CORPORATE SECURITY THREATS WITHIN THE COMMUNICATION ASPECT

Assist. Prof. Sabahudin Hadžialić, Ph.D. candidate
Email: sabahudin.hadzialic@iu-travnik.com
International University Travnik, Bosnia and Herzegovina
Communication Science Faculty (II cycle), UNINETTUNO University, Rome, Italy

Abstract: The future of business lies within a wholly digital network through interactively connected world. Without the right systems, but also without high level of social responsibility based on cultural, social and all other sensitive human existence related issues within the understandings of management of the firm and also without focusing in place to manage and protect the firm, businesses are faced with challenges of problems with data security. Through this paper-case study will be shown how Human errors; Disgruntled employees; Property Theft / Misplacement of the records; Cyber criminals; Insufficient Network security; Accessibility to information and Social Networks might jeopardize security of the enterprise, regardless if we are talking about small and/or big business in Bosnia and Herzegovina. The importance of the final outcomes lies not only in protecting the firm from all kinds of security threats, but also in establishing of the proper systems through adequate use of new communication technologies and through education & information security trainings, adequate recovery plans and constant evolving of the risks with which firm might be faced.

Keywords: Corporate security, communication, business, protection, security threats

> *If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology."*
>
> *– Bruce Schneier*

Introduction

Enormous technological advancement in the development of computer networks and information systems has given to us great possibilities of processing, storage and transmission of digital data, both in small and in big business in Bosnia and Herzegovina. Changes in communication and information technology and their application have caused a number of issues that are related to the security of business assets in the firm. Reaching the consensus in the security of information system, among various stakeholders of corporate security within the organization has become more difficult than solving many technical problems. We are witnessing the appearance of strong external coalitions that change the traditional centralized and hierarchical organizations in loosely organic networks. These organizations are based more on cooperation than on control. To be more efficient, more effective and to be able to better respond to external influences, organizations give great importance to the application of computer networks and computer information systems and in the same time forgetting the human factor. The problem is that many firms, without careful planning and understanding of security concerns, implement IT in their organization of work. "Security blindness" on the issue of IT security is not a new concept of today. Due to the unpredictability of what's coming in the future and on the basis of existing competitive trends, security managers are only seemingly key figures that determine the success or failure of the wellbeing of the company. Their role is evolving, depending on the entire culture of communication within the firm, or its entire employees. In this paper I would like to show the model how to give guidelines on which aspects we must have an influence to be able to have more integrated security of information and communication system and to have that become constituent part of the business organization.

1. Contemporary challenges of assumptions of solutions for the future

Researches up to now have led to the conclusion that technological factors are not the only key factors within the effectiveness of information security, and that we must involve human factors, but also the factors of internal organization of the firm. Exceptional, first challenge that I would like to underline is the lack of education of employees, in other words - their indifference for the common good in today's Bosnia and Herzegovina in regards the security movements in and around the firm. The problem is now already within the human and cultural characteristics/natures, and especially when employees who deal with information and communication security communicate with other employees. One study showed that communication about the risks has a significant role for the most goals in the management of security[167]. Other types of challenges are related to the organizational challenges[168] associated, both directly and indirectly with Property theft / misplacement of the records; Cyber criminals; Insufficient Network security; Accessibility to information and Social Networks. Because of too many obligations for employees who deal directly with information and communication security, it often happens that employees make mistakes and come up with deviations from optimal security[169]. To control access to sensitive data that are distributed through the firm is often not an easy job and present a significant challenge. Cloud computing[170], according to its main determinants facilitates activities that ensure the availability of the system and its maintenance. These are the grid computing, virtualization, computer enterprise as a service (utility computing) and autonomic computing. The advantages of using cloud services are: a) Centralization - The data are centralized and stored in one place where they are always available, which allows the mobility for user; b) Permanent availability – Towards the service is possible to approach from different locations where there is an Internet connection (and it is now available almost everywhere); c) Model of the rental services - For the services in the "cloud" there is no need to invest in expensive IT infrastructure, train and recruit personnel for maintenance of the services. Cloud services are used only when you need them, and about the administration, support and development of

[167] Koskosas, I. V., Paul, R. J. (2004): *The interrelationship and effect of culture and risk communication in setting Internet banking security goals,* Proceedings of the 6th international conference on Elctronic commerce, pp. 341-350.

