Factors Affecting Information Security Behaviour

A.Rajendran, S.M.Furnell and T.Gabriel

Centre for Security, Communications and Network Research,
Plymouth University, Plymouth, UK
e-mail: info@cscan.org

Abstract

The reason behind inconsistent acceptance and compliance level of employees within organisation has been hard to understand. Personality, organisational culture and environment are said to be the reasons behind such inconsistent compliance behaviour of an employee. But aspects such as personality, socio-organisation factors, educational best practice are been neglected till date during the ongoing training of employees for betterment of acceptance and compliance behaviour. Initial study targeted the likely relation between socio-organisation factors and personality of a person, which gave out the likely process that initiates the security behaviour out of an employee. A model is designed, which best describes and includes all possible influence an employee might get and derives the security behaviour of the employee based on it. The model exhibits a nature to advocate, what causes an employee to behave the way they do. Organisation can make use of this to differentiate security compliant employee with the non-compliant employee and produce effective mitigation plans.

Keywords

Personality, socio-organisation factors, training, compliance behaviour, Information Security.

1 Introduction

With the recent technological advancements and increase in security threats, the importance of sticking with the security focused policies is high on recognition much more than previously it was. A number of studies held so far have suggested that the success of security policies and controls will ultimately depend upon the levels of acceptance and compliance among the underlying staff. A well designed and implemented security system still as to rely on the people it was meant to govern, the human factor importance is significant in this scenario. A fact worth mentioning is that the majority of the troubling incidents related to security had the human factor playing a crucial part, this also led researchers term humans as the weakest link in an organisation. One can implement technical solutions for the related issues, but we still fail to control and handle human factor (Gonzalez et al. 2002; Vroom & Von Solms, 2004).

Compliance behaviour of an employee within an organisation is something of wide range. It is very much inconsistent, so that the researchers who tried to interpret the compliance behaviour of employees came up with number of categories to assume the level of compliance levels. Furnell & Thompson (2009) had developed eight compliance level ranging from culture to disobedience and went on to say that

employees could be mapped in any of those level of compliance depending on the security behaviour they exhibit.

The cause for such discrepant compliance behaviour is said to be personality and socio-organisation factors surrounding the employee. Research purpose was drawn upon the above two reasons, to find the process of resultant security behaviour and subsequent compliance of an employee. The major topics considered include lack of user awareness, personality as a filter, organisation culture, environment, education and importantly deriving a mechanism that derives compliance behaviour of person, which an organisation can later use.

2 Background

2.1 End user behaviour

End user behaviour has been a major concern and organisations are now turning their head towards human factor. Organisations are becoming aware of the major incidents occurring due to the involvement of human element in security breaches. Employees are the cause of highest rate of abuse within an organisation. To add on top of that, 60%-80% of all network misuse is perpetrated by people inside the organisation (Woodhouse, 2007). Major surveys such as CSI (*Computer security institute*), BERR (*Business Enterprise and Regulatory Reform)* and ISBS *(Information Security Breaches Survey*) concur with internal threat in the form of human. The solution for such incidents may seem to be with organisation's security practices and implementation of security policy, but the significant activity of non-compliant behaviour due to personality indifference and external influence would lead to ineffectiveness of security policy.

2.2 Lack of employee awareness

Lack of effectiveness or ineffective nature of the security policy can be attributed to lack of awareness among employees. Effectiveness comes, when every user is aware of what they do and their respective consequences of their actions, awareness does not rise from self-realisation alone. Awareness among users should be cultivated by organisations security training and security culture. Ruighaver et al. (2007) argue that organisational culture plays an important role in end user activities, and suggest it should be a process of continual development rather than a one-time process, which many organisations fail to address. Security awareness is the basis of preventing all major threats from causing damage or even from happening itself. Organisations are most benefitted from employee's awareness and most affected due to employee's lack of awareness. Malwares comes into an organisation with the help of employee within the organisation. Lack of awareness constructs this sort of actions from employees, which confirms the fact people commit mistake not the computers (Lacey, 2009).

3 Organisation culture

Organisation culture or corporate culture is a deep aspect, which is entwined upon each section of an organisation. The organisation culture exist whether management or employees within an organisation aware of it or not. Vroom & Von Solms (2004) state that, organisation culture is about shared ideas between staff, the norms followed, and system structure which enforces its values followed on staff. This in turn becomes a network of learned behaviour, which flows from top level of organisation to bottom level of organisation. Organisation's security culture is a sub form of organisation culture. It is created out of influence from organisation culture and could also be created by the unknown factors outside of organisation. Security culture is defined from the fact, how members within an organisation are conscious of security and follow it (Woodhouse, 2007). This may not necessarily be with the ideals of organisation and how organisation wants their member's security orientation to be. Organisation's culture is an influence that extends its reach on organisational security culture and may obstruct change. So organisation culture could be the single most important factor in deciding the success or failure of the organisation and to think security culture could be affected by organisation culture one need to proceed cautiously.

