The Impact of Corporate Culture in Security Policies – A Methodology

Edmo L. Filho[1], Gilberto T. Hashimoto[1], Pedro F. Rosa[1], Joao H. P. de Souza[2]
Universidade Federal de Uberlândia[1]
Uberlândia – Minas Gerais – Brazil
Universidade de São Paulo[2]
São Paulo – São Paulo – Brazil
edmo,gilbertot@algartelecom.com.br,
frosi@facom.ufu.br, joaohs@usp.br

Albene Teixeira Chaves
UNIMINAS/FACIMINAS – União Educacional Minas Gerais
Uberlândia – MG – Brazil
atchaves2@gmail.com

***Abstract*—Despite security policies, standards, awareness strategies and tools currently in place, employees are still being involved in risky behaviors that jeopardizes businesses. Meanwhile, although security policies are the cornerstone of well-designed security strategies, recent studies have demonstrated poor adherence or even negligence in accordance with the rules security policies specify. This observed behavior is related to the fact that business permeates different countries, cultures, and understanding human nature and culture is still a key success factor to information security not well-supported by established security policy development and deployment methodologies. As its outcome, this paper addresses a ubiquitous methodology to develop security policies considering the evaluation of culture and its impacts over security policy adherence.**

Keywords-security policy; awareness; culture, congruence model.

I. INTRODUCTION

As far as employees are using business networks to communicate, collaborate and access data, critical corporate information is being introduced into a broader environment that is more vulnerable and difficult to protect. Employees have available an increasing number of interactive applications and devices such as smart phones and handhelds. Besides that, individuals find it difficult to have a true boundary between work and home life [1] and they spend time sharing personal and business information on social networking sites [2]. As a result the frontiers between working inside or outside the company have completely disappeared and calling into question the traditional method to secure the perimeter.

The situation is further complicated by the increasing in the outsourcing activities. Although outsourcing can increase information security risks, in today's increasingly global competitive environment, most organizations have had to transform and outsourcing is a common strategy to reduce costs. In addition, this strategy can pose a company to different cultures in the same business process or a project.

The current scenario can lead to the extension and potential dilution of protection controls and an increase in the number of third parties given the same access rights and privileges as "natural" employees. Examples of common risks and mistakes [3]-[4]-[5] include (being not limited to): using unauthorized programs, misuse of corporate computers, unauthorized physical and network access, misuse of passwords and transfer sensitive information between work and personal computers.

Corporate culture is the total sum of the customs, values, traditions and meanings that make a company different from others. It is often called "the character of an organization" since it embodies the vision of the company's founders. The values of a corporate culture influence the ethical standards within a corporation, as well as managerial and security behavior.

Senior management may try to determine a corporate culture. They may wish to impose corporate values and standards of behavior that specifically reflect the objectives of the organization. Generally, these corporate values and standards of behavior are derived from the culture of the nation. As a consequence an obstacle to adherence of corporate culture naturally arises when companies extrapolate its frontiers by business expansion or acquisition of other companies. Regional and cultural differences will manifest themselves in a variety of security threats and business risks.

In addition, there will also be an extant internal culture within the workforce. Work-groups within the organization have their own behavioral quirks and interactions which, to an extent, affect the whole system. Roger Harrison's four-culture typology, and adapted by Charles Handy, suggests that unlike organizational culture, corporate culture can be imported. For example, computer technicians will have expertise, language and behaviors gained independently of the organization, but their presence can influence the culture of the organization as a whole.

Security Policies [8] are the cornerstone of a successfully information security architecture, because it provides clear instructions about information security and establishes management support. Policies are used as a reference point for a wide variety of information security activities including: designing controls into application systems and networks, establishing user access controls, conducting cybercrime investigations; and keep workers aware of punishment related to security violations.

 ISBN: 978-1-61208-133-5

However, in order to be effective security policies must be accompanied by an exhaustive and endless awareness program. The education and training helps minimize the cost of security incidents, and assure the consistent implementation of controls across an organization's information systems and business process.