[168] Werlinger. R., Hawkey, K., Beznosov, K.: Human (2008), Organizational and Technical Challenges of Implementating IT Security in Organizations, HAISA '08, Human Aspects of Information Security and Assurance, pp. 35-48.

[169] Kraemer, S., Carayon, P. (2007): Human errors and violations in computer and information security: The viewpoint of network administrators and security specialists, Applied Ergonomics, 38(2), pp. 143-154.

[170] Cloud computing is a revolutionary concept that offers a new way to access personal data and applications, which are no longer located on the computer but on the "cloud" - which means that you can access the program, records and documentation from multiple devices, anytime and from different locations and all you need is an internet connection. As a result of mentioned, users of services in the "cloud" can, in a better, faster and easier way, use and modify data. (Comment S.H.)

business applications concern is taken care by the side of service providers (such as Webit[171]). In the service are included the upgrades, all security mechanisms, archiving, co-location of data, user support, etc…; d) Controlled user access – Through the user administration is easy to restrict access to users (such as internally at the premises of the firm, look only at the part of the data), as well as the possibility to change, delete and/or export data; e) The security of your data - When using program services in the "cloud" the possibility of data loss is very small - if the service provider uses a range of security mechanisms (example: co-location - data within multiple places), daily data backups, etc., there is practically no risk.

Studies have shown that financial organizations (such as banks, insurance companies, retirement's funds) are investing more resources in security data from other firms and that larger firms are investing more resources than smaller firms[172]. Also, researches have shown that the quality of the implementation of information and communication security depends largely on the support of top management[173]. One paper even determine this factor as a critical factor[174] and some studies shows that management of the firm does not know about all security measures that can be implemented and that management is prepared to introduce these measures, only if they know for them. Because of the mentioned it has been an importance of education of the management in regards security measures[175]. One of the critical factors is certainly the allocation of resources, which is especially difficult in the field of IT activities by the reason of the presence of the business environment surrounding it, which is full of rapid changes in the very new technologies[176]. The third category of challenges relates to technological problems[177]. The main challenge in addressing technological problems is the complexity of the system itself. Complex computer networks with many nodes and users, the use of different technologies (firewall, intrusion detection system, anti-virus programs) are creating a major challenge in the management of the system. Information and telecommunications security has spread to the whole business, the protection of information in all aspects of the firm. We need to expand the existing principles of confidentiality, integrity and availability towards business objectives in the context of security within the firm[178].

[171] Webit (first seen on 21.11.2016): http://www.webitcongress.com/

[172] Kankanhalli, A. (2003): An integrative study of information systems security effectiveness, International Journal of Information Management, 23(2), pp. 139-154.

[173] Chang, S. E., Ho, C. B. (2006): Organizational factors to the effectiveness of implementing information security management, Industrial Management & Dana Systems, 106(7), pp. 345-361.

[174] Knapp, K. J. (2006): Information security: management's effect on culture and policy, Information Management & Computer Security, 14(1), pp. 24-36.

[175] Straub, D. W., Welke, R. J. (1998): Coping with system risk: security planning models for management decision making, MIS Quarterly, 22(4), pp. 441-469.

[176] Ashenden, D. (2008): Information Security Management: A Human Challenge?, Information Security Technical Report, 13(4), pp. 195-201.

