International Journal of Innovative Research in Information Security (IJIRIS) ISSN: 2349-7009
Issue 04, Volume 3 (April 2016) www.ijiris.com

Information Security Policy Development: A Literature Review

Noli B. Lucila Jr.
College of Science, Bicol University, Legazpi City, Philippines

Abstract— Information security policy is one of the most important security controls, and considered as the foundation of any security regime in an organization. In fact, failure to formulate an information security policy is said to be one of the deadly sins in information security management. It is also evident that many organizations face difficulty constructing this document, its content and structure in particular. In this vein, a number of developed policy frameworks or models in the formulation of information security policy have been proposed and published in academic journals. The purpose of this study, therefore, was to review the actual state of the literature for the last 15 years (2001-2015) focusing on information security policy frameworks and models. This paper has found that there is still limited number of frameworks and models available, supported by empirical surveys. Since the development and implementation of an information security policy involves social, political, economic and technological factors, this paper, therefore, suggests further research towards an integrated theory-based security policy frameworks and models using social and organizational theories. In addition, existing models or frameworks from other fields such as management, engineering, social sciences may also be considered.

Keywords—information security policy development, information security policy, information security

I.

1. INTRODUCTION

Given the prevalence of security risks, many organizations today need to ensure that information, as business resource, are adequately protected [1]. In this vein, information security continues to be a key IT management concern for corporate executives [2]. Although technologies and tools are fundamental components in information security, an entirely technical approach without taking appropriate policies and procedures into consideration is still inadequate [3]. Existing literature suggests that end users are considered the weakest link in an information security chain [4][5][6]. In fact, information security-related incidents commonly happen because of abuse and misuse of resources by trusted personnel [7][8][9], and consequently this 'insider threat problem' is more elusive than any other threat [10]. Similarly, according to the Global Information Security Survey [11], one of the key obstacles in information security effectiveness is the lack of information security awareness among users. Therefore, it is important to note that incorporating technology, process and people into any security measures provides a holistic security solution [12][13]. With this, many organizations today have implemented information security policy [14][15] to elevate their security level [16].

Information security policy, as one of the most important controls [17] and considered as the foundation of any security regime [18], should be established prior to planning, implementing, and maintaining information security in an organization [19]. In fact, one of the deadly sins in information security management is the failure to formulate an information security policy [20]. ISO/IEC describes information security policy as a document used 'to provide management direction and support for information security in accordance with business requirements and relevant laws and regulations' [21]. In addition, it contains a number of rules for protecting organizational resources [22] along with employees' roles and responsibilities to safeguard these resources [23], as well as, a clear definition of security violation and disciplinary action [17]. Although guidelines and standards on information security policy are widely available, many are sceptics, particularly the researchers and practitioners, towards the use and effectiveness of security policies [24][25]. First, most of these standards are generic or universal in scope which they can easily overlook the business requirements of an organization [26]. Second, content and quality are not their primary concern; they just simply focus on the existence of processes [25]. Finally, in information security domain, there is no single security solution, nor a single security policy that can fit all organizations [27].

Therefore, as noticed in the existing literature, practitioners and researchers have carried out studies on formulation of information security policies. In essence, information security policy frameworks provide a high-level and comprehensive strategy for assessing, improving, or developing information security policy of an organization, and in shaping the overall security solutions in respect to its business objectives [28]. In this vein, this study examines the existing literature for different frameworks and models designed for the formulation of information security policy. In fact, according to Baskerville and Siponen [29], there have been limited studies (e.g. [30]) on this aspect carried out from 1999 and earlier. Moreover, there are methods designed for developing and managing information systems that recognized the importance of security policy, however, most of them provide little help with respect to policy formulation, or do not provide any specific support at all. Others present different management security principles, but not on the issue of information security policy formulation [29].

