5-2012

Employee Compliance with Information Systems Security Policy in Retail Industry. Case: Store Level Employees

Bertrand Muhire
University of Massachusetts Boston

Employee Compliance with Information Systems Security Policy in Retail Industry. Case: Store Level Employees

---

Honors Thesis

Bertrand Muhire
May, 2012

University of Massachusetts Boston
Advisor: Ramakrishna Ayyagari, PhD
Director: Jeffrey Keisler, PhD

Table of Contents

Introduction

In this digital era, information has become a very important component to any type of organizations. For some, it is not only an important component of daily routine operations but also required for competitive advantage. From big corporations to small businesses, non-profit organizations and governments, organizations need to safeguard and secure their information by implementing information security policies and make sure that all employees comply with such policies.

Since information is growing faster than in the previous decades, there is a need to safeguard and manage that information efficiently and effectively in order to make it useful. One of the ways to have reliable and useful information is to protect and secure it by following organizations' information systems security policies. Bulgurcu *et al.(2010)* remark that understanding compliance behavior is crucial for organizations that want to leverage their human capital as employees behave differently therefore comply differently with IS security policies. Previous research has shown that employees violation of IS security policies is due to negligence and/or ignorance of the IS security policies on the part of employees (Vroon and von Solms 2004).

The 2012 Data Breach Investigation Report, a study conducted by the Verizon RISK Team with cooperation from the Australian Federal Police, Dutch National High Tech Crime Unit, Irish Reporting and Information Security Service, Police Central e-Crime Unit, and United States Secret Service says that nearly 90% of the reported total of 855 breaches are a result of deliberate and malicious employee actions. These internal Insiders are trusted and privileged at different security levels. They include company executives, employees, independent contractors, interns, etc.

In order to maintain compliance standards with information security policies, managers have to make decisions on the use of effective techniques to deal with non-compliance; these include correctional responses like sanctions, information security training or additional systems security features and layers (with the associated costs to the organization that include less flexibility in routine operations). To achieve that, they need to assess and understand factors behind employees' non compliance in order to address it efficiently.

Information security policy (ISP)

Bulgurcu et al. (2010) define information security policy as a statement of the roles and responsibilities of the employees to safeguard the information and technology resources of their organizations. Whitman (2008) defines ISP as a policy that encompasses established rules that address specific security issues by providing instructions to the employees as to what they should do when they interact with the information and technology resources of their organizations

Previous studies on information security policy compliance

A number of theories have been developed and applied to particular cases in different work environments. Previous researchers have focused on studying the factors underlying employees' compliance behaviors and have used different populations for study. The most prominent theories used to explain compliance behavior, from behavioral sciences, are the deterrence theory and the neutralization theory. With regard to IS security, the deterrence theory suggests that 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 (Siponen *et al*. 2010). The neutralization theory, as an excellent predictor of employees' intentions to violate IS security

policy, suggests that employees fail to comply with IS security policies because they perceive their workload as high, they are busy with other assignments, security policies slow them down, and other work is more important (Puhakainen 2006). They suggest that policy awareness campaigns and educational sessions on neutralization need to be examined in order to identify effective means of inhibiting the use of neutralization techniques and thus improve IS security compliance (2010). In this study, we build from the importance of educational sessions, and focus on formal school education to try to understand the role of education level with respect to information security policy compliance.

There are many factors that influence employees' behaviors towards compliance to IS security policies. In their research, Pahnila *et al*. concluded that attitude, normal beliefs (social positive pressure) and habits have a significant effect on intention to comply with IS security policies. They argue that threats, sanctions and rewards don't have a significant impact on employees' intentions to comply with IS security policies. It is important to have a clear and concise communication from managers and IS security staff to employees about the importance of complying with IS security policies (2007). This study will explore the education level as one of the factors that influence compliance behaviors. Since their research was conducted on a population composed of individuals in managerial positions, Pahnila *et al*. recommended future research that would use a different type of population.

Another theory also confirmed that factors that motivate employees to comply with IS security policies extend beyond compliance instruments such as sanctions and rewards (Bulgurcu *et al*. 2010). Their study results indicate that beliefs about overall assessment of consequences are the immediate antecedents of attitude (2010).

They recommend further research to study different other individual factors to explain compliance from a different perspective.

