Information Security Policies: A Review of Challenges and Influencing Factors

Mutlaq Alotaibi[1], Steven Furnell[1, 2, 3] and Nathan Clarke[1, 2]
[1] Centre for Security, Communications and
Network Research, Plymouth University, Plymouth, UK
[2] Security Research Institute, Edith Cowan University, Perth, Western Australia
[3] Centre for Research in Information and Cyber Security, Nelson Mandela Metropolitan University, Port Elizabeth, South Africa
mutlaq.alotaibi@plymouth.ac.uk

Abstract— **Organisations increasingly perceive their employees as a great asset that needs to be cared for; however, at the same time, they view employees as one of the biggest potential threats to their cyber security. Employees are widely acknowledged to be responsible for security breaches in organisations, and it is important that these are given as much attention as are technical issues. A significant number of researchers have argued that non-compliance with information security policy is one of the major challenges facing organisations. This is primarily considered to be a human problem rather than a technical issue. Thus, it is not surprising that employees are one of the major underlying causes of breaches in information security. In this paper, academic literature and reports of information security institutes relating to policy compliance are reviewed. The objective is to provide an overview of the key challenges surrounding the successful implementation of information security policies. A further aim is to investigate the factors that may have an influence upon employees' behaviour in relation to information security policy. As a result, challenges to information security policy have been classified into four main groups: security policy promotion; noncompliance with security policy; security policy management and updating; and shadow security. Furthermore, the factors influencing behaviour have been divided into organisational and human factors. Ultimately, this paper concludes that continuously subjecting users to targeted awareness raising and dynamically monitoring their adherence to information security policy should increase the compliance level.**

Keywords: human factor; Information security policy; user behaviour; information security managemen; Compliance managementt.

I. INTRODUCTION

A security policy is defined in a formal document that specifies what constuitutes acceptable and unacceptable behaviour of users in relation to dealing with information assets in a secure manner. It is a part of formal information security control and a baseline statement on the information security tasks which should be carried out by employees. According to SANS [1], a security policy is typically "a document that outlines specific requirements or rules that must be met, in the information/network security realm, policies are usually point-specific, covering a single area". Organisations ought to view having information security policies and procedures in place as being just as important as having technical solutions to hand [2]. The implemention of such technical measures alone does not guarantee a safe computing environment. As part of their implementation guidance, organisations should establish a set of information security policies, which are approved by top management then distributed amongst and communicated to all employees.

Nowadays, the majority of organisations are aware of the importance of information security policy. According to PricewaterhouseCooper [4], 98% of large organisations and 60% of small organisations have a documented information security policy. However, employees' compliance with information security policy is still of great concern to many organisations. According to the E&Y global information security survey [5], 57% of organisations consider their employees to be the most likely source of an attack, with 38% viewing careless or unaware employees as the most likely threat. Moreover, the UK information breaches survey [6] found that 70% of organisations with a poorly understood security policy had staff-related breaches, whereas only 41% of organisations where the policy was well understood had any of these. Therefore, when employees have a good understanding of security policy, this positively affects the overall security of an organisation. Arguably, the human factor is still the weakest link in the information security chain, causing an increase in the number of security threats. As such, many end users are still unaware of the importance of information security and the relevant organisational requirements. Chan and Mubarak [7] found that more than fifty per cent of the employees in their study were unaware of the existence of information security policy in their organisations.

The successful implementation of information security policy is associated with challenges in areas such as management policy, dissemination, user awareness and user behaviour. A number of factors have a direct affect on user behaviour in relation to information security policy, and these can be categorised into human and organisational factors. The purpose of this paper is to investigate and better understand the major challenges associated with information security policy and the factors that affect the successful adoption and use of security policies. This paper conducts a review based upon a number of scientific papers retrieved from various academic databases, such as IEEE, ACM, Springer and ScienceDirect, and the reports of several information security institutes, such as SANS, PwC and E&W.

978-1-908320/73/5/$31.00 © 2016 IEEE

The paper is organised in the following manner: section II explains the key challenges related to information security policy and section III discusses in detail the human and organisational factors that affect human behaviour in relation to information security. Finally, the conclusion and future work in this area are offered in section IV.