Therefore, the purpose of this study was to explore and review the actual state of research in the existing literature for the last 15 years (2001-2015) for different frameworks and models designed in the formulation of information security policy, and provide suggestions for further information security research. This paper is organized as follows: the next section briefly lays out the methodological approach conducted during research. This is followed by the review of studies on information security policy formulation frameworks/models found in the current literature. The Information Security Policy Development section is followed by the Discussion and Conclusions.

II. METHODOLOGY

This paper has benefitted from scholarly, peer-reviewed, leading English journals. The review's emphasis is on the development of an information security policy, particularly focusing on security policy frameworks and models. Although there are available rankings for Information Systems journals (e.g. [31], [32]), most of these academic journals do not cover information security. For instance, Computers & Security, and other information security journals are not included in the rankings. In this vein, I based my search process on six electronic database resources: Association for Computing Machinery (ACM) Digital Library, EBSCO (Elton B. Stephens Co.) Online, IEEE/IET Electronic Library, JSTOR, Proquest Online, ScienceDirect (Freedom Collection), and Google Scholar. Accordingly, the keywords "information security policy", "information security" and "security policy" have been used in search for scholarly journal articles within the last 15 years (2001-2015) of publication period. In addition, usage of the Boolean "OR" was employed to filter the returned results based on the "Title" or "Abstract" or "Subject Terms" containing the specified keywords.

Moreover, a detailed investigation of the returned results was carried out, by checking the content of the paper, particularly abstract, keywords, and conclusion, in order to gather an initial set of academic journal articles relevant for the objective of this review. Finally, after completing the electronic database search, I scanned each article thoroughly from the initial set of academic journal articles to gain relevant information on the development of an information security policy. For the purpose of this study, it limits to the organizational aspect (high-level) of information security policy which expresses security objectives and concerns at the highest level of abstraction. However, this paper does not cover the technical perspective of security policies (e.g. [33], [34], [35], [36], [37]).

III. INFORMATION SECURITY POLICY DEVELOPMENT

Many organizations today have implemented various security controls and measures to ensure the effective working of information security [14][16][18]. One of these major mechanisms is the information security policy which is a direction-giving document for information security within an organization [17]. Existing literature suggests that the development of an information security policy is a necessary foundation of organizational security programs in protecting them against the increasing levels of security attacks from internal and external sources [16] [38]. However, many organizations face difficulty on putting this document together particularly as to what constitutes a policy and what it should look like [17] [38]. In addition, literature suggests that the formulation of an effective security policy in an organization is a multifaceted task [17]. Similarly, according to Karyda et al. [14], development of such policy is not a straightforward task which consequently depends on many factors. In fact, various international standards such as ISO/IEC, COBIT, BS7799 are widely available to provide guidance and requirements for writing an effective information security policy.

A. Information security standards

Among the most widely used methods of security management are the information security management standards which provide authoritative statements, procedures as well as best practices to be adopted by organizations in demonstrating their commitment to information security [39][25][40]. In fact, organizations may use these standards in applying for certification, accreditation and compliance of their organizational information security [26].

According to Höne and Eloff [17], although these standards acknowledge the importance of information security policy, some of them allocate only a limited number of paragraphs on the topic which demonstrate what an information security policy should contain, and what it should look like. Essentially, these security standards suggest that information security policy should contain a statement specifying management's commitment towards information security, along with users' roles and responsibilities as well as a clear definition of security violation and disciplinary action [17]. However, Höne and Eloff [17] recommend that these security standards should not be relied upon exclusively for guidance since they are not comprehensive in their coverage concerning the formulation of an information security policy.

In addition, Siponen and Willison [26] found that most of these standards are generic or universal in scope which they can easily ignore different security requirements among organizations. Hence they argue that these standards should be considered by practitioners as a reference on information security management. Similarly, Siponen [25]argues that these standards are mainly concerned with the existence of processes rather than the content and quality of these processes. According to Siponen [25], ISO/IEC 17799, for instance, suggests that employees should follow security procedures correctly by providing information security awareness activities, but it does not present how employees should be trained or motivated.

