Information security governance control through comprehensive policy architectures

Rossouw Von Solms
Director: Institute of ICT Advancement
NMMU
Port Elizabeth, South Africa
rossouw.vonsolms@nmmu.ac.za

Kerry-Lynn Thomson
Institute of ICT Advancement
NMMU
Port Elizabeth, South Africa
kerry-lynn@nmmu.ac.za

Prosecutor Mvikeli Maninjwa
Institute of ICT Advancement
NMMU
Port Elizabeth, South Africa
s20514610@live.nmmu.ac.za

Abstract— **Information Security Governance has become one of the key focus areas of strategic management due to its importance in the overall protection of the organization's information assets. A properly implemented Information Security Governance framework should ideally facilitate the implementation of (directing), and compliance to (control), Strategic level management directives. These Strategic level management directives are normally interpreted, disseminated and implemented by means of a series of information security related policies. These policies should ideally be disseminated and implemented from the Strategic management level, through the Tactical level to the Operational level where eventual execution takes place. Control is normally exercised by capturing data at the lowest levels of execution and measuring compliance against the Operational level policies. Through statistical and summarized analyses of the Operational level data into higher levels of extraction, compliance at the Tactical and Strategic levels can be facilitated. This scenario of directing and controlling defines the basis of sound Information Security Governance. Unfortunately, information security policies are normally not disseminated onto the Operational level. As a result, proper controlling is difficult and therefore compliance measurement against all information security policies might be problematic. The objective of this paper is to argue towards a more complete information security policy architecture that will facilitate complete control, and therefore compliance, to ensure sound Information Security Governance.**

Keywords*-Information security governance; direct-control; policy architecture; information security policies.*

I. INTRODUCTION

In today's business world, information is one of the most important assets in most organizations. It has been noted as one of the three most valuable assets in most organizations, namely: people, physical property and information [1, p. 83]. Information is no longer only used as a business enabler, but also to gain a competitive advantage [2]. Therefore, information security is of extreme importance as it helps reduce information risks, ensures business continuity, and maximizes return on investments and business opportunities [3]. If this information is compromised, an organization may not only lose its competitive advantage, but its very existence. This is due to the fact that information has the potential to damage an organization if it is inaccurate and error prone, in the wrong hands or unavailable when needed [4, p.1]. Therefore, information must be protected, through a process generally called information security.

As information, and the related information and communication technologies, is critically important to the wellbeing and success of an organization, it is imperative that the practice of information security is properly mandated and instructed from the highest to the lowest levels. Executive management, at the Strategic management level, should ideally issue directives as to how this critical asset should be protected. These Strategic level directives should ideally be interpreted and expressed in related information security policies to dictate to lower levels of management how the process of information security should be interpreted and implemented. The relationship between the directives and subsequent policies are usually represented in a structure called the information security policy architecture [5, pp. 21-30].

Governance in general, and therefore also Information Security Governance, normally comprises of processes called directing and controlling. Directing refers to the process of stating what is to be expected or accomplished, usually documented in the form of policies. On the other hand, controlling refers to the process of determining whether the individual policies have been complied with. This also is generally referred to as compliance checking [2].

The objective of this paper is twofold, firstly; to determine whether general information security policy architectures are adequate to facilitate proper controlling and therefore compliance checking. Secondly, if general information security policy architectures are found to be not suitable for proper controlling purposes, determine what should ideally be done to make this possible.

The rest of the paper is structured as follows. In the next section, governance in general will be discussed with the emphasis finally in Information Security Governance. This will be followed by a more detailed discussion on the governance aspects related to information security. The directing and controlling aspects, related to Information Security Governance, will be discussed in detail followed by some discussion of what would constitute a good Information

Security Governance environment. Finally, an 'ideal' information security policy architecture will be proposed.

II. INFORMATION SECURITY GOVERNANCE

As information technology is so fundamental in the daily activities of an organization, it is important for the information technology infrastructure to be governed properly. The Institute of Directors Report [6] on Corporate Governance emphasizes the value of good Information Technology (IT) Governance. It emphasizes that IT Governance should focus on strategic alignment, value delivery, risk management, and resource management. According to the IT Governance Institute [7], IT Governance consists of the leadership, organizational structures and processes that ensure that the organization's information technology sustains and extends the organization's strategies and objectives. Furthermore, IT Governance should result in the amalgamation of good practices to ensure that the organization's information technology supports the business objectives, maximizes benefits and opportunities, and helps in gaining competitive advantage [7].

