ISSN: 0975-766X
CODEN: IJPTFI
Available Online through **Research Article**
www.ijptonline.com

POLICY COMPLIANCE IN INFORMATION SECURITY

Manjula R, Kaustav Bagchi, Sushant Ramesh, Anush Baskaran
Email: sushant.ramesh2013@vit.ac.in

Received on: 15.10.2016 *Accepted on: 12.11.2016*

Abstract

In the past century, the emergence of information technology has had a significant positive impact on human life. While companies tend to be more involved in the completion of projects, the turn of the century has seen importance being given to investment in information security policies. These policies are essential to protect important data from adversaries, and thus following these policies has become one of the most important attributes revolving around information security models. In this research, we have focussed on the factors affecting information security policy compliance in two models: The theory of planned behaviour and the integration of the social bond theory and the involvement theory into a single model. Finally we have given a proposal of where these theories would be successful.

Keywords: Information Technology, Information Security, Involvement Theory, Policies, Social Bond Theory.

I. Introduction

Information security is defined as a three pronged concept with the three main characteristics being availability, confidentiality and integrity. However, cyber security or internet security includes supplementary features that are not restricted by the traditional boundaries of traditional information security. One of the primary features is analyzing the scope for human error and implementing remedial or preventive actions. Hence, joint cooperation between the various departments within an organisation is absolutely vital in order to set up a secure framework for both cyber security and information security. Information security violations may not only result in additional charges for companies, but they may also result in dire effects on the reputation of an organization. Accepted information security etiquette, along with the methodological aspects of information security, can completely mitigate the perilousness of information security violations in organizations. Past surveys have shown that creating awareness among the members in an organization can create a remarkably positive effect on the information security of that organization. The awareness of information security policies should ideally stem from the experienced and senior members of the organization which in turn, leads the other employees to gain the abilities and skills required to successfully manage information security by complying with the policies, thus leaving little to no scope for error. Internet-based technologies have many merits to add to organizations and their clients, but due to the rise in web-based technologies, information security violations are an extremely widely disputed concern. There are various technological methods to tackle information security such as authentication, and intrusion detection systems, anti-virus, anti-malware, firewalls and anti-spyware. While these aspects can definitely help to address security concerns, they cannot assure a secured environment for data. The major root of breaching by hackers is the users themselves. The users themselves are capable of committing multiple errors such as sharing a password with someone, writing down access codes on a piece of paper, downloading duplicitous software’s from the internet and also opening emails from unknown senders. Therefore, there is a need to combine the technological aspects of information security along with a system of acceptable behavior for the users and employees. Hence, there must exist multiple security approaches in order to avoid and reduce the risks associated with information security violations. The aim of this review paper is to discuss the different models that have been incorporated in organizations, to make sure employee within organizations comply with security policies. Moreover the factors revolving around such models, which ensure its success has been presented.

II. Literature Survey: [1] Abawajy, J. “User preference of cyber security awareness delivery methods” discusses and evaluates the effects of miscellaneous information security recognition delivery methods used in boosting the information security awareness and behaviour of end-users, from the wide range of delivery methods available. [4] Bulgurcu, B., Cavusoglu, H., & Benbasat, I. “Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness” helps to identify the antecedents of employee compliance with the information security policy (ISP) of an organisation. It also investigates the rationality-based factors that drive an employee to comply with requirements of the ISP with regard to protecting an organisation’s resources. [9] Herath, T. & Rao, H. “Protection motivation and deterrence: a framework for security policy compliance in organisations” develops an Integrated Protection Motivation and Deterrence model of security policy compliance under the basis of Taylor-Todd's Decomposed Theory of Planned Behaviour. In addition, it assesses the consequence of organisational obligations on the intentions of employees’ security compliance. [12] Höne, K. and Eloff, J.H.P. “Information security policy — what do international information security standards say?” provides a study on the the different information security standards and addresses the processes needed for successfully implementing an information security policy.[13] Ifinedo P. “Understanding information systems security policy compliance: An integration of the theory of planned behaviour and the protection motivation theory" investigates information systems security policy compliance by drawing upon two pertinent theories which are the theory of planned behaviour and the protection motivation theory. A research model that merged elements of the aforementioned theories was suggested and justified.

[15] Lee G, Lee WJ, Sanford C. "A motivational approach to information providing: A resource exchange perspective" assesses both intra-personal and interpersonal incitements and appropriate work circumstances that preside over the effects of motivation on information providing and information sharing.

[17] Seppo Pahnila, Mikko Siponen, Adam Mahmood. "Employees' Behaviour towards IS Security Policy Compliance" proposes different approaches for ensuring the compliance of careless employees with an organisation's information security. It suggests a theoretical model which consists of the various parameters that determine employees' information security policy compliance.