Johnston *et al*. (2010) focused more on predicting employees' behaviors towards compliance with IS security policy. The research concluded that properly worded communications will spur responses from users that are consistent with the organization's goals with regard to the adoption of secure behaviors (Johnston *et al*. 2010). The use of threat as a way to predict employees' behaviors is a limitation to this study as behavior was not tested under their study. The research was conducted in an academic setting where faculty, staff and students individuals made up the sample in the experiment. They agree that this population under study was a more knowledgeable group and that their findings can be generalized to university settings, educated and professional employees. This limitation opens doors to further research using a different group.

A conceptual framework was designed by Siponen where he argues that all approaches affecting the behavior of the user (increasing awareness, etc) should, in order to be effective, satisfy the requirements of behavioral theories and provide answers for end-users, explaining (or letting them observe) why they should follow security guidelines (2000).
In this respect, Siponen notes, a set of persuasive approaches based on morals and ethics, wellbeing, a feeling of security, rationality, logic and emotions is set out (2001). His study doesn't reference any particular population to test the relevance of his findings, therefore opening doors for further research.

As part of a group of studies that focused on predicting employees' compliance behaviors, Boss *et al*. concluded that mandatoriness and its antecedents significantly impact individual precaution-taking behaviors.

They introduced the concept of mandatoriness in the context of information systems' security and show that when individuals view a policy as mandatory they will take precautions as required. They studied the concept of mandatoriness and concluded that different employees understand and adhere to policies differently (2009).

Boss *et al.* study also shows that as a result of understanding employees behaviors, managers need to emphasize the specification of policies and evaluation of those policies for non-compliance, while giving less emphasis to reward (2009). Besides the proposed important managerial implications, this study has one main limitation: the use of a single respondent to measure both the dependent and the independent variables that could lead to common bias.

The population used for this study included employees who used computers on a daily basis. They included support staff, professional services, technical services, nurses and nursing services, physicians, and management, therefore excluding low education and low pay employees.

Summary table of literature

Study	Main variables	Theory/Model used	Method	Key findings	Contribution	Sample used	Recommendation
Bulgurcu, Burcu (2010)	Information security awareness, Sanctions, Intent to comly, etc	Theory of planned behavior	Survey	Evidence of the significant impact of motivational factors other than rewards and sanctions that reinforce an	Theoretical explanation and empirical support for the impact of an employee's beliefs about the	Employees who use the IT resources of their organizations and had access to the	

				employee's compliance behavior	consequences of compliance and non-compliance with the ISP on attitude toward compliance with the ISP	Internet	
Siponen, Mikko (2010)	Intent to comply, Education, Age, work experience	Neutralization theory; Deterrence theory	Survey	Neutralization is an important factor to take into account with regard to developing and implementing organizational security policies and practices		Office personnel at two Finnish organizations	
Johnston, Allen C. (2010)	Behavioral intent , Social influence, Response efficacy, Self-efficacy, Threat severity , Threat susceptibility	Fear Appeal Model	Laboratory experiment	End users are not consistent in their behavioral intentions to comply with recommendations to protect their informational assets	Applying a well-established theory to the field of Information Systems	Staff, faculty and students	Further research using different subject pools and organizational environments

Puhakainen, Petri (2010)	Universal constructive theory; Elaboration likelyhood model	Interviews, Participatory observation,	Successful IS security policy compliance training should take into account the learner's previous knowledge regarding IS security policy compliance.	Information security training	Employees with a college degree in Finland	Using different population or culture to test research findings

Previous methodologies on information security policy compliance

Different types of methods have been used to study employees' compliance with information systems security policy. Behavioral theories from other fields, mainly psychology and criminology, have been used in designing models and hypotheses from different perspectives of employees' behaviors towards information security policies.

In their research, Siphoned *et al* (2010) used hypothetical modeling to study employees' behaviors with regards to compliance with information systems security policies. Scenario-based methods using the tool "What is the chance that you would do what Pekka [the adapted individual in the scenario] did in the described scenario" were used to measure the dependent variable "*Intention to violate information security policy"* on an 11-point scale from 0 to 10. They also collected biographical data like age, gender, work, and experience combined with another 10-point scale used to measure a single-item that asked respondents to rate hoe believable the scenario was, from 0 (not believable) to 10 (100% believable) (2010).

