Security by Compliance? A Study of Insider Threat Implications for Nigerian Banks

Tesleem Fagade(✉) and Theo Tryfonas

Cryptography Group, University of Bristol, Bristol, UK
{tesleem.fagade,theo.tryfonas}@bristol.ac.uk

Abstract. This work explores the behavioural dimension of compliance to information security standards. We review past literature, building on different models of human behaviour, based on relevant theories like deterrence theory and the theory of planned behaviour. We conduct a survey of IT professionals, managers and employees of selected banks from Nigeria as part of a sector case study focussed in this region. Our findings suggest that security by compliance as a campaign to secure information assets in the Nigerian financial institution is a farfetched approach. In addition to standards, banking regulators should promote holistic change of security culture across the sector. Based on an established model of Information Security Governance Framework, we propose how information security may be embedded into organisation security culture in that context.

Keywords: Information security · Compliance · Insider threats · Standards · Information security culture

1 Introduction

Information security management policies are often difficult to be successfully implemented because significant issues of diffused liability and incentives are not appropriately distributed. Information systems exploitation is not always a consequence of technical or policy failure, but often due to the lack of balanced incentives between the designers and users of such systems [1]. Despite managements' efforts to protect organization data, problems of identity theft, database breaches and stolen passwords continue to be major challenges faced by corporate organizations and government agencies [2]. Today, one of the biggest challenges faced by organisations is system misuse by insiders, whose actions are deeply rooted on non-compliance to regulatory standards. It has been established that the weakest link in information security defence is the human element [3, 4], implying that of the most considerable threats comes from insiders. Lack of compliance by employees to information security policies is claimed to be responsible for more than half of information systems security breaches [5]. It is often difficult for organisations to balance the psychological, incentive and communication need of employees due to the complex nature of human behaviour. If all end-users are rational, cyber security will be a straight game between defenders and attackers of information assets. However, insider actions that are not necessarily

T. Tryfonas (Ed.): HAS 2016, LNCS 9750, pp. 128–139, 2016.
DOI: 10.1007/978-3-319-39381-0_12

malicious but inconsistent with policy and difficult to explain (e.g. clicking on links in phishing emails) place attackers at significant advantage against system defenders and wider risk exposure to organisation security.

The ISO/IEC27001 is an international standard for best practices in Information Security Management Systems (ISMS), which outline comprehensive requirements for safeguarding organisations information assets. It defines baseline requirements and controls for the assessment of ISMS, under the principle of confidentiality, integrity and availability [6]. Standards guidelines did not necessarily address how to capture the thought process of system adversaries; there seem to be more concerted effort on the implementation of physical, policy and technical measures to mitigate anticipatory threats. Some of the previous research on this subject [7] identified that the size and need of organisations vary when it comes to protecting IT infrastructure, and that different organisations require different security treatments. Hence, the one-cap-fits-all approach of Standards undermine the effectiveness of security by compliance.

1.1 'Compliant Security'

It is quite possible to meet compliance requirements and still be insecure within the context of information security. Organisations can easily implement all of the baseline security requirements in Standards to become compliant, yet not secure. For instance, compliance requirement of the National Institute of Standards and Technology (NIST) suggests that data should be encrypted at FIPS 140 level. If a full disk encryption is carried out but the encryption key is stored on the same disk, compliance requirements may have been addressed while still insecure. A secure and compliant approach would be full disk encryption and independent key management.

Business executives often focus on the cost of implementing compliance programs and once achieved, they operate under the assumption that compliance equates security. In practice, control baseline may be enough for business executives and regulators, but it is insufficient in providing holistic security protection. Security auditors and management may combine efforts to develop useable security policies but employee compliance to policies cannot be guaranteed. In a publicly reported 2014 cyber heist [9, 10], a Nigerian bank lost £23.5m through an insider operating with rogue third party contractors. Incidentally, the bank has been certified ISO27001 compliant, in line with the regulatory requirement of Central Bank of Nigeria (CBN). The CBN is Nigerian apex bank responsible monitoring, reforming and regulating the activities of banks and other financial institutions in Nigeria [8]. This goes to show that organisations can implement the toughest security policies, but performance is largely down to users. Cyber criminals would rather target authorized users who already sits within an organisation, than having a crack at multiple layers of outside facing firewalls.