II. KEY INFORMATION SECURITY POLICIES RELATED CHALLENGES

A number of researchers have addressed the challenges associated with information security policy. Based on their assessments, we have classified those challenges into four major groups, as illustrated in the following table:

Table I. An information security policy challenges

Group #	Main challenge	Sub-challenges	Sources
1	Security policy Promotion	• Dissemination • Awareness Raising • Training • Enforcement and Monitoring	[8] [6] [9] [10] [11] [2]
2	Non-Compliance with Security Policy	• Malicious behaviour • Negligent behaviour • Unawareness	[12] [13] [14] [15] [16]
3	Security Policy Management and Updating	• Regular review and update • Policy management • Technology advances • Designing good policy	[17] [18] [19]
4	Shadow Security	• Unclear security policies • Unusable security mechanisms • High compliance cost	[20] [21] [22]

A. *Security policy Promotion*

Organisations encounter challenges associated with the promotion and dissemination of their information security policies. In research conducted by the Economist Intelligence Unit [8], most of the IT managers claimed that their organisations had developed information security policies to overcome many concerns, but only a few of these organisations had seriously instilled this culture into their employees. This is supported by PwC [6], who state that "Although there are more written policies in place to guide employees' behaviours towards security, we haven't yet seen this translate into better understanding of these policies". A survey carried out by Prince [9] revealed that more than half of the members of staff in organisations did not participate in any kind of security awareness training. This study confirms that the absence of training results in violations of policy and the occurrence of behaviour that poses a risk to the organisation. Despite the presence of the best information security awareness programmes, obstacles exist that make the successful implementation of awareness activities more challenging. These common obstacles are: 1) Implementation of new technology; 2) One size fits all; 3) Too much information; 4) Lack of organisation; 5) Failure to follow up; 6) No explanation of why [10][11].

Depending on the enforcement and monitoring of a security policy, implementing security monitoring tools can help to identify any security policy breaches that may occur. However, these monitoring tools are not widely implemented in organisations [2].

B. *Non-Compliance with Security Policy*

Non-compliance with information security policy is considered to be primarily a human problem rather than a technical issue. Researchers have mentioned three types of non-compliance behaviour: malicious behaviour, negligent behaviour and unawareness. The main motivation for malicious behaviour is malicious intent to bring harm to an organisation's information assets [12] [13], whereas negligent behaviour is intent to violate an organisation's security policy but not to harm that organisation [14]. The third type of non-complaint behaviour is due to unawareness, whereby end users are unaware of the importance of information security and the relevant organisational requirements. Khan *et al.*'s [15] research indicated that more than fifty percent of employees are unaware of the existence of an information security policy in their organisation. Moreover, Greitzer *et al.* [14] state that users tend to dislike the active controls that are imposed on their PCs, and this can be seen in many organisations. The reason for users having an aversion to these controls is that they impose a group of no commands (e.g. no Google apps, no Facebook, no Skype, etc.).

There is a direct relationship between the problems faced by many organisations and lack of attention paid to information security awareness and training [16]. Security awareness and training can play a supplementary role alongside information security policy in order to reduce the number of potential insider threats. If there is a comprehensive and effective information security culture in an organisation and the users are applying it, this will make a difference.

C. *Security Policy Management and Updating*

Many organisations do not continuously review and update their information security policy. Colwill [17] states that "security policy, controls, guidelines and training are lagging behind changes". Moreover, designing and managing a security policy that meets all the important criteria can be a challenge for many organisations [18]. Furthermore, many organisations do not update their policy to be more in line with rapidly and constantly developing technology. A study conducted by Protiviti [19] found that only 24% of the respondents had a cloud acceptable usage policy in place. Evidently, this indicates that many organisations ignore the importance of updating their policies. Organisations should consistently review and update their policies to ensure that those policies are still meeting all their needs and ensure that updates are disseminated to all employees.