[20] Shropshire J, Warkentin M, Sharma S. "Personality, attitudes, and intentions: Predicting initial adoption of information security behaviour" incorporates discipline and cooperation into a conceptual model of security software.

[22] Siponen M, Vance A. "Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations" provides a compelling explanation for IS security policy violations and offers new insight into how employees rationalize their behaviour in association with the failure to comply with information systems security policies.

[23] Sohrabi Safa, N., Von Solms, R. and Furnell, S. "Information security policy compliance model in organisations" analyses the different parameters affecting information security and provides two models that help improve the information security in an organisation.

[24] Warkentin, M. and Willison, R. "Behavioural and policy issues in information systems security: the insider threat" is a survey on the various threats to the security of an organisation and the various studies done relating to information security.

III. Motivation

The need for Information Security Organization Policies(ISOP) in this day and age is crucial for an organization to be successful, as security threats today come in various forms. And to keep their information safe, is one of the top priorities of any organization.

Security threats can categorized as:

- External Threats: These can come in human as well as non-human forms. Human based attack activity is getting increasingly alarming as the number of hackers, spies and criminals keeps increasing every day. Non-human threats in the form of malware are also very dangerous as new types of virus, Trojans etc. are developed and are capable of penetrating even the most strong security measures.
- Internal Threats: Another threat to information security comes from internal threats. These can be caused by the employees of an organization being sloppy and lazy in forming security measures. Also, being unaware of certain security measures can be a major factor of security breaches such as downloading malicious internet content, accidental information leakage and other such illegal activities.
- Due to these threats, the importance of employees to follow the ISOP is ever increasing. Various factors are involved in ensuring that employees realize and follow these policies. The models mentioned in the paper discuss these factors and provide scenarios where each of the models have their own advantages and disadvantages.

IV. Types of Policy Compliance Models implemented in organizations:

IV.I Model A - A model based on the Theory of Planned Behavior, Based on the definitions provided in Table 1, the model here explains an employee’s intention to comply with the Information Security Policy. The various factors that affect the compliance of policies within the organization includes:

- Attitude towards compliance: This refers to the employee’s belief that performing the compliance behavior will lead to positive consequences such as more security and benefits for the firm.
- Rewards: The proposed incentives or rewards offered to employees who comply with the ISOP.
- Work Impediment: This is the detriment caused to an employee’s everyday tasks which result due to the compliance with ISOP
- Intrinsic Cost: This refers to the negative effects an employee might face due to noncompliance with the ISOP.
- Vulnerability: This refers to the risks an organization’s security faces in case employees fail to comply with the ISOP.

Table-1. Various Constructs in the Theory of Planned Behavior.

Sr. No.	Construct	Definition
1	Compliance with regards to the Information Security Organization Policy(ISOP)	The degree to which performance of compliance behavior is valued

Sr. No.	Construct	Definition
2	Normative Beliefs	The expectations of executives, colleagues and managers giving rise to a perceived pressure about compliance with the ISOP
3	Behavioral Beliefs	An employee's belief about the consequences of his/her particular behavior
4	Control Beliefs	Perceived presence of factors that may hinder or ease the performance of a certain behavior.
5	Self-efficacy to comply	An employee's judgment of competency with regard to fulfilling requirements of ISOP
6	Intention to comply	An employee's intention to protect the information resources of his organization from breaches

Another factor that is very important for Information Security is Information Security Awareness (ISA). This is defined as the knowledge an employee has about the ISOP of his company. This knowledge greatly affects his attitude towards compliance with these policies. For example, an employee who is aware of the importance of information security policies to the full extent is more likely to adhere to these policies than an employee who is not fully aware. Keeping such factors in mind, the proposed model of ISOP compliance are shown in Figure 1.