4 Socio-organisation factors

All the facts and illustration relayed so far highlighted the importance of human factors and organisational factors role, which are highlighted by many studies undertaken so far in improving information security (Lacey, 2009; Dhillon & Backhouse, 2001; Vroom and Von Solms, 2004). Human factor and organisation factor combined are known to be Socio-Organisational factor. Socio-organisational perspective is way forward for betterment of information security rather than the technical and functional aspects of information security (Dhillon & Backhouse, 2001). Socio-Organisational perspective is significant, since technologies ensuring information security are designed, maintained and operated by human agents in an organisation. So it is necessary to understand these socio-organisational factors in order to deliver the assessing mechanism dealing with compliance behaviour.

Socio organisation factors in others words can be described as an influencing factor that works in conjunction with personality of the person. Humans pose such critical threat due to their nature of susceptibility to external pressure applied on them. Influence can be from anywhere as put forward by Lacey that 'Local roles, environments and business objectives shape user attitudes and behaviour' (Lacey, 2009). This describes the importance of the influence factors outlined in matters dealing with information security. The much discussed organisation culture in itself is an influence factor, which could motivate employees within the organisation towards security culture. It has a strong influence on organisational security, which might lead to obstruct change in positive or negative direction (Nosworthy, 2000). Security practices and policy in place also has huge interest in how security orientations of staff are influenced. The extent, a staff understands security policy have impact on security breaches of an organisation. The security policies that are appropriately worded and well intentioned lead to less security breaches (ISBS, 2010).

4.1 Local roles, environment, and mentoring

Local roles might be the employee job role in itself, which could alter the way they comply with information security. Environment includes influence from those who are around us including colleagues, friends and families. Yuen et al. (2009) had taken influence in context of workplace and other in their home. In the organisation context the most influencing factors are security culture of an organisation (e.g. group effect, peers and etc,), and ability of a person. Whereas in home environment, family, peer, mass media influence, perceived usefulness and self-efficacy plays a role in determining outcome of person's security behaviour (Yuen.et al. 2009). Mentoring and training was largely considered as solution for improving security orientation of employees in an organisation. Gabriel (2010) in his work had similar views to spread security awareness among colleagues by means of mentoring. This method was adopted since Gabriel believed colleague behaviour to be more effective and influence the outcome of the other employee's security behaviour.

4.2 Learning Theories & training

Training and educating staff is for their own betterment as well as betterment of organisation that trains their staff. The effectiveness of training varies from person to person. Every employee has different of opinion in the way they want to be trained. That's where the learning theories come into play due to the individual difference in personality. People learn efficiently in their preferred way of learning and tend to change ones behaviour permanently; these learning come out of one's own experience rather than from external body states (Landy, 1985). Learning theories address the way people learn and it is about how behaviour patterns develop from social environment. Armitage et al. (2007) in their work provided the support to learning theories despite shortfalls in it. The learning theory is helpful in understanding the insights of how people learn though it cannot be seen as an exact blueprint of learning nature.

5 Personality as a filter

The personality of a person is the prime factor in security orientation of an employee, which changes the outcomes of all the inputs that feeds into them (Gabriel, 2010). As a human one would find a resilient nature towards change in terms of security, which is a major factor in non-acceptance and non-compliance behaviour. With further research, personality as a prime factor in resisting change turned to be a filter rather being a blockade of security orientation. For example training from an organisation does not go completely ignored, some part of the security facts do get into the employee mindset and they begin to follow as they see it fit or appropriate to them. The personality of person does not bear a direct consequence on security behaviour. The security behaviour of a person is resultant of personality combined with organisation or organisation independent variables. Employee attitude towards compliance and security behaviour arise in conjunction with organisational constraints imposed and psychological process involved within an employee.

6 A model for understanding security behaviour

The process of how personality and socio-organisation factors could lead to a resultant behaviour was described so far. The concerned learning theories, in the way employees get addicted to or affiliated to certain methods of learning were discussed as part of educating them to improve compliance behaviour. From this point on, a model that could lead the organisation or management in identifying the employee compliance behaviour shall be out laid.