While compliance processes are aimed at hardening organisations security defence, sometimes, how standards are interpreted can actually contribute to a porous security postures. If employees consider guidelines difficult to interpret or irrelevant to a business unit, it can easily give ground to non-compliance by way of accidental or deliberate introduction of threats to the environment [11]. Cases of security breaches due to negligence, intent and lack of understanding of policy requirements continue to make rounds

despite the certification status attained by other Nigerian banks. Some employees continue to ignore security guidelines, while some find the extra steps introduced to complete tasks as interfering with job productivity. It has been suggested that users often fail to adhere to policy requirements because it is burdensome and there is no rational justification to comply from users' economic perspective; especially if the benefit is largely speculative, or the consequence is of little or no harm to the users [12]. There is a thin line between security and productivity [13], some employees often felt compelled to opt for productivity at the expense of security and compliance, when additional steps are required to complete a task. In a survey of more than 500 professionals, over 60 % admitted to using personal accounts to store and disseminate sensitive organisation data [14], because they felt that consumer options are more intuitive and easier to use than approved technology that sits within policy guidelines. Policy is an important aspect of security but it is only as effective as the technology and people backing it.

In this paper we explore the behavioural dimension of compliance to information security. Building on different models of human behavior, including deterrence theory and the theory of planned behavior (Sect. 2), we conduct a survey of IT professionals, managers and employees of selected banks from Nigeria as part of a sector case study focussed on the region (Sect. 3). In light of our results and discussion (Sects. 4 and 5) and based on an established model of Information Security Governance Framework (Sect. 5), we propose how information security may be embedded into organisation security culture in that context (Sect. 6).

2 Relevant Work

Security standards and written policies assume perfect rationale of users of information assets. Humans are not programmable machines, and often behave in manners that are completely out of the norm [15]. There are many studies on why it is challenging to enforce compliance in humans. Starting with technical security, [16, 17] pointed out why it is difficult to audit human behaviour in the same way technical auditing tools work. Irrational behaviour borders on frustration, anger or despair propelled by lack of job satisfaction, vendetta, financial and personal problems [18]. However, when organisations conduct security audits, it is the technical side that is often mostly addressed. Log files may capture and report unauthorized insider activities but the behaviour and motive is not necessarily captured. Therefore technical security audits verify consequences of behaviour but not the actual behaviour itself.

Organisations often apply deterrence measures to enforce policy compliance but studies [19, 20] based on deterrent theory suggested that employees' motivation differs across organisations, therefore, deterrent measures that work with one organisation may not necessarily fit into another. Deterrence implies rational behavior and even standards like ISO/IEC27001, COBIT and NIST draw on the principle of General Deterrence Theory [18], where rational users of information assets are expected to fit within a certain frame of reference. Unfortunately; that is not always the case. Deterrent actions, through reward or punishment has been shown to fail in organisations. Again, contrary to perfect rational assumption, punishing employees for accidental misuse or negligence may yield

negative consequences. Besides, it is impractical, time consuming and expensive to monitor employees continuously in order to enforce or deter certain behaviours. Without a grounded insight into the understanding of employees' motivation, deterrent measures as a means to address insider threat may not necessarily work.

Other works that explored the theory of planned behaviour [21, 22] suggested that training and awareness are the most significant factors that influence human behaviour and attitude towards information security. It was argued that attitude, perceived expectation and subjective norm are the incentive components of behavioural intention. Hence, change in employee attitude that is in line with corporate expectations can be addressed with information security awareness campaigns. Although, some organisations put concerted effort into training with the hope of addressing security awareness gaps, but it is clear that training is not sufficient to ensure compliance and training is not the same as security culture [4]. What then can be done to ensure compliant behaviour? Can change be unforced? How can compliance be integrated into organisation security culture? This is the open space that our work tries to address in our specific context.

3 Research Method

Survey methodology can be used to study employees' opinion, attitude and behavioural patterns within the context of information security [23]. We carried out a survey of four banks in Nigeria to gain the understanding of how security awareness and employee behaviour impacts on policy compliance. The survey is designed to capture how compliance-certified financial institutions implement policies and how employees respond to situations within the context of information security. The banks selected for this survey have all obtained ISO27000 certifications, in line with the directives of CBN. In view of the banks' reluctance to share vulnerability information, results are anonymously obtained for this work.