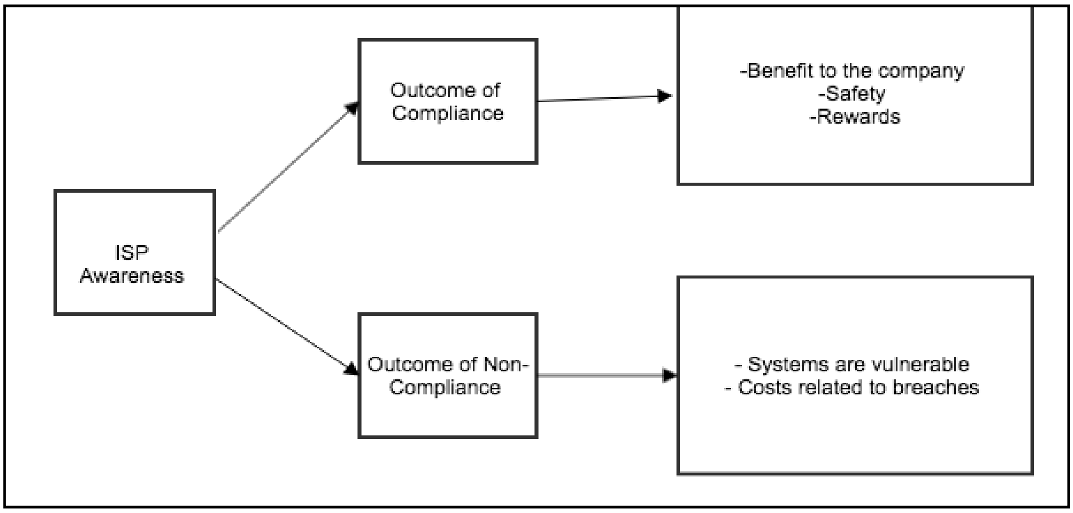

Figure 1. Factors related to compliance of ISOP.

This model shows that employees who are familiar with the intrinsic benefits, rewards, cost of non-compliance are more likely to have a positive attitude regarding the ISOP. Further, an employee's ISA has an influence over his compliance with the ISOP. Also, ISA influences work impediment negatively.

IV.I.I Advantages

- The model draws a connection between beliefs of an employee about ISOP with the information security of the company.
- Focuses on ISA, which helps employees recognize and relate to need for information security and the vulnerabilities faced in case these policies are not followed.
- Allocates rewards for when ISOP is adhered to, thus giving employees more of an incentive to follow the same.

IV.I.II Disadvantages

- Might require employees to be trained regarding ISA, thus taking a lot of precious time and resources.
- Adhering to some of the ISOP might have a negative effect on work impediment.

IV.II Model B - A Model Based On Social Bond Theory and Involvement Theory

The social bond theory relies on the fact that workers with a stronger social bond are less prone to deviating from Information Security Organizational Policies (ISOP). Deviance of such policies occur when there is a strain in the relationship between the worker and the society around him. The factors revolving around this theory are shown in Figure 2.

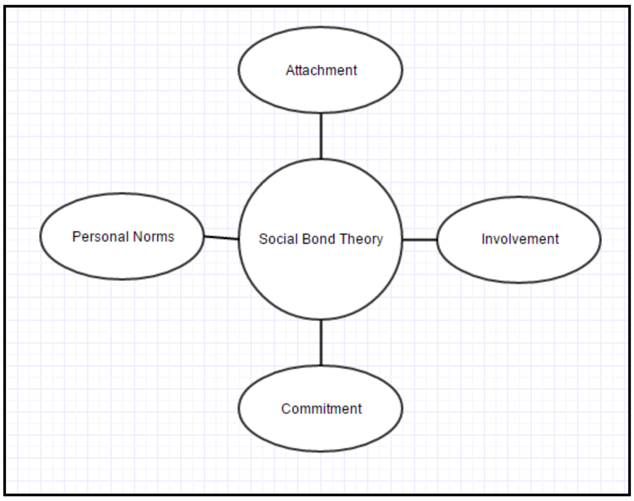

Figure 2. Factors influencing Social Bond Theory.

Involvement theory states that the level of involvement of an employee affects whether he complies with an ISOP or not. This involvement incudes the willingness to share security knowledge, ability to work together, and the time, effort put in to make sure that information within an organization is secure.

This model combines the concepts of both the social bonding theory and the involvement theory. It stresses particularly on the importance of sharing knowledge that has been acquired, in order to increase awareness of information security, as well as the time and energy spent in acquiring novel knowledge rather than improving the strength of barriers for information protection.

In addition to this, collaboration is said to be an important practice in the policy compliance model. Compliance refers to working in a group to collect, integrate and disseminate information with respect to incident handling. Compliance make sure that information about security breaches is spread from one group to another, which makes handling them much easier.

In regard to the above factor, employees within an organization share information only when they tend to gather in groups, attend video lectures, seminars and workshops and show information security involvement in organizations. The company generally makes sure that the employees are updates about various security threats constantly through such intervention. This intervention is said to have increased the employee awareness and the willingness to follow security policies.

Experience is a very important factor in following the security policies within an organization. It is through experience that a person is aware about several security vulnerabilities, how it was tackled with. When a worker is experienced, he can share this knowledge with his colleagues and will be a valuable asset to the organization.