D. *Shadow Security*

Two types of user behaviour associated with information security policy have been identified in the literature: compliance and non-compliance. However, Kirlappos *et al.* [20] have suggested a third type of user behaviour, which is shadow security. Shadow security is defined as "employees

going around IT to get the IT services they want on their own''[21]. Such employees implement their own security solutions when they believe that compliance is beyond their capacity or will affect their productivity. For example, if a password security policy requires employees to choose a strong password (12 character length, upper letters and symbols), some employees may find it difficult to memorise the password, and therefore, they may write the password on a sticky notes and put it on the computer screen. In the aforementioned example, an employee is considered to be complaint with password policy; however, they are also impementing shadow security policy, and this may threaten an organisation's security. Hence, shadow security may create a false sense of security. The risk that the organisation may be at due to their shadow security policy are not usually perceived by employees who play around with the main security policy. Thus, the employee does not understand the risk that the organization may be at due to this behaviour.

Shadow security may affect the success of policy implementation, for instance, ineffective communication of a policy to the management and security policies not being reviewed and evaluated in a timely manner; however, shadow security can make this task more difficult. Moreover, the presence of shadow security behaviour may lead to the emergence of a non-compliance culture within an organisation as a whole [22]. Furthermore, if employees play around with official security policy, they may not provide feedback on the shortcomings of that policy and suggest alternative solutions.

According to Kirlappos *et al*. [20], organisations should pay attention to reducing the cost of compliance with unusable security mechanisms and unclear information security policies, which may not provide efficient protection for an organisation because employees will attempt to find ways to play around with them as they are undesirable or impractical in their opinion.

III. FACTORS INFLUENCEING USER'S BEHAVIOR

Multiple research studies have attempted to identify the different reasons for the various levels of compliance with information security policy. Academic literature and the reports of information security institutes relating to information security policy compliance have been reviewed, and the influencing factors have been categorised into two types: organisational and human. In Kraemer *et al*. [23], the authors highlight the way in which organisational and human factors are directly related to information security vulnerabilities. The following section investigates these factors.

A. Organisational factors

Although compliance with security policy is first and foremost a human issue, organisational factors found to be influencing users' compliance have been explored in several studies. Table II summarises the important factors that influence user compliance with information security policy, and these are also discussed in the paragraphs that follow.

1) Information Quality

In the literature, the information quality of a security policy (date flow) is generally seen as a factor that is strongly related to employees' compliance with information security policy. Inadequate policies can contribute negatively towards non-compliance. Hence, inadequate organisational procedures may lead to a lack of skills, knowledge and ability to deal with security requirements [14]. A study conducted by Pahnila *et al*. [24] found that information quality has a significant effect on actual information security policy compliance. Furthermore, Bulguru *et al.* [25] investigated the impact of three quality dimensions, clarity, adaptability and consistency, on employees' compliance with security rules and regulations and highlighted their significance.

Table II Major organizational factors that influence user's behaviour

Factor	Description	Research Method	Source
Information Quality (Data flow)	The facilitating conditions and information quality have a significant impact on user compliance behaviour.	Questionnaire (Participant:245)	[24]
		Theoretical	[14]
		Questionnaire (Participant:464)	[25]
Motivation	Motivation, such as rewards, has a significant impact on users' perception of the benefits of compliance.	Questionnaire (Participant:464)	[25]
		Theoretical	[26]
Sanction (Deterrence)	Sanctions (deterrence) are one of the important factors that affect employees' actual compliance with established information security policy.	Questionnaire (Participant:464)	[25]
		Questionnaire (Participant:113)	[27]
		Questionnaire (Participant:917)	[28]
Awareness & Training	Information security awareness has a direct effect on user compliance behaviour.	Questionnaire (Participant:464)	[25]
		Action research (Participant:16)	[29]
		Questionnaire (Participant:308)	[7]
Computer Monitoring	Computer monitoring tools are negatively associated with information security policy non-compliance intention.	Questionnaire (Participant:232)	[30]
		Questionnaire (Participant: 304)	[31]
Persuasion	Persuasion technology can raise security awareness and then increase level of complaince.	Experiment (Participant:30)	[32]
		Theoretical	[11]

2) Motivation

Motivators can be used to encourage users to comply with information security policy [26]. A good example of a motivator is a reward, which is defined as a tangible or intangible gift that is granted to an employee who complies with the requirements of security policy. Several studies have revealed that rewards have a significant impact on an employee's perception of the benefits of compliance. For instance, Bulgurcu *et al.* [25] empirically investigated the role of rewards in driving employees to comply with the

requirements of security policy and found that rewards have a significant impact on employees, making them more compliant.

