Communications of the IIMA

Volume 16 | Issue 4 Article 2

2018

Employee Compliance to Information Security in Retail Stores

Bertrand Muhire

Ramakrishna Ayyagari
University of Massachusetts Boston, r.ayyagari@umb.edu

INTRODUCTION

"…people are often the weakest link in the security chain…" – Symantec white paper on 'Cyber Security for Retail Services' (Symantec, 2015)

Consumers do not believe retailers are investing enough in security measures and do not trust retailers to safeguard information (Security, 2016). Previous research has argued that addressing consumers' feelings of insecurity is important in retail settings (Koistinen & Järvinen, 2016; Priporas, Stylos, & Fotiadis, 2017). Bonderud (2016) argues that security risks come from retailers themselves, as they do not prepare appropriately. This paper argues that proper preparation for security involves paying attention to human element in retail settings.

Topics related to security are an integral part of retail industry. Security in retail industry can project many different images – issues of unethical behavior by customers (e.g. shoplifting) (Mitchell, Balabanis, Schlegelmilch, & Cornwell, 2009; Perlman & Ozinci, 2014), surveillance methods (e.g., security cameras) (Kajalo & Lindblom, 2015; Perlman & Ozinci, 2014), and security of employees and customers (e.g. situation crime prevention) (Kajalo & Lindblom, 2015). In this paper, a key area of retail security that is addressed – information security in retail settings. The authors emphasize the human element in retail security by focusing on retail employees.

This work complements broader security literature in retail settings. Previous research has mainly focused on the security issues of new channels (e-commerce, m-commerce) and on consumers' shopping experience. For example, e-commerce has explored topics of how to instill confidence in consumers by studying issues of trustworthiness and perceived risk of online channels (Benedicktus, Brady, Darke, & Voorhees, 2010; Meents & Verhagen, 2018; Nepomuceno, Laroche, & Richard, 2014). Security in retail setting has also focused on online shopping experience. Previous research indicates that security and privacy concerns play a role in consumers' shopping experience (Heinze, Thomann, & Fischer, 2017; Lian & Lin, 2008; Nepomuceno et al., 2014). Consequently, retailers typically focus on improving consumer confidence by providing messages of 'safe' online shopping. Messages typically focus on the kind of technology used to keep consumers' information safe (encryption, tools used to scan for malware, vulnerabilities etc. see Appendix A). Although this is necessary for retailers' security, it is not sufficient. Purely technological solution to security is not going to work(Mitnick, 2003).

Recent breaches in retail industry indicate that even though retailers have security tools to protect consumers' information, it does not always work. For example, data breach from Point of Sale (POS) systems at Buckle stores indicate

that hackers were able to infiltrate POS. Even though Buckle stores had installed chip-readers at POS, the use of magnetic stripe on credit cards resulted in the data breach (http://www.fraud.org/the_buckle_breach). In other words, although purely technological solution (chip-reader) was a secure option, the use of magnetic strip is a result of interaction of various organizational issues (security culture, awareness about these issues, compliance behaviors to policies etc.). As this example shows, focus on organizational issues plays an important role in information security beyond technological solutions(Paulsen & Coulson, 2011).

Organizations are socio-technical systems and a holistic approach to security needs to involve a socio-technical solution. Individuals are an integral part of organizations and their interactions with technology can be a weak link. Researchers argue that employees are the weakest link in the security chain of an organization (Crossler et al., 2013; Mitnick, 2003; Warkentin & Willison, 2009). Employees can become an asset to information security, rather than a liability if they choose pro-security behaviors(Paulsen & Coulson, 2011). These behaviors are molded by organizational policies and their adherence towards these policies. Accordingly, research on information security has studied why employees comply or do not comply with information security policies (Aurigemma & Mattson, 2017; Bulgurcu, Cavusoglu, & Benbasat, 2010; Dols & Silvius, 2010; Guo, 2013; Siponen & Vance, 2010; Vroom & von Solms, 2004).

This study focuses on information security compliance of store-level workers in retail industry setting. The reasons for this are twofold: (i) retail industry suffers numerous breaches (Maheshwari, 2014) and (ii) previous information security research has mostly focused on knowledge workers. Two of the biggest breaches of recent times are that of Home Depot and Target (Maheshwari, 2014) amounting to compromise of more than 90 million card data. Even with Payment Card Industry Data Security Standard (PCI-DSS) compliance requirement, breaches in retail industry have not abated (Taylor, 2018). In addition, the nature of retail industry (numerous entry points, open access etc.) is inherently counter to security practices that restrict and control access. Further, previous information security compliance literature has called for research on different samples (Johnston & Warkentin, 2010). Therefore, the authors study information security compliance behavior in a retail setting.