The survey was conducted online and it followed a methodology as described in [23, 24]. Questions are divided into 3 parts; security culture statements, knowledge and awareness statements and demography. Security culture statement assesses the behavioural pattern of employees that could undermine effective implementation of policies. Knowledge and awareness statement assesse the understanding of security policy requirements, while the demography question captures survey representatives for segmentation analysis. The recruitment strategy for this work is based on random selection from a presumably representative group of bank employee.

The survey questions follow a Likert scale response model (strongly agree, agree, uncertain, disagree and strongly disagree), except question 1, which is on survey demography. Survey tool chosen for this work is Google Forms, an online survey application that allows real time response, collation and analysis of data. The survey was conducted over 2 weeks and respondents were invited to take part in through email communication, after obtaining initial clearance from the CISO. Table 1 shows extracted sample of questions contained in the online survey.

Table 1. Extracts from the online information security survey

	Demography					
1	What is your job level/department in your organization?	Executive/ senior level manager	IT department	Operations	HR & Administration	Others: Please specify
		Strongly agree	**Agree**	**Uncertain**	**Disagree**	**Strongly disagree**
	Security culture statements					
2	Information Security interferes with job productivity.	○	○	○	○	○
3	You can share your password with other people if you trust them.	○	○	○	○	○
4	It is safe to open any email attachment if it is not in the spam/junk box.	○	○	○	○	○
	Knowledge/awareness statements					
9	Your organisation has information security policy and you know where to locate a copy.	○	○	○	○	○
10	Your organisation has provided security awareness and training to all employees.	○	○	○	○	○
11	You know how to identify and report suspicious/actual security breaches.	○	○	○	○	○
12	Information is permanently lost when files on hard drives are erased or formatted.	○	○	○	○	○

4 Results and Analysis

The demography of respondents is shown in Fig. 1. 15.8 % represents the executive/ senior manager level, 12.3 % from the IT department, 14 % from HR and administration, 40.4 % from Operations and 17.5 % represents other categories. Job functions of other categories include marketing, accountancy, risk management, sales and predictive analysis. Our data is analyzed by assigning a range values from 1 to 5 for each survey question categorized under the security culture statements and the knowledge/awareness statements. Such that, if a statements is true from security standpoint, 5 corresponds to 'strongly agree' and 1 corresponds to 'strongly disagree'. We then analyzed respondents by demography based on collective points. The maximum score per respondent is 55 points, which implies good security behaviour and compliance, while lower scores down to the minimum of 11 points lean towards poor security posture and non-compliance. Results from the security culture statement and knowledge/awareness statements is shown in Fig. 2.

As a summary, more than 50 % of respondents view security measures as inconvenient add-on but necessary in getting some jobs done. Organisations need to ensure that security steps are viewed and implemented as part of job requirements. It is interesting to see that 12.1 % strongly disagree and 9.1 % disagree that their organisations has information security policy and they know where to locate a copy. Users who are not aware of organisation information security policy or know where to locate a copy pose a significant risk. It could be that such users simply forget that security policy exists or find policy statements hard to understand. When asked if respondents know how to report actual (or suspicious) security incidents, 22.6 % of respondents have no idea on

how to do that. When users cannot identify a potential security threat or who to contact when there is a breach/compromise, such users may continue to expose information assets to threat by making further use of compromised devices. A significant number or respondents constituting 28 % are misinformed on how to dispose of sensitive electronic information. They assumed that data is permanently lost when deleted or when hard drives are formatted, this can pose a significant risk to an organisation. Forensic solutions that can erase end-of-life classified data need to be integrated in asset disposal policy.

