Information Security Policy Development and Implementation: A content analysis approach

Conference Paper · July 2014

CITATIONS
20

READS
4,744

1 author:

Stephen Flowerday
Rhodes University
124 PUBLICATIONS **1,471** CITATIONS

SEE PROFILE

Information Security Policy Development and Implementation: A Content Analysis Approach

T. Tuyikeze[1] and S. Flowerday[2]

[1]Walter Sisulu University, East London, South Africa
[2]University of Fort Hare, East London, South Africa
e-mail : ttuyikeze@wsu.ac.za; sflowerday@ufh.ac.za

Abstract

The literature clearly agrees that the major threat to an organization's information security is caused by careless insider employees who intentionally or unintentionally misuse the organization's information assets (Bulgurcu *et al.,* 2010). This paper posits that one important mechanism to encounter insider threats is through the development of an effective information security policy. The research question posed by this paper is what processes organizations should follow in developing an effective information security policy. In order to answer this question, the paper follows the steps of the content analysis research technique. The primary objective of this paper is to define a model for the formulation, implementation and enforcement of an information security policy in an organization. A content analysis on current information security policy development and implementation methods is conducted from secondary sources in order to obtain a deep understanding of the processes that are critical to the information security policy development life cycle. The proposed model provides the various steps required in the development, implementation and evaluation of an effective information security policy.

Keywords

Information security policy, information security policy development and implementation, content analysis research technique

1. Introduction

Organizations are enormously dependent on Information Technology (IT) as it supports day-to-day transactions and many critical business functions. IT stores confidential information such as organizations' financial records, medical records, job performance reviews, trade secrets, new product developments and marketing strategies, which all must be protected to ensure organization survival. However, this dependency has unfortunately resulted in an increase of potential threats to the organization's information (Edwards, 2011). The literature review indicates that both intentional and unintentional insider threats are considered as one of the top ranked threats to information security over the past decade (Richardson, 2009). The Cybersecurity Watch Survey (2011) found that the damage caused by insider (employees or contractors with authorized access) attacks was bigger than outsiders (those without authorized access to network systems and data). The most common insider e-crimes were: unauthorized access to corporate information (63%);

unintentional exposure of private or sensitive data (57%); virus, worms, or other malicious code (37%); theft of intellectual property (32%).

This paper argues that one important mechanism to encounter the insider threats is through the formulation, implementation and enforcement of effective information security policies. According to Bacik (2008), information security policy architecture is a set of documents, comprising policies, guidelines, standards, procedures, and memorandums that collectively contributes to the protection of organizational assets. The remainder of this paper is organized as follows: In the next section, a discussion of the challenges pertaining to information security development is provided. Section 3 and its sub-sections explore the steps of the content analysis research technique and how they have been applied in this research paper in order to answer the research question. Finally, section 4 concludes the paper.

2. Challenges in developing effective information security policy

Maynard and Ruighaver (2006) argue that the major potential problem in the current security policy development practice is attributed to the lack of guidance as to how to develop security policy contents. We found no evidence that shows step-by-step processes of developing and implementing an information security policy. The literature concentrates on the description of the structure and the content of the security policy, but in general, fails to describe the processes used to generate the output of the information security policy. Due to the lack of the security policy development guidance, security policy developers often use commercially available sources or templates available from the internet in order to develop their policies (Karin and Eloff, 2004). The resulting policy document will, however, not give proper direction for information security protection. In this case, the policy statements developed may not be directly attributed to the risks they are designed to nullify; therefore, they do not combat the security threats that the specific organization is facing.

Furthermore, Tuyikeze and Flowerday (2013) compared a sample of existing security policy development methods. Their finding revealed basic steps for the development of a security policy document. It also showed some similarities where there is an agreement on the same steps, while also showing differences on the importance of the steps to be followed. Having noticed that there is a gap in the current security policy development methods; and that the literature does not offer comprehensive methodology or mechanisms that show in detail the processes of developing an information security policy, a more pragmatic strategy becomes a necessity. A content analysis of security policy development is conducted from secondary sources in order to uncover the processes necessary for the formulation, implementation and application of an effective information security policy.