The population for this study was administrative personnel from three organizations in Finland: a university, a major electrical company, and the corporate office of a large supermarket chain. For the university sample, approximately half of the respondents were IT support staff with a master's degree, while the other half were administrative staff with a university or a technical degree. In the corporate office sample, nearly all employees held a master's degree and for the electrical company sample most respondents were administrative staff and possessed a university degree (2010). The total number of respondents from the three samples was 1449.

Using a laboratory experiment, Johnston *et al*. studied the influence of fear appeals on the compliance of end users with recommendations to enact specific individual computer security actions towards mitigation of threats (2010).

They studied a university population that included faculty, staff, and students whom are frequently susceptible to the threat of spyware. Three samples were created from randomly selected participants and were administered the survey for a pretest.

From a total of 780 solicited participants, a total of 311 subjects responded and 275 produced usable data. The survey comprised of messages that measured six constructs: behavioral intent, social influence, response efficacy, self efficacy, threat severity, and threat susceptibility. These constructs were multi-item scaled and adapted to relate specifically to the context of security responses to spyware (2010). Clear statements on personal consequences were included in the survey to emphasize computer infection by spyware and subjects responded differently. This shows that the application of such statements resulted in change in variables which show that subjects

were aware of the manipulation. The limitation to this method is that results of the study cannot be generalized to the general public, as Johnston *et al*. conclude, since the population selected for the study is highly knowledgeable in information security.

As an improvement to the field of information security and based on critics of previous studies that they lacked empirically and theoretically grounded methods to study compliance to information security policy, Pahnila *et al*. developed a model that focused on three main factors: attitude towards compliance, intention to comply and actual compliance with information systems security policies which are based on the widely used Theory of Reasoned Action (TRA) (2007). Their model and hypotheses were tested using a web-based questionnaire administered to employees in Finland. The population of this study was 750 employees of a large group in Finland. The group has business subsidiaries in food and groceries, specialty goods, hotels and restaurants, hardware and agriculture, automobiles and service stations. A total of 240 responders provided usable and reliable data and regression analysis was used to find whether the proposed hypotheses were supported and founded.

Based on scales that are proven reliable, a survey method was used by Bulgurcu *et al*. to test a model and formed hypotheses in the context of information security policy compliance with reference to behavioral theories and employees awareness of information security policies. Their model, derived from the Theory of Planned Behavior (TPB), explains an employee's intention to comply with the information security policy and focused on attitudes towards compliance, employees' normative beliefs about compliance, and employees' self efficacy in complying with information security policy.

The survey was pretested and refined especially in cases where some study constructs did not meet the existing measuring scales. In the latter case, new measures were developed by closely following the definition of constructs in the study (2010). A total number of 3,150 invitation emails were sent to potential participants employed by a diverse group of organizations to form a more diverse sample population. A total number of 1,098 accepted the invitation and 928 of them decided to participate in the survey.

An exclusion criterion was applied to filter out those participants whose companies did not have explicitly written information security policies. As a result, a sample of 464 usable questionnaires provided data that was used in the analysis where the measurement of the structural model was estimated using the partial least squares (PLS) approach. Overall, the literature on information security policy compliance includes a number of studies on information security compliance behaviors of IT professionals, accountants, lawyers, healthcare professionals, etc. leaving aside employees with a lower level of education who might be less compliant to information security policies in their organizations. Since previous research studies recommend further research using different types of populations, and based on previous literature, this research will address information security policy compliance using a population with a relatively lower education level compared to populations used by previous research studies

Research questions and Hypotheses

The importance of information security in the work place has pushed for a need for empirical studies on employees' compliance with information security policies. Siponen *et al* note that employees' failure to comply with information systems security policies is a major concern for information technology security managers (2010).

The present study looked into past studies and used a different population to understand the relationship between the level of education and information security policy awareness. Therefore the research questions are:

1. What is the impact of the level of education on employees' compliance behaviors?
2. Does the level of education affect policy awareness, therefore affecting employees' compliance behaviors?

Based on recommendations from previous studies to further research on information security policy compliance using different types of populations, and in line with existing literature, this study tests the relationships between the variables level of education, information security awareness, information security policy awareness and intent to comply, therefore the following hypotheses were developed.

We posit that the higher an employee's level of education and technology knowledge, the more the intent to comply with the ISP (Bulgurcu et al. 2010). From this assumption, we posit that the higher the education level the more employees know and understand information security policy

H1: There is a strong relationship between the level of education and information security policy awareness.