The following sections are organized as follows. First, a brief literature review of research in information security compliance behaviors is provided. Next, the research model and hypotheses are presented. Third, research methodology and the results are reported. Finally, the implications from this study are discussed.

LITERATURE REVIEW

To understand the human aspect of security, users' security behaviors need to be studied. Therefore, the authors draw on the Behavioral Information Security research for understanding security behaviors and proposing ways to enhance compliance with Information Security policies (Crossler et al., 2013). Information security policies (ISP) describe the roles and responsibilities of the employees to safeguard the information and technology resources of their organizations (Bulgurcu et al., 2010).

Previous research has shown that employees violation of Information security policies is due to negligence and/or ignorance of the Information security policies on the part of employees (Vroom & von Solms, 2004). To achieve compliance with information security policies, managers need to understand factors behind employees' non-compliance, and use techniques to deal with non-compliance. Some of the techniques include correctional responses like sanctions, and information security training (Guo & Yuan, 2012; Ifinedo, 2012; Puhakainen & Siponen, 2010).

Researchers draw on Theory of Planned Behavior (TPB) to study users' behaviors interacting with technology (Mathieson, 1991). According to TPB, attitude towards the behavior is proposed as a key predictor of behavior intention. Research studies in various contexts, including behavioral security and retail, have shown that attitude is one of the key predictors of behavioral intention (Casidy, Phau, & Lwin, 2016; Hansen, Møller Jensen, & Stubbe Solgaard, 2004; Ifinedo, 2012; Mathieson, 1991; Shropshire, Warkentin, & Sharma, 2015; Syed & Nazura, 2011). In addition, users form an intention towards a behavior before performing the actual behavior (Ajzen, 1991). Researchers have used intention as a predictor for actual behavior as observing the actual behavior is challenging. This is similar to the use of intentions to investigate behaviors in retail literature (Das, 2014; Nascimento, Oliveira, & Tam, 2018; Rana & Paul, 2017; Sreen, Purbey, & Sadarangani, 2018; Yeo, Goh, & Rezaei, 2017).

Security behaviors include actions that not only involve what to do, but also what not to do. Therefore, researchers have drawn on Deterrence theory to incorporate appropriate concepts while studying information security behaviors(D'Arcy & Herath, 2011). Deterrence theory focuses on creating an environment that discourages certain behaviors in an organization. When applied to information security, the use of sanctions as an organizations' response to employees non-compliance to IS security policies is a widely suggested approach to reduce computer abuse and improve employee compliance with IS security policies (Herath & Rao, 2009; Johnston & Warkentin, 2010). In addition, security

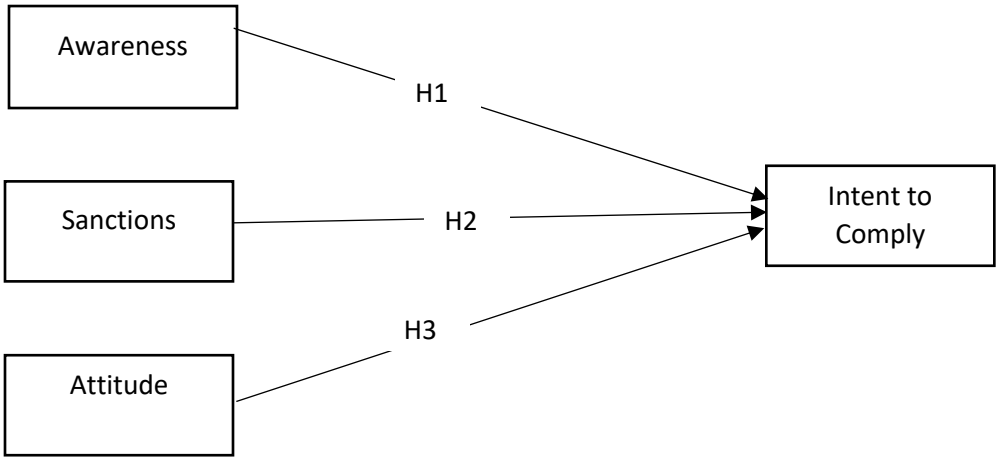
awareness programs act as deterrents, and guide security behaviors (D'Arcy, Hovav, & Galletta, 2009; Ifinedo, 2012).

To summarize, attitude, intent to comply, sanctions and awareness, and are used as main variables in this study. We limit our study to these parsimonious set of variables although other variables exist in this research domain.