3. A content analysis of information security policy development

This paper uses a content analysis research technique to find the solution of the questions raised in this paper. Krippendorff (2004) defines content analysis as: “a

research technique for making replicable and valid inferences from text to their context of use, with the purpose of providing knowledge, new insights, a representation of facts and a practical guide to action". Having mentioned that content analysis is a research technique, it must follow a well-structured process to ensure reliability and validity (Du Preez, 2010). Krippendorff (2004) highlights six steps that should be followed while conducting a content analysis. These are: *Unitizing, Sampling, Coding, Reducing, Inferring and Narrating*. Each of the six steps of the content analysis is discussed on how it has been applied in this research paper.

3.1. Unitizing

The process of content analysis begins with the creation of a scheme of categories composed of the various analysis units (Elo and Kyngas, 2007). A unit of analysis can be a word, sentence, or portion of words (Elo and Kyngas, 2007). 'Unitizing' refers to a systematic approach for distinguishing segments of texts that are of interest to a content analysis (Krippendorff, 2004). For the nature of this study, a search string like: "information security policy", "security policy development", "security policy implementation" and "security policy formulation" was used to gather information regarding the security policy development methods from the literature.

3.2. Sampling

Krippendorff (2004) highlights that sampling enables the content analyst to save on the research efforts by cutting observations to a manageable subset of units that are statistically or conceptually representative of the whole population. A combination of various publications sources was utilized in order to answer the question posed in this research paper. A total number of 21 documents were chosen for the sample of this paper. These documents constitute the top cited papers on Google. The category of these samples varies from journal article papers, conference proceedings papers, industry policy publications and industry policy reports. During the selection of the sample, the reputation of the author, depending for example on the number of people who cited the article, was taken into account. Secondly, the reputation of the journal or the conference was considered. More importantly, the publications that provided relevant contents directly related to the research topic under study were highly selected. This entails an extensive analysis of the literature review. After the process of selecting the sample has been established, the coding process commences.

3.3. Coding

Coding entails the process of converting texts from the sample into analysable units (Krippendorff, 2004). In order to avoid human errors, the coding step was conducted by the use of the MAXQDA software package. The twenty one sample documents were imported into the MAXQDA. Each document was individually coded by highlighting the sentence or the paragraph that mentions the process of developing security policy. On completion of the coding process, a total number of 36 codes

emerged and 552 accumulative codes. There was a variation of the codes from general to specific. General code was for example security policy construction, while the specific ones were draft the policy, write policy and write policy procedure. The general codes are grouped under one category in the next stage referred as the reducing step.

3.4. Reducing

The main objective of reducing is to decrease the number of codes into categories that can be easily interpreted (Du Preez, 2010). Most of the codes that have high frequency of occurrence were related to the process of constructing the policy, management support and information security policy compliance and enforcement. The 36 codes that emerged during the coding process were reduced to 10 categories. For example, the codes labelled "identification of vulnerabilities", "identification of threats" and "identification of assets to be protected" were grouped under one category named 'risk assessment' as they are all part of evaluating the security risk processes.

Category label	Number of tags	Cumulative tags
1. Information security policy construction	85	85
2. Management support	78	163
3.Information security policy compliance and enforcement	72	235
4. Information security policy implementation	68	303
5. Risk assessment	63	366
6. Information security policy monitoring, review and assessment	54	420
7. Employee support	51	471
8. International security standards	32	503
9. Information security policy stakeholders	28	531
10. Law and regulation requirements	21	552

Table 1: List of categories identified

In the next section, the last 2 steps of the content analysis are discussed.

3.5. Inferring and Narrating

In order to answer the research question posed in this paper, the 10 categories were analyzed and interpreted so that a model for information security policy development can be inferred from these categories.

3.5.1. Risk assessment

The literature provides different activities that need to be carried out during the risk assessment process. First, the assets that the organization needs to protect must be identified (Kadam, 2007). Secondly, a list of all the threats that can cause harm to the organization's assets is identified. Thirdly, the likelihood of threats exercising system

vulnerability is determined. Information can have multiple vulnerabilities, for instance terminated employees' system identifiers (ID) that were not removed from the system (NIST, 2012). Fourth, the threats and vulnerabilities which cause a security failure and the associated impacts are assessed in terms of the organization's loss of integrity, availability and confidentiality. The risk assessment helps to make decision on which risks the organization is willing to accept and the ones it must mitigate. Lastly, the controls that must be implemented in order to mitigate the risks are identified (NIST, 2012). For example, an information security policy should be chosen as the main control to mitigate the risk of insider employees who negligently put the organization's information assets at risk. Once the risk assessment process is accomplished, the information security policy construction process begins.