3) Sanction (Deterrence)

The existing literature has highlighted the importance of sanctions (deterrents) in relation to changing users' behaviour towards information security policy, making them more compliant, and a number of studies have offered empirical support for this claim. According to Bulgurcu *et al*. and Cheng *et al.* [25][28], sanctions are one of the most important factors affecting the actual compliance of employees with established security policies. Similarly, a study conducted by Harris and Furnell [27] investigated the impact of sanctions on employees' compliance with information security policy, particularly on the use of shaming punishment as a deterrent, 71% of the participants indicated that they would be more likely to follow security policy if their employers were willing to shame those who did not comply.

4) Awareness raising and Training

Previous studies on information security have highlighted the impact of security awareness on employees' behaviour. According to Bulgurcu *et al.* [25], awareness has a significant influence on an employee's intention to comply. Puhankinen *et al.* [29] carried out action research to validate a training programme on information security policy compliance. The results of the study suggested that increased awareness and training programmes have an impact on users' compliance with information security policy. Chan and Mubarak [7] concluded that a "lack of awareness and knowledge of policies may have allowed for staff to violate such policies".

5) Computer Monitoring

Security monitoring and auditing tools can be utilised to change unwanted behaviour in order to enforce information security policy. Once users are fully aware of these tools, they are encouraged to change their behaviour and be more compliant. A number of studies have provided empirical evidence of the relationship between computer monitoring and complaint behaviour. These studies [30][31] found that an individual's information security compliance is influenced by computer monitoring and auditing tools. As such, monitoring tools assist in mitigating non-compliance behaviour.

6) Persuasion

Persuasion is an integral part of our lives and of human interaction. Fogg [33] described persuasive technology (PT) as "interactive computing systems designed to change people's attitudes and behaviours". Persuasive computing technology can affect people's attitudes and bring about some constructive changes in many domains, for example, marketing, health, safety and the environment. Marketing is perhaps the most significant domain in which persuasive technologies are used to encourage customers to buy products and services. With regard to information security, the results of an empirical study by Yeo *et al*. [32] suggest the significance of persuasive technology in changing end-users' behaviour. Furthermore, Qudaih *et al.* [11] indicate that using persuasive technology to disseminate policies and procedures can lead to effective information security awareness programmes.

A. Human factors

Achieving compliance with information security policy would be a difficult task without the interaction of users, and therefore, controlling user behaviour in relation to these policies is the key to success. In the literature, several human factors have been investigated by many researchers and reported to have an impact on user behaviour, whether negative or not. Below in Table III are some of the factors that may influence the user's intention to comply.

Table III Major human factors that influence user's behaviour

Factor	Description	Research Method	Source
Perception (Situation Awareness)	Human interpretation or recognition of sensory information has a considerable impact upon user behaviour. Perceived benefit of compliance.	Theoretical	[34]
		Expermint (Participant:64)	[35]
Personality	There is a relationship between these personality traits and information security compliance behaviour. For example, carelessness can make users non-compliant.	Survey +Experiment (Participant:481)	[36]
		Theoretical model (Participant:120)	[37]
Technology democracy	Users demand more freedom to use a wider variety of applications and devices to do their work more effectively, which can be classified as asking for more 'technology democracy'.	Theoretical	[38]
		Questionnaire (Participant:390)	[39]
		Theoretical	[40]
Cultural factors	Culture leads to increased compliant security behaviour and security culture is positively associated with security compliance intention.	Theoretical	[38]
		Questionnaire (Participant:232)	[30]
		Theoretical	[12]
Gender	There is an opinion that males are more likely to be non-compliant with information security policy than females.	Technical report about violations, In the 550 extracted cases, 94 % of the insiders were male	[41]
		Technical report	[43]
Satisfaction	Job satisfaction increases the intention of users to comply with information security policy.	Survey Participant:118)	[44]
		Survey Participant:232)	[30]
Habits	Habits have a significant effect on employees' compliance with IS policy.	Theoretical model (Participant:245)	[24]
		Theoretical model (Participant:312)	[45]