RESEARCH MODEL AND HYPOTHESES

Figure 1 shows the proposed research model. In the following paragraphs, the hypotheses shown in Figure 1 are developed.

Figure 1: Proposed Model and Hypotheses



Individuals cannot comply with policies if they are not aware of the policies. Arguments based on Deterrence theory posits that certain organizational controls can discourage individuals from engaging in unwanted behaviors. In Information Security literature, it is argued that using proactive measures like security training and awareness results in decrease of security policy violations (Guo & Yuan, 2012; Ifinedo, 2012). In other words, using awareness programs like policy handouts, videos, newsletters etc. would make the employees be constantly aware of security policies and lead to compliant behaviors (D'Arcy et al., 2009; Karjalainen & Siponen, 2011; Puhakainen & Siponen, 2010). Similar arguments are made in retail literature where compliance improves when employees are educated on the store's policies (Rigotti, Stoto, Bierer, Rosen, & Schelling, 1993) and brand awareness is positively linked to purchase intentions (Das, 2014). Therefore, it is hypothesized that

> H1: Individual's awareness of ISP will have a positive relationship on the intent to comply with ISP.

In addition to awareness, another deterrent control that is shown to be effective in compliant behaviors are the sanctions for non-compliant behaviors(Guo & Yuan, 2012). Deterrence concepts are not new to retailing literature. Consumers' intent to act dishonestly are effected by the perceived consequences of their actions (Cole, 1989). If an individual perceives that the rewards of engaging in a behavior are not worth the risks, then the individual is deterred from engaging in the action. In the Information Security context, if an individual perceives that non-compliance behaviors lead to sanctions such as negative performance reviews, loss of employment, disapproval of peers etc., then the individual is less likely to be non-compliant to Information Security Policies(D'Arcy & Herath, 2011; Herath & Rao, 2009; Hu, Xu, Dinev, & Ling, 2011; Ugrin & Michael Pearson, 2013). Therefore, it is hypothesized that

H2: Individual's perceived sanctions will have a positive relationship on the intent to comply with ISP.

Drawing on the Theory of Planned Behavior, it is argued that attitude influences behavioral intentions (Ajzen, 1991). If an individual evaluates the behavior in question positively, then it is likely that the individual will engage in the behavior. In this context, if an individual perceives organization's information security policy positively, then it is likely that they will engage in compliance behavior. On the other hand, if an individual perceives the policy as a nuisance, then it is likely that they will not engage in behaviors compliant with security policy. Previous research in both information systems and retail literature support the effect of attitude on intention (Casidy et al., 2016; Faqih, 2016; Mathieson, 1991; Shropshire et al., 2015; Sreen et al., 2018). Therefore, it is hypothesized that

H3: Attitude towards compliance with ISP will have a positive relationship on the intent to comply with ISP.

METHODOLOGY

The authors used survey methodology to test the proposed relationships and structural equation modeling is used for statistical analyses. Since the goal of this research is to test information security compliance behaviors in a retail setting, a home improvement store was chosen for data collection. The sample is derived from employees at a home improvement store in USA. The organization is a well-known retailer with over 2000 stores across North America with revenues in excess of 75 billion. The store-level employees help customers find right products, help with questions regarding home improvement projects and execute purchase processes. The workflow of these employees demands that the employees are moving within the store. In addition, the employees handle credit card data either physically or over the phone (for phone orders). This environment is different from

typical work environment of a knowledge worker. The access to stores is open access, employees frequently step out from the sales terminal, and the employees are likely from different educational background than knowledge workers.

To test the hypothesized model, existing scales from information security literature are used to measure the constructs used in this study (Bulgurcu et al., 2010; Siponen & Vance, 2010). Appendix B shows the measurement items for each of the constructs used in this study. Surveys containing items for variables used in the study were distributed to 100 store-level employees. Participation was voluntary and responses were anonymous, as the survey required no personal or identifying information. The survey also captured basic socio-demographic information.

RESULTS

Seventy-two usable responses were received. 53% of respondents were female. Almost 70% of the respondents did not have a bachelor degree. This indicates that respondents in this study come from a different educational background than a typical knowledge worker[1].

Table 1: Factor loadings and reliabilities

Construct	Items	Factor Loadings	Composite Reliability
Awareness	Awrn1	0.856	
	Awrn2	0.922	0.81
	Awrn3	0.804	
Attitude	Att1	0.744	
	Att2	0.765	0.71
	Att3	0.714	
Sanctions	Sanc1	0.912	
	Sanc2	0.733	0.81
	Sanc3	0.933	
Intent To Comply	IC1	0.803	
	IC2	0.934	0.79
	IC3	0.757	

To test the measurement model, all the items are loaded on their respective latent factors. The goodness-of-fit measures for the measurement model are CFI

[1] A post-hoc analysis indicated that mean-differences for 'intent to comply' exist for different education levels. Specifically, intent to comply was significantly higher for 'college graduates' than for respondents with 'high school degree'. Therefore, this result provides support for using non-knowledge workers as a research sample.