The information technology infrastructure is used to process, store and transmit information. As already noted, information is a particularly significant asset to most organizations. It is often described as the core of the electronic economy and is vital for the successful operation of most organizations. It has also been noted that information is no longer only used as a business enabler, but also to gain a competitive advantage [2]. Therefore, information assets should be protected using good Information Security Governance practices.

Information Security Governance should promote good information security practices through clear direction and should provide organizations with an understanding of what is necessary for a comprehensive information security plan. This information security plan should also reflect the organization's needs and risk appetite [8].

Comprehensive Information Security Governance practices should include strategic direction for information security and activities that ensure that executive management directives are implemented and compliance to them is monitored [2].

III. GOVERNANCE OF INFORMATION SECURITY

As stated previously, governance generally comprises two main processes, namely, directing and controlling. Information Security Governance practices should facilitate this through strategic direction for information security and activities to ensure these strategic directives are implemented and extensive monitoring activities to ensure proper control should be introduced. This section briefly discusses this concept of directing and controlling further, with emphasis on the three management levels that exist in an organization, namely: Strategic, Tactical, and Operational.

Directing occurs when executive management gives directives as to what needs to be done in order to achieve the organization's information security objectives. Controlling occurs when compliance checking is undertaken to confirm whether executive management directives are being adhered to. Both directing and controlling should occur at all the management levels, namely: Strategic, Tactical and Operational. At the Strategic level, executive management should indicate the importance of information assets to an organization through the development of a set of directives outlining the objectives to protect the information assets. At the Tactical level, the directives from the Strategic level should be used to create policies and organizational standards and guidelines. These policies should then translate into lower-level policies at the Operational level. The output from the policies at the Operational level forms the basis of execution of these directives on the lowest level, as shown in Figure 1.

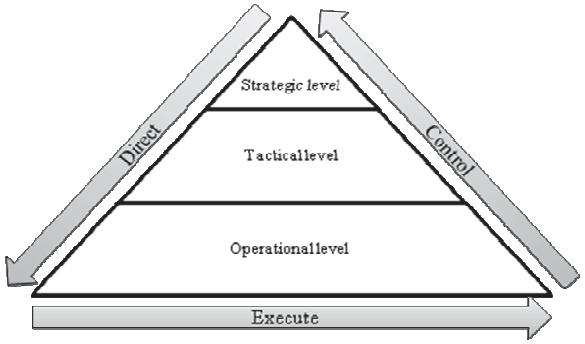

Figure 1: Information security governance model [2]

As can be seen in figure 1, directing should start at the Strategic level, and continue through the Tactical level, to the Operational level. In the direct process, the executive level directions are disseminated and cascaded into lower-level information security policies. Controlling captures the operational data from the lowest execution layer to assist in reporting to the Tactical level and subsequently to the Strategic level.

If Information Security Governance practices are applied effectively, it should be possible to trace executive management directives from the Strategic, through the Tactical, onto the Operational level. Further, control or compliance checking should begin with the operational data captured at the lowest execution layer, through the Operational level, the Tactical level, to the Strategic level. It can be argued that it is only when directing and controlling are done at all management levels that an organization can truly claim compliance to Information Security Governance [2].

Therefore, as seen in this section, the proper governance of information security, to a large extent, is dependent on the strategic directives of executive management for the protection of information assets. These directives should then be disseminated through the related information security policies at both the Tactical and Operational levels. Data at the execution layer, below the Operational level, should be captured and used for control purposes to ensure compliance to the information security policies at the Operational level, Tactical level, and eventually executive management's strategic direction.

IV. DIRECTING INFORMATION SECURITY

The importance of executive management recognizing the significance of, and giving directives for information security can never be overemphasized. These directives are normally based on a number of factors, including the strategic vision of the organization, legal and regulatory prescriptions, the role of IT and its alignment with the organization's strategy, and competitiveness [2].

Executive management directives are normally 'expanded' into a Corporate Information Security Policy (CISP). This kind of a policy is also sometimes referred to as the Enterprise Information Security Policy (EISP), an information security program policy, a general security policy, an IT security policy, a high-level information security policy, or more simply an information security policy [9, p. 113]. For the purpose of this paper, these types of policies will be referred to as Strategic level policies. These policies are normally the highest-level of information security policies, and, together with management directives, reside at the Strategic management level. They form a basis for all related lower-level, more detailed policies related to information security [10, p. 64].