A group of 8, IT security professionals from diversified backgrounds in Plymouth University were carefully chosen and invited in conducting of a focus group. *The head of ICT, head of records management, senior HR advisor, IT security research student, System & middleware manger, IT security & Privacy senior lecturer, researcher on relation between personality & security behaviour, head of school of computing and mathematics (project supervisor) and a ICT staff* were the participants invited. The agenda set at the focus group was to validate and enhance the initial model created, which best describes the socio-organisation factors surrounding an employee's personality within organisation and outside of organisation. The outcome of focus group was pleasing since, every participant acknowledged the concept of the model in front of them. With due discussion and questions raised some of the influencing factors were questioned but finally every factor were accepted to have an impact on employees one way or the other. Also some suggestions regarding omitted factors were added to help improve the model.

Issues concerning influence factors having conflict of interest among them were raised. Especially the credibility of perceived benefits as a non-workplace influence factors were subjected to intense criticism, but it was made clear that initial realisation of personal and group benefit come outside of organisation and was added without any change. Noticeable change included of adding colleague behaviour and supervisor/management leadership under *workplace interaction* category and inclusion of *wider awareness* influence to accommodate external scenarios which an employees are aware off. Figure 1 is the refined research model by taking into account the feedback of focus group participants. The model describes key factors of possible influence and tries to explain the process behind the security behaviour of an employee. The influence categories within the model are described below to bring forth the nature of each category considered.

- *Job characteristics* - The job factors such as varied role, job satisfaction, pressure of important task at hand and managing time exerts influence over the staff, on how they end up following IT security. This influence may be positive or negative depending upon on the situation. E.g. jumping guidelines due to concentrate on job at hand

- *Organisational factor* - This generally relates to the positive influences that may be exerted over employees by the organisation in the form of security policy, security training. Even employee aware of organisations disciplinary procedures and security monitoring can make a difference in final actions. E.g. security policy in place could be used as a driving factor to educate and train.

- *Workplace interactions* – The way colleagues or supervisor behave within organisation could influence the action taken by the employee coming in contact with them by means of idealised influence and intellectual stimulation. E.g. supervisor/management, getting in regular touch with their employee and encouraging them to follow IT security guidelines.

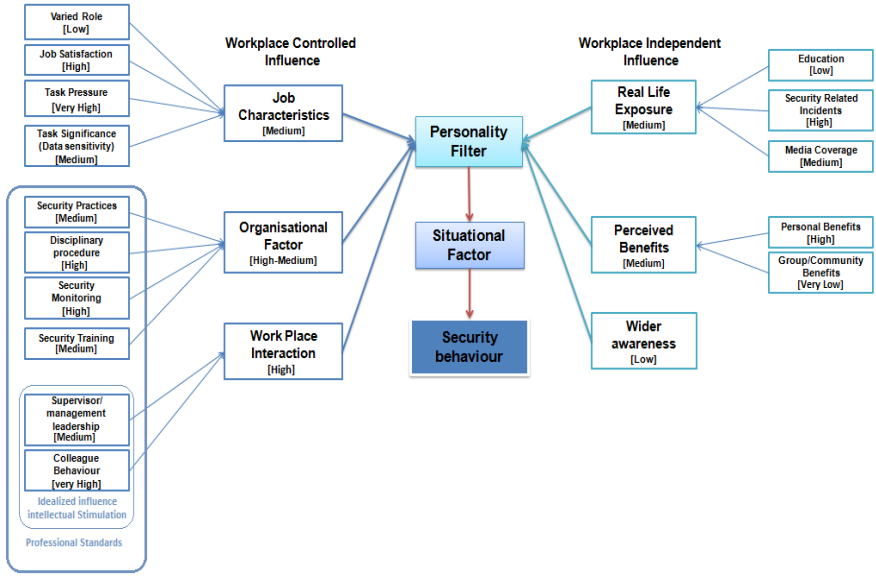

Figure 1: A framwork for understanding security compliance

- *Real life exposure* - The exposure to the security and related incidents that a person has experienced in real life or through education or through a friend can influence how they may react in future. Even media coverage could play a part in it. E.g. malware infections, social networking incidents, phishing incidents and etc

- *Perceived Benefits* - This refers to the personal or community benefits employees are aware off by means of self realisation and follow IT security accordingly. E.g. using strong passwords to protect files or website accounts.

- *Wider awareness* – External scenario that could change security orientation of an employee, when they come to know such things. E.g. Change in cyber law

6.1 Weightage of influence factors

As seen in the figure 1, Weightage of influence factors were given, in order to showcase the extent each influence factors within the research model have an impact on a person. During the focus group participants were targeted with questions related to the way they perceive some of the influence factors and their impacts, so each participant's perception were taken as feedbacks in the way they sounded it. The Weightage were given based on the feedbacks given by participants of focus group

and in consideration of the previous research works. Though most of the influence factors were rated based on the above stated conditions, but few influence factors were unexplored topics. In order to give a complete idea for the observer of the research, assumptions were made by correlating the influence factors with the impact it could have and Weightage were given in accordance with that. The assumptions may be wrong at times and could lead in wrong directions, but one must bear in mind these assumptions were made for guidance. These are the expected results rather than the obtained results, once the model is fully developed and ready for implementations all these assumptions made can be verified.