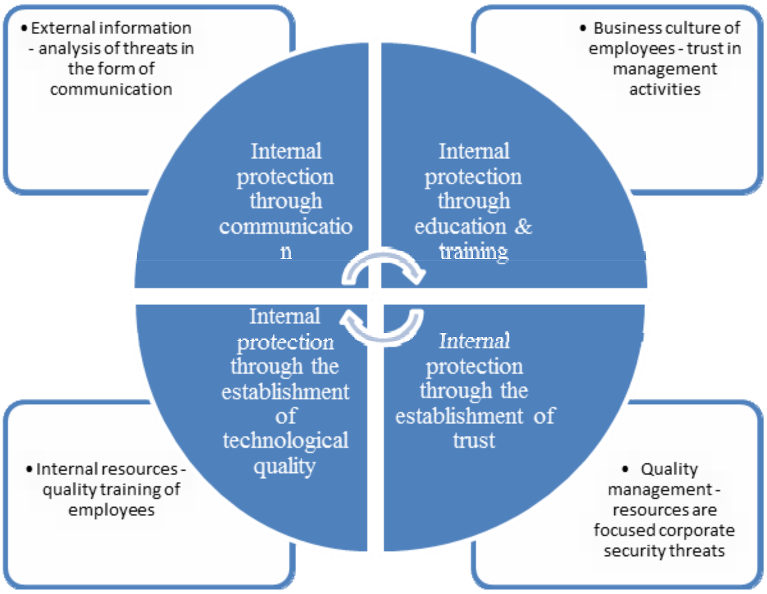
[177] Werlinger. R., Hawkey, K., Beznosov, K. (2009): Human, Organizational and Technical
Challenges of Implementating IT Security in Organizations, HAISA '08, Human Aspects of Information Security and Assurance, pp. 35-48.

[178] Ashenden, D. (2008): Information Security Management: A Human Challenge?, Information Security Technical Report, 13(4), pp. 195-201.

2. Model of integration of security within the information technologies with the aim of annulling of eventual threats to the security environment of enterprises

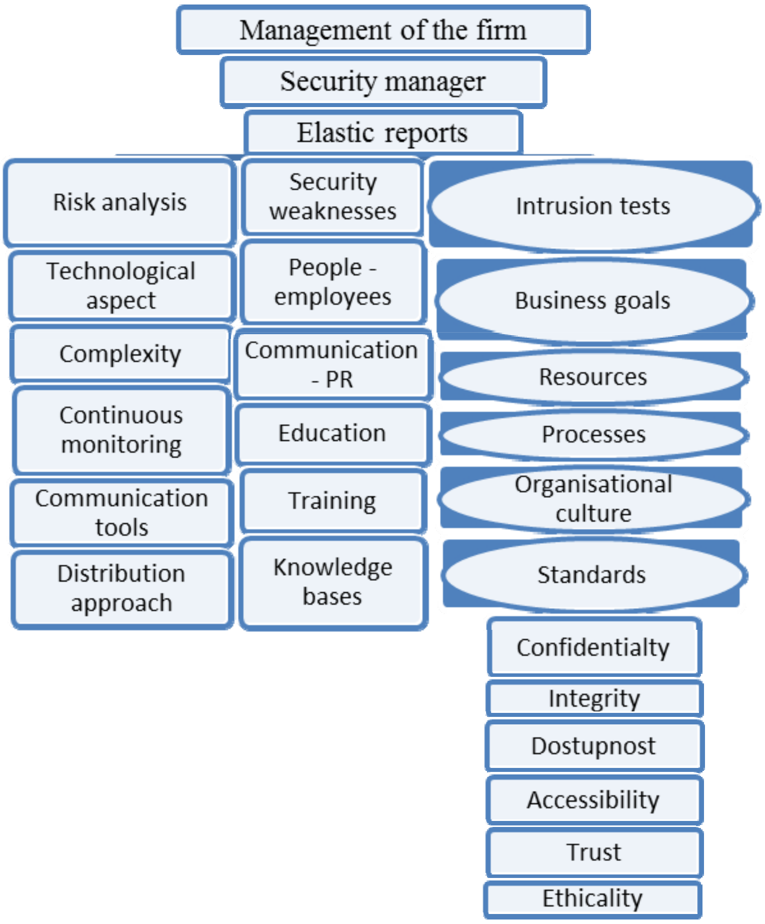
Just the mentioned title connects communication aspect of self-corporate security into a single unit combining immediate, human factor, as well as technical shaping of the relations in the firm, but also towards external audiences, as businesses, as well as to the comprehensive contacts of different forms and content. The situation analysis is one of the most important ways of considering the problems in and around the security system of a one firm also in Bosnia and Herzegovina. It requires the establishment of procedures for monitoring and follow-up activities in and around the communication system, the process of valorization of internal strengths and weaknesses, as well as the timely response of decision makers. Risks threatening the company instigate the firms to protect themselves in as much as possible manner to protect its business, employees, assets and capital, clients and associates, and documentation and knowledge.