1) Perception (Situation Awareness)

Perception is considered to be a key component of human behaviour and a major part of intelligence [34]. In other words, human interpretation or recognition of sensory information has a considerable impact upon user behaviour. Therefore, the perception of IT users has a great impact on their behaviour and decisions. A study by Huang *et al.* [35] regarding users'

perception of information security found that their perception is determined by several factors, such as awareness, knowledge, controllability, severity and possibility. If there is a gap between the real level of information policy and the security perception of end users, their behaviour and decisions will be influenced accordingly [35]. Essentially, having a complete image and full awareness of what is occurring in the information security policy space will positively impact upon the ability of users to recognise potential threats. Situational awareness (SA) can be considered as knowledge about a particular domain. Generally, having adequate situational awareness leads to effective decision-making and assists in reducing the potential user error rate. In other words, unintentional insider threats, such as errors, might be correlated with poor understanding of situational awareness rather than poor decision-making. In the computer world, when users have incomplete or inadequate SA, the organisational risks will be increased by user errors that may lead to computer system failures. Therefore, employees should keep up to date with the latest threat patterns and the consequential security requirements. An example of this is a user being unaware of a phishing campaign, which may lead to failure to maintain network security.

2) Personality

In psychology, five traits are often used to describe human personality: openness, agreeableness, extraversion, conscientiousness and neuroticism. A study performed by Shropshire *et al*. [37] investigated the nature of the relationship between these personality traits and information security compliance behaviour. The research sample was one hundred and twenty users. The research model was based on the five major personality traits, and the final result was that conscientiousness and agreeableness have a significant impact on user compliance with information policy. Another study was designed by Mcbride *et al.* [36] to increase understanding of the individual personality traits that shape behaviour and impact upon users' intention to comply with information security policy. They implemented and empirically validated a comprehensive theoretical model that aimed to assess the impact of the personality factors. The results of the research on 481 participants indicated that the more open, conscientious and agreeable participants were more likely to comply with information security policy. Conversely, the participants who were more extrovert and neurotic were more likely to violate information security policy.

3) Technology democracy

The systems and applications that are used at work and at home have converged and become interwoven over recent years. Some applications that were used in home environments are now used in business systems as well. This will pose a challenge to the status quo of the technology used in organisations [38]. As reported by the Econimist Intelligence Unit (EIU) [8], users today demand more freedom to use a wider variety of applications and devices in order to do their work more effectively, which can be classified as asking for more 'technology democracy'. According to Colwill [38], when more mixing between the work and home environments occurs, employees will be more likely to demonstrate unintelligent behaviour regarding security. As demonstrated by the National Computing Centre [40], staff members are more likely to fail to establish a boundary between their work and home environments, and they can fall into the trap of 'trusting innocence' and start posting personal and business information on social networks.

4) Cultural factors

According to Greene and D'Arcy [30], security culture is positively associated with security compliance intention. Concurring with this view, Colwill [38] states that organisational culture and regional/national culture must be considered when analysing insider threats since these have a direct effect on the efficacy of levels of information protection and behaviour. Usually, it is difficult for westerners to understand some of the cultural, religious and societal pressures of others communities. According to Crossler *et al.* [46], the majority of Behavioural InfoSec research has been conducted within western cultures, which limits its applicability to other cultures; however, some studies have been conducted within Asia and elsewhere. To elaborate on the cross-cultural differences, the Chinese culture is an example of a highly collectivistic one, while the American culture is an example of a highly individualistic one. At another level, the culture within an organisation or corporate culture must be analysed to comprehend how employees behave. A corporate culture can exist even though members of the organisation are not consciously aware of its existence [12]. Hence, the key challenge is to add security culture to organisational culture when the former is not a fundamental part of the latter.

5) Gender

Munshi *et al*. [47] argue that gender in relation to insider threats is rarely investigated in the academic literature. However, the importance of gender as an influence on behaviour has been cited in the academic literature in the form of reported incidents. In Hanley *et al.*'s [41] study, 94% of insider incidents were associated with males while a technical report by Cappelli *et al.* [43] also found that the majority of insider incidents were male initiated.