0.983, and RMSEA 0.049. These values are within the proposed values of 0.9 for CFI and 0.08 for RMSEA(Kline, 2005), indicating that the measurement model is a good fit.

Factor loadings, composite reliability and average variance extracted (AVE) are used to test the convergent validity and reliability of measures used in this study. Table 1 shows the factor loadings and reliabilities for each construct. All the composite reliability values exceed the recommended cutoff of 0.7. In addition, all the factor loadings are above 0.7 and the AVE for each construct is above .5 (Fornell & Larcker, 1981). This implies that the at least 50 % of the measured variance among items is explained by the modeled constructs.

Table 2 show the inter-construct correlations and the diagonal values show the square root of average variance extracted for each construct. Chin (1998) suggests that if square root of AVE for each construct exceeds inter-construct correlations, then discriminant validity is exhibited. Results from Table 2 indicate that measured constructs indicate discriminant validity. In summary, the measured constructs exhibit accepted reliability and validity standards.

Table 2: Inter-construct correlations

	Awareness	Attitude	Sanctions	Intent to Comply
Awareness	**0.86**			
Attitude	0.19	**0.74**		
Sanctions	0.15	0.54	**0.86**	
Intent to Comply	0.37	0.59	0.41	**0.83**

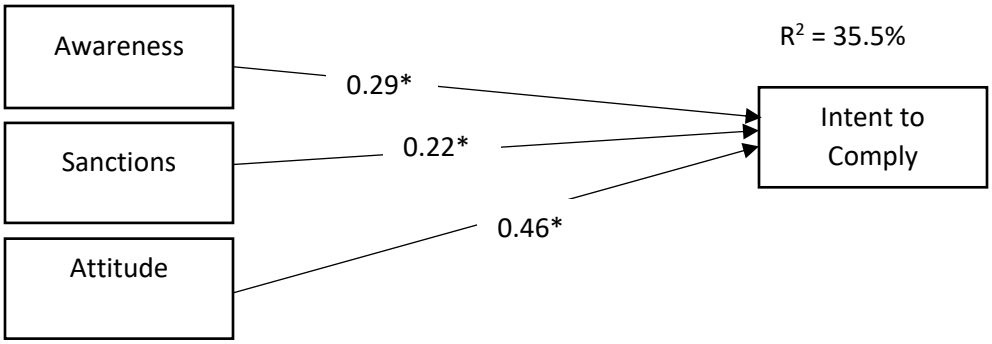
Diagonal elements are square root of AVE for each construct

To test the hypotheses, the structural path reflecting the proposed model were added. The fit statistics for structural model are CFI = 0.95, RMSEA = 0.08. These values are above the suggested cutoff values of 0.9 for CFI and 0.10 for RMSEA (Kline, 2005). The proposed model was able to explain 35.5% of variance in intent to comply (R^2 = 35.5%). Figure 2 shows the path coefficients from the structural model used to test the hypotheses.

Hypothesis 1 argued that individuals' awareness of the policies would be positively related to compliance intentions (H1). The results support this assertion with a path coefficient (β) of 0.29 significant at p=0.05. In hypothesis 2, the importance of sanctions in guiding behavior is proposed. A significant relationship between sanctions and intent to comply was found at 5% level of significance with

β of 0.22. Hypothesis 3 about attitude' effect on intent to comply was also supported at 5% level of significance with β of 0.46.

Figure 2: Proposed model with path coefficients



DISCUSSION

In this paper, the retail employees' intention to comply with information security policies was investigated. As information security becomes integral in retail settings, a holistic approach to security that goes beyond technological tools is necessary. In this approach, employees are seen as a key participant in ensuring information security(Mitnick, 2003). A security aware and compliant employee is a good defense to security attacks (like phishing, social engineering, fraud etc.). The results indicate that if the employees see the policies as a necessary step to achieve security, they will be prone to be compliant to policies. Alternatively, if they perceived the policies as a nuisance to their workflow, then compliance will be low. In addition, as the employees become aware of the policies and the reasons for the policies (for example – password policy could explain the need for complex password in addition to the requirements of password) they will be more likely to be compliant to those policies(Ayyagari & Figueroa, 2017). Lastly, perceived sanctions convey the seriousness of the policies and results from this study suggest that it improves compliance.