3.5.2. Information security policy construction

One of the categories that emerged during the coding process with the highest number of codes is the writing of the security policy. Since the chosen sample deals with the information security policy development, it is not surprising that there was an enormous number of codes. The following constitute the activities of constructing a security policy: Executive management provides *high level security policy* that contains directives. These directives give a sense of the company's overall security policy philosophy (Diver, 2007). The high level information security policies emanating from the executive management are transformed into *organizational standards and guidelines* (Von Solms *et al.,* 2011). Organizational standards are detailed statements of what should be done to comply with the policy (Grobler and Von Solms, 2004), but not how to do it (Mauritian Computer Emergency Team, 2011). Lastly, the detailed information security policies are supported by lower level security policies also called procedures (Von Solms *et al.,* 2011). Procedures provide the step-by-step detailed instructions on how to carry out the requirements of an information security policy (Diver, 2007). Once the information security policy construction is complete, the next stage deals with its implementation across all levels of the organization.

3.5.3. Information security policy implementation

After the creation of the security policy is complete, the most difficult part of the policy development process is rolling it out to the organization (Kadam, 2007). The introduction of a new information security policy brings changes in the way employees behave in handling the organization's information. The whole idea is to gain support from the organization's community to accept the new changes. This can be achieved by educating and training employees on the new information security policy requirements. The objective of the information security awareness is to make sure that all stakeholders are aware and understand their responsibilities towards the security policy requirements (Talbot and Woodward, 2009). In order to reach such an audience, different business communication (notices, intranet, posters, newsletters, etc.) should be used to promote security policy awareness. Information security researchers agree that the Security Education, Training and Awareness (SETA) program are three important pillars that are crucial to control the information security

misuse (D'Arcy *et al.,* 2009). D'Arcy *et al.* (2009) states that "SETA program extends beyond just "awareness of security policy and often includes on-going efforts to (1) convey knowledge about information risks in the organizational environment, (2) emphasize recent actions against employees for security policy violations, and (3) raise employee's awareness of their responsibilities regarding organizational information resources". Once the information security policy has been implemented in the organization and all employees have been trained and educated on the new information security policy requirements, it is crucial to put mechanisms in place that ensure the compliance and enforcement of the new information security policy.

3.5.4. Information security policy compliance and enforcement

A number of theories have been developed underlying employees' behavioural intention towards the compliance of information security policies. Within the chosen sample, Bulgurcu *et al. (*2010) argue that the General Deterrence Theory (GDT) and Theory of Planned Behaviour (TPB) are examples of theories that ensure information security policy compliance. GDT predicts that the increase in the severity of punishment on those who violate the rules of the organization reduce some criminal acts (Blumstein *et al.,* 1978). A study conducted by Siponen *et al.* (2010) found that the use of sanctions is a good approach to encounter the employees who violate information security policy and consequently reduce the computer abuse. Based on the TPB, Bulgurcu *et al.* (2010) posit that an employee's intention to comply with the organization's security policy is influenced by *normative norms*, *perceived behavioural control* and *attitude* toward compliance. The theory explains the intention of an individual to perform a given behaviour (Fishbein and Ajzen, 1975). Normative beliefs reflect normative expectations of peers or colleagues (Fishbein and Ajzen, 1975). These constitute the social pressures from the employees' managers, information security policy development team and colleagues.

3.5.5. Information security policy monitoring, review and assessment

The need to periodically or non-periodically review and update the security policy is indispensable to the organization (Talbot and Woodward, 2009). Hong (2006) suggests that the information security policy should be evaluated and reviewed on regular basis to make sure that the latest threats, new regulations and government policies are kept up to date. To facilitate the security policy review and maintenance, Talbot and Woodward (2009) advise the use of an automated system of review scheduling which timely alerts when a major change to the existing security practices have occurred. Importantly, the security violations, deviations, and audit information should also be reviewed (Diver, 2007) as the result of this process help to identify the area where the policy was not enforced or where frequent policy deviations occurred.

3.5.6. Management support

Bayuk (2009) argues that the first step in composing a security policy is to get the top management's opinions on how they understand security in the organization.

"The implementation of security policy must start from the executive management" (Bayuk, 2009). Johnson and Merkow (2010) posit that: "without executive support, policies are just words. To have meaning, they must be given the right priority and be enforced". Indeed, top management is important in enforcing information security policy so that employees can take the policy requirements seriously. Furthermore, management plays key role in approving the policy and making sure that there is enough budget to cover all resources required.