However, some reports argue that both genders pose an equal threat to information security. For instance, a study by Kowaski *et a.l* [48] found that 50% of insider threats were associated with females and 50% with males.

6) Satisfaction

Satisfaction, or employee satisfaction, is defined as an employee's overall feeling of well-being while at work. It is widely believed that an employee who is satisfied with his or her employer is more likely to comply with the organisation's information security policy. Therefore, users who report positive feelings about their organisation are expected to have a good sense of their responsibilities, especially in terms of compliance with information security policy. A number of studies have investigated the relationship between job satisfaction and employee compliance. These studies have provided empirical support for the claim that job satisfaction has a positive impact on compliance with security policy. For example, Greene and D'Arcy [30] examined the influence of job satisfaction on user's IS policy compliance decisions. In their theoretical research model, they postulated that satisfaction is positively associated with security compliance

intention. The research model was tested on 223 survey participants, and the results suggested that job satisfaction contributes to security policy compliance. In addition, Greene and D'Arcy [30] found a strong relationship between users' intention to comply with information security and job satisfaction. Hence, there is a link between job satisfaction and compliant behaviour; higher job satisfaction motivates users to comply.

7) Habits

A habit is automatic or unintentional behaviour, as opposed to conscious behaviour. Thus, automaticity is the key element of the habit constrict. Usually, habits can be evaluated by measuring previous behaviour or behavioural frequency. Habit theory suggests that people perform many actions without making conscious decisions and then get accustomed to performing these actions. There is an argument that habits explain information technology usage. It is argued that the actual behaviour of users is highly influenced by their technology usage habits. In this vein, some researchers are of the opinion that habitual behaviour explains information security policy non-compliance. Pahnila *et al.* [24] investigated the factors that impact upon users' compliance via a theoretical model; one of these factors was the users' habits. Empirical support was provided for their model by over 245 participants from a Finnish company. The study showed that users' habits have a significant impact on intention to comply with information security policy. Another study by Herath and Rao [45] came to the same conclusion regarding the impact of habits on user behaviour. Therefore, it is very important for any organisation to get its employees into the right habits; safe ones that help them to comply with information security policy. Changing users' behaviour or breaking old habits of dealing with information assets is not straighforward. However, organisations can mitigate this issue by: identifying the problem, finding solutions and monitoring the effectiveness of those solutions.

IV. CONCLUSIONS AND FUTURE WORK

The objective of this paper has been to explain and discuss the current issues associated with information security policy, inparticular the factors that impact upon users' behaviour in relation to this. All personnel in organisations should be able to understand the information security policies of their employers. All users need to be consistently given awareness training and education on the implemented security policy. Without such training and education, the security policy will have no impact on the employees. It is equally important that compliance with security policy is enforced. Otherwise, employees' commitment to the policy will decrease over time. Technology can play a major part in compelling employees to adhere to the security policy of their orgaanisation. Therefore, continuously subjecting users to targeted awareness raising and dynamically monitoring their adherence to information security policy should increase their compliance level.

Our future work entails focusing on this issue and proposing a framework to enhance users' compliance by relying on three significant aspects: monitoring, persuasion and the influencing factors upon users' behaviour.

REFERENCES

[1] SANS, "Information Security Policy Templates," 2014. [Online]. Available: http://www.sans.org/security-resources/policies/general. [Accessed: 15-May-2015].

[2] K. J. Knapp, R. Franklin Morris, T. E. Marshall, and T. A. Byrd, "Information security policy: An organizational-level process model," in Computers & Security, 2009, vol. 28, no. 7, pp. 493–508.

[3] ISO, "SO / I BSI Standards Publication nformati on technol ogy — Securi ty techni ques — nformati on securi ty management systems — Requi rements," 2013.

[4] PriceWaterhouseCooper PwC, "2015 INFORMATION SECURITY," 2015.

[5] 2014 EY Global information, "Get ahead of cybercrime EY ' s Global Information," 2014.

[6] PriceWaterhouseCooper PwC, "INFORMATION SECURITY BREACHES SURVEY 2014," 2014.