Before the implications are discussed, the authors acknowledge the limitations of this study. The sample used in this research came from one store of a multinational company. Therefore, researchers are cautioned to generalize the study results without further testing in other settings. The constraints of study design also yield certain limitations. The authors did not measure actual compliance behaviors, compliance intentions are used. Further, the use of cross-sectional data provides an indication of correlation rather than causation. Future research could potentially use data across time to test causality.

The results from this study provide some managerial tools to enhance security policy compliance in retail settings. As employees' awareness about ISP improves, individuals are better informed about the expected behaviors. It is also important to be clear on the sanction policy and follow-up on the violations. Management could conduct security training to increase awareness to policies and sanctions. Trainings are an integral part of retail to address loss prevention(NRF, 2018). Security culture is shaped and reflected in organization's training programs. Retail organization's culture is also shown to be a strong indicator of compliance (Church, 2014). Therefore, organizations should strive to develop a security-aware culture(Paulsen & Coulson, 2011).

Increasing awareness through training and educational programs can also benefit the organization in other ways. Service is a key part of retail industry and service employees face situations of fuzzy requests from customers that could fall beyond normal duties. These tricky situations can have profound impact on the organization, especially when the requests are information security related. Identification of these tricky requests and appropriate handling of these kind of situations are necessary to ensure compliance(Sijun Wang, Sharon E. Beatty, & Liu, 2012).

In addition, service encounters are shown to impact customers (Grandey, Goldberg, & Pugh, 2011). As information security concerns enter the common sphere of knowledge of customers, the employees' behavior and attitudes towards security could portray organization's information security effectiveness to customers. Such portrayal is important as customers' information security perceptions are linked to continued use of services(Liao & Shi, 2017). In other retail contexts, addressing security is shown as an important factor to building consumer trust (Nilashi, Ibrahim, Reza Mirabi, Ebrahimi, & Zare, 2015; Toufaily, Souiden, & Ladhari, 2013).

CONCLUSION

In conclusion, as the retail industry faces continued information security threats, this study highlights the importance of human element in retail information security. Drawing on behavioral information security research, this study validates the key role of awareness, sanctions and attitude towards information security policies in increasing compliance of retail store employees. As Symantec (2015) and anecdotal evidence in retail industry suggests, humans are the weak link in the security chain. The authors urge future security research in retail literature to focus on the human element.

REFERENCES

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes, 50*(2), 179-211. doi:https://doi.org/10.1016/0749-5978(91)90020-T

Aurigemma, S., & Mattson, T. (2017). Deterrence and punishment experience impacts on ISP compliance attitudes. *Information and Computer Security, 25*(4), 421-436. doi:doi:10.1108/ICS-11-2016-0089

Ayyagari, R., & Figueroa, N. (2017). Is Seeing Believing? Training Users on Information Security: Evidence from Java Applets. *Journal of Information Systems Education, 28*(2), 115-122.

Benedicktus, R. L., Brady, M. K., Darke, P. R., & Voorhees, C. M. (2010). Conveying Trustworthiness to Online Consumers: Reactions to Consensus, Physical Store Presence, Brand Familiarity, and Generalized Suspicion. *Journal of Retailing, 86*(4), 322-335. doi:10.1016/j.jretai.2010.04.002

Bonderud, D. (2016). Retail Security Risks: 2016 Midyear Roundup. Retrieved from https://securityintelligence.com/retail-security-risks-2016-midyear-roundup/

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-A527.

Casidy, R., Phau, I., & Lwin, M. (2016). The role of religious leaders on digital piracy attitude and intention. *Journal of Retailing and Consumer Services, 32*, 244-252. doi:https://doi.org/10.1016/j.jretconser.2016.04.006

Church, N. F. (2014). Impact of culture on retail industry compliance. *Journal of Business and Retail Management Research, 9*(1), 89-97.

Cole, C. A. (1989). Deterrence And Consumer Fraud. *Journal of Retailing, 65*(1).

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & Security, 32*, 90-101. doi:10.1016/j.cose.2012.09.010

D'Arcy, J., & Herath, T. (2011). A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings. *European Journal of Information Systems, 20*(6), 643-658. doi:10.1057/ejis.2011.23

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. doi:10.1287/isre.1070.0160

Das, G. (2014). Linkages of retailer awareness, retailer association, retailer perceived quality and retailer loyalty with purchase intention: A study of

Indian food retail brands. *Journal of Retailing and Consumer Services, 21*(3), 284-292. doi:https://doi.org/10.1016/j.jretconser.2014.02.005

Dols, T., & Silvius, A. (2010). Exploring the influence of national cultures on non-compliance behavior. *Communications of the IIMA, 10*(3), 2.