7 Conclusion

At present the created research model is a tool to understand compliance behaviour of an employee rather than a fully-fledged mechanism that can measure compliance behaviour immediately. Though, with further improvements it can become a fully-fledged mechanism to evaluate likely capability and commitment in relation with IT security. The model is a tool that explains how various influence factors within organisation and outside of organisation have an impact on an employee, and also explains how the system of personality within a person works and reacts to such external influence.

One may ask how does personality and influence factors can be related. In all due likeliness, personality have two distinguished facets namely consciousness and agreeableness. These two personality facets are put forward by researchers (Cellar et al. 2001; Shropshire et al. 2006) as the two facets that have high probability of relation with IT security compliance. Then one must assume that the level of agreeableness and consciousness is directly proportionate to the person's likely capability to get influenced by the external influence factors. This in turn affects the compliance nature of the employee within organisation. So once the organisations test the personality aspect of an employee through numerous personality tests available and also get the likely result of influence factor, the understanding would be much accurate to pin point issues behind behaviour of a person and train them based on those results. In the present state of the model, it is not possible to accurately pin point the exact issue behind behaviour of a person instead an organisation can use it to understand the likely scenarios a person can get influenced by and expect the nature of compliance behaviour and train the employees accordingly.

The outcomes obtained from the extensive research made were pleasing to see, though the same cannot be said about the implementation part of the research model created. The implementations of the research model were stalled to later date due to the limited time and resources. Broadness of influence factors and relatively unknown measurable nature of the influence factors were another reason in delay of implementation. But once implemented the extraction of fruitful deliverables out of this model are not constrained in a particular direction and can fit the needs of organisation, the way they see it fit.

8 References

Armitage, A., Bryant, R., Dunnill, R., Flannagan, K., Hayes, D., Hudson, A., Kent, J., Lawes, S., and Renwick, M., (2007*).”* Teaching and Training in Post Compulsory Education”. (3rd ed), Maidenhead, Open University Press. ISBN 0-3352-2267-6

Cellar, D. F., Z. C. Nelson and C. M. Yoke (2001). "The five factor model: Investigating the relationships between personality and accident involvement." Journal of Prevention & Intervention in the Community 22(1): pp43-52.

Dhillon, G., and Backhouse, J. (2001), “Current direction in IS security research: towards socio-organizational perspectives”, Information Systems Journal 11, pp127–153.

Furnell, S.M., and Thompson, K, L., (2009), “From culture to disobedience: Recognising the varying user acceptance of IT security”, Computer Fraud & Security, Volume 2009, Issue 2, pp5-10

Gabriel, T., (2010), “Personality Type – a valid indicator of security champions?”. Master thesis: University of Plymouth.

Gonzalez, J and Sawicka, A, (2002), “A Framework for Human Factors in Information security” , WSEAS international conference on information security, Rio de Janeiro, Brazil

ISBS, (2010), “Information Security Breaches survey” http://www.infosec.co.uk/files/isbs_ 2010_technical_report_single_pages.pdf. (Accessed on 19/01/2010)

Lacey, D., (2009), “Managing the Human Factor in Information Security”, Chichester: John Wiley & Sons

Landy, F. L., (1985), “Psychology of Work Behaviour”, The Dorsey press.

Nosworthy, J, (2000), “Implementing information security in the 21st Century – do you have the balancing factors?” Computers and Security 19(4): pp337–47.

Ruighaver, A. B., Maynard, S. B., and Chang, S., (2007), “Organisational security culture: Extending the end-user perspective”, Computers & Security 26: pp56 – 62

Schein, E.H. (1999), “The corporate culture survival guide”, San Francisco, California, United States of America: Jossey-Bass Publishers.

Shropshire, J., Warkentin, M., Johnston, A. C., Schmidt, M. B., (2006), “Personality and IT security: An Application of the five factor model”, Proceedings of the Twelfth Americas Conference on Information Systems, Acapulco, Mexico, August 4-6

Vroom, C., von Solms, R., (2004), “Towards information security behavioural compliance”, Computers and Security 23(3):pp191-8.

Woodhouse, S., (2007), “Information security: End user behaviour and corporate culture”, 7th IEEE International Conference on computer and information technology, pp767-774.

Yuen B. Ng., Kankanhalli, A., Yunjie, X., (2009), “Studying users' computer security behaviour: A health belief perspective”, Elsevier: Decision Support Systems 46 , pp815–825.