As explained in the previous paragraph, the Strategic level policies are normally expanded or disseminated into a series of information security policies, providing more detail at every lower level. Some refer to these policies as issue-specific policies. These kinds of policies provide detailed instructions in the use of the organization's processes, technologies, or systems [9, p. 118]. A few examples of aspects in these policies include Internet usage, email usage, incident response, disaster/business continuity planning, viruses and worms, hacking, home use of organization's computer equipment, use of personal equipment on organization's network, use of telephones, fax, photocopying equipment, etc. [9, p. 119]. For the purpose of this paper, these policies will be referred to as Tactical level policies as they normally reside at the Tactical management level. This is where organizational policies will normally end.

These Strategic and Tactical level policies are normally organized in an Information Security Policy Architecture (ISPA). An ISPA is a representation of all the information security related policies in a hierarchical format. This helps an organization to be acquainted with all the information security policies it has in use, as well as how they are related to one another [5, pp. 21-30].

However, during the course of this study, it has been noted that there could exist a problem of policy documentation not being extended further down into the Operational level policy documentation targeted to the technical audience or personnel. A thorough literature survey has confirmed that an extremely large portion of research has mainly focused on information security policies and related documentation targeted to either the general end-users or management. Less emphasis has been given to the Operational level policy documentation targeted to the technical audience. The following is a list of the main sources of information security policy documentation literature that do not take the technical audience into account [3]; [19-32].

Therefore, it can be argued that in most cases in literature, and therefore organizational practices, the ISPA does not extend to policies that logically reside at the Operational level. This does not necessarily mean these kinds of policies do not exist in organizations. It could be they are just managed in isolation to the rest of the organization's information security policies since they are not included in the ISPA.

Policies at the Tactical level are usually supported by associated Procedures or even organizational Standards [9, p. 111]. However, Operational level policies might also be supported by their own associated Procedures and/or organizational Standards. Thus, Procedures and Standards or Guidelines from the Tactical level are not the only documentation supposed to reside at the Operational level, but should coexist with the actual Operational level policies, together with their Procedures, Guidelines and Standards. Therefore, it can be claimed that there is indeed a 'break' or 'gap' in the direct process, as depicted in figure 2.

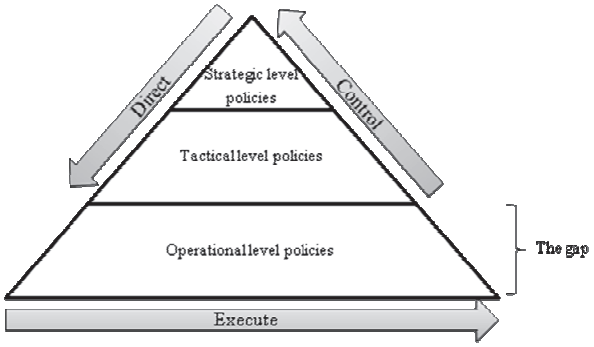

Figure 2: Operation level policies not included in organization's policy architectures

In the next section, information security related policies or directives at the Operational level, that are seemingly excluded from most ISPAs and therefore unrelated to the Tactical level policies, will be discussed.

V. OPERATIONAL LEVEL POLICIES

In an organization, information security policies are targeted to different audiences, namely: management, end-users, and technical personnel [11]. Certain Operational level policies (or Operational directives) are targeted to both end-users and technical personnel active at the Operational level. However, the Operational level policies this paper is focusing on are those that are primarily targeted to the technical personnel.

There are different terminologies used to refer to these Operational level policies, namely: system-specific policies [9, p. 124], technical controls [9, p. 125], low-level policies [12], application-specific policies [13, pp. 97-99], and may easily be confused with configurations and tunings [12]. These Operational level policies are most of the times differently planned or structured than the higher level policies. They often function as a documentation of technical standards or settings

to be used when configuring or maintaining systems, for example, to configure and tune a network firewall.

This paper will focus on two typical broad categories of these Operational level policies. The first category is access control, which covers the low-level settings for controlling logical access to organizational systems. The second category is computer networking, which covers the network settings to ensure a secure and reliable network. The configuration settings for the following might typically be found in such low-level policies; aspects on remote access, VPN (virtual private network), ACLs (access control lists), RBAC (role-based access control), DAC (discretionary access control), MAC (mandatory access control), firewall security, and routing [14]; [15]; [16]; [11]. Thus, it is clear that low-level security configurations and setting are indeed recorded in low-level policies that can typically be positioned at the Operational management level.