Firewall [7]-[12] and Intrusion Prevention System (IPS) [6] are important building blocks of a security topology. Network and/or security administrators often rely on their services to protect against the majority of threats and to enforce security policies. However, security is not keeping up with technological and social changes in the workplace, there are ways to circumvent or ignore enforcement rules and, depending on the way security policies are deployed, people's culture has strong influence on adherence or not of these security policies.

Even in experienced international companies, many well-meaning universal applications of management theory ended up being a fiasco when these practices were faced with other cultures. It is not different when considering a security policy. What performs well in a country company may not in another country. Security controls need to be workable in a variety of environments and developed, implemented and supported with people's behavior in mind.

The goal of this paper is to propose and evaluate a method to develop and deploy security policies considering the diversity of culture that companies may confront. The groundwork of the methodology is built over an integrated and consistent approach. As far as we know, to evaluate the impacts of people's culture in the security policy development and deployment is a hard task. In Section II, III, and IV the necessary background to develop the methodology is presented. In Section V, the methodology is described and detailed. In Section VI, the most important results are shown. Finally, section VII presents some concluding remarks and suggestion for future work.

II. CORPORATE CULTURE BACKGROUND

Culture is a common system of meanings, which shows what people should pay attention, how should act and what to value. Strong culture is said to exist where staff respond to stimulus because of their alignment to organizational values. In such environments, strong cultures help companies operate with efficiency, cruising along with outstanding execution and perhaps minor tweaking of existing procedures.

Conversely, there is weak culture where there is little alignment with organizational values and control must be exercised through extensive procedures and bureaucracy. Considering security policies, this control is mainly exercised through application of enforcement rules by configuration and usage of security appliances.

Where culture is strong people do things because they believe it is the right thing to do, however there is a risk of another phenomenon, "group think". This is a state where people, even if they have different ideas, do not challenge organizational thought, and therefore there is a reduced capacity for innovative thoughts. This could occur, for example, where there is heavy reliance on a central charismatic figure in the organization, or where there is an evangelical belief in the organization's values, or also in groups where a friendly climate is at the base of their identity (avoidance of conflict). In fact group think is very common, it happens all the time, in almost every group. Members that are defiant are often turned down or seen as a negative influence by the rest of the group, because they bring conflict.

Of all the data losses reported by the UK Government after the nefarious case of the leaking of personal details of 25 million people in a single incident involving the UK Government's Revenues and Customs Department (HMRC), 95% is due to cultural factors or the behavior of people whilst only 5% is believed to be due to technology issues [13].

Every culture distinguishes itself from others by means of specific solutions to specific problems [14]. The categories of problems can be viewed under three aspects: problems that arise from people's relationship, passage of time and environment. Due to its main objective the article focus on people's relationship and the five guidelines to understand the ways humans relate to each other:

Universalism versus Particularism – In the universalism approach is possible to define what is good and what is bad and this criterion is always applicable. In the Particularism culture more attention is given to the obligations of the relationships and specific circumstances. For example, instead of assuming that a good law should always be followed, the Particularism reasoning is that friendship has special obligations and hence may be a priority.

Individualism versus Collectivism – People see themselves primarily as individuals or basically part of a group? Moreover, it is more important to concentrate on the individual so that they can contribute to the community, or is it more important to consider the community first?

Neutral or Emotional – The nature of our interactions should be objective and impartial or is it acceptable to express emotion? In several places the business relationships are generally tools for reaching an objective. Emotions are avoided in order not to compromise discussions. However, several cultures consider the manifestation of emotions a natural part of business.

Specific versus Diffuse – When the person is engaged in a business relationship, there is real and personal contact rather than the specific relationship recommended in the contract.

Achievement versus Attribution – Achievement means that the person is judged by his recent activities and history. Attribution means that the status is conferred by birth, kinship, gender or age, but also for their connections, who you know and professional training.

Innovative organizations need individuals who are prepared to challenge the status quo—be it groupthink or bureaucracy, and also need procedures to implement new ideas effectively.