[7] H. Chan and S. Mubarak, "Significance of Information Security Awareness in the Higher Education Sector," Int. J. Comput. Appl., vol. 60, no. 10, pp. 23–31, 2012.

[8] Economist Intelligence Unit EIU, "Power to the people? Managing technology democracy in the workplace," 2009.

[9] P. Prince, "More Than Half of Enterprise Employees Receive No Security Training: Survey Finds," security week, 2014. [Online]. Available: http://www.securityweek.com/more-half-enterprise-employees-receive-no-security-training-survey-finds. [Accessed: 01-May-2015].

[10] The European Network and Information Security Agency (ENISA), "The new users ' guide :How to raise information security awareness," 2010.

[11] H. a Qudaih, M. a Bawazir, S. H. Usman, and J. Ibrahim, "Security Awareness in an Organization," Persuas. Technol. Contrib. Towar. Enhanc. Inf. Secur. Aware. an Organ., vol. 10, no. 4, pp. 180–186, 2014.

[12] S. Furnell and K.-L. Thomson, "From culture to disobedience: Recognising the varying user acceptance of IT security," Comput. Fraud Secur., vol. 2009, no. 2, pp. 5–10, Feb. 2009.

[13] S. Alfawaz, K. Nelson, and K. Mohannak, "Information security culture: A behaviour compliance conceptual framework," in Conferences in Research and Practice in Information Technology Series, 2010, vol. 105, pp. 47–55.

[14] F. L. Greitzer, J. Strozer, S. Cohen, J. Bergey, J. Cowley, A. Moore, and D. Mundie, "Unintentional Insider Threat: Contributing Factors, Observables, and Mitigation Strategies," in 2014 47th Hawaii International Conference on System Sciences, 2014, pp. 2025–2034.

[15] B. Khan, K. S. Alghathbar, S. I. Nabi, and M. K. Khan, "Effectiveness of information security awareness methods based on psychological theories," in African Journal of Business Management, 2011, vol. 5, no. 26, pp. 10862–10868.

[16] S. Furnell, "Malicious or misinformed? Exploring a contributor to the insider threat," in Computer Fraud and Security, 2006, vol. 2006, pp. 8–12.

[17] C. Colwill, "Human factors in information security: The insider threat - Who can you trust these days?," Inf. Secur. Tech. Rep., vol. 14, no. 4, pp. 186–196, 2009.

[18] G. Silowash, D. Cappelli, and A. Moore, "Common Sense Guide to Mitigating Insider Threats 4th Edition," 2012.

[19] Global consulting firm Protiviti, "Bridging the Data Security Chasm," 2014.

[20] I. Kirlappos, S. Parkin, and M. A. Sasse, "' Shadow Security ' as a tool for the learning organization," 2015, vol. 45, no. 1, pp. 29–37.

[21] I. Kirlappos, S. Parkin, and M. A. Sasse, "Learning from 'Shadow Security' : Why understanding non-compliant behaviors provides the basis for effective security," 2014, no. February.

[22] a Da Veiga and J. Eloff, "A framework and assessment instrument for information security culture," in Computers & Security, 2009.

[23] S. Kraemer, P. Carayon, and J. Clem, "Human and organizational factors in computer and information security: Pathways to vulnerabilities," Comput. Secur., vol. 28, no. 7, pp. 509–520, 2009.

[24] S. Pahnila, M. Siponen, A. Mahmood, P. O. Box, F.- Oulun, and E. M. Siponen, "Employees ' Behavior towar ds IS Secur ity Policy Compliance University of Oulu , Department of Information Processing," October, pp. 1–10, 2007.

[25] B. Bulgurcu, H. Cavusoglu, and I. Benbasat, "Information Security Policy Compliance: An Empiracal Study of Rationality-Based Beliefs and Information Security Awareness," MIS Q., vol. 34, no. 3, pp. 523–548, 2010.

[26] K. Parsons, A. Mccormac, M. Butavicius, and L. Ferguson, "Human Factors and Information Security : Individual , Culture and Security Environment," in Science And Technology, 2010, p. 45.