H1a: The level of education has a positive impact on information security policy awareness

From the study of Buldurcu et al. (2010) information security awareness was linked with a direct influence on an employee's attitude toward compliance with the ISP, therefore we posit that:

H2: There is a strong relationship between Information security awareness and information security policy compliance.

H2a: Information security awareness has a positive impact on information security policy compliance.

Method

Survey

Surveys were used to collect data from workers in retail industry in order to test relationships between the three research variables namely the level of education, information security awareness, information security policy awareness and intent to comply.

The survey was designed based on previous studies. All measurements items have been used by Bulgurcu et al. (2010) and included three main constructs; General Information Security Awareness (GISPA), Information Security Policy Awareness (ISPA) and Intent to Comply (IC). The following table provides constructs definitions as described by Bulgurcu et al (2010).

Construct	Definition	Adapted from
General Information Security Awareness (GISPA),	Employee's overall knowledge and understanding of potential issues related to information security and their ramifications	Bulgurcu et al. 2010

Information Security Policy Awareness (ISPA)	Employee's general knowledge about information security and his cognizance of the ISP of his organization	Bulgurcu et al. 2010
Intent to Comply (IC)	Attitude toward the decision to comply with the ISP	Bulgurcu et al. 2010

Based on the above constructs, measurements items were developed and a 5 point Likert scale was used along measurement statements to capture respondents' opinions. The survey was also used to capture basic socio-demographic information; age, and gender.

Sample

Based on recommendations from previous studies, the population for this study was different from populations previously used. Respondents were a convenience sample of employees at a Boston area retail store of one of the largest retail chain in the United States with revenues over 50 Billion and overseas operations . Participation was voluntary and responses were anonymous as the survey required no personal or identifying information. Respondents completed surveys outside their work place to avoid bias from co-workers, supervisors and managers.

Out of 120 surveys that were distributed, 72 surveys provided useful responses; therefore the sample consists of a total of 72 respondents which is a 60% of the targeted sample.

Gender	
Males	34
Females	38
Education level	
Less than high school	0

High school	28
Some college	20
Undergraduate degree	22
Graduate degree	0
No response	2

Out of 72 respondents, 7 have two or less years of work experience, 19 of them have three to five years, 23 have six to eight years and 22 have nine years and more.

The survey also captured respondents' age groups. Out of 72 respondents, 16 were between 18 to 30 years old, 25 were between 31 and 50, 22 were between 51 and 70, and 8 were 71 years old and more.

Data analysis

Collected data was coded in Microsoft Excel and exported into SPSS for analysis. First missing data were fixed using the missing data function in SPSS which uses averages to fill in the missing data for each entry; then means were calculated for each measurement item. Descriptive statistics, linear regression and correlation were used as tools to test hypotheses.

We expect significant differences in intent to comply and information security awareness based on different levels of education Awareness.

Results and discussion

For the independent variable Education level, since there was no respondent with less than high school diploma (Education level =1) and a graduate degree (Education level =4), we retained only three groups with nominal numbers assigned to each group during the data coding in MS Excel. The groups are high school diploma (2), some college (3) and college degree (4)

We first tested if there was a significance difference among the three different groups. We used the ANOVA test and the following table shows a significant difference between groups for the independent variables, since the significance coefficients for both ISPA (.006) and IC (.000) are closer to zero.

Analysis of variances between groups (ANOVA)

		Sum of Squares	df	Mean Square	F	Sig.
ISPA	Between Groups	7.780	2	3.890	5.435	.006
	Within Groups	49.381	69	.716		
	Total	57.160	71			
IC	Between Groups	6.881	2	3.440	9.960	.000
	Within Groups	23.835	69	.345		
	Total	30.716	71			

ISPA = Information Security Policy Awareness; IC = Intent to Comply

Comparison of Education level groups

Dependent Variable	(I) Education	(J) Education	Mean Difference (I-J)	Std. Error	Sig.
ISPA	2	3	.45238	.24102	.153
		4	.78571*	.24102	.005
	3	2	-.45238	.24102	.153
		4	.33333	.25507	.396
	4	2	-.78571*	.24102	.005
		3	-.33333	.25507	.396
IC	2	3	.47078*	.16745	.017
		4	.72835*	.16745	.000
	3	2	-.47078*	.16745	.017
		4	.25758	.17721	.320
	4	2	-.72835*	.16745	.000
		3	-.25758	.17721	.320

Education levels: 2=high school degree, 3= some college, 4=college degree

ISPA = Information Security Policy Awareness; IC = Intent to Comply

* The mean difference is significant at the 0.05 level.