Hence, practitioners should be aware of this problem, and that researchers can also help by carrying out case or action research that investigates how the objectives of these information security management standards were applied and achieved from in-depth experiences and lessons learned in organizations [25]. Existing literature shows that there is still limited number of research dealing on this topic. One notable example, however, is the study of Ku et al. [15] which presents an empirical evidence on how a successful example of governmental institute in Taiwan has self-adopted the information security management system (ISMS), British Standard 7799 (ISO 27001). It was carried out through a single case study examining how departments achieve the governmental policies, and what the critical factors of self-implementation of ISMS are. Finally, since there are strong criticisms from information security researchers and practitioners on the use of security policy standards, several studies have been carried out dealing on information security policy particularly on the development of policy frameworks and models.

B. Information security policy frameworks/models

As noticed in the extant literature, there have been a number of frameworks/models designed for the development of information security policies. Essentially, information security policy framework is a high-level and comprehensive strategy in shaping organization's tactical security solutions in relation to its business objectives, and consequently, they may refer to it for assessing, improving, or developing their information security policy [28]. Moreover, most policy frameworks have clear security goal perspectives and logically organized steps on creating and maintaining effective security policies [41].

1) Knapp et al. [38], *"Information Security Policy: An Organizational-level Process Model"*

This information security policy model for modern organizations is a general yet comprehensive process depicting a larger organizational context that includes key external and internal influences which materially impact organizational processes. Through a qualitative methodology, data were collected from 220 certified information system security professionals (CISSPs) from over 25 countries and various industries using an open-ended question to capture the top five information security issues faced by organizations. In addition, this question elicited key information on the development and implementation processes of information security policy, and organizational issues that influence policy development. Further, to validate their designed model, a three-phase validation process was conducted: an expert panel of practitioners; on-location interviews with security managers at two technology-intensive organizations; and a presentation at a well-regarded information security conference. This consequently led to necessary improvements of the model which reflect the recommended practices of their sample of certified professionals. As a result, their model highlights the most salient and relevant aspects that are supported in the literature: emphasis on training and awareness, the necessity of policy enforcement, the cyclical nature of policy management, the role of corporate governance, and the effect of the internal and external influences on the policy process.

Moreover, this model, a comprehensive, real-world representation of an information security policy process in modern organizations, provides unique value as it was captured from the broad experiences of those who have been most active in developing and implementing organizational information security policies. However, they acknowledge some limitations of their study. One of them is the cross-cultural differences that may influence the development and management of an organization's policy, but then from their sample responses no significant cultural difference was detected since CISSP certification requirements, and the very nature of Internet security threats may have limited many cultural differences. Another is that their proposed model describes a generalized framework rather a specific model for a single organization in which not all of its elements will apply in the same way to all organizations.

2) Karyda et al. [14], *"Information Systems Security Policies: A Contextual Perspective"*

Although there are several surveys that have been conducted investigating security management issues, most of them are commercially-oriented using quantitative methods, and cover a broad range of information security issues, rather than focusing specifically on the issues pertaining the application of security policies and their effectiveness [14]. Therefore, the authors filled in this gap by examining the processes involved in the formulation, implementation and adoption of information security policies on a specific organizational context through the use of the theory of contextualism. Moreover, since the application of security policies is a human factor in which their behavior cannot be fully predicted, theory of contextualism was employed to interpret the diverse aspects of human action. The main concepts in contextualism are the context, the content and the process of organizational change which are all interrelated. In addition, contextualism is used in research to trace their dynamic interlinking over time, and explain how this change has been shaped by the processes within the specific context where they take place.

In order to provide them with an understanding of the dynamics of the formulation and application of security policies, and to give them an insight into the contextual factors, they adopted primarily explorative and descriptive research approach which was carried out in two separate case organizations: the case of a public sector social security organization, and the case of a non-governmental centre for the treatment of dependent individuals. As a result of their study, security policy formulation and implementation are affected by the different contexts within which they take place.

In addition, organizational structure and the organizational culture elements play an important role for the successful development and implementation of a security policy.

