comparison analyses of independent variables with 3 or more levels, i.e., ISP Awareness, Age, and IT Knowledge with the dependent variable (impact of employee's habits on ISPC). The results specifically show which groups differed from each other. Regarding ISP Awareness and Habit, there was a statistically significant difference between the following groups: 1 = Completely aware and 3 = Somewhat aware (p = .007), 1 = Completely aware and 4 = Completely unaware (p = .002), 2 = Mostly aware and 3 = Somewhat aware, (p = .036), and 2 = Mostly aware and 4 = Completely unaware (p = .010). However, there were no differences between the following groups: 2 = Mostly aware and 1 = Completely aware (p = .535) and 3 = Somewhat aware and 4 = Completely unaware (p = .427). These results emphasize that habits as a regular tendency or practice toward complying with the ISP are reinforced and strengthened by those being more aware of the ISP in their workplace.

Regarding Age and Habit, there was a statistically significant difference between groups 1 = 31–40 and 3 = Above 50 (p = .014). However, there was no significant difference between groups 1 = 31–40 and 2 = 41–50 (p = .594; groups 2 = 41–50 and 1 = 31–40 (p =.954); and groups 2 = 41–50 and 3 = Above 50 (p = .118). These results emphasize that that habits as a regular tendency or practice toward complying with the ISP are better reinforced and strengthened with older subjects.

Regarding IT knowledge and Habit, there was a statistically significant difference between groups 1 = Very High and 3 = Low (p = .007); and groups 2 = Moderate and 3 = Low (p = .008). However, there was no difference between groups 1 = Very High and 2 = Moderate (p = .673). These results emphasize that habits as a regular tendency or practice toward complying with the ISP are better reinforced and strengthened with subjects with higher IT knowledge.

Table 3: Multiple Comparisons - ISP Awareness and Habit

(I) ISP Awareness	(J) ISP Awareness	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval	
					Lower Bound	Upper Bound
1	2	.3319	.22419	.535	-.3023	.9661
	3	.7898*	.22375	**.007**	.1568	1.4228
	4	1.2247*	.30654	**.002**	.3575	2.0918
2	1	-.3319	.22419	.535	-.9661	.3023
	3	.4579*	.15485	**.036**	.0198	.8959
	4	.8928*	.26054	**.010**	.1558	1.6298
3	1	-.7898*	.22375	**.007**	-1.4228	-.1568
	2	-.4579*	.15485	**.036**	-.8959	-.0198
	4	.4349	.26016	.427	-.3010	1.1708
4	1	-1.2247*	.30654	**.002**	-2.0918	-.3575
	2	-.8928*	.26054	**.010**	-1.6298	-.1558
	3	-.4349	.26016	.427	-1.1708	.3010

*1 = Completely aware, 2 = Mostly aware, 3 = Somewhat aware, 4 = Completely unaware | *The mean difference is significant at the .05 level.*

Table 4: Multiple Comparisons – Age and Habit

(I) Age	(J) Age	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval	
					Lower Bound	Upper Bound
1	2	-.1725	.16880	.594	-.5900	.2450
	3	-.5165*	.17399	**.014**	-.9469	-.0862
2	1	.1725	.16880	.594	-.2450	.5900
	3	-.3440	.16502	.118	-.7522	.0642
3	1	.5165*	.17399	**.014**	.0862	.9469
	2	.3440	.16502	.118	-.0642	.7522

*1 = 31–40, 2 = 41–50, 3 = Above 50 | *The mean difference is significant at the .05 level*

Table 5: Multiple Comparisons – IT Knowledge and Habit

(I) IT Knowledge	(J) IT Knowledge	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval	
					Lower Bound	Upper Bound
1	2	.1702	.19086	.673	-.3019	.6423
	3	.6797*	.21252	**.007**	.1541	1.2054
2	1	-.1702	.19086	.673	-.6423	.3019
	3	.5095*	.16063	**.008**	.1122	.9068
3	1	-.6797*	.21252	**.007**	-1.2054	-.1541
	2	-.5095*	.16063	**.008**	-.9068	-.1122

*1 = Very High, 2 = Moderate, 3 = Low | *The mean difference is significant at the .05 level.*

DISCUSSION

This study was undertaken to reveal the impact of employee's habits on ISPC giving attention to ISP awareness, gender, age, and IT knowledge. Specifically, the study sought to find out whether there were significant mean differences between each independent variable (ISP Awareness, Gender, Age, and IT Knowledge) and the dependent variable (impact of employee's habits on ISPC).