We compared means of the three education groups to check the relevance of the difference between the groups. For the dependent variable ISPA, we can observe that group 2 and group 3 have mean difference of .45238 which is not as significant as the mean difference between group 2 and group 4, where the mean difference is .78571 and the has a very significance (.005)
For the independent variable IC, the mean difference between group 2 and group 3 is .47078 with a significance coefficient at .017. Then, the mean difference between group 2 and group 4 is .72835 with a significance coefficient of .000.
For both variables, the mean difference between group 3 and group 4 is not that significant as it is .33333 for ISPA with a significance coefficient of .396 (which implies a lower significance level) and .25758 for IC and a significance coefficient of .320.

Correlations

After checking the relevance of the existing differences between the three education level groups, we run a Person's correlation test to find the correlation coefficients between each of the variables IC, ISPA and GSA.

		IC_AVG	ISPA_AVG	GSA_AVG
IC	Pearson Correlation	1	.386**	.488**
	Sig. (2-tailed)		.001	.000
	N	72	72	72
ISPA	Pearson Correlation	.386**	1	.608**
	Sig. (2-tailed)	.001		.000
	N	72	72	72
GSA	Pearson Correlation	.488**	.608**	1
	Sig. (2-tailed)	.000	.000	
	N	72	72	72

ISPA = Information Security Policy Awareness; IC = Intent to Comply; GSA = General Security Awareness

**. Correlation is significant at the 0.01 level (2-tailed).

The above table presents Pearson's correlation coefficient and they all are positive. It also shows the significance of the correlation between the three variables. ISPA is positively correlated with IC with a coefficient of .386; and is strongly correlated with GSA with a coefficient of .488.
There's also a very strong correlation between GSA and ISPA with a coefficient of .608 and a significance coefficient of .000.

Hypotheses testing

This research studies the effect of the level of education on employees' intent to comply with information security policy. In accordance with Bulgurcu et al. whom posit that the higher an employee's level of education and technology knowledge, the more the intent to comply with the ISP (2010), we posit that

H1: There is a strong relationship between the level of education and information security policy awareness.

And

H1a: The level of education has a positive impact on information security policy awareness

Based on the results, hypotheses *H1 and H1a* are founded. There is a strong difference between group 2 (high school level) and group 4 (college degree) ISP Awareness; the mean difference for group 2 and group 4 is .78571 with a significance at 0.005 while there from group 3 to group 4 the mean difference is only .3333 without a very high significance (only at .396).
The same results show that education level has a positive impact on ISP Awareness.

Panhila et al. pointed out the importance of ISP awareness in a way that effective IS security requires that employees are not only aware of, but also comply with the IS security policies and guidelines (2007). Based on the above argument we hypothesize that:

H2: There is a strong relationship between Information security awareness and information security policy compliance.

Our research findings support Hypotheses *H2.* The correlation and significance coefficients prove that there is strong relationship between ISP Awareness and intent to comply, and it is very significant (correlation coefficient r=.386) and the significance coefficient is .001.
These findings also show that ISP Awareness has a positive impact on intent to comply. Findings support the hypothesis:

H2a: Information security awareness has a positive impact on information security policy compliance.

The higher correlation coefficient between ISP Awareness and Intent to comply (r=.386) implies that ISP Awareness exerts a positive and negative influence on Intent to Comply; which means that the more employees are aware of ISP the more they are likely to comply with it; and they are less likely to comply when they are not aware of the policy.

Implications and future research

These research findings demonstrate that the level of education has an impact on employees' compliance behaviors. The same findings also show that education has a positive effect on information security policy awareness, which in turn affects employees' compliance behaviors.

Numerous previous studies concerning computer security and information assurance have involved higher education employees or students (Aytes and Connolly 2004; Warkentin et al. 2004). This research used a population which relatively has a lower level of education and tested its impact on employees' compliance behaviors. Previous studies have focused on other factors such as sanctions, rewards, training on information security, and a lot more from a behavioral research perspective like fear of sanctions, self-efficacy, social influence, etc (Warkentin et al. 2004).

