Linnæus University
Sweden

Degree project

Cyber security Measures in SMEs: a study of IT professionals’ organizational cyber security awareness

Author: Milos Zec
Supervisor: Miranda Kajtazi
Examiner: Christina Mörtberg
Date: 2015-06-08
Course Code: 5IK10E, 30 credits
Subject: Information Systems
Level: Master

Department of Technology

Abstract

With the significant growth and high business dependency on cyber space nowadays, organizations are exposed to dangers such as attacks coming from Internet than ever before. The existence of this actual issue alerts organizations to develop and always use up to date cyber security measures. The current trends indicate that most vulnerable organizations to cyber-attacks are small and medium enterprises (SMEs). According to previous studies the primary reason for this occurrence is SMEs' lack of investment in cyber security. However, this study considers that there are additional contributors for SMEs being more often cyber-attacked than large enterprises. In order to understand these additional contributors a theoretical framework has been developed that considers cyber security from three aspects: organizational, technological and psychological. The organizational aspect presupposes that the ones who create cyber security measures are exposed to unclear and undefined decision processes and rights that lead to system vulnerabilities. The technological aspect focuses on disclosing IT professionals' failure in their organizations to meet foundational technological measures, such as the existence of Internet firewall, logs of system events, existence of hardware and software inventory list, data backup, antivirus software and password rules. Lastly, the psychological aspect, explains how guilt and shame affect counterproductive work behavior and therefore influence the cyber security decisions made by IT professionals. The collected data analysis, that is based on interviews with IT professionals across 6 organizations in Republic of Slovakia, show that cyber-security is yet to be developed among SMEs and it is an issue that must not be taken lightly. Results show that the IT professionals in these organizations need to strengthen and develop their security thinking and to bring their awareness to a higher level, in order to decrease the vulnerability of informational assets among SMEs. It is believed that a perspective on understanding decision-making processes upon the cyber security measures by IT professionals in SMEs may bring a theoretical redirection in the literature, as well as an important feedback to practice.

Keywords: cyber security, SMEs, IT professionals, decision-making, security counter measure

Acknowledgments

I would like to express my sincere gratitude to my thesis supervisor Miranda Kajtazi for her continuous support, patience motivation and knowledge. Her guidance helped me in all the time of research and writing of this thesis. Besides my thesis supervisor, I would like to thank my professor Christina Mörtberg for her insightful comments and encouragement, but also for the hard questions that incented me to widen my research from various perspectives.

I thank my fellow students for the inspiring meetings that helped us learn through the interaction. Many interesting ideas came from our stimulating discussions.

I would like to thank my partner for supporting me spiritually throughout writing this thesis and my life in general.

List of abbreviations

CRM – Content Relationship Management System
CS – Cyber Security
CSIRT - Computer Security Incident Response Team
CWA - Complete awareness
CWB – Counterproductive Work Behavior
EU – European Union
fMRI - Functional Magnetic Resonance Imaging
HUWA - High unawareness
ICT – Information and Communication Technology
IS – Information System
IT – Information Technology
LOE - Lack of empowerment
LOR - Lack of resources
NGL - Negligence
PTC - Partial compliances
PTT - Predominant technological theme
SME – Small and Medium Enterprises
USB - Universal Serial Bus
VOIP – Voice Over Internet Protocol

Table of contents

List of figures

List of tables

1 Introduction

In today's business global environment companies struggle to obtain and keep sustainable competitive advantage on the market that in return requires being object to changes that need to be performed in business (Fiol, 2001; Kotter, 2012; Reed and DeFillippi, 1990). In order to achieve this aim most of business organizations find resort in some kind of information system (IS). However, implementing IS and information technology (IT) demands analyzing many important organizational aspects and "as applications of information systems technology become wider and more complex, companies need more formal planning processes" (McFarlan, McKenney & Pyburn, 1983, p. 156). One of those important organizational aspects certainly represents the field of cyber security (CS). According to Dhillon and Backhouse (2000) business organizations are not anymore valued only by their physical assets but also by networks that are created with other organizations where CS has been gaining a significant growth of its importance and existence. Although there are no manuals for planning and implementing CS organizational measures (Atoum, Otoom, & Amer, 2014), most of business organizations worldwide are using some kinds of tools or policies to cope with security in the cyber space in order to prevent external and internal cyber-attacks into their IS. However, Kindervag et al. (2011) assert that even the enterprises in possession with very mature and advanced cyber security measures cannot avoid each single attack in their system and especially if the attackers are supported by financial and time resources. Despite this, it is very important for all organizations to have developed some cyber security measures for the purpose of decreasing the possibilities of these kinds of attacks, big or small enterprises respectively.