3.5.7. Employee support

Employee support consists of end-users who carry out different activities in an organization. Maynard *et al.* (2011) suggest that the end-user community needs to be part of the development effort to ensure that the multidisciplinary nature of the organization is incorporated in the information security policy development process. Diver (2007) recommends that the end-users must be involved earlier in the policy development so that they can identify errors and difficulties and correct them before the security policy deployment. "If the policy documents are hard to understand, users may not read them fully or may fail to understand them correctly" (Diver, 2007). In order to have an effective information security policy, everyone in the organization must practice them. If employees practice the information security policy requirements day-to-day, it helps to create a security culture that protects the organization's information.

3.5.8. International security standards

Diver (2007) and Hong *et al* (2006) agree that international standards such as ISO 27002 are good starting point to implement the information security policy which therefore improves an organization's information security. In addition, Bayuk (2009) supports the idea of using international standards as a baseline framework because they increase trust with the organization's stakeholders. Bayuk (2009) states "…this is a reasonable approach as it helps to ensure that that the policy will be accepted as adequate not only by company management, but also by external auditors and others who may have a stake in the organization's information security program". Undoubtedly, an international security standard that has been approved by security experts can definitely provide the basis requirements to start developing an information security policy.

3.5.9. Regulations requirements

The main reason to develop information security policy is to mitigate the various security risks that organizations face. One of the risks that organizations face is the increasing legal requirements (Doherty *et al*., 2009). Edwards (2011) argues that organizations must first identify and understand all regulatory requirements that dictate the creation of such policies before writing the information security policy. Avolio and Scott (2007) suggest that information security policy developers should familiarize themselves with penalties of non-compliance with laws, as this will aid the organizations to prioritize their policies and implement the proper level of

discipline to employees who violate the policies. Therefore, it is necessary that organizations obtain legal advice to ensure that their policies are legally binding (Maynard *et al.*, 2011) and the employees violating such policies will be legally liable of their behaviour.

3.5.10. Information security policy stakeholders

The development of an effective security policy requires a combination of different skills emanating from different stakeholders experiences (Diver, 2007). Maynard *et al.* (2011) recommend the involvement of ICT Specialists and security specialists in the policy development process because they have technical knowledge of the systems that the information security policy intends to protect as well as the security of these systems. Diver (2007) posits that the human resource department should review and/or approve the security policy based on how the policy relates to organization's existing policies. This is necessary to make sure that there is a consistency between the organization's security policies with the standard organizational practices (Maynard *et al.*, 2011). The inclusion of multiple stakeholders is crucial to the organization because it gives the whole organization a sense of security policy ownership and facilitates the security policy acceptance and adoption. The next section discusses the model construction.

4. Model construction

Based on the analysis and interpretation of the ten categories discussed, different dimensions of the model are proposed. The first dimension is the security policy development as it encompasses the processes needed to develop an information security policy such as risk assessment, policy construction, policy implementation, policy compliance and policy monitoring, assessment and review. The second dimension is the security policy drivers as it is composed of threats that put the organization under pressure to have mechanisms to protect their information. The third dimension is the security policy guidance because it is constituted by security standards that guide organizations in constructing an information security policy. The fourth dimension is concerned with the support of the policy. Management, employees and stakeholders need to support the security policy in order for it to survive and attain its objectives. Lastly, the organization needs to use existing theories to understand the employees' behavioral intention with regard to information security policy compliance. These dimensions are shown in the proposed model in Figure 1.