The fact that respondents participated in the study without pressure form top management and peer influence, implies reduced bias therefore the strength of this research. We understand a larger sample (only 72 respondents for this study) would provide stronger and richer results, therefore addressing the main limitation of this study.

This research will contribute to the growing knowledge on information security policy compliance in work places. It looks at the problem of information security policy compliance from a different perspective compared to previous studies. It should also serve as a guide to help information security administrators and managers to efficiently address the problem of non-compliance. This study should help managers understand the importance of information security policy awareness and its implication on compliance. As a contribution to the field of information security, this research provides a new approach to understanding factors underlying information security policy compliance. From this study managers and information security administrators should understand and take into account the impact of education on information security policy awareness when they make strategic decisions on information security policies and their implementation to address the problem of non-compliance.

Conclusion

In recent years, the problem of employee compliance with information security policy has become a major concern for organizations. Mostly because employees misuse or abuse information technology resources in their work places which result in costly consequences like compromised data, which leads to an organization's reputation therefore performance.

Based on previous research studies that recommended further research on employee compliance using a different type of population; this study focused on employee compliance in retail industry particularly store employees. This type of population is different from the previously used population in a way that the level of education is generally lower (high school to some college years in college, and some but few college graduates).

The results showed that the there is a strong and positive relationship between the level of education and information security awareness. Results also showed that the level of education has a positive impact on employees' intent to comply because the higher the level of education implies the more employees are aware of information security policy and are likely to comply with it. The assumption is that they understand better the importance such a policy and the consequences of non-compliance to their organization.

This research will help information security managers address the problem of information security compliance because it provides them with an understanding of one of the many factors underlying employee compliance behaviors.

References

Aytes, K., and Connolly, T. 2004. "Computer Security and Risky Computing Practices: A Rational Choice Perspective," Journal of Organizational & End User Computing (16:3), pp. 22-40.

Bulgurcu, B., Cavusoglu, H., Benbasat, I. "Information security policy compliance: An empirical study of Rationality-Based Beliefs and Information Security Awareness". MIS Quarterly, Vol. 34, No. 3, September 2010, pp 523-548.

Boss S. R., Kirsch L. J., Angermeier I., Shingler R. A., Boss R. W., "If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security". European Journal of Information Systems, Vol. 18, pp 151-164.

Johnston, A. C., Warkentin, M. "Fear appeals and information security behaviors: An empirical study". MIS Quarterly, Vol. 34, No. 3, September 2010, pp 549-566.

Puhakainen,P. "A design theory for information security awareness", unpublished PhD thesis, University of Oulu, Finland, 2006.

Puhakainen,P., Siponen M. "Improving employees' compliance through information systems security training: An action research study". MIS Quarterly, Vol. 34, No. 4, December 2010, pp 757-778.

Punhila, S., Siponen M., Mahmood A. "Employees' behavior towards IS security policy compliance". Proceedings to the 40th Hawaii International Conference on System Science, 2007.

Siponen M. “A conceptual foundation for organizational information security awareness”. Information Management and Computer Security Journal, 8, 1 (2000), pp 31-41

Siponen M., Vance A. “Neutralization: New insights into the problem of employee information systems security policy violation”. MIS Quarterly, Vol. 34, No. 3, September 2010, pp 487-502.

Vroom, C., von Solms, R. “Towards information security behavioral compliance”. Computers and Security, Vol. 23, No.3, pp 191-198.

APPENDIX A: Survey

1. This research project will study policy compliance behaviors.
2. Questions are designed to measure your opinions on specific statements on the survey and will take approximately 10 minutes to respond.
3. There is no right or wrong answers; we just need your opinion.
4. **Confidentiality**: The information you will provide will not be published or presented in a way that would allow anyone to identify you. No names, phone numbers or addresses will be collected.
5. You may terminate participation at any time without consequences.