The previous trends showed that in the period from 1982 to 2000 there were 38% of internal security incidents and 31% of external ones but this trend changed from 2000 to 2003 by altering this ratio to 71% of external and 5% of internal incidents (Byres and Lowe, 2004). The recent studies (Gostev, 2012; Raiu, 2012; Watters et al., 2012) show an increasing number of cyber-attacks globally by each year and that this number will continue its growth. Moreover, cyber-criminals are becoming more and more sophisticated in using new methods and tools for cyber-attacks in economic activity areas by targeting businesses as the actual attacking methods are becoming less effective (Gostev, 2012). Despite being aware of the growing trend of cyber-attacks and their sophistication globally, official statistics are not able to identify the exact volume of cyber incidents due to organizations' reluctance to report them (Byres and Lowe, 2004; Choo, 2011). According to Choo (2011) this reluctance comes from three reasons. Firstly, organizations' fear of negative publicity and weakening of competitive advantage, secondly, disbelief of prosecuting the perpetrators and finally, the lack of belief that the cyber-attack was not serious enough for being reported. The term "cyber security" started being mentioned at the beginning of early 1990s (Hansen and Nissenbaum, 2009; Nissenbaum, 2005) and since then its popularity has been growing in today's contemporary business. However, the latest trends emphasize that the majority of cyber-attacks victims are SMEs or to be more specific, the group of firms that employ from 11 to 250 employees (Verizon Risk Team, 2012, p. 11).

It is believed that the situation is not different in Republic of Slovakia. Slovakia has received a significant rise in foreign direct investments (Investment in Slovakia, 2013, pp. 22-23) from big international companies that potentially increases the possibility of cyber-attacks from outside the country and therefore requires careful consideration for creation of effective cyber security measures. The volume of SMEs in Slovakia is 99.9% and the rest are the large enterprises which indicate that economy of this country heavily depends on SMEs (European Commission, 2014). Such a high presence of SMEs in Republic of Slovakia calls for attention and requires to be researched in the field of cyber security measures in SMEs in this country. Additionally, the SMEs are often in supply chain or some kind of partnerships with the large enterprises which makes them being an attractive object of cyber-attacks (Verizon, 2012).

However, although a number of developments have been witnessed in the area of cyber-security, in particular from a practical point of view, organizations develop pre-cautions (Hu, Hart and Cooke, 2007); governments develop new protection agendas (Choo, 2011); home users are more aware of cyber-attacks (Kritzinger, E. and von Solms, S. H., 2010); there are still major holes in cyber security that are SMEs object to experience through their business performance (Julisch, 2013).

1.1 Research Problem

Although, most of SMEs globally have implemented some type of cyber security measures, those measures are in many cases minimal (Byres and Lowe, 2004). However, the minimal cyber security measures are often not sufficient and need to be re-evaluated and updated over the time (Byres and Lowe, 2004; Kindervag et al., 2011) due to cyber threats develop and change rapidly (Choo, 2011). In addition there are many SMEs that persistently invest their resources into cyber security measures, but their ISs are still weak and harmful to cyber-attacks (Julisch, 2013). The aforementioned argumentation represents a challenging situation and brings up a question interest about how these organizations are led by when creating their cyber security measures but their efforts remain unsuccessful. According to Julisch (2013) the answer lies within three aspects, namely psychological, technological and organizational. These three aspects contain four anti-patterns. The first anti pattern is under psychological aspect and is called *"Overreliance on intuition to make security decisions"* (Julish, 2013, p. 2206). The main drawback of this anti-pattern occurs when decision makers make decisions about creating cyber security measures by over relying on their intuition and experience but not on existing statistical trends and impacts of cyber-attacks. The technological aspect implies two anti-patterns. First is called *"Leaving cracks in the security foundation"* and the second *"Overreliance on knowledge versus intelligence"* (Julish, 2013, p. 2206). While the first suggests that IT professionals frequently neglect security basics while creating cyber security measures which "becomes the root cause of many cyber incidents", the second emphasizes IT professionals' overreliance on rather static and universal knowledge of products such as for instance antivirus software and internet firewalls (Julish, 2013, p. 2206). Finally, the organizational aspect presupposes that the ones who create cyber security measures are exposed to unclear and undefined decision processes and rights that lead to system vulnerabilities, which represents the fourth anti-pattern that is called *"Weak security governance"* (Julish, 2013, p. 2207).

In summary, SMEs exposure to minimal cyber security measures which are often insufficient and therefore require re-evaluation, place these organizations into a challenging situation and create an urge to understand what are SMEs led by when creating their cyber security measures.

1.2 Overall Research Aim

For the purpose of formulating the research questions in this study, one overall aim was created. The achievement of this aim helps us later to answer the research questions. The aim of this study is to provide new insights in regard to organizational, technological and psychological aspects of cyber-security measures by looking at how they influence CS in SMEs at an overall organizational level.