2.1. Graph/Chart – Interaction of security protection within communication aspect


• External information - analysis of threats in the form of communication
• Business culture of employees - trust in management activities
Internal protection through communicatio n
Internal protection through education & training
Internal protection through the establishment of technological quality
Internal protection through the establishment of trust
• Internal resources - quality training of employees
• Quality management - resources are focused corporate security threats

Through the above chart/graph, as well as the communication of the graph/chart down below that follows this model I want to show how to integrate the security of the information and communication system in the organization in order to achieve security framework that would encourage management of the firm (on the top of the executive chain of decision-making) to make security information system become an integral component in all aspects of business operations of the firm. Personal experience in the management of firm, but also coordination, both public and private sector during the decades-long presence as an owner and / or the director or coordinator of communications relations within one and / or more companies, allowing me expanded access of understanding, but also upgrading of the existing security threats if we look at communication forms aimed towards appropriate protection and security in Bosnia and Herzegovina. High-quality forms of internal interactions with external forms of communication aspect of the security is the presumption of upgrading of the own vision for the survival of one firm within *the Scylla and Charybdis* of doing business in the market, but only if the game of the interaction within the business plan in the legislative and given forms of open market where we have a free market not only in the aspect of respect for the game business where the goal is not only "cheat, outplay and/or overcome" the other one (it is in Bosnia and Herzegovina very much present case in the past twenty years and more), but to create a presumption that the just "game of business" should be based on respect the other and different one when it comes to business ethics, as far as, of course, it is possible in the world of the neo-liberal economy where the corporate form of business operations stifles small and with the security and communication aspects unprepared firms through different forms of appearances - manipulating with prices, buying of staff , and similar.

2.1.1. Model of security integration within information technologies



2.2. Management of the firm

Management the firm is, faced with threats to the corporate security within communication aspect, responsible for the protection of assets (all its forms) of the firm. However, due to bad personnel policy, lack of education, nepotism and banal lack of understanding of the significance of threats to corporate security within the communications aspect comes to the various, if we can call it like that, incidents due to failure within the frame of the management and chain business policies, directives, and the actual implementation of the above[179].

2.3. Security manager

Security manager is extremely important person in this model. He is a mediator between the company's management and lower levels which are dealing with security of the firm. The qualities that are necessary for security managers are: experience; knowledge regarding the incidents, weaknesses; risk analysis and risk management; planning; knowledge of policies and standards; processes and procedures; methodologies and frameworks[180].

2.4. Elastic reports

The advantage of elastic reports is that the information within the report are shaped and compiled in accordance with users of the reports. Also, during the framing and unifying reporting towards the managers of the firms, I suggest that should not be exaggeration at the beginning within the report when it comes to its scope, but to make a brief summary and overview of all, with as little information as possible, and the details to be provided on request by the side of management of the firm. That has to be done to have well-prepared summary, as well as a report on demand, might help in understanding the priorities. According to ISO / IEC 27001[181] risks need to be evaluated, processed, selected and implement controls, observe, and again re-evaluate and revise them.

2.5. Technology

The complexity is the characteristics of technology, when it comes to security of information and communication systems. Studies have shown that tools should have the possibility of cooperation among users of the tools[182]. Through these tools would be improved communication between employees who are working on security together with the management of the firm and by that will make better, faster and better decisions.

2.6. Employees of the firm

[179] Humphreys, E. (2008): Information security management standards: Compliance, governance and risk management, Information Security Technical Report, 13(4), pp. 247-255.

[180] Purser, S. (2004): A practical Guide to Managing Information Security, Artech House.