Most organizations are facing some kind of transformation and traditional cultures are facing the impacts of globalizations and being rebuilt, including perceptions and behavior towards security. If not addressed clearly, cultural

 ISBN: 978-1-61208-133-5

changes can cause uncertainty and doubts in employees or third parties, impacting adherence to security policies.

The Congruence Model [15] is a methodology to address the cultural and business changes. The methodology deals with changes to both formal and informal cultures as well as the infrastructure and business processes. The congruence approach is already being applied by the security community [13].

III. SECURITY POLICY BACKGROUND

In spite of organization's size, their businesses, or the extent to which it uses technology, information security is an important matter that should be addressed by explicit policies. However, the settlement of security policies is itself based on a specific framework that requires methodology to write, structure, effective review, approval, enforcement and awareness process [8]-[9].

Security policies are high-level statements that provide guidance to those who must make present and future decisions. An information security policy document is vital for many reasons. Beyond the definition of roles and responsibilities for workers, partners, suppliers, a policy document sensitizes them to the potential threats, vulnerabilities and problems associated with modern information systems. A consistent awareness program is fundamental to achieve the security policy goals. Education and training helps minimize the cost of security incidents, and helps assure the consistent implementation of controls across an organization's information systems.

The well-known methodologies for developing security policies [8] do not address the issue of corporate culture in depth, only guidance to make policies compliance to corporate culture is provided. Many obstacles to compliance of security policies arise when these policies are deployed as canned goods in different cultures. For example, is difficult to understand some of the cultural, religious and societal pressures of the India's caste system and its implications: orders are expected to be obeyed and the rules required at work will always be less important than behavior deep-rooted over countless generations.

Figure 1 depicts the approach mainly used around the world to develop and deploy security policies.

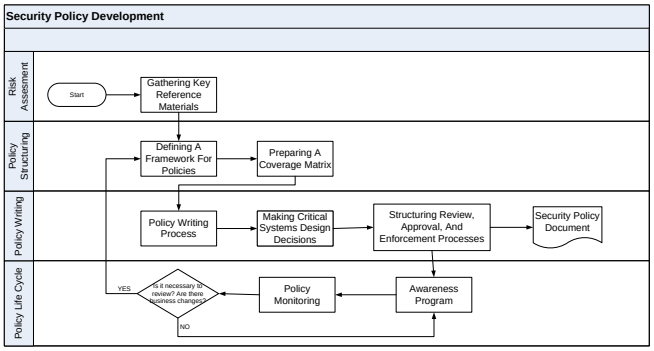

Figure 1. Security Policy development fluxogram.

Legal aspects are also an important aspect of security policy life cycle. Each country has its own legal system that must be evaluated before developing or deploying an imported policy.

Currently, the effectiveness of security policies considering data leakage is an important concern. Regardless of the type or mode of data leakage, recent research [9] reveals that one out of four companies does not even have a security policy and for businesses with policies, the findings reveal a significant gap between the beliefs of security staff regarding employee compliance and the actual behavior of them. The reasons why employees knowingly overlook or bypass security policies and put corporate data at risk are mainly a result of a failure to communicate security policies and create an awareness behavior in accordance with local culture.

The proposed methodology presents an adaptive strategy to security policy development and awareness program based on the analysis of the culture throughout the five guidelines to understand the ways humans relate to each other and the application of the Congruence Model.

IV. AWARENESS BACKGROUND

The data loss issue encompasses everything from confidential information about one customer being exposed, to strategic files of a company's product being sent to a competitor. Whether deliberate or accidental, data loss occur any time employees, third-party, or other insiders release sensitive data about customers, finances, intellectual property, or other confidential information in violation of company policies and regulatory requirements.

Beyond the methods used to educate about information security the approach needs to sensitize employees to the types of attacks that they might encounter. Employee thinking needs to be stimulated via real-world examples. The awareness program must include topics about the threats, and on how to secure "your own" environment. The awareness approach is a key success factor to the development of a security framework and shall be measured. Surveys are a traditional method of measuring awareness [11]. However, measuring attitudes and awareness have a poor correlation with behavior.