3) Rees et al. [41], *"PFIRES: A Policy Framework for Information Security"*

Policy Framework for Interpreting Risk in E-Business Security (PFIRES) provides a starting-point for information security professionals and top management to guide them in developing, implementing, and maintaining security policy. PFIRES was developed by adopting other methodological approaches such as the new product development life cycle, and the systems development life cycle (SDLC). Essentially, PFIRES offers systematic, well-defined processes, and yet dynamic framework in which organizations can adapt rapidly to changing business scenarios and security-related requirements. It has four major phases in which two main steps are included for each of these phases. These are: Assess (policy assessment and risk assessment), Plan (policy development and requirements definitions), Deliver (definition and implementation of controls), and Operate (monitoring of operations, review of trends and management of events). In addition, for every step there are feedback mechanisms to ensure that the necessary requirements of the prior step are satisfied.

4) Anand et al. [42], *"Security Policy Management Process within Six Sigma Framework"*

Anand, Saniie and Oruklu [42] proposed a security policy creation and management process based on the Six Sigma DMAIC (Define-Measure-Analyze-Improve-Control) methodology, an industrial process model used in business management to create an efficient system by putting customer centric needs in perspective with business data. This study argues that threats have a direct implication on policies. Hence, security policies need to be quantified against the identified and analyzed threats in information security management system.

In addition, with the use of the Six Sigma process model, security policy management process can easily be integrated with industrial processes, which in turn allows other processes to be integrated with security policy. Likewise, the proposed model can easily control the deployment of security policy by providing an explicit feedback mechanism. Lastly, the designed model provides a means to quantify risks in security policy management for decision making.

As noticed in the literature, there have been limited studies on the development of an information security policy particularly on the design of policy frameworks and models. In this vein, however, several studies have been carried out pertaining to the formulation of a security policy. For instance, Doherty and Fulford [7] argue that information security policy and strategic information systems plan (SISP) should be closely and explicitly aligned. Essentially, according to Doherty and Fulford [7], the key objective of strategic information systems planning is to identify opportunities to exploit information, and to ensure that this information is of the highest quality possible; whereas the information security policy provides a framework to ensure that systems are developed and operated in a secure manner. With this, they developed a model that enhances the traditional SISP process into a security-oriented SISP. Similarly, Hughes and Stanton [3] suggest that information security policy needs to be aligned with the organization's IT security goals, and comply with legal, statutory, regulatory or contractual requirements.

Likewise, Kadam [43] addresses the development and implementation process and strategies of an information security policy of an organization by mapping some possible answers for the what, why, how, who, where and when questions related to developing and implementing an information security policy. He further argues that it is important for an organization to conduct a business impact analysis (BIA) which is the best tool in understanding the importance of information security in an organization, and for encouraging the mind space of the top management for formulating an information security policy. From the BIA, all the recognized issues will be subsequently followed through during the detailed formulation of an information security policy. Similarly, Hong et al. [16] investigate the dominant factors for an organization to build an information security policy. It shows that functions, contents, implementation and procedures of an information security policy may contribute to the perceived elevation of information security. In addition, some organizational characteristics (i.e. organizational type, MIS/IS department size) might be good predictors for the adoption of an information security policy.

IV. DISCUSSION

As can be seen in the previous section, there are a number of guidance for formulating an information security policy which are widely available (e.g. information security management standards, best practices); however, there are also criticisms from both information security researchers and practitioners towards the use and effectiveness of security policies. With this, different information security policy frameworks and models have been developed. For instance, Anand et al. [42] argue that to have an effective policy management model in an industrial setting, the model should also be based on an industrial process. In this vein, security policy management process was integrated within the Six Sigma framework which provides a quantified risk analysis by correlating security tools with each phase of the process. They further argue that policy management and risk-based decisions can easily be quantified.