Faqih, K. M. S. (2016). An empirical analysis of factors predicting the behavioral intention to adopt Internet shopping technology among non-shoppers in a developing country context: Does gender matter? *Journal of Retailing and Consumer Services, 30*, 140-164. doi:https://doi.org/10.1016/j.jretconser.2016.01.016

Fornell, C., & Larcker, D. F. (1981). Evaluating Structural Equation Models with Unobservable Variables and Measurement Error. *Journal of Marketing Research, 18*(1), 39-50. doi:10.2307/3151312

Grandey, A. A., Goldberg, L. S., & Pugh, S. D. (2011). Why and When do Stores With Satisfied Employees Have Satisfied Customers?: The Roles of Responsiveness and Store Busyness. *Journal of Service Research, 14*(4), 397-409. doi:10.1177/1094670511410304

Guo, K. H. (2013). Security-related behavior in using information systems in the workplace: A review and synthesis. *Computers & Security, 32*, 242-251. doi:10.1016/j.cose.2012.10.003

Guo, K. H., & Yuan, Y. (2012). The effects of multilevel sanctions on information security violations: A mediating model. *Information & Management, 49*(6), 320-326. doi:https://doi.org/10.1016/j.im.2012.08.001

Hansen, T., Møller Jensen, J., & Stubbe Solgaard, H. (2004). Predicting online grocery buying intention: a comparison of the theory of reasoned action and the theory of planned behavior. *International Journal of Information Management, 24*(6), 539-550. doi:https://doi.org/10.1016/j.ijinfomgt.2004.08.004

Heinze, J., Thomann, M., & Fischer, P. (2017). Ladders to m-commerce resistance: A qualitative means-end approach. *Computers in Human Behavior, 73*, 362-374. doi:https://doi.org/10.1016/j.chb.2017.03.059

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

Hu, Q., Xu, Z., Dinev, T., & Ling, H. (2011). Does deterrence work in reducing information security policy abuse by employees? *Commun. ACM, 54*(6), 54-60. doi:10.1145/1953122.1953142

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security, 31*(1), 83-95. doi:https://doi.org/10.1016/j.cose.2011.10.007

Johnston, A. C., & Warkentin, M. (2010). Fear Appeals And Information Security Behaviors: An Empirical Study. *MIS Quarterly, 34*(3), 549-A544.
Kajalo, S., & Lindblom, A. (2015). Creating a safe and pleasant shopping environment: a retailer's view. *Property Management, 33*(3), 275-286. doi:10.1108/PM-10-2014-0042
Karjalainen, M., & Siponen, M. (2011). Toward a New Meta-Theory for Designing Information Systems (IS) Security Training Approaches. *Journal of the Association for Information Systems, 12*(8), 518-555.
Kline, R. B. (2005). *Principles and Practice of Structural Equation Modeling*. New York, NY: The Guilford Press.
Koistinen, K., & Järvinen, R. (2016). Comparing perceived insecurity among customers and retail staff during service encounters. *Journal of Retailing & Consumer Services, 31*, 80-92. doi:10.1016/j.jretconser.2016.03.014
Lian, J.-W., & Lin, T.-M. (2008). Effects of consumer characteristics on their acceptance of online shopping: Comparisons among different product types. *Computers in Human Behavior, 24*(1), 48-65. doi:https://doi.org/10.1016/j.chb.2007.01.002
Liao, Z., & Shi, X. (2017). Web functionality, web content, information security, and online tourism service continuance. *Journal of Retailing and Consumer Services, 39*, 258-263. doi:https://doi.org/10.1016/j.jretconser.2017.06.003
Maheshwari, S. (2014). Home Depot Hack Is Now The Biggest Retail Breach In U.S. History. Retrieved from https://www.buzzfeed.com/sapna/home-depot-hack-is-now-the-biggest-retail-breach-in-us-histo?utm_term=.ob4N5E8Mg#.kdyv56mdg
Mathieson, K. (1991). Predicting User Intentions: Comparing the Technology Acceptance Model with the Theory of Planned Behavior. *Information Systems Research, 2*(3), 173-191. doi:10.1287/isre.2.3.173
Meents, S., & Verhagen, T. (2018). Reducing consumer risk in electronic marketplaces: The signaling role of product and seller information. *Computers in Human Behavior, 86*, 205-217. doi:https://doi.org/10.1016/j.chb.2018.04.047
Mitchell, V., Balabanis, G., Schlegelmilch, B., & Cornwell, T. (2009). *Measuring Unethical Consumer Behavior Across Four Countries* (01674544). Retrieved from http://ezproxy.lib.umb.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=43707385&site=ehost-live
Mitnick, K. D. (2003). Are You the Weak Link? *Harvard Business Review, 81*(4), 18-20.
Nascimento, B., Oliveira, T., & Tam, C. (2018). Wearable technology: What explains continuance intention in smartwatches? *Journal of Retailing and*