An adaptive strategy to the awareness program is based on marketing, psychology principles, and a qualitative information security awareness scorecard [10]. Blogs and social network forums integrated with monitoring process are used to energize employee involvement. The expected results may be evaluated through internal quizzes considering a rewarding process.

Repetition of information security policy ideas is essential. Repetition impresses users and other audiences with the importance that management places on information security. Education also prevents workers from saying "I never heard about that."

The channels used to express a policy will determine how the policy should be written. For example, if videotape will be used, then an abbreviated colloquial style should be employed. If a policy document will reside on an intranet web server, then a more graphic and hypertext-linked style is

 ISBN: 978-1-61208-133-5

appropriate. If policies will be issued through a series of paper memos, then short and concise text-oriented expressions will be required. The ways that the organization currently uses or intends to use information security policies should also be examined [8].

The education process must consider the third parties as they are now always present somewhere in the organizations. Effective education is difficult in multicultural an outsourced environments where suppliers are growing rapidly and hiring hundreds of new employees to support companies' requirements. The cost and time spent to education tends to prove its benefits in a short time.

V. PROPOSAL

Based on the analysis of the culture throughout the five guidelines to understand the ways humans relate to each other, it is possible to define four types of companies related to corporate culture: the Family, Eiffel Tower, Guided Missile and Incubator [14]. Figure 2 summarizes the relationship between the employees and their notion of company.

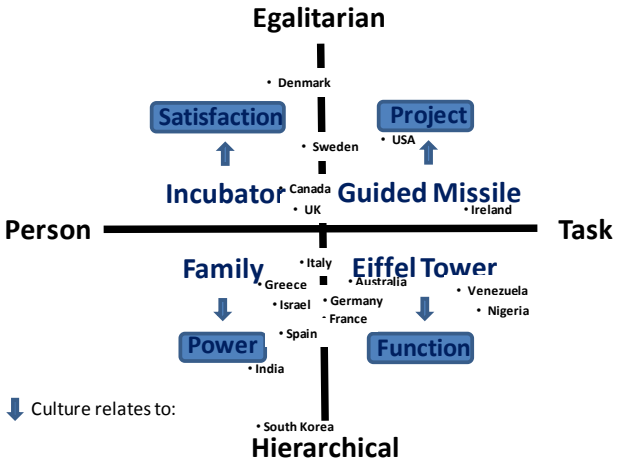

Figure 2. Cultures of the company.

A comprehensive study on the types of culture related to companies and how to determine the type through research can be found at [14] and Trompenaars' database. Examples from the 16 questions used to measure corporate culture include how to measure the hierarchy level and conflicts.

According to the type of corporate culture that will be generally derived from the culture of the nation, security policies will have more adherence or not depending on the strategy to develop and implement.

Another important study of how values in the workplace are influenced by culture can be found at [16]. For example, "*Brazil's highest Hofstede Dimension is Uncertainty Avoidance (UAI) is 76, indicating the society's low level of tolerance for uncertainty. In an effort to minimize or reduce this level of uncertainty, strict rules, laws, policies, and regulations are adopted and implemented. The ultimate goal of this population is to control everything in order to eliminate or avoid the unexpected. As a result of this high Uncertainty Avoidance characteristic, the society does not readily accept change and is very risk adverse*".

For the purpose of this article the factors thinking, learning and change (responses) should be evaluated in order to determine the impacts in the development and awareness process of security policies.

The Family culture deals more with the intuition than rational process. It focuses on the development of people over people's performance. The knowledge is based on trial and error and the individual is more important than the task. The change process is essentially political and top down. The mentors and managers are important actors in the learning process. Pattern examples of national corporate culture include France, Spain, India and Japan [14].

The Eiffel Tower considers that in order to perform his functions the professional must accumulate the necessary skills and always keep evolving. Human resources are evaluated like financial capital and cash. The change process in this culture is always slow, executed through rules of change and considering a formal process. This kind of culture doesn't adapt well to turbulent environments. Companies with this culture profile generally avoid and resist to changes. Examples include Germany, Holland and Denmark [14].