[181] ISO/IEC 27001 - Information security management – „The ISO 27000 family of standards helps organizations keep information assets secure.Using this family of standards will help your organization manage the security of assets such as financial information, intellectual property, employee details or information entrusted to you by third parties. ISO/IEC 27001 is the best-known standard in the family providing requirements for an information security management system (ISMS)“ - First seen on WWW - 15.11.2016: http://www.iso.org/iso/iso27001

[182] Barrett, R., Prabaker, M., Takayama, E. (2004): Field Studies of Computer System Administrators: Analysis of System Management Tools and Practices, In CSCW '04, pp.388-395.

When the employees of the firm are in question in regards security, a critical success factor is internal communication (including internal PR). Why is there this difference in approaches to this issue? Most likely because the language used by employees who deal with security is often the technical language and in that form difficult to reach the company's management. As I mentioned, it is necessary to bypass the problem with receptive language within the communication. Why not also apply the theoretical and cultural approach that refers to understanding the superior knowledge of the person you are addressing as security managers and by that making closer the substance in a way to adapt the interaction profession language, business relationships and everyday communication. Education and training can help to overcome all the mentioned main problems because in that way it raises awareness about the importance of security in the firm. Human errors in disposition of available data, without focus on a particular security, are certainly a security threat to the firm and its overall assets. By storing knowledge and through its accumulation is built security of the information and communication system, and as we have already mentioned that security manager should be "The player of changes", but to be able to become that, there must be certain prerequisites created by (I called them with sporting terms for easy understanding of broader picture of the appearance):

- "physical therapists" - these are, due to my opinion, figures in engineering, maintainers of software and hardware of the security system
- "fitness coaches" who care for the bigger picture, that the work of "physical otherapist" being in the right place, at the right time.

"The players of changes" are the ones who can lead and make applications at the strategic level. Because of this, without "physical therapist", or security experts, there is no good security. But there must be a "fitness coaches" who directed the entire security and worry about security from upper levels (from the management of the firm).

2.7. Organization

As I already mentioned, the focus on business goals is important because of the communication, having in mind that without guiding on business objectives, we will never be able to convince management that the security of the information and communication systems is extremely important link in the organization of business activities of the firms. Through reports and security managers, tools for security and communication, should be given emphasis on business goals and in that case we will get more support from the company's management, without whose support and allocation of resources, there is no good security[183]. Management definitely needs to look at the costs and benefits of having the information and communication security. It is best to invest as many resources as needed - no more and no less - because if you invest less, security suffers, if you invest too much, we spent the resources and have not received a significant added value[184]. What is neglected in Bosnia and Herzegovina is certainly organizational culture explained and defined by scholars who are

[183] Kankanhalli, A. (2003): An integrative study of information systems security effectiveness, International Journal of Information Management, 23(2), pp. 139-154.

[184] Humphreys, E. (2008): Information security management standards: Compliance, governance and risk management, Information Security Technical Report, 13(4), pp. 247- 255.

engaged in the management as samples of assumptions, or heuristics[185], that individuals will use as a directive in response to the situations in the firm in which they have not been previously involved[186]. In my opinion, communication, also within public relations, inner part of the mentioned in firms, at all levels of responsibility, is also extremely important for the implementation of just ISO standards. At the same time, free time, which employees have and spend on social networks during the working day[187], through using their mobile devices, IPod's and / or computers[188], must be regulated through the code of conduct for online behavior, education, training and / or direct conversation security experts with employees, it has been created the necessary conditions to circumvent the "innocence" of cheaply communication within social networks and finally come to an understanding of security threats in the comprehensiveness of the above - there are no small and / or major threats to the security. There are just threats, because, should not be forgotten that "the avalanche was the snowflake at the beginning[189]."