Individuals with the highest mean score belonged to those indicating completely aware of ISP within their workplace. This followed by those with mostly aware of ISP. Those indicating somewhat aware and completely unaware of ISP scored the lowest mean scores respectively. These findings suggest that habits as a regular tendency or practice toward complying with the ISP are reinforced and strengthened by those being more aware of the ISP in their workplace. Awareness translates to recognizing, understanding, and being able to identify possible security threats. As the results of this study imply, employees' awareness of a firm's ISP is imperative to security. The goal should be to educate employees so that all employees are aware of ISP policies and security challenges. An organization's security awareness training should include a system for reporting and resolution, an incident log, awareness training, and testing employees' knowledge. External sources for security training should also be considered. Training for new hires and continuous updates for all employees are measures that every company should employ, whether it is internal or external. The cost of not having such a system in place is likely to be devastating to an organization in terms of both time and expense.

Female subjects received a higher mean score than male subjects. This translates into female subjects responding better to their habits as a regular tendency or practice toward complying with the ISP in their workplace. Ang (2017) found that the Internet habit strength was positively linked to online communication and that the link was significantly greater for females than it was for males. This may be true in the case of the impact of habits toward complying with ISPC. The findings of this study regarding gender merit future research.

Older subjects received the highest mean score, and the youngest subjects received the lowest mean score. This suggests that habits as a regular tendency or practice toward complying with the ISP are better reinforced and strengthened with older subjects. These results likely indicate that older individuals have more experience and knowledge of the repercussions of non-compliance, which confirm the importance of a proven system for security awareness through training not only by organizations but by institutions of higher education as well. A study by Fatokun et al. (2019) confirms the need for this through results found in their study indicating that both undergraduate and postgraduate students are not familiar with some of the common cyber-threats.

Individuals with very high knowledge of IT had the highest mean score. This followed by those with moderate and low IT knowledge respectively. These findings suggest that habits as a regular tendency or practice toward complying with the ISP are better reinforced and strengthened with subjects with higher IT knowledge. As the saying goes, *knowledge is powe*r. This finding is not surprising and should emphasize to employers the need to, first of all, hire highly qualified staff and secondly to provide continual training so that the knowledge base of all employees remains updated.

CONCLUSIONS

This study looked at the impact of employee's habits on information security policy (compliance, specifically ISP awareness, gender, age, and IT knowledge, and sought to answer the following research question: Are there significant mean differences between the levels of each independent variable (ISP Awareness, Gender, Age, and IT Knowledge) and the dependent variable (impact of employee's habits on ISPC)?

Results revealed that individuals with the highest mean score belonged to those indicating that they were completely aware of ISP within their workplace; female subjects received a higher mean score than male subjects; older respondents received the highest mean score and the youngest subjects received the lowest mean score, and individuals with very high knowledge of IT had the highest mean score. The primary contribution to the discipline is that significant differences exist between the levels of the following variables — awareness, gender, age, and knowledge when measured against the variable — the impact of employee's habits on ISPC.

According to these results, the impact of employee's habits indeed has an impact on ISP compliance with specific attention to ISP awareness, gender, age, and IT Knowledge. As a result of these findings, employers and those in institutions of higher education should have a better understanding of ISPC's critical components and be able to act on them accordingly through hiring and training practices.

This study has limitations that may influence the generalizability of the findings. We used a sample of university faculty and staff in a mid-sized university in the USA. We recommend that this study be carried out using samples from organizations other than higher education institutions. We also used a sample of convenience, though accepted among the research community, a random sample may yield different results.