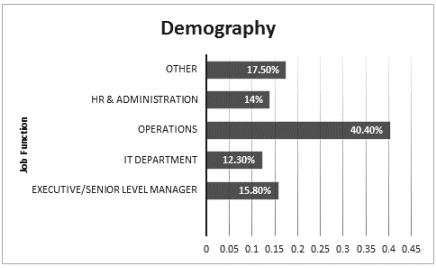

Fig. 1. Demography of respondents

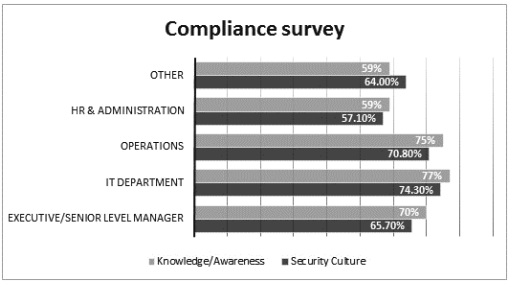

Fig. 2. Information security compliance results

The survey findings indicate that there is a high sense of security awareness but secure practice and behaviour is low, which can have a significant impact on compliance. Although, not surprising, there seem to be higher evidence of compliance by employees in the IT department more than any other respondents. Considering that this survey is administered on employees from compliant certified financial institutions, it supports our understanding that security by mere compliance is a wishful approach to information security issues in Nigerian banking institutions.

5 Information Security Cultural Framework

Organizational culture has been described as the shared values, behaviour, attitude and practices that sustain connections among people, processes and policies. It is suggested that the management and governance of security is most effective when it is integrated into the culture of organisational behaviour and actions [25]. Habitual behaviour propagates, and it often require concerted efforts to break the norm. If organisations want to project the habit of secure behaviour, perhaps a long term goal that is in line with the direction of an organizational security culture is a better approach [4], rather than focusing on quick certification status, then assuming that all technical and human processes are secured. Organizational security culture is defined as the assumptions, attitudes and perceptions that are accepted and encouraged with the aim of protecting information assets, so that attributes and custom of information security begins to emerge as the way things are done in an organisation [26]. Thus a strong information security culture is vital for managing organisational information assets. A number of studies recognized the need for creating security culture [17, 27–29] where employees have the attitude, skill and knowledge to support

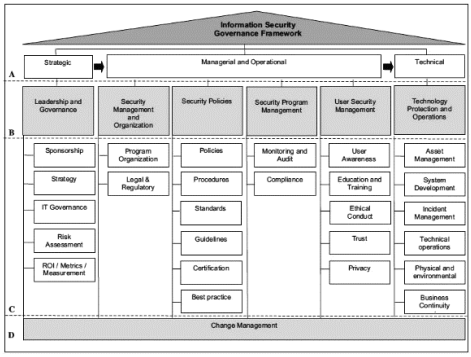

Fig. 3. Information Security Governance Framework (adopted from [31])

information security objectives. However, steps on how to embed security into the culture of an organisations are not addressed [30].

We will use a model of information security governance framework adopted from [31], in an attempt to show how information security culture can influence a change in organisation security postures. Although, the adopted framework did not specifically elaborate on how security practices can be embedded in organisation culture, but it provided a single point of reference and comprehensive structure upon which organisations can cultivate an acceptable level of information security culture. The frame work shown in Fig. 3 provided a starting point for the governance of information security. It explains how guidelines and control implementations can identify and address the technical, procedural and human components of information risks.

The information security governance framework is derived from the integration of four different information security frameworks; ISO/IEC27001, PROTECT, Capability Maturity Model and Information Security Architecture (ISA) [31]. Key categories of the framework that is most relevant to this work are discussed below:

1. Leadership and governance

This category comprises of executive level sponsor of policies and strategies for addressing the threats of information security. This category also covers the compilation and measurement of control effectiveness, in ensuring that organisation long term security goals are met.

2. Security management and organisations

This category addresses organisations legal and regulatory requirements for information security, for instance, it is now a regulatory requirement for all Nigerian banks to be ISO27001 certified. Also, the National Information Technology Development Agency (NITDA) guidelines on data protection draft (2013), requires that all federal agencies and private organisations that owns, use or deploy information systems within Nigeria is covered by the guidelines [32]. Organisation information security design, composition and reporting structure is also addressed in this category.

3. Security policies

Security policies must be implemented through effective process and compliance while taking into account other components like legal and ethical considerations.

Security policies are the overall organisation intention and direction as expressed by the management [33]. Policies provide specific guideline for employee behaviour and procedures when interacting with information systems. Example may include point-specific policy statement covering internet acceptable use.

4. Security program management

This category involves auditing and compliance monitoring of both technical and human elements of security programs. It must be ensured that policies, processes, procedures and controls are managed through continuous monitory, for timely response to security breaches. Employee behaviour monitoring could include internet usage and technology monitoring could be network traffic monitoring.