Moreover, in a security policy management process, feedback is necessary to mitigate the evolving threats during formulation and evaluation of an information security policy. This feedback mechanism is exhibited both in the frameworks of Anand et al. [42] and Rees et al. [41]. PFIRES, on the other hand, was adopted from other methodological approaches specifically the new product development life cycle and the systems development life cycle [41]. Just like with other development approaches, PFIRES is a step-by-step security policy development process, and yet it is dynamic in which it can adapt rapidly to evolving threats and changing business requirements. These two frameworks were developed using various models from other fields such as management and software development.

On a different note, an organizational-level process model [38] was conceptualized from the broad experiences of information security professionals who have been most active in developing and implementing information security policies in their respective organizations. The proposed process model describes a generalized framework rather a specific model for a single organization. Thus, this model provides an illustrative framework that can guide organizations in the development and management of information security policy from a holistic or systems perspective that takes into consideration the overall flow, interacting phases, along with the internal and external influences, as important factors in the policy process. On the contrary, Karyda et al. [14] designed a security framework based on the theory of contextualism to understand the different contextual factors that affect the dynamic nature of information security policy adoption. Theory of contextualism has been largely used as an analytical instrument for exploring the relationship and interplay between the strategic change, the context of change, and the process of managing change in organization studies. In their findings, security policy formulation and implementation are affected by the different contexts within which they take place. In addition, according to Karyda et al. [14], organizational structure and the organizational culture elements are imperative in the development and implementation of a security policy. This notion was supported by many advocates that security policy development is substantially influenced by an organization's culture [44]. While others suggest that an information security policy should be designed to uphold the organization's core mission and cultural values ([16][45] [46]).

Moreover, it is important to note that information security is a balance between protecting information and allowing authorized access [47]. Hence, information security policy authors need to take extra effort understanding the functions of all users to ensure that the security measures will not stop them from achieving their tasks [3]. Finally, an information security policy is said to be effective when it is communicated well to the users wherein they can identify what is expected from them in terms of handling information resources [24].

V. CONCLUSIONS

Information security policy is one of the most important security controls which is regarded as the foundation of information security that should be established prior to planning, implementing, and maintaining information security in an organization. Absence of information security policy is said to be one of the deadly sins in information security management. However, development and implementation of an information security policy, is a complex and multifaceted activity, and depends on many factors. In fact, many organizations face difficulty on putting this document together particularly the structural arrangements and its contents. With this, security practitioners refer on the commonly available guidance, standards and best practices in formulating an information security policy; however, there are criticisms towards the use and effectiveness of security policies. In this vein, a number of information security frameworks and models have been developed for the past 15 years.

The purpose of the current study, therefore, was to examine the current literature on the development process of an information security policy particularly by looking at the existing frameworks and models, and detect the gaps and suggest some possible research. This review study has found that there is a limited number of frameworks and models on the development of an information security policy. It was also noted that support for these models are limited in terms of empirical surveys. In general, limited empirical studies are available pertaining to the formulation and implementation of an information security policy in organizations. Therefore, this paper suggests for possible studies wherein researchers and practitioners may look into their self-constructed information security policy supported by empirical evidence. In addition, adoption of existing models or frameworks from other fields such as management, engineering, social sciences may also be considered in the design of security policy. Finally, since information policy involves social, political, economic and technological factors, social and organizational theories may be used in order to examine and understand the dynamic nature and complexities of the formulation process. Hence, research towards an integrated theory-based security policy frameworks and models on the development of an information security policy should be further looked into.

REFERENCES

[1] B.C. Stahl, N.F. Doherty and M. Shaw, "Information security policies in the UK healthcare sector: A critical evaluation," *Information Systems Journal*, vol. 22, pp. 77-94, 2012.

[2] J. Luftman and B. Derksen, "Key issues for IT executives 2012: Doing more with less," *MIS Quarterly Executive*, vol. 11, no. 4, pp. 207-218, 2012.

[3] M. Hughes and R. Stanton, "Winning security policy acceptance," *Computer Fraud & Security*, pp. 17-19, 2006.