REFERENCES

Alhogail, A. (2015). Design and validation of information security culture framework. *Computers in Human Behavior, 49*, 567-575.

Ang, C. S. (2017). Internet habit strength and online communication: Exploring gender differences. *Computers in Human Behavior*, *66*, 1-6.

Bamberg, S., Ajzen, I., Schmidt, P. (2003). Choice of travel mode in the theory of planned behavior: The roles of past behavior, habit, and reasoned action. *Basic and Applied Social Psychology, 25*(3), 175–188.

Bamberg, S., Schmidt, P. (2003). Incentives, Morality, or Habit? Predicting Students' Car Use for University Routes with the Models of Ajzen, Schwartz, and Triandis. *Environment and Behavior, 35*(2), 264-285.

Bélanger, F., Collignon, S., Enget, K., Negangard, E. (2017). Determinants of early conformance with information security policies. *Information and Management, 54*(7), 887-901.

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), 523-548.

Cavusoglu, H., Mishra, B., Raghunathan, S. (2004a). A Model for Evaluating IT Security Investments. *Communications of the ACM, 47*(7), 87-92.

Cavusoglu, H., Mishra, B., Raghunathan, S. (2004b). The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers. *International Journal of Electronic Commerce, 9*(1), 69-104.

Cheng, G., Guan, Y. Chau, J. (2016). An empirical study towards understanding user acceptance of bring your own device (BYOD) in higher education. *Australasian Journal of Educational Technology, 32*(4), 1–17.

Cheng, L., Li, Y., Li, W., Holm, E., Zhai, Q. (2013). Understanding the violation of IS security policy in organizations: an integrated model based on social control and deterrence theory. *Computers and Security, 39*, 447-459.

Chul, W. Y., Sanders, G. L., Cerveny, R. P. (2018). Exploring the influence of flow and psychological ownership on security education, training and awareness effectiveness and security compliance. *Decision Support Systems, 108*, 107-118.

D'Arcy, J., Devaraj, S. (2012). Employee misuse of information technology resources: testing a contemporary deterrence model. *Decision Science, 43*(6),1091–1124.

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

Da Veiga, A., Martins, N. (2014). Information security culture: a comparative analysis of four assessments", Proceedings of The European Conference on Information Management and Evaluation, 49-57.

Da Veiga, A., Martins, N. (2015). Improving the information security culture through monitoring and implementation actions illustrated through a case study. *Computers and Security, 49*, 162-176.

Fatokun, F. B., Hamid, S., Norman, A., Fatokun, J. O. (2019). The Impact of Age, Gender, and Educational level on the Cybersecurity Behaviors of Tertiary Institution Students: An Empirical investigation on Malaysian Universities. *Journal of Physics: Conference Series, 1339*, 26-27.

Furnell, S., & Rajendran, A. (2012). Understanding the influences on information security behaviour. *computer Fraud & security*, *2012*(3), 12-15.

Guo, K. H., Yuan, Y., Archer, N. P., Connelly, C. E. (2011). Understanding non-malicious security violations in the workplace: a composite behavior model. *Journal of Management Information Systems, 28*(2), 203-236.

Han, J., Kim, Y. J. and Kim, H. (2017). An integrative model of information security policy compliance with psychological contract: examining a bilateral perspective. *Computers and Security, 66*, 52-65.

Herath, T., Rao, H. R. (2009). Encouraging information security behaviors in organizations: role of penalties, pressures and perceived effectiveness. *Decision Support Systems, 47*(2), 154-165.

Hu, Q., Dinev, T., Hart, P., Cooke, D. (2012). Managing employee compliance with information security policies: the critical role of top management and organizational culture. *Decision Sciences, 43*(4), 615-660.

Ifinedo, P. (2013). Information Systems Security Policy Compliance: An Empirical Study of the Effects of Socialization, Influence, and Cognition. *Information & Management, 51*(1), 69-79.