Whitman and Mattord [9, p. 124] stated that the Information Security Policy Architecture (ISPA) should ideally tie together all information security related policies, from the Corporate Information Security Policy (CISP) right down to the lowest level technical or operational information security policies. Thus, the Operational level policies should ideally be motivated and directed by higher-level policies. This means that these Operational level policies should technically dictate what is directed in the higher-level policies, and they should be included in the ISPA.

However, traditionally, organizations have adopted a bottom-up approach in the creation of these low-level policies. In this approach, the technical staff would initiate the process of information security configuration and settings at the technical level and then propagate their findings upward to management as proposed policy recommendations. As a result of this bottom-up approach followed at the Operational level, these policies might not be tightly linked to the Tactical level policies and therefore not necessarily contribute directly to the directives stemming from the higher-level policies [17]. This principle is graphically presented in figure 3.

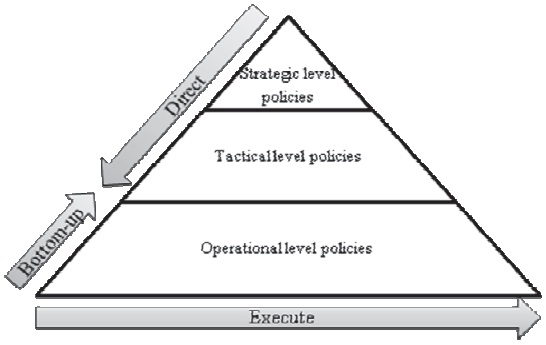

Figure 3: The traditional bottom-up approach to the creation of Operational level policies

When tightly aligned with Tactical and Strategic level policies, these Operational level policies could greatly aid in capturing and implementing the original executive level directives. Further, they can be used for controlling purposes. This would further enhance compliance measurement, as compliance would be measured from the Operational level to the Tactical level, and then to the Strategic level. Ultimately, this would enhance Information Security Governance. This aspect of controlling is further discussed in the following section.

VI. CONTROLLING INFORMATION SECURITY

As highlighted previously, the relationship between the functions of directing and controlling is cyclic by nature and is often referred to as the Direct-Control Cycle [2]. Directing is the process of stating what is expected through policies and controlling is the process of verifying that the policies are being complied with. In order to effectively control, it is necessary to capture data to test for compliance with the policies which were drafted and implemented through directing. At the Operational level, this data could be extracted from, for example, log files of operating systems, databases and firewalls [2].

When measuring compliance, it is important for an organization to do so in a comprehensive manner. Compliance measurement should start from the Operational level. At the Operational level, all policy related activities should be captured and stored as compliance measurement data. After the measurement data has been extracted from the Operational level, compliance to the Operational level policies should be measured, and information security reports should be distributed to the Tactical level. At the Tactical level, further compliance to the related Tactical level policies should be measured. As a result, reports on compliance and conformance to the Strategic level policies should be more accurate as they reflect the data from all three management levels [18]. This 'flow' of control from the Operational level to the Strategic level is graphically represented in Figure 4.

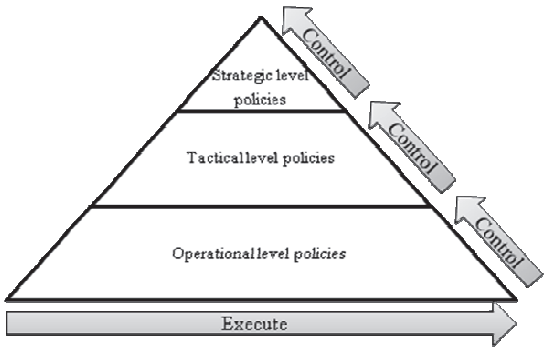

Figure 4: Control at all management levels

Therefore, comprehensive and complete control, from an Information Security Governance point of view, should ideally begin with data from the Operational level, where compliance is checked against Operational level policies, to the Tactical level, where compliance is checked against Tactical level policies, and then to the Strategic level, where compliance is checked against Strategic level policies and directives.