[4] J. Wade, "The weak link in IT security," *Risk Management*, vol. 51, no. 7, pp. 32-37, 2004.

[5] M. Warkentin and R. Willison, Guest Editorial: "Behavioral and policy issues in information systems security: The insider threat," *European Journal of Information Systems*, vol. 18 , no. 2, pp. 101-105., 2009.

[6] Q. Hu, Z. Xu, T. Dinev and H. Ling, "Does deterrence work in reducing information security policy abuse by employees?," *Communications of the ACM*, vol. 54, no. 6, pp. 54-60, 2011.

[7] N.F. Doherty and H. Fulford, "Aligning the information security policy with the strategic information systems plan," *Computers & Security*, vol. 25, pp. 55-63, 2006.

[8] J. Choobineh, G. Dhillon, M.R. Grimaila and J. Rees, "Management of information security: Challenges and research directions," *Communications of the Association for Information Systems*, vol. 20, pp. 958- 971, 2007.

[9] D.S. Wall, "Enemies within: Redefining the insider threat in organizational security policy," *Security Journal*, vol. 26, no. 2, pp. 107-124, 2013.

[10] K.R. Sarkar, "Assessing insider threats to information security using technical, behavioural and organisational measures," *Information Security Technical Report*, vol. 15, pp. 112-133, 2010.

[11] Ernst & Young, "Fighting to close the gap: Ernst & Young's 2012 global information security survey.," EYGM Limited, U.K., 2012.

[12] G. Dhillon and G. Torkzadeh, "Value focused assessment of information system security in organizations," *Information Systems Journal*, vol. 16, no. 3, pp. 293-314, 2006.

[13] A. Da Veiga and J.H.P. Eloff, "An information security governance framework," *Information Systems Management*, vol. 24, pp. 361-372, 2007.

[14] M. Karyda, E. Kiountouzis and S. Kokolakis, "Information systems security policies: A contextual perspective," *Computers & Security*, vol. 24, no. 3, pp. 246-260, 2005.

[15] C.-Y. Ku, Y.-W. Chang and D.C. Yen, "National information security policy and its implementation: A case study in Taiwan," *Telecommunications Policy*, vol. 33, pp. 371-384, 2009.

[16] K.-S. Hong, Y.-P. Chi, L.R. Chao and J.-H. Tang, "An empirical study of information security policy on information security elevation in Taiwan," *Information Management & Computer Security*, vol. 14, no. 2, pp. 104-115, 2006.

[17] K. Höne and J.H.P. Eloff, "Information security policy – what do international information security standards say?," *Information Security Policy*, pp. 402-409, 2002.

[18] J.M. Hagen, E. Albrechtsen and J. Hovden, "Implementation and effectiveness of organizational information security measures," *Information Management & Computer Security*, vol. 16, no. 4, pp. 377-397, 2008.

[19] V. Pathari and R. Sonar, "Identifying linkages between statements in information security policy, procedures and controls," *Information Management & Computer Security*, vol. 20, no. 4, pp. 264-280, 2012.

[20] B. von Solms and R. von Solms, "The ten deadly sins of information security management," *Computers & Security*, vol. 23, no. 5, pp. 371-376, 2004.

[21] ISO/IEC, "International standard ISO/IEC 27002," International Organization for Standardization (ISO), Switzerland, 2007.

[22] E. Kolkowska and G. Dhillon, "Organizational power and information security rule compliance," *Computers & Security*, pp. 1-9, 2012.

[23] B. Bulgurcu, H. Cavusoglu and I. Benbasat, "Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness," *MIS Quarterly*, vol. 34, no. 3, pp. 523-548, 2010.

[24] K. Höne and J.H.P. Eloff, "What makes an effective information security policy?," *Network Security*, vol. 6, pp. 14-16, 2002.

[25] M. Siponen, "Information security standards focus on the existence of process, not its content," *Communications of the ACM*, vol. 49, no. 8, pp. 97-100, 2006.