2.8. General principles

The traditional principles of security of information systems are confidentiality, integrity and availability. But they are quite limited. They refer to the data contained on the computer, where confidentiality is relating to the prevention of unauthorized access, while integrity refers to the prevention of unauthorized modification of data while under the availability it refers to protect against unauthorized long-term ownership of data or resources. As it was suggested[190], these principles should be extended to several other principles relating to employees in the firm, in accordance with the extended understanding of information and communication security. Responsibility is the first additional principle. Security experts agree that at least a third of security incidents occurred and was caused by employees of the firm and it is necessary to create an internal environment of the active participants of business operations in such form of interactive participation that the employee, but also the company are satisfied with their own positions and activities in this field. Trust is a principle in modern organizations where there is less emphasis on external control and greater self-control and the responsibility also becomes an important factor. The equally relevant are data as well as data users, and therefore we must have all in mind in order to fully provide security at the level of the firm.

[185] Heuristic, is any approach to problem solving, learning, or discovery that employs a practical method not guaranteed to be optimal or perfect, but sufficient for the immediate goals. Where finding an optimal solution is impossible or impractical, heuristic methods can be used to speed up the process of finding a satisfactory solution.

[186] Johnson, G., Scholes, K. (2002): Exloring Corporate Strategy, Prentice Hall.

[187] In Bosnia and Herzegovina even more than should and could (Comment: S.H.)

[188] Thus, even an innocent form of direct communication between employees and people close to him, can, through social networks (FB, Twitter, LinkedIn, MySpace, Instagram, etc.) be a potential source of disruption of corporate security of the firm. (Comment, S.H.)

[189] Sabahudin Hadžialić – thoughts – First seen on WWW - 21.11.2016: http://sabihadzi.weebly.com

[190] Dhillon, G., Blackhouse, J. (2000): Information System Security Management in the New Millennium, Communication of the ACM, 43(7), pp. 125-128, 2000.

Conclusion

Corporate security threats within the communication aspect of it as a form of information and communication systems evolirala with the technical level of the entire company. The responsibility extends from the top to the bottom of the organization. The integration of information and communication security organization is still a problem because it is not yet taken seriously enough within the business. I have tried, in this paper, to show the model, which initially tries to point out the important aspects on which we need to consider how to better integrate information and communication security in the corporate governance of companies, while taking into account that, as far as possible, annul the threats that we have listed in the introduction to this work. There are three important things that the focus should be:

- Technological factors (Computer enterprise in the cloud as the current form of the attraction interactive-seat space);
- b) People-employees
- The organization of the enterprise.

In further work, it is necessary to present the proposed model and security experts, with appropriate survey, get feed-back on the proposed model in order to improve the above, but also how, within the area of operations in Bosnia and Herzegovina.

Next to it was the institutional integration proposed, the Model T to higher quality, targeted comprehensiveness, problem solving corporate security threats within the communication aspect. The key to success is communication with company management to ensure resources for safety and after that guided them as concrete, real measures of information and communication security. Either way, from human resources, through direct communication of public relations, both internal and external, may well depend on the totality of the business, but also the security of a company in Bosnia and Herzegovina.

And last but not least, my thought that might be the initiation better security within the enterprise, and it especially within the system permenentnog thenološkog development: *"It is not enough to have knowledge within the security skills - more than that we need skills within the knowledge of security"* .

LITERATURE

[1] Ashenden, D. (2008): Information Security Management: A Human Challenge?, Information Security Technical Report, 13(4), pp. 195-201.
WWW (First seen on 20.11.2016):
https://www.researchgate.net/publication/250689808_Information_Security_management_A_human_challenge?el=1_x_8&enrichId=rgreq-306d7af215b2feed742628b3a4ad0945-XXX&enrichSource=Y292ZXJQYWdlOzI4MzMwMjg0OTtBUzozMTkxOTI3NTcxNDU2MDRAMTQ1MzExMjg5MjQzMA==

[2] Barrett, R., Prabaker, M., Takayama, E. (2004): Field Studies of Computer System Administrators: Analysis of System Management Tools and Practices, In CSCW '04, pp.388-395.
WWW (First seen on 20.11.2016):
https://www.researchgate.net/publication/222813678_Usable_autonomic_computing_systems_The_system_administrators'_perspective

[3] Chang, S. E., Ho, C. B. (2006): Organizational factors to the effectiveness of implementing information security management, Industrial Management & Dana Systems, 106(7), pp. 345-361.
WWW (First seen on 21.11.2016):
https://www.researchgate.net/publication/220672528_Organizational_factors_to_the_effectiveness_of_implementing_information_s