VII. THE 'IDEAL' INFORMATION SECURITY GOVERNANCE ENVIRONMENT: A COMPREHENSIVE INFORMATION SECURITY POLICY ARCHITECTURE

Comprehensive Information Security Governance is, to a large extent, dependent on the comprehensiveness of the organization's Information Security Policy Architecture (ISPA). Directing and controlling functions should be achieved through the information security related policies at all levels. Ideally, directing functions should be evident from the Strategic level, through Strategic level directives and policies, to the Tactical level, through Tactical level policies, and then to the Operational level through Operational level policies.

To enable this 'ideal' Information Security Governance environment, it is necessary that the directing arrow, represented in the figures, does not stop at the Tactical level, but continues through to the Operational level. The Tactical level polices should be derived from the Strategic level policies and directives. Further, the policies at the Operational level should be derived from the policies at the Tactical level. In an ideal ISPA, this would then ensure that the direct arrow continues unbroken from the Strategic level to the Operational level. This, in turn, would allow for an unbroken control arrow to extend from the Operational level, and the data collected there, to the Strategic level.

It is of extreme importance that the Operational level policies are developed from the Tactical level policies, rather than the traditional bottom-up approach. Further, it is important that these policies are included in the organization's ISPA. Managed this way, Operational level policies can benefit Information Security Governance control, as control would be measured from the lowest level of execution, guided by these policies. Therefore, potentially, more accurate high-level reports could be produced on the overall compliance to management directives.

These Strategic, Tactical, and Operational level policies should be logically organized in an Information Security Policy Architecture (ISPA) as depicted in figure 5 below, contributing to sound Information Security Governance.

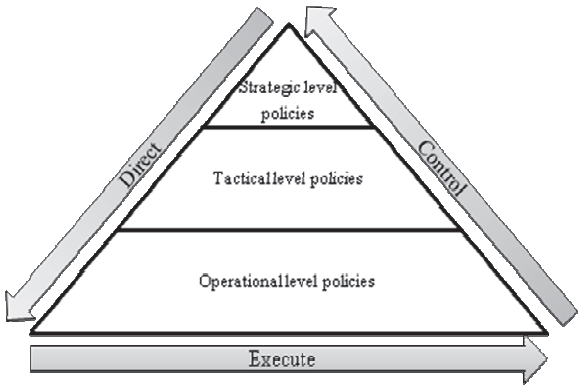

Figure 5: A comprehensive Information Security Policy Architecture

VIII. CONCLUSION

It is well accepted that information is no longer only used as a business enabler, but also to gain a competitive advantage. Therefore, comprehensive Information Security Governance practices should be practiced by organizations. Proper Information Security Governance has been noted to consist of the direct and control activities that should be performed at all management levels, namely: Strategic, Tactical, and Operational level. Policies residing at each of these levels should be represented in an organization's Information Security Policy Architecture (ISPA).

As was highlighted, however, in most cases, the ISPA does not include those policies residing at the Operational level. Very often, the Operational level policies that do exist in an organization were developed following a bottom-up approach. This means that, typically, Operational level policies are not directly related to the Tactical or Strategic level policies. Therefore, a 'break' or 'gap' is evident in both the direct and control processes.

The 'ideal' ISPA, however, does not have any 'breaks' or 'gaps' in the direct and control processes from the Strategic, to the Tactical, to the Operational level and therefore sound Information security Governance can more easily be facilitated.

REFERENCES

[1] Kovacich GL, Halibozek EP. Security metrics management. Elsevier: USA, 2006.

[2] Von Solms R, Von Solms B. Information security governance: A model based on the Direct-Control cycle. *Computers & Security*, Vol 25, 2006; **6** : 408 – 412.

[3] ISO/IEC 27002. Information technology – Security techniques – Code of practice for information security management. ISO/IEC: Switzerland, 2005.

[4] Killmeyer J. Information security architecture. Auerbach Publications: Boca Raton, 2006.

[5] Bacik S. Building an effective information security policy architecture. CRC Press, Taylor & Francis Group: Boca Raton, 2008.

[6] Institute of Directors. King III report on corporate governance for South Africa. Parktown, September 2009.

[7] IT Governance Institute. COBIT 4.1. IT Governance Institute: USA, 2007.

[8] Love P, Reinhard J, Schwab AJ, Spafford G. Information security governance. Institute of Internal Auditors: USA, 2010.

[9] Whitman ME, Mattord HJ. Management of information security, second edition. Course Technology Cengage Learning: USA, 2008.