Consumer Services, *43*, 157-169. doi:https://doi.org/10.1016/j.jretconser.2018.03.017

Nepomuceno, M. V., Laroche, M., & Richard, M.-O. (2014). How to reduce perceived risk when buying online: The interactions between intangibility, product knowledge, brand familiarity, privacy and security concerns. *Journal of Retailing & Consumer Services*, *21*(4), 619-629. doi:10.1016/j.jretconser.2013.11.006

Nilashi, M., Ibrahim, O., Reza Mirabi, V., Ebrahimi, L., & Zare, M. (2015). The role of Security, Design and Content factors on customer trust in mobile commerce. *Journal of Retailing & Consumer Services*, *26*, 57-69. doi:10.1016/j.jretconser.2015.05.002

NRF. (2018). 2018 National Retail Security Survey In N. R. Foundation (Ed.).

Paulsen, C., & Coulson, T. (2011). Beyond awareness: Using business intelligence to create a culture of information security. *Communications of the IIMA*, *11*(3), 4.

Perlman, Y., & Ozinci, Y. (2014). Reducing shoplifting by investment in security. *Journal of the Operational Research Society*, *65*(5), 685-693. doi:10.1057/jors.2013.37

Priporas, C.-V., Stylos, N., & Fotiadis, A. K. (2017). Generation Z consumers' expectations of interactions in smart retailing: A future agenda. *Computers in Human Behavior*, *77*, 374-381. doi:https://doi.org/10.1016/j.chb.2017.01.058

Puhakainen, P., & Siponen, M. (2010). Improving Employees' Compliance Through Information Systems Security Training: An Action Research Study. *MIS Quarterly*, *34*(4), 757-778. doi:10.2307/25750704

Rana, J., & Paul, J. (2017). Consumer behavior and purchase intention for organic food: A review and research agenda. *Journal of Retailing and Consumer Services*, *38*, 157-165. doi:https://doi.org/10.1016/j.jretconser.2017.06.004

Rigotti, N. A., Stoto, M. A., Bierer, M. F., Rosen, A., & Schelling, T. (1993). Retail Stores' Compliance With a City No-Smoking Law. *American Journal of Public Health*, *83*(2), 227-232.

Security. (2016). Shoppers Blame Retailers for Security Breaches. *Security*.

Shropshire, J., Warkentin, M., & Sharma, S. (2015). Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. *Computers & Security*, *49*, 177-191. doi:https://doi.org/10.1016/j.cose.2015.01.002

Sijun Wang, Sharon E. Beatty, & Liu, J. (2012). Employees' Decision Making in the Face of Customers' Fuzzy Return Requests. *Journal of Marketing*, *76*(6), 69-86. doi:10.1509/jm.10.0529

Siponen, M., & Vance, A. (2010). Neutralization: New Insights Into The Problem Of Employee Information Systems Security Policy Violations. *MIS Quarterly, 34*(3), 487-A412.

Sreen, N., Purbey, S., & Sadarangani, P. (2018). Impact of culture, behavior and gender on green purchase intention. *Journal of Retailing and Consumer Services, 41*, 177-189. doi:https://doi.org/10.1016/j.jretconser.2017.12.002

Syed, S. A., & Nazura, M. S. (2011). Applying the Theory of Planned Behavior (TPB) in halal food purchasing. *International Journal of Commerce and Management, 21*(1), 8-20. doi:doi:10.1108/10569211111111676

Symantec. (2015). Cyber Security for Retail Services. Retrieved from https://www.symantec.com/content/dam/symantec/docs/white-papers/cybersecurity-retail-en.pdf

Taylor, A. B. (2018). Retailer Data Breaches in 2018: Was Your Favorite Store Hacked? Retrieved from https://www.kiplinger.com/article/spending/T048-C011-S001-retailer-data-breaches-2018-favorite-store-hacked.html

Toufaily, E., Souiden, N., & Ladhari, R. (2013). Consumer trust toward retail websites: Comparison between pure click and click-and-brick retailers. *Journal of Retailing & Consumer Services, 20*(6), 538-548. doi:10.1016/j.jretconser.2013.05.001

Ugrin, J. C., & Michael Pearson, J. (2013). The effects of sanctions and stigmas on cyberloafing. *Computers in Human Behavior, 29*(3), 812-820. doi:https://doi.org/10.1016/j.chb.2012.11.005