The Guided Missile culture reviews its objectives through a constant feedback process. Then it is a circular and not linear culture. It rarely changes its main objective and everything necessary is done to keep and achieve the objectives. The directions are corrective and conservative. The learning process includes the personal contact and interactions within a group. It has a practical approach instead of theoretical and focuses on the problems instead of discipline. Changes are fast in this kind of culture, as the objectives moves new groups of work are formed to support the new demands and the old groups are diluted. This culture tends to be individualist. Examples include Canada, USA and United Kingdom [14].

The Incubator culture is based on the idea that people's satisfaction is more important than the company itself. To tolerate the company the main people's objective is to serve the incubator for self-expression and self-satisfaction. Companies in this kind of culture often operate as an intense emotional environment, having a minimal hierarchical structure and the authority is strictly personal. When the members are in harmony the change process is usually fast and spontaneous. This culture is creative, although doesn't survive to changes on the demand patterns. Sweden is a common example of this culture [14].

Figure 3 depicts the relation between the types of culture and the level of difficult to develop and deploy security policies.

As the authors could observe during the process of development and deployment of security policies in the last 10 years considering wholesale, telecom, data center, agribusiness, transportation and real estate companies – some of them multinational – formal cultures tends to facilitate the whole process. However, exceptions can happen.

 ISBN: 978-1-61208-133-5

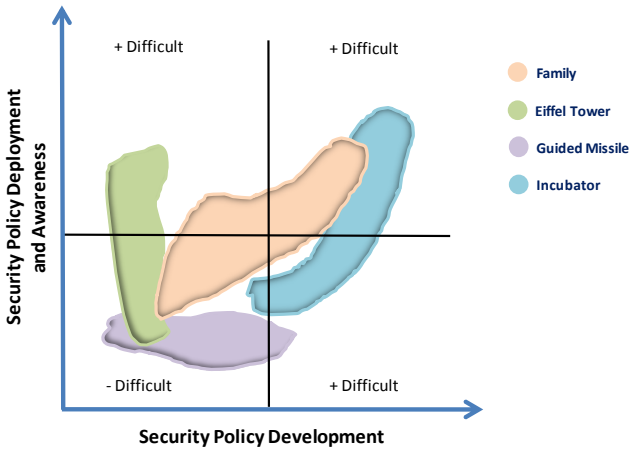

Figure 3. Impacts of culture in Security Policy process.

Table I depicts the relation between corporate culture, the security policy development, awareness process and the necessary steps to include in the traditional security policy development process after the analysis of the culture pattern predominant in the organization.

The pattern analysis must follow or be included in the Risk Assessment phase. The guidelines are an adaptation of Trompenaars' "how to manage and be managed by the corporate culture" to the Security Policy (SP) development and deployment phases .

TABLE I. CORPORATE CULTURE AND SECURITY POLICY

Culture	SP Development	SP Deployment	Awareness
Family	• Top Down approach[1]; • Conquer the corporate leaders[2]; • Evangelize the CEO and leaders[3]; • Abuse of risk examples to convince them[4]. • Make the leaders feel more powerful and with more control through SP's; • Show to the leaders the **impacts of errors** more than the advantages of SP's	• 1 and 2; • Make people feel as the "owner of the process[4]"	• 1 and 4; • Conquer the team's members; • Repetition is a must[6];
Eiffel Tower	• 1 and 2; • Show the leaders the **advantages** of SP's[5];	• Decentralized; • Usage of Project Management methodology.	• The awareness program should sell SP as status;
Guided Missile	• Top Down and decentralized approach. • 5; • Present the avoided risks in financial numbers;	• Usage of project management methodology.	• The awareness program must show results in financial numbers and impact over "salary".
Incubator	• Decentralized approach. • Discover the most influent individuals of the network and evangelize them.	• Make people feel SP as innovative and important to their objectives. • 6.	• The awareness program should create "challenge conditions"; • 6.