[4] Dhillon, G., Blackhouse, J. (2000): Information System Security Management in the New Millennium, Communication of the ACM, 43(7), pp. 125-128, 2000.
WWW – First seen on 25.11.2016:
https://www.researchgate.net/publication/242104189_Technical_opinion_Information_system_security_management_in_the_new_millennium?el=1_x_8&enrichId=rgreq-306d7af215b2feed742628b3a4ad0945-XXX&enrichSource=Y292ZXJQYWdlOzI4MzMwMjg0OTtBUzozMTkxOTI3NTcxNDU2MDRAMTQ1MzExMjg5MjQzMA==

[5] Humphreys, E. (2008): Information security management standards: Compliance, governance and risk management, Information Security Technical Report, 13(4), pp. 247-255.
WWW: (First seen on 22.11.2016):
https://www.researchgate.net/publication/222409464_Information_security_management_standards_Compliance_governance_and_risk_management

[6] ISO/IEC 27001 - Information security management – „The ISO 27000 family of standards helps organizations keep information assets secure.Using this family of standards will help your organization manage the security of assets such as financial information, intellectual property, employee details or information entrusted to you by third parties. ISO/IEC 27001 is the best-known standard in the family providing requirements for an information security management system (ISMS)“ - First seen on WWW - 15.11.2016: http://www.iso.org/iso/iso27001

[7] Johnson, G., Scholes, K. (2002): Exloring Corporate Strategy, Prentice Hall.
WWW: (First seen on 22.11.2016):
https://www.researchgate.net/publication/222409464_Information_security_management_standards_Compliance_governance_and_risk_management

[8] Kankanhalli, A. (2003): An integrative study of information systems security effectiveness, International Journal of Information Management, 23(2), pp. 139-154.

[9] Knapp, K. J. (2006): Information security: management's effect on culture and policy, Information Management & Computer Security, 14(1), pp. 24-36.

[10] Koskosas, I. V., Paul, R. J. (2004): *The interrelationship and effect of culture and risk communication in setting Internet banking security goals,* Proceedings of the 6th international conference on Elctronic commerce, pp. 341-350. WWW - First seen on 20.11.2016 -

https://www.researchgate.net/publication/221550465_The_interrelationship_and_effect_of_culture_and_risk_communication_in_setting_internet_banking_security_goals?el=1_x_8&enrichId=rgreq-306d7af215b2feed742628b3a4ad0945-XXX&enrichSource=Y292ZXJQYWdlOzI4MzMwMjg0OTtBUzozMTkxOTI3NTcxNDU2MDRAMTQ1MzExMjg5MjQzMA==

[11] Kraemer, S., Carayon, P. (2007): Human errors and violations in computer and information security: The viewpoint of network administrators and security specialists, Applied Ergonomics, 38(2), pp. 143-154.
WWW – First sen on 23.11.2016:
https://www.researchgate.net/publication/7001854_Human_errors_and_violations_in_computer_and_information_security_The_viewpoint_of_network_administrators_and_security_specialists

[12] Purser, S. (2004): A practical Guide to Managing Information Security, Artech House.

[13] Straub, D. W., Welke, R. J. (1998): Coping with system risk: security planning models for management decision making, MIS Quarterly, 22(4), pp. 441-469.
WWW – First seen on 22.11.2016:
https://www.researchgate.net/publication/220260271_Coping_With_Systems_Risk_Security_Planning_Models_for_Management_Decision_Making?el=1_x_8&enrichId=rgreq-306d7af215b2feed742628b3a4ad0945-XXX&enrichSource=Y292ZXJQYWdlOzI4MzMwMjg0OTtBUzozMTkxOTI3NTcxNDU2MDRAMTQ1MzExMjg5MjQzMA==

[14] Werlinger. R., Hawkey, K., Beznosov, K.: Human (2008), Organizational and Technical Challenges of Implementating IT Security in Organizations, HAISA '08, Human Aspects of Information Security and Assurance, pp. 35-48.