Workers play a very important role with respect to the human factor of information security as they directly come into contact with information security. Committed individuals make sure that they follow the rules in order to be promoted within an organization and wouldn’t want to break any rules. Hence, attachment and commitment to an organization plays an important role in securing the organization from security breaches.

The model was tested based on a survey, and structural equation modelling was used to determine quantitative values that show the relationship between the unobservable variables shown above. Both the measurement model and the structural model was made use of to find a threshold value and give a quantitative value to each of the relations, and discard any relations below the threshold.

In conclusion, the results from this model show us that, while all the above factors presented play a major role in following ISOP, the impact of attachment towards ISOP was not statistically significant as various other factors like selfishness of an individual may be more.

IV.II.I Advantages

- The model is highly scalable and can be extended to various other factors affecting ISOP compliance like age, gender etc.

- The constructs in this model can be applied similar models to create new integrative models.
- Following this model leads to employees sharing stronger bonds with themselves and with the organization, thus increasing employee loyalty.

IV.II.II Disadvantages

- The findings of this model were based on a survey taken from companies willing to provide details regarding their information security policies. The generalization of this model might not be viable due to the lack of information security policies implemented in many established institutions.
- Many participants of the survey may have given double information, which could not be controlled, hence providing inaccurate results.

V. Comparative Study

As can be seen from the above details, both these models are based on different theories and have their advantages and disadvantages. In different situations, different models would be preferred.

Table 2 : A comparative study between the two models presented.

Type of Model	Organization Size		Employee Incentives
	Small	Large	
Model A	✖□	✔□	Rewards and Benefits provided by the company
Model B	✔□	✖□	Social Relations within the organization

As shown in Table 5.1, Model B, which is based on Social Bond and Involvement theory, would be more suited in a small scale organization where most employees know each other and share strong ties with the organization, thus making them much more likely to follow the ISOP. This model, however, might not be as effective in an organization which hires thousands of new people each year, as these people might not share as strong a bond with each other and the organization. In this scenario, Model A, which lays out rewards to employees who follow the ISOP might be more beneficial as it would give the employees more incentive to follow the ISOP. Another key factor which may affect policy compliance among employees is their preference, i.e. what aspect of their organization life they assign higher priority to. When employees are more influenced by the bonuses and rewards that they achieve, (which usually occurs in large organizations) they are more likely to comply with the information security policies when Model A is implemented. Likewise, when employees are motivated by the social bonds they form with other employees and the organization, (as in the case of small companies) they is a much larger probability of them giving high importance to the ISOP. This too has been shown in Table 5.1.

VI. Conclusion

In this review paper, factors affecting the compliance of Information Security Policies of the theory of planned behavior and theory of social bonds and involvement theory were studied. Furthermore, the comparative study of where these models are likely to succeed has been laid out. However, this barely scratches the surface. It can be concluded, that other than these factors, there are several other factors to be taken into consideration like organization size, organization needs and employee preference. These above factors can be taken into consideration while deciding a compliance model.

References

1. Abawajy J. User preference of cyber security awareness delivery methods. Behav Inf Technol 2014;33(3):236–47. doi:10.1080/ 0144929X.2012.708787.
2. Ben-Asher, N. and Gonzalez, C. (2015) ‘Effects of cyber security knowledge on attack detection’, Computers in Human Behavior, 48, pp. 51–61. doi: 10.1016/j.chb.2015.01.039.
3. Bernard R. Information lifecycle security risk assessment: a tool for closing security gaps. Comput Secur 2007;26(1):26–30. http://dx.doi.org/10.1016/j.cose.2006.12.005.
4. 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. Retrieved from http://www.jstor.org/stable/25750690.
5. Casper WJ, Harris CM. Work-life benefits and organizational attachment: self-interest utility and signaling theory models. J Vocat Behav 2008;72(1):95–109. http://dx.doi.org/10.1016j.jvb2007.10.015.
6. Chapple CL, McQuillan JA, Berdahl TA. Gender, social bonds, and delinquency: a comparison of boys’ and girls’ models. Soc Sci Res 2005;34(2):357–83. http://dx.doi.org/10.1016/j.ssresearch.2004.04.003.
7. Furnell S, Clarke N. Power to the people? The evolving recognition of human aspects of security. Comput Secur 2012;31(8):983–8. http://dx.doi.org/10.1016/j.cose.2012.08.004.