Jenkins, J. L., Durcikova, A., Burns, M. B. (2013). Simplicity is bliss: controlling extraneous cognitive load in online security training to promote secure behavior. *Journal of Organizational and End User Computing, 25*(3), 52-66.

Johnston, A., Warkentin, M. (2010). Fear appeals and information security behaviors: an empirical study. *MIS Quarterly, 34*(3), 549–566.

Lee, S. M., Lee, S., Yoo, S. (2004). An integrative model of computer abuse based on social control and general deterrence theories. *Information and Management, 41*(6), 707–718.

Limayem, M, Hirt, S. G., Cheung, C. M. K. (2007). How habit limits the predictive power of intention the case of information systems continuance. *MIS Quarterly, 31*(4), 705–737.

Limayem, M., Hirt, S. G. (2003). Force of habit and information systems usage: Theory and initial validation. *Journal of the Association for Information Systems, 4,* 65–97.

Mertler, C.A., & Vannatta, R.A. (2010). *Advanced and multivariate statistical methods. Los Angeles, CA: Pyrczak.*

Mitnick, K. D., Simon, W. L. (2002). *The Art of Deception: Controlling the Human Element of Security*, Indianapolis, IN: Wiley Publishing, Inc.

Moody, G. D., Siponen, M., Pahnila, S. (2018). Toward a unified model of information security policy compliance, *MIS Quarterly, 42*(1), 285-311.

National Institute of Standards and Technology. (1996). Generally Accepted Principles and Practices for Securing Information Technology Systems; SP 800-14; NIST: Gaithersburg, MD, USA.

Nieles, M., Dempsey, K., Pillitteri, V. (2017). An Introduction to Information Security. *NIST Special Publication 800-12 Revision 1.* Retrieved May 12, 2020 from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf

Padayachee, K. (2012). Taxonomy of compliant information security behavior. *Computers & Security, 31*(5), 673-680.

Pahnila, S., Siponen, M. Mahmood, A. (2007). Employees' behavior towards IS security policy compliance. In: *Proceedings of the Annual Hawaii International Conference on System Sciences*, Honolulu, Hawaii, January 03–06, pp. 1–10.

Posey, C., Roberts, T. L., Lowry, P. B. (2015). The impact of organizational commitment on insiders' motivation to protect organizational information assets. *Journal of Management Information Systems, 32*(4), 179-214.

Safa, N. S., Solms, R. V. Furnell, S. (2016). Information security policy compliance model in organizations. *Computers and Security, 56*, 70-82.

Siponen, M., Pahnila, S., Mahmood, M. A. (2010). Compliance with Information Security Policies: An Empirical Investigation. *Computer, 43*(2), 64-71.

Triandis, H. (1977). *Interpersonal Behavior*, Pacific Grove, CA: Brooks/Cole Publishing Company.

Tsohou, A., Karyda, M., Kokolakis, S. (2015). Analyzing the role of cognitive and cultural biases in the internalization of information security policies: recommendations for information security awareness programs. *Computers and Security, 52*, 128-141.

Vance, A., Siponen, M., Pahnila, S. (2012). Motivating IS security compliance: insights from habit and protection motivation theory. *Information and Management, 49*, 190–198.

Verplanken, B, Aarts, H. (1999). Habit, attitude, and planned behaviour: is habit an empty construct or an interesting case of goal-directed automaticity? *European Review of Social Psychology, 10*(1), 101–34.

Verplanken, B., Orbell, S. (2003). Reflections on past behaviour: A self-report index of habit strength. *Journal of Applied Social Psychology, 33*, 1313–1330.

Warkentin, M., Willison, R. (2009). Behavioral and Policy Issues in Information Systems Security: The Insider Threat. *European Journal of Information Systems, 18*(2), 101-105.

Yazdanmehr, A., Wang, J. (2016). Employees' information security policy compliance: a norm activation perspective. *Decision Support Systems, 92*, 36-46.

Yung, C. W., Sun, R., Yenchun, J. W. (2020). Smart city development in Taiwan: From the perspective of the information security policy. *Sustainability, 12*(7), 2916.