5. User security management

User security awareness, ethical conduct and trust are all addressed in this category. Ethical conduct is a vital component of security culture, it must be developed and communicated as part of a corporate code of conduct. For instance, organisation ethics may include unauthorized data alteration or disclosure. Security awareness program needs to be promoted and maintained throughout the organisation and the management need to find ways to integrate the element of mutual trust between all stakeholders.

6. Technology protection and management

This involves physical and technical protection measures around information assets. As part of the implementation of the security governance framework, it must be ensured that appropriate technology controls are included in asset management, technical operations, physical environments and business continuity. Continuous monitoring of technical controls is also important in order to keep pace with rapid technology changes.

6 Embedding Security in Organisational Culture

An organisation's compliance status does not necessarily present desired changed behaviour of employees. However, given objective situations, it is unlikely that employees would be tempted to break the law, if compliance is ingrained into organisation cultural and daily routine [34]. Embedding security into organisation culture must adopt a top-bottom approach, starting with management buy-in and then gradually including everyone in the organisation. It has been shown that top management buy-in and support has enormous impact on policy enforcement and organisational culture [35]. Management top hierarchy are responsible for imposing measures which can have great influence on employee attitude, behaviour and motivation; hence, there has to be a demonstration of commitment by the management before there can be any success of integrating security in organisation culture.

Using data security as an example, some organisations understand the need for data protection but may not know how to prioritize that for all employees. Since most organisations are covered by national or international data protection acts; this should be the starting point for embedding data security into organisation culture. Management top hierarchy should be able to understand and communicate their organizations' legal/regulatory obligations under data protection laws. Data protection should then be included in organisation information security policy, which may further include policy

subsets like regular data backups and unauthorized use of portable devices on corporate computers. Policy subsets should show clear guidelines and best practices for ensuring data confidentiality, integrity and availability at all times. Through user awareness and ethical code of conduct programs, employees should become sensitized about organization's position on data protection. It should be communicated why data is vital for business continuity, how data loss may impact on business and what measures can be taken to ensure data security. Most importantly, data security should become the responsibility of all employees and not only dedicated to a small unit of staff.

Technical solutions that complement a data protection policy can then be introduced as part of security plan. Although, employees often see security steps as inconvenient add-ons that impact on productivity; technical solutions can be introduced gradually, while focusing initially on components that constitute everyday security issues. Policy subset that safeguards data loss may require that employees must regularly backup data, but compliance can be enforced if data backup becomes part of job functions. Technical solutions that can be leveraged as part of data security strategy may simply be a system, which forces or reminds employee to do a data backup every day. Perhaps, if all employees that interact with information systems cannot logoff after a day's work without completing backups to the central server, this function will become embedded in the organisation security culture where data backups become part of job requirement, rather than inconvenient security measure. Other policy subsets can then be applied to support compliance, for instance, disabling the USB ports on all organisation computers to control unauthorized copying of confidential information. Also, implementing a system that compel users to change passwords at intervals may ensure compliance and reduce threats posed by employees that are susceptible to social engineering.

Through these measures, employees will become involved in the process of security whereby **security requirements are incorporated within operational system architecture.** As employees learn to comply with the requirements of a policy, and observed behavioural change starts to emerge to the point where secure behaviour becomes second nature, a change in organizational culture which is also security driven will become evident. Thereafter, management can begin to gently introduce other policy requirements in stages until the entire policy becomes embedded in the organizational culture. Through continuous assessment, the effectiveness of each security component embedded in the organisation culture can be measured over a given period of time. Security metrics may be based on how many times an organisation has recorded incidents of data loss since data backup has become part of job requirements. Employees will ultimately identify those changes as part of corporate culture and may not require extra motivation, reward or punishment to perform those functions. There are additional benefits of improved reputation and efficiency for organisations that have sound security practices integrated in its culture, ultimately becoming compliant and secured.

7 Conclusion

We believe that in addition to compliance, organisations need to cultivate information security culture because compliance is not the same as security. In addition, there is no

guarantee that employees will comply with policy requirements. Human factors continue to represent the gap between processes and technology, and there is no difference between malicious intent, negligence or external attacks in terms of diminishing IT functions. There is insufficient understanding of the risks posed by users of information assets, therefore, management are mostly focused on achieving compliance status without necessarily understanding that compliance is just a part of information security.