8. Hepler, J. (2015) ‘A good thing isn’t always a good thing: Dispositional attitudes predict non-normative judgments’, Personality and Individual Differences, 75, pp. 59–63. doi: 10.1016/j.paid.2014.11.016.
9. Herath, T. and Rao, H.R. (2009) ‘Protection motivation and deterrence: A framework for security policy compliance in organisations’, European Journal of Information Systems, 18(2), pp. 106–125. doi: 10.1057/ejis.2009.6.
10. Herath, T. and Rao, H.R. (2009) ‘Encouraging information security behaviours in organisations: Role of penalties, pressures and perceived effectiveness’, Decision Support Systems, 47(2), pp. 154–165. doi: 10.1016/j.dss.2009.02.005.
11. Hirschi, T. and Voss, H.L.(1970) ‘Causes of delinquency’, American Sociological Review, 35(6), p. 1114. doi: 10.2307/2093404.
12. Höne, K. and Eloff, J.H.P. (2002) ‘Information security policy — what do international information security standards say?’, Computers & Security, 21(5), pp. 402–409. doi: 10.1016/s0167-4048(02)00504-7.
13. Ifinedo P. Understanding information systems security policy compliance: an integration of the theory of planned behavior and the protection motivation theory. Comput Secur 2012;31(1):83–95. http://dx.doi.org/10.1016/j.cose.2011 .10.007.
14. Ifinedo P. Information systems security policy compliance: an empirical study of the effects of socialisation, influence, and cognition. Inf Manage 2014;51(1):69–79. http://dx.doi.org/10 .1016/j.im.2013.10.001.
15. Lee G, Lee WJ, Sanford C. A motivational approach to information providing: a resource exchange perspective. Comput Human Behav 2011;27(1):440–8. http://dx.doi.org/10.1016/j.chb.2010 .09.006.
16. Safa NS, Sookhak M, Von Solms R, Furnell S, Ghani NA, Herawan T. Information security conscious care behaviour formation in organizations. Comput Secur 2015;53(0):65–78. http://dx.doi.org/10.1016/j.cose.2015.05.012.
17. Seppo Pahnila, Mikko Siponen, Adam Mahmood. Employees' Behaviour towards IS Security Policy Compliance. System Sciences, 2007. HICSS 2007. doi: 10.1109/HICSS.2007.206.
18. Shaw RS, Chen CC, Harris AL, Huang H-J. The impact of information richness on information security awareness training effectiveness. Comput Educ 2009;52(1):92–100. http://dx.doi.org/10.1016/j.compedu.2008.06.011.
19. Shibchurn J, Yan X. Information disclosure on social networking sites: an intrinsic–extrinsic motivation perspective. Comput Human Behav 2015;44(0):103–17. http://dx.doi.org/10.1016/ j.chb.2014.10.059.

20. Shropshire J, Warkentin M, Sharma S. Personality, attitudes, and intentions: predicting initial adoption of information security behavior. Comput Secur 2015;49(0):177–91. http://dx.doi.org/ 10.1016/j.cose.2015.01.002.
21. Siponen M, Adam Mahmood M, Pahnila S. Employees' adherence to information security policies: an exploratory field study. Inf Manage 2014;51(2):217–24. http://dx.doi.org/10.1016/j.im.2013 .08.006.
22. Siponen M, Vance A. "Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations". Management Information Systems Quarterly. Vol. 34, No. 3 (September 2010), pp. 487-502. http://www.jstor.org/stable/25750688.
23. Sohrabi Safa, N., Von Solms, R. and Furnell, S. (2016) 'Information security policy compliance model in organizations', Computers & Security, 56, pp. 70–82. doi: 10.1016/j.cose.2015.10.006.
24. [24] Warkentin, M. and Willison, R. (2009) 'Behavioral and policy issues in information systems security: The insider threat', European Journal of Information Systems, 18(2), pp. 101–105. doi: 10.1057/ejis.2009.12.
25. Webb J, Ahmad A, Maynard SB, Shanks G. A situation awareness model for information security risk management. Comput Secur 2014;44(0):1–15. http://dx.doi.org/10.1016/j.cose.2014 .04.005.
26. Werlinger R, Hawkey K, Botta D, Beznosov K. Security practitioners in context: their activities and interactions with other stakeholders within organizations. Int J Hum Comput Stud 2009;67(7):584–606. http://dx.doi.org/10.1016/j.ijhcs.2009 .03.002.
27. Woon IMY, Kankanhalli A. Investigation of IS professionals' intention to practise secure development of applications. Int J Hum Comput Stud 2007;65(1):29–41. http://dx.doi.org/10.1016/ j.ijhcs.2006.08.003.
28. Zhai Q, Lindorff M, Cooper B. Workplace Guanxi: its dispositional antecedents and mediating role in the affectivity–job satisfaction relationship. J Bus Ethics 2013;117(3):541–51. doi:10.1007/s10551-012-1544-7.