There are different methods to apply the guidelines that will depend on the available time and resources. Understanding corporate culture, security professionals will have strong likelihood to establish security policies integrated into the organization's culture.

VI. EVALUATION

In spite of the methodologies already in place and the proposal, developing and deploying security policies is not a easy project even in corporate cultures classified as guided missile. The authors' experience and observation through the last 10 years showed that evangelization is a good strategy. Being nearest the employee and third party bring results in a short time than being far from.

Security metrics is a nascent discipline with more questions than answers [17]. Moreover, the choice of security metrics may lead to a false sense of security or otherwise misdirect security efforts and strategy. Measurement does not guarantee safety as usually the metrics are related to past events.

The best way to measure the effectiveness of the proposal is to observe human behavior towards information security. The number of incidents per amount of employees is a suggested metric to be monitored. Then, it is necessary to put in place tools to monitor frauds and other incidents.

Table II presents examples of the most predominant type of culture [14], the difference between the number of end users and the number of decision makers who are aware of a policy regarding acceptable use of company resources [9].

Why is there a lack of connection between policy makers and the employees who must conform to policies every day? According to the survey results [9] one crucial reason is a lack of direct and consistent communication, and 11% of employees say that security policies were never communicated to them or that they were never educated about the policy.

TABLE II. THE DISCONNECT BETWEEN END USER AND SECURITY POLICY AWARENESS

Country	End User	Decision Makers	Culture
USA	45%	76%	Guided Missile
France	49%	74%	Eiffel Tower

 ISBN: 978-1-61208-133-5

Italy	46%	77%	Family
India	54%	77%	Family
UK	50%	71%	Incubator

Europe had the highest prevalence of this belief, where the United Kingdom – Incubator – (25%) and France – Eiffel Tower – (20%) far exceed the global average. Germany – Eiffel Tower – also has a high percentage of employees who claim that IT never communicates security policies to them (16%).

The survey results associated with the analysis of corporate culture support the author's proposal and the relation presented in Figure 3.

VII. CONCLUSION AND FUTURE WORK

The organization's performance rests upon the alignment of each of the components – the work, people, structure and culture – where the higher the congruence between them, higher will be the performance of the organization. Information security risks may damage the desired company results and security policies are the cornerstone of a security framework – the starting point to avoid or minimize damages.

However, the methodologies already in place to develop security policies didn't consider the impacts of culture in adherence to them. Information security risks are a critical issue for companies, as the number of incidents continues to increase. Whether it's a malicious attempt, or an inadvertent mistake, these risks can decrease a company's trademark, reduce shareholder value, and blemish the company's goodwill and reputation. Furthermore, applied security technology is not enough once the human factor is essentially the weakest part considering corporate culture.

The article proposes a starting point to discuss and evolve the impacts of culture in security policies adherence. The article also presents a methodology which, in a nutshell, is to include in the Risk Assessment phase the verification of the predominant pattern of culture in the organization, and after that follow the proposed guidelines to the specific culture in order to achieve success. The proposal is likely to progress in conjunction with further research in this area.

Future work is necessary to investigate an evolution of the corporate culture analysis considering automation of the process through the usage of OWL (Web Ontology Language). Ontologies have been used to knowledge management and organization [18], for example, in Artificial Intelligence (AI) ontologies have been used to explicitly declare the knowledge embedded in knowledge-based system and to facilitate knowledge share and re-use. Another challenge is to develop an effective method to evaluate employees' adherence and commitment to security policies considering the established corporate culture.

REFERENCES

[1] J. Walker, R. Samani, M. Henshaw, A.Yeomans, P. Wood, T. Holman, M. Westmacott, A. Davis, O. Ross, A. Sehmbi, L. Orans, and S. Janes, "CW Security Think Tank: How to prevent security breaches from personal devices in the workplace", 12/07/2010, http://www.computerweekly.com/Articles/2011/01/05/244377/CW-Security-Think-Tank-How-to-prevent-security-breaches-from-personal-devices-in-the.htm 03/24/2011.