[27] M. Harris and S. Furnell, "Routes to security compliance: Be good or be shamed?," Comput. Fraud Secur., vol. 2012, no. 12, pp. 12–20, 2012.

[28] L. Cheng, Y. Li, W. Li, E. Holm, and Q. Zhai, "Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory," Comput. Secur., vol. 39, no. PART B, pp. 447–459, 2013.

[29] P. Puhakainen and M. Siponen, "R ESEARCH A RTICLE I MPROVING E MPLOYEES ' C OMPLIANCE T HROUGH I NFORMATION S YSTEMS S ECURITY T RAINING :," 2010, vol. 34, no. 4, pp. 757–778.

[30] G. Greene and J. D'Arcy, "Assessing the Impact of Security Culture and the Employee-Organization Relationship on IS Security Compliance," in 5th Annual Symposium on Information Assurance, 2010, pp. 1–8.

[31] J. D'Arcy, A. Hovav, and D. Galletta, "User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach," Inf. Syst. Res., vol. 20, no. 1, pp. 79–98, 2009.

[32] A. Yeo, M. Rahim, and Y. Ren, "Use of Persuasive technology to change end user's IT security aware behavior: a pilot study," in World Academy of Science, Engineering and Technology, 2008, vol. 2, no. 10, pp. 193–199.

[33] B. Fogg, "Persuasive computers: perspectives and research directions," in ... the SIGCHI conference on Human factors in computing ... , 1998, vol. 98, no. April, pp. 225–232.

[34] R. Proctor, Sensation and perception, 3rd ed. John Wiley and Sons, New York, 2006.

[35] D. L. Huang, P. L. Patrick Rau, G. Salvendy, F. Gao, and J. Zhou, "Factors affecting perception of information security and their impacts on IT adoption and security practices," in International Journal of Human Computer Studies, 2011, vol. 69, pp. 870–883.

[36] M. Mcbride, L. Carter, and M. Warkentin, "Exploring the Role of Individual Employee Characteristics and Personality on Employee Compliance with Cybersecurity Policies 1," 2012.

[37] J. Shropshire, M. Warkentin, A. Johnston, and M. Schmidt, "Personality and IT security: An application of the five-factor model," Am. Conf. Inf. Syst., pp. 1–8, 2006.

[38] C. Colwill, "Human factors in information security: The insider threat – Who can you trust these days?," in Information Security Technical Report, 2009, vol. 14, no. 4, pp. 186–196.

[39] EU, "Power to the people? Managing technology democracy in the workplace," 2009.

[40] A. Mohamed, "Security trends for 2009," 2009. [Online]. Available: http://www.computerweekly.com/feature/Security-trends-for-2009. [Accessed: 15-Jan-2015].

[41] M. Hanley, T. Dean, W. Schroeder, and R. Houy, "An Analysis of Technical Observations in Insider Theft of Intellectual Property Cases," 2011.

[42] "Common sense guide to prevention and detection of insider threats 3rd edition–version 3.1," in Published by CERT, 2009, pp. 1–88.

[43] D. Cappelli, A. Moore, R. Trzeciak, and T. J. Shimeall, "Common sense guide to prevention and detection of insider threats 3rd edition–version 3.1," 2009.

[44] Y. Xue, H. Liang, and L. Wu, "Punishment, justice, and compliance in mandatory IT settings," in Information Systems Research, 2011, vol. 22, pp. 400–414.

[45] T. Herath and H. R. Rao, "Protection Motivation and Deterrence: a Framework for Security Policy Compliance in Organisations," Eur. J. Inf. Syst., vol. 18, no. 2, pp. 106–125, 2009.

[46] R. Crossler, A. Johnston, and P. Lowry, "Future directions for behavioral information security research," Comput. ... , vol. 32, pp. 90–101, Feb. 2013.

[47] A. Munshi, P. Dell, and H. Armstrong, "Insider threat behavior factors: A comparison of theory with reported incidents," in Proceedings of the Annual Hawaii International Conference on System Sciences, 2011, pp. 2402–2411.

[48] E. Kowaski, D. Cappelli, and A. Moore, "Insider Threats Study: Illicit Cyber activity in the Information Technology and Telecommunication Secror," Mellon Universit, 2008.