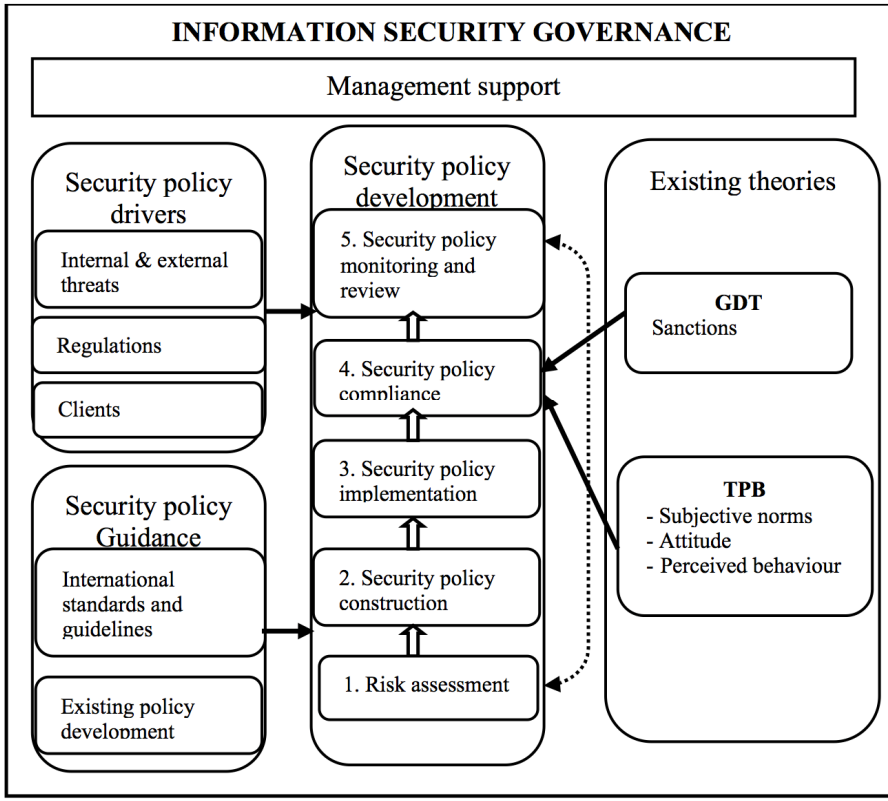

Figure 1: Information security policy development model

The different components that are shown in Figure 1 are considered to be the main pillars of the information security policy development processes.

5. Conclusion

The research question posed by this paper is what processes organizations need to follow in developing and implementing an effective information policy. The list of the ten categories that emerged during the reducing stage of the content analysis was analysed and interpreted so that a model for information security policy development could be inferred from the emerged ten categories. The proposed model provides the different dimensions that a specific organization needs to take into account during the information security policy development and implementation process. It ensures both comprehensive and sustainable information security policies.

6. References

Avolio, M. and Scott, P. (2007). "Producing your network security policy". *WatchGuard Technologies, Inc.*

Bacik, S. (2008). Buildling an Effective Information Security Policy Architecture . *Boca Raton: CRC Press*.

Bayuk, J. (2009). "How to Write an Information Security Policy". *Computerworld*.

Bulgurcu, B., Cavusoglu, H. and Benbasat, I. (2010). "Information Security Policy Compliance: An empirical study of rationality-based beliefs and information security awareness". *MIS Quarterly,* 34(3), pp. 523-548.

Cybersecurity Watch Survey. (2011). "Organizations Need More Skilled Cyber Professionals to Stay Secure". *CSO Magazine*.

D'Arcy, J., Hovav, A. and Galletta, D. (2009). "User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach". *Information Systems Research,* 20(1), pp. 79-98.

Diver, S. (2007). "Information Security Policy – A Development Guide for Large and Small Companies". *SANS Institute*. South Africa.

DuPreez, R. (2010). "A model for green IT strategy: a content analysis approach". *Nelson Mandela Metropolitan University:* Port Elizabeth, South Africa.

Fishbein, M. and Ajzen, I. (1975). "Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research": MA, Addison-Wesley.

Kadam, A. W. (2007). "Information Security Policy Development and Implementation". *Information Systems Security,* 16(5), pp. 246-256.

Krippendorff, K. (2004). "Content analysis: an introduction to its methodology" (2nd ed.). Sage Publications, Inc.

Mauritian Computer Emergency Team. (2011). "Guidelines on Information Security Policy". *Mauritius: National Computer Board*. CMSGu2011-04.

Maynard, S., Ruighaver, A. and Ahmad, A. (2011). "Stakeholders in security policy development". *Proceedings of the 9th Australian Information Security Management Conference*. Perth Western, Australia.

Richardson, R. (2009). "CSI Computer Crime & Security Survey". *Computer Security Institute*.

Talbot, S. and Woodward, A. (2009). "Improving an organisations existing information technology policy to increase security". *Proceedings of the 7th Australian Information Security Management Conference*. Perth, Western Australia.

Tuyikeze, T. and Flowerday, S. (2013). "Information Security Policy Maturity Model (ISPMM) ". *Joint International Conference on Engineering Education and Research and International Conference on Information Technology*. Cape Town, South Africa.

Von Solms, R., Thomson, K.-L. and Maninjwa, M. (2011). "Information security governance control through comprehensive policy architectures". *ISSA*. Johannesburg, South Africa.