[2] E. L. Filho, G. Hashimoto, P. Rosa, and J. Machado, "A Security Framework to Protect against Social Networks Services Threats" Proc. IARIA Symp. The Fifth International Conference on Systems and Networks Communications (ICSNC) 2010, IEEE Press, Aug. 2010, pp. 189-194, doi: 10.1109/ICSNC.2010.36.

[3] W. Willinger, R. Rijaie, M. Torkjazi, M. Valafar, and M. Maggioni, "Research on online social networks: time to face the real challenges," ACM SIGMETRICS Performance Evaluation Review, Dec. 2009, pp. 49-54, doi: 10.1145/1710115.1710125.

[4] CISCO (2008), "Data Leakage Worldwide: The High Cost of Insider Threats", http://www.cisco.com/en/US/solutions/collateral/ns170/ns896/ns895/white_paper_c11-506224.html 03/23/2011.

[5] CISCO (2008), "Data Leakage Worldwide: Common Risks and Mistakes Employees Make", http://www.cisco.com/en/US/solutions/collateral/ns170/ns896/ns895/white_paper_c11-499060.html 03/23/2011.

[6] M. Rash, A. Orebaugh, G. Clark, B. Pinkard, and J. Babbin, "Intrusion Prevention and Active Response: Deploying Network and Host IPS", SYNGRESS PUBLISHING, p. 4-20, 2005.

[7] E. L. Filho, "Arquitetura de Alta Disponibilidade para Firewall e IPS Baseada em SCTP", Department od Computer Science, Federal University of Uberlândia, p. 50-59, 2008.

[8] C. Wood, "Information Security Policies Made Easy" 10th Edition, INFORMATION SHIELD, Inc., 2005.

[9] CISCO (2008), "Data Leakage Worldwide: The Effectiveness of Security Policies" http://www.cisco.com/en/US/solutions/collateral/ns170/ns896/ns895/white_paper_c11-503131.html 03/23/2011.

[10] G. Stewart, "Maximising the Effectiveness of Information Security Awareness Using Marketing and Psychology Principles" Department of Mathematics, Royal Holloway, University of London, RHUL-MA-2009-2, Feb. 2009.

[11] C. Roper, J. Grau, and L. Fischer, "Security Education, Awareness and Training, SEAT from Theory to Practice". ELSEVIER BUTTERWORTH-HEINEMANN, 2006.

[12] E. L. Filho, G. Hashimoto, and P. Rosa, "A High Availability Firewall Model Based on SCTP Protocol," Proc. IARIA Symp. Systems and Networks Communications (ICSNC 08), IEEE Press, Dec. 2008, pp. 202-207, doi: 10.1109/ICSNC.2008.63.

[13] C. Colwill, "Human Factors in Information Security: The Insider Threat – Who Can You Trust These Days?", ELSEVIER, Inform. Secur. Tech. Rep. (2010), doi: 10.1016/j.isrt.2010.04.004.

[14] F. Trompenaars and C. Hampden-Turner, "Riding The Waves of Culture: Understanding Diversity in Global Business", 2th Edition, MCGRAW-HILL, 1998.

[15] O. Wyman, "Congruence Model: A Roadmap for Understanding Organizational Performance", http://www.oliverwyman.com/ow/pdf_files/Congruence_Model_INS.pdf 03/23/2011.

[16] G. Hofstede, "Cultural Dimensions", http://www.geert-hofstede.com/ 03/23/2011.

[17] C. Nelson, "Security Metrics An Overview", ISSA Journal, August 2010, pp. 12-18.

[18] E-S. Abou-Zeid and J. Molson, "Towards a Cultural Ontology for Interorganizational Knowledge Processes", IEEE Press, Jan. 2003, vol. 1, pp. 8c, Proceedings of the 36th Annual Hawaii International Conference on System Sciences (HICSS'03), doi: 10.1109/HICSS.2003.1173645.

 ISBN: 978-1-61208-133-5