Education level		**Gender**	
Less than high school	O	Male	O
High school degree	O	Female	O
Some college	O		
Undergraduate degree	O		
Graduate degree	O		

1. In the context of your work environment…

	Strongly agree	**Agree**	**Neutral**	**Disagree**	**Strongly disagree**
Overall, I am aware of the potential information security threats and their negative consequences.	O	O	O	O	O
I understand the concerns regarding information security and the risks they pose to companies in general.	O	O	O	O	O

2. In the context of your work environment, answer the following regarding Information Security Policy (ISP)

	Strongly agree	**Agree**	**Neutral**	**Disagree**	**Strongly disagree**
I know the rules and regulations prescribed by the information security (ISP) policy of my company.	O	O	O	O	O
I understand the rules and regulations prescribed by the information security policy (ISP) of my company.	O	O	O	O	O
I know my responsibilities as prescribed in the information security policy (ISP) to enhance the information security of my company.	O	O	O	O	O

3. To me, complying with the requirements of the information security policy (ISP) is….

Very necessary	Necessary	Neutral	Unnecessary	Unnecessary
O	O	O	O	O
Very beneficial	Beneficial	Neutral	Unbeneficial	Very beneficial
O	O	O	O	O
Very important	Important	Neutral	Unimportant	Very unimportant
O	O	O	O	O
Very useful	Useful	Neutral	Useless	Very useless
O	O	O	O	O

4. In the context of your work environment, answer the following regarding Information Security Policy (ISP)

	Strongly agree	Agree	Neutral	Disagree	Strongly disagree
I intend to comply with the requirements of the ISP of my company in the future.	O	O	O	O	O
I intend to protect information and technology resources according to the requirements of the ISP of my company in the future.	O	O	O	O	O
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.	O	O	O	O	O

5. In the context of your work environment, answer the following regarding Information Security Policy (ISP)

	Very likely	Likely	Neutral	Unlikely	Very unlikely
What is the chance you would receive sanctions if you violated the company information security policy (ISP)	O	O	O	O	O
What is the chance that you would be formally sanctioned if management learned that you had violated company information security policy (ISP)?	O	O	O	O	O
What is the chance that you would be formally disciplined if management learned you had violated company information security policy (ISP)?	O	O	O	O	O

Work experience (in years)		**Age group**	
0 - 2	O	18-30	O
3 - 5	O	31-50	O
6 - 8	O	51-70	O
10 – and more	O	71 - more	O

APPENDIX B: Consent form

University of Massachusetts Boston
Department of MSIS, College of Management
100 Morrissey Boulevard
Boston, MA. 02125-3393

Consent Form for Bertrand Muhire's Thesis Survey- "Employee Compliance with Information Systems Security Policy in Retail Industry. Case: Store Level Employees"

You are asked to take part in a research project that will study policy compliance behaviors. The researcher is Bertrand Muhire, Honors student in the department of Management Science and Information Systems, telephone number 85-266-001. Please read this form and feel free to ask questions. If you have further questions later Bertrand or professor Ramakrishna Ayyagari will discuss them with you. His telephone number is 617-287-7890.

This study will focus on factors that influence policy compliance behaviors. Participation in this study will take not more than 20 minutes. If you decide to participate in this study, you will be asked to fill out a two page survey composed of questions that were designed to measure your opinions on specific statements on the survey. You may speak with Bertrand to discuss any questions related to study participation.

Your part in this research is confidential. That is, the information gathered for this project will not be published or presented in a way that would allow anyone to identify you. Information gathered for this project will be stored in a locked file and only the research team will have access to the data.

The information collected will not include information that specifically identifies you such as your name or telephone number. After you return the research materials, there will be no way of linking your identity to the data collected.

The decision whether or not to take part in this research study is voluntary. If you do decide to take part in this study, you may terminate participation at any time without consequence. Whatever you decide will in no way have consequences to you.

You have the right to ask questions about this research before you sign this form and at any time during the study. You can reach Bertrand or professor Ayyagari. If you have any questions or concerns about your rights as a research participant, please contact a representative of the Institutional Review Board (IRB), at the University of Massachusetts, Boston, which oversees research involving human participants. The Institutional Review Board may be reached at the following address: IRB, Quinn Administration Building-2-080, University of Massachusetts Boston, 100 Morrissey Boulevard, Boston, MA 02125-3393. You can also contact the Board by telephone or e-mail at (617) 287-5374 or at human.subjects@umb.edu.

Signatures

I HAVE READ THE CONSENT FORM. MY QUESTIONS HAVE BEEN ANSWERED. MY SIGNATURE ON THIS FORM MEANS THAT I CONSENT TO PARTICIPATE IN THIS STUDY. I ALSO CERTIFY THAT I AM 18 YEARS OF AGE OR OLDER.

_____ _____

_____

Signature of Participant and Date Signature of Researcher

Printed Name of Participant Typed/Printed Name of Researcher