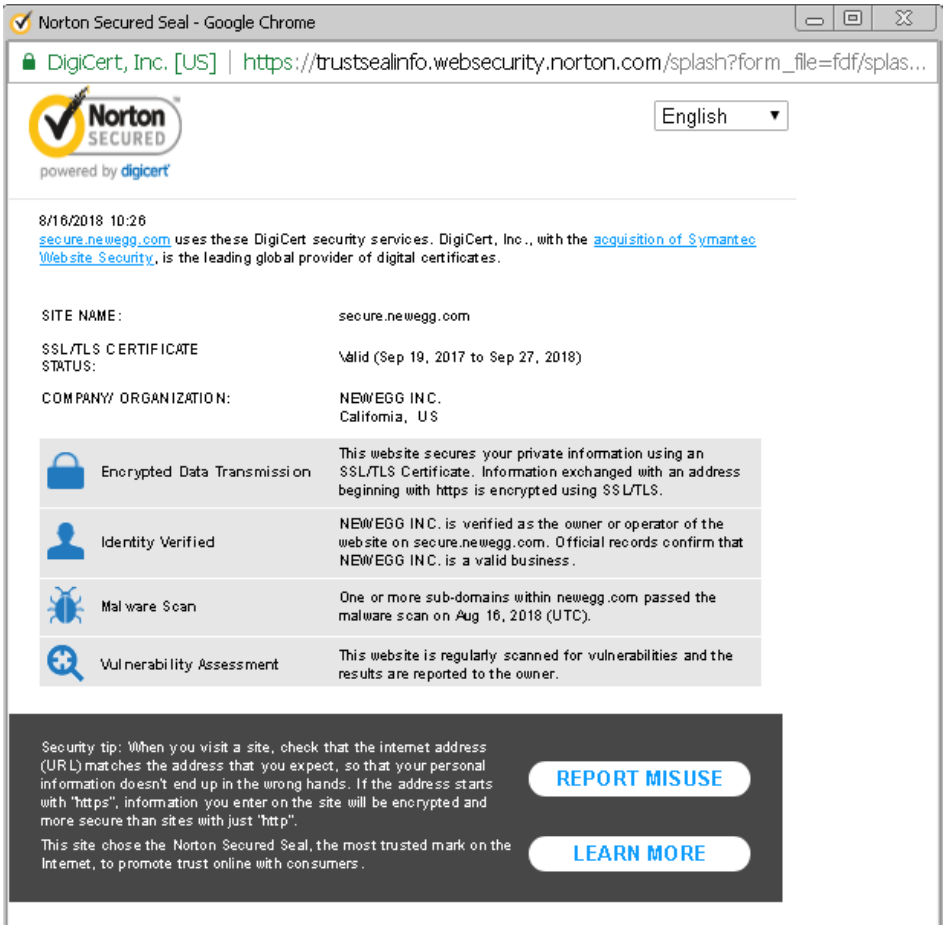
Vroom, C., & von Solms, R. (2004). Towards information security behavioural compliance. *Computers & Security, 23*(3), 191-198. doi:10.1016/j.cose.2004.01.012

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. doi:10.1057/ejis.2009.12

Yeo, V. C. S., Goh, S.-K., & Rezaei, S. (2017). Consumer experiences, attitude and behavioral intention toward online food delivery (OFD) services. *Journal of Retailing and Consumer Services, 35*, 150-162. doi:https://doi.org/10.1016/j.jretconser.2016.12.013

Appendix A

A typical retailer's website indicating the security tools used



Appendix B

Measures used in this study

Construct	Items
Awareness	• I know the rules and regulations prescribed by the information security (ISP) policy of my company. • I understand the rules and regulations prescribed by the information security policy (ISP) of my company • I know my responsibilities as prescribed in the information security policy (ISP) to enhance the information security of my company
Attitude	To me, complying with the requirements of the information security policy (ISP) is…. • Not beneficial…beneficial • Not important…important • Not useful…useful
Sanctions	• What is the chance you would receive sanctions if you violated the company information security policy (ISP)? • What is the chance that you would be formally sanctioned if management learned that you had violated company information security policy (ISP)? • What is the chance that you would be formally disciplined if management learned you had violated company information security policy (ISP)?
Intent to Comply	• I intend to comply with the requirements of the ISP of my company in the future. • I intend to protect information and technology resources according to the requirements of the ISP of my company in the future. • I intend to carry out my responsibilities prescribed in the ISP to enhance the information security of my company when I use information and technology in the future