The strongest influence on organisation culture begins with the position of leadership. Leadership acceptance and active participation in holistic cultural change, is a key aspect of information security. Executive level security representation and a change in management behaviour, will reflect on employees' behaviour too. Information security channel of communication should be clearly defined and all employees need to be part of security. Often, organisations have dedicated IT units that enforce the implementation of information security policies, rather than promoting a sense of shared responsibility where security is a required function for everyone. Once the overall mind-set of an organisation begins to change, a culture where security is pivotal will begin to emerge and compliance will inevitable become an integral part of organizational culture. If policy compliance becomes natural to employees, it will be much easier for new employees to emulate acceptable behaviour through observation. It is unlikely that information security culture can be covered by a single framework or few technical solutions. Future research may consider how to integrate other frameworks with the one adopted for this work and also suggest how human-centric technical solutions can be integrated into organisation security culture. This model hasn't been tested in other security domains, but it has been subjected to critique from industry experts with good feedback on its feasibility. As part of future work, there will be a robust comparative empirical model to test the validity of observations made through this work.

References

1. Ross, A.: Security Engineering: A Guide to Building Dependable Security Systems, 2nd edn. Wiley, New York (2008)
2. Corriss, L.: Information security governance: integrating security into the organizational culture. In: Proceedings of the 2010 Workshop on Governance of Technology, Information and Policies, Austin, Texas, USA, pp. 35–41. ACM (2010)
3. Aurigemma, S., Panko, R.: A composite framework for behavioral compliance with information security policies. In: Proceedings of the 2012 45th Hawaii International Conference on System Sciences, pp. 3248–3257. IEEE Computer Society (2012)
4. Renaud, K., Goucher, W.: The curious incidence of security breaches by knowledgeable employees and the pivotal role a of security culture. In: Tryfonas, T., Askoxylakis, I. (eds.) HAS 2014. LNCS, vol. 8533, pp. 361–372. Springer, Heidelberg (2014)
5. Siponen, M., Vance, A.: Neutralization: new insights into the problem of employee systems security policy violations. MIS Q. **34**(3), 487–502 (2010)
6. ISO/IEC 27001:2013 Information technology - Security techniques - Specification for an Information Security Management System. The British Standard Institute 2014
7. Karjalainen, M., Siponen, M.T., Puhakainen, P., Sarker, S.: One size does not fit all: different cultures require different information systems security interventions. In: PACIS, p. 98 (2013)
8. Central Bank of Nigeria (2015). http://www.cenbank.org/. Accessed 04 Dec 2015