[26] M. Siponen and R. Willison, "Information security management standards: Problems and solutions," *Information & Management*, vol. 46, pp. 267-270, 2009.

[27] M.E. Whitman, A. Towsend and R. Aalberts, "Information systems security and the need for policy," in: G. Dhillon, editor. *Information security management: Global challenges in the new millennium*, Idea Group Publishing, 2001.

[28] M.E. Palmer, C. Robinson, J.C. Patilla and E.P. Moser, "Information security policy framework: Best practices for security policy in the e-commerce age," *Information Systems Security,* vol. 10, no. 2, pp. 1-15, 2001.

[29] R. Baskerville and M. Siponen, "An information security meta-policy for emergent organizations," *Logistics Information Management,* vol. 15, no. 5/6, pp. 337-346, 2002.

[30] G. Dhillon, Managing information systems security, London: Macmillan Press, 1997.

[31] K. Peffers and T. Ya, "Identifying and evaluating the universe of outlets for information systems research: Ranking the journals," *Journal of Information Technology Theory and Application,* vol. 5, no. 1, 2003.

[32] R.K.Jr. Rainer and M.D. Miller, "Examining differences across journal rankings," *Communications of the ACM,* vol. 48, no. 2, pp. 91-94, 2005.

[33] A. Lin and R. Brown, "The application of security policy to role-based access control and the common data security architecture," *Computer Communications,* vol. 23, pp. 1584-1593, 2000.

[34] W. Itani and A. Kayssi, "SPECSA: A scalable, policy-driven, extensible, and customizable security architecture for wireless enterprise applications," *Computer Communications,* vol. 27, pp. 1825-1839, 2004.

[35] S.M. Foley and W.M. Fitzgerald, "Management of security policy configuration using a semantic threat graph approach," *Journal of Computer Security,* vol. 19, pp. 567-605, 2011.

[36] L. Karadsheh, "Applying security policies and service level agreement to IaaS service model to enhance security and transition," *Computers & Security,* pp. 315-326, 2012.

[37] D. Unal and M.U. Caglayan, "A formal role-based access control model for security policies in multi-domain mobile networks," *Computer Networks,* vol. 57, no. 1, pp. 330-350, 2013.

[38] K.J. Knapp, R.F.Jr. Morris, T.E. Marshall and T.A. Byrd, "Information security policy: An organizational-level process model," *Computers & Security,* vol. 28, pp. 493-508, 2009.

[39] J. Backhouse, C.W. Hsu and L. Silva, "Circuits of power in creating de jure standards: Shaping an international information systems security standard," *MIS Quarterly,* vol. 30, pp. 413-438, 2006.

[40] E. Humphreys, "Information security management standards: Compliance, governance and risk management," *Information Security Technical Report,* vol. 13, pp. 247-255, 2008.

[41] J. Rees, S. Bandyopadhyay and E.H. Spafford, "PFIRES: A policy framework for information security," *Communications of the ACM,* vol. 46, no. 7, pp. 101-106, 2003.

[42] V. Anand, J. Saniie and E. Oruklu, "Security policy management process within six sigma framework," *Journal of Information Security,* vol. 3, pp. 49-58, 2012.

[43] A.W. Kadam, "Information security policy development and implementation," *Information Systems Security,* vol. 16, pp. 246-256, 2007.

[44] A. Ruighaver, S. Maynard and S. Chang, "Organisational security culture: Extending the end-user perspective," *Computers & Security,* vol. 26, pp. 56-62, 2007.

[45] K.-L. Thomson, R. von Solms and L. Louw, "Cultivating an organizational information security culture," *Computer Fraud & Security,* pp. 7-11, 2006.

[46] T. Kayworth and D. Whitten, "Effective information security requires a balance of social and technology factors," *MIS Quarterly Executive,* vol. 9, no. 3, pp. 163-175, 2010.

[47] G.V. Post and A. Kagan, "Evaluating information security tradeoffs: Restricting access can interfere with user tasks," *Computers & Security,* vol. 26, pp. 229-237, 2007.