[10] Von Solms R, Von Solms SH. Information security governance. Springer Science+Business Media, LLC: USA, 2009.

[11] Cisco Networking Academy. CCNA Security 1.0: Implementing network security, Chapter 9: Managing a secure network, 2009. Retrieved on 01 March 2010 from http://r125cnap1.nmmu.ac.za/CCNA_Security_English/index.html

[12] Verma D. The generic provisioning problem, 2000. Retrieved 30 May 2010 from http://www.informit.com/articles/article.aspx?p=130819

[13] Peltier TR, Peltier J, Blackley JA. Information security fundamentals. Auerbach Publications: Boca Raton, 2005.

[14] Samarati P, Vimercati SC. Access control: policies, models, and mechanisms. *Foundations of Security Analysis and Design* 2001, 137-196. Retrieved 01 Aug 2010 from www.utc.edu/Faculty/Li-Yang/CPSC461/samarati03-ac.pdf

[15] Liu AX, Gouda MG. Firewall policy queries, *IEEE Transactions on Parallel and Distributed Systems,* Vol. 20, 2009. **6**: 766-777. Retrieved 15 April 2010 from

http://portal.acm.org/citation.cfm?id=1550403.1550570&coll=GUIDE&dl=GUIDE&CFID=84866131&CFTOKEN=19142232

[16] He Q, Anton AI. Requirements-based access control analysis and policy specification, Information and Software Technology, Vol. 59, 2005. **6**: 993-1009. Retrieved 15 April 2010 from http://portal.acm.org/citation.cfm?id=1518331.1518547&coll=GUIDE&dl=GUIDE&CFID=84866131&CFTOKEN=19142232

[17] Ramanathan RR. Information security top-down, 2004. Retrieved 25 Aug 2010 from http://www.securitymagazine.com/Articles/Feature_Article/61f65404864d8010VgnVCM100000f932a8c0____

[18] Olivier C, Von Solms R, Cowley L. Information Integrity Assurance for Networks: Let's learn from the financial model. *Computer Fraud & Security* 2006; **8** : 7 – 14.

[19] Doherty NF, Fulford H. Do information security policies reduce the incidence of security breaches: an exploratory analysis. *Information Resources Management Journal (IRMJ)*, vol. 18, 2005, p. 21–39.

[20] Chipperfield C. From security policy to practice: Sending the right messages. *Computer Fraud & Security*, vol. 2010, 2010, pp. 13-19.

[21] Doherty NF, Fulford H. Aligning the information security policy with the strategic information systems plan. *Computers & Security*, vol. 25, 2006, p. 55–63.

[22] Doherty NF, Anastasakis L, Fulford H. The information security policy unpacked: A critical study of the content of university policies. *International Journal of Information Management*, vol. 29, 2009, p. 449–457.

[23] Fulford H, Doherty NF. The application of information security policies in large UK-based organizations: an exploratory investigation. *Information Management & Computer Security*, vol. 11, 2003, p. 106–114.

[24] Goel S, Chengalur-Smith I.S.N. Metrics for characterizing the form of security policies. *The Journal of Strategic Information Systems*, vol. 19, 2010, pp. 281-295.

[25] Hone K, Eloff J.H.P. Information security policy–what do international information security standards say? *Computers & Security*, vol. 21, 2002, p. 402–409.

[26] Karyda M, Kiountouzis E, Kokolakis S. Information systems security policies: a contextual perspective. *Computers & Security*, vol. 24, 2005, p. 246–260.

[27] Knapp KJ, Morris RF, Marshall TE, Anthony T. Information security policy : An organizational-level process model. *Computers & Security*, 2009, pp. 1-16.

[28] Mader A, Srinivasan S. Curriculum development related to information security policies and procedures. *Proceedings of the 2nd annual conference on Information security curriculum development*, ACM, 2005, p. 49–53.

[29] McKenna B. Keeping it real: Updating your security policy in 2010. *Infosecurity*, vol. 7, 2010, p. 18–21.

[30] Von Solms R, Von Solms B. From policies to culture. *Computers & security*, vol. 23, 2004, p. 275–279.

[31] Wiant TL. Information security policy's impact on reporting security incidents. *Computers & Security*, vol. 24, 2005, p. 448–459.

[32] Siponen M, Mahmood MA, Pahnila S. Are employees putting your company at risk by not following information security policies? *Communications of the ACM*, vol. 52, Dec. 2009, p. 145.