9. Chima, O.: How Bank Insiders Connive with Fraudsters. This Day Live (2015). http://www.thisdaylive.com/articles/how-bank-insiders-connive-with-fraudsters/204219/. Accessed 03 Dec 2015
10. Morgan, L.: Nigerian bank IT worker on the run after £23.5m cyber heist, IT Governance Blog (2014). http://www.itgovernance.co.uk/blog/nigerian-bank-it-worker-on-the-run-after-23-5m-cyber-heist/. Accessed 18 Dec 2015
11. Da Veiga, A., Eloff, J.H.P.: A framework and assessment instrument for information security culture. Comput. Secur. **29**(2), 196–207 (2010)
12. Herley, C.: So long, and no thanks for the externalities: the rational rejection of security advice by users. In: Proceedings of the 2009 Workshop on New Security Paradigms Workshop. Oxford, United Kingdom, pp. 133–144. ACM (2009)
13. Albrechtsen, E.: A qualitative study of users' view on information security. Comput. Secur. **26**(4), 276–289 (2007)
14. GlobalSCAPE. Protecting Digitalized Assets in Healthcare. Whitepaper (2013). http://dynamic.globalscape.com/files/whitepaper_healthcare.pdf. Accessed 18 Dec 2015
15. Alavi, R., Islam, S., Mouratidis, H.: A conceptual framework to analyze human factors of information security management system (ISMS) in organizations. In: Tryfonas, T., Askoxylakis, I. (eds.) HAS 2014. LNCS, vol. 8533, pp. 297–305. Springer, Heidelberg (2014)
16. Wall, J.D., Iyer, L. Salam A.F., Siponen, M.: Conceptualizing Employee Compliance and Non-compliance in Information Security Research: A Review and Research Agenda. Dewald Roode Information Security Workshop, Niagara Falls, New York (2013)
17. Vroom, C., von Solms, R.: Towards information security behavioural compliance. Comput. Secur. **23**(3), 191–198 (2004)
18. Theoharidou, M., Kokolakis, S., Karyda, M., Kiountouzis, E.: The insider threat to Information Systems and the effectiveness of ISO17799. Comput. Secur. **24**(6), 472–484 (2005)
19. Park, S., et al.: Towards understanding deterrence: information security managers' perspective. In: Kim, K.J., Ahn, S.J. (eds.) Proceedings of the International Conference on IT Convergence and Security 2011, vol. 120, pp. 21–37. Springer, Netherlands (2011)
20. D'Arcy, J., Herath, T.: A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings. Eur. J. Inf. Syst. **20**(6), 643–658 (2011)
21. Waly, N., Tassabehji, R., Kamala, M.: Measures for improving information security management in organisations: the impact of training and awareness programmes. In: Proceedings of the UK Academy for Information Systems Conference, Oxford, Paper, vol. 8 (2012)
22. Gundu, T., Flowerday, S.V.: Ignorance to awareness: Towards an information security awareness process. SAIEE Africa Res. J. **104**(2), 69–79 (2013)
23. Da Veiga, A., Martins, N., Eloff, J.H.P.: Information security culture - validation of an assessment instrument. South. Afr. Bus. Rev. **11**(1), 147–166 (2007)
24. Deloitte. Insight into the Information Security Maturity of Organisations, with a Focus on Cyber Security. Central Asia Information Security Survey Result (2014). https://www2.deloitte.com/content/dam/Deloitte/kz/Documents/risk/KZ_Deloitte_Information_Security_Survey_2014_EN.pdf. Accessed 16 Dec 2015
25. Department of Homeland Security. Build Security In. Governance and Management (2015). https://buildsecurityin.us-cert.gov/articles/best-practices/governance-and-management. Accessed 08 Jan 2016
26. Martins, A., Elofe, J.: Information security culture. In: Ghonaimy, M.A., El-Hadidi, M.T., Aslan, H.K. (eds.) Security in the Information Society: Visions and Perspectives, pp. 203–214. Springer US, MA (2002)

27. Sherif, E., Furnell, S., Clarke, N.: An identification of variables influencing the establishment of information security culture. In: Tryfonas, T., Askoxylakis, I. (eds.) HAS 2015. LNCS, vol. 9190, pp. 436–448. Springer, Heidelberg (2015)
28. Furnell, S., Clarke, N.: Organizational security culture: Embedding security awareness, education, and training. In: Proceedings of the IFIP TC11 WG, vol. 11, pp. 67–74 (2005)
29. Ruighaver, A.B., Maynard, S.B., Chang, S.: Organizational security culture: Extending the end-user perspective. Comput. Secur. **26**(1), 56–62 (2007)
30. Lim, J.S., Ahmad, A., Chang, S., Maynard, S.: Embedding information security culture emerging concerns and challenges. In: PACIS 2010 Proceedings. Paper 43 (2010)
31. Veiga, A.D., Eloff, J.H.P.: An information security governance framework. Inf. Syst. Manage. **24**(4), 361–372 (2007)
32. NITDA. National Information Technology Development Agency: Guidelines on Data Protection (2013). http://www.nitda.gov.ng/wp-content/uploads/Guidelines-on-Data-Protection-Final-Draft-3.5.pdf. Accessed 08 Jan 2016
33. Merete Hagen, J., Albrechtsen, E., Hovden, J.: Implementation and effectiveness of organizational information security measures. Inf. Manage. Comput. Secur. **16**(4), 377–397 (2008)
34. Jackson, J., Bradford, B., Hough, M., Myhill, A., Quinton, P., Tyler, T.R.: Why do people comply with the law? Legitimacy and the influence of legal institutions. Br. J. Criminol. **52**(6), 1051–1071 (2012)
35. Knapp, K.J., et al.: Information security: management's effect on culture and policy. Inf. Manage. Comput. Secur. **14**(1), 24–36 (2006)