In order to address the aim mentioned above comprehensively, the following characteristics will be tackled to better understand the lack of cyber security level among SMEs:

- **Aim - organizational level:** New insights about organizational, technological and psychological aspects in CS and their influence on CS in SMEs

In order to achieve the aim, this study considers foundational cyber security measures from technological aspect, adapted measures from organizational aspect as well as a new psychological aspect that is presented in the text further.

However, the focus of this research is on IT professionals that are in the role of IT staff with responsibility to create cyber security measures by using their decisions for this purpose. The phenomenon of IT staff in this context will be researched within SMEs in a specific country (Republic of Slovakia).

1.2.1 Research Questions

Having considered the previously described research problem and formulated overall aim abovementioned, two research questions were derived. We believe that answering the first question is going to bring us closer to the way of SMEs' dealing with cyber security measures creation in their challenging situation. Therefore, the first question is as follows:

What is the awareness level of IT professionals among SMEs for dealing with cyber security measures creation from technological, organizational and psychological aspects?

The second research question is intended to help us to grasp what are additional possible contributors of SMEs being in this challenging situation when it comes to the field of cyber security. The question is as follows:

What are the reasons that SMEs are more open to cyber-attacks than large enterprises?

1.3 Topic Justification

There are several reasons that motivate this research. First, cyber security adds an extra dimension in difference to information security due to, beside information it also includes humans as targets that can participate in cyber-attacks without their awareness. Beside information and people there is an additional implication of cyber-attacks for the whole society due to cyber security includes ICT infrastructure and devices that can be accessed over computer network (Hathaway et al., 2012). From this reason IT staff needs to be aware of the current cyber technologies (Kumar, Mohan, and Holowczak, 2008) when taking into account what cyber security measures they will choose and employ for protecting information systems.

Second, despite ICT development breakthroughs which led to cyber security trends improve rapidly over the time (Baheti and Gill, 2011), the number of new cyber-attacks is exceeding business organizations abilities to go along and cope with them readily (Symantec Team, 2012). Some of the causes of SMEs' inability to cope with this problem could be that IT staff "expose their firms to unfamiliar risks of which they are unaware, refuse to acknowledge, or are often poorly equipped to manage" (Loch, Carr and Warkentin, 1992, p. 173) and that these organizations are too static and lack of flexibility in their approach for solving these issues (Julisch, 2013).

Third, the recent trends show that cyber-attacks dominate in occurrence in SMEs than in large enterprises (Symantec Team, 2014; Verizon Risk Team, 2012) that greatly harms these organizations financially. According to Ponemon Institute (2011) SMEs suffer much larger costs per capita than large enterprises i.e. $1,088 versus $284. The aforementioned arguments show that SMEs, that represent the back bone for most of the economies worldwide, are endangered and confronted to a significant issue that needs to be tackled at an academic and practical level.

Finally, there are plenty of newspaper articles writing about SMEs inability of tackling cyber security measures or about their ignorance in this domain nowadays that are written and made available very recently (Anderson, 2015; Ashford, 2014; Bradley and Vaizey, 2015; Brooke, 2015; Jee, 2014). This fact indicates that this topic is very popular in the global contemporary business nowadays with an increasing tendency of worldwide interest.

The abovementioned arguments represent a rationale for conducting this research and therefore tackle cyber security features in relation with IT staff and SMEs.

1.4 Research Contribution

There are several contributions of this study. Firstly, it contributes to researchers who are interested to explore on what basis cyber security measures are created by IT professionals in SMEs when it comes to organizational, technological and psychological aspects. Secondly, a potential contribution of this research is to understand if IT staff, while creating cyber security measures, unconsciously contribute to the rising trend of cyber–attacks on SMEs as well as beside low financial investments in security in SMEs (Rodriguez and Martinez, 2013) to reveal additional reasons of SMEs being more attacked in the cyber space than the large enterprises nowadays. Thirdly, due to direct foreign investments of international companies in Slovakia is in its raise, IT professionals of these companies might find this study interesting for exploring how cyber security measures are created in SMEs in this country. Therefore, this information could be useful due to big enterprises usually have SMEs in their supply chain or have some other kind of cooperation. Finally, this study may be of help to SMEs' IT professionals to obtain an insight which can be taken into consideration when making decisions about creating cyber security measures for IS in organization that they work for.

1.5 Scope and Limitations

Due to increasing accessibility of organizations to the Internet and rapid development of ICT, these organizations are becoming vulnerable to varied cyber threats (Jouini, Rabai, and Aissa, 2014). Although cyber security represents a global issue, delimitation of this research will be that it will only examine SMEs on the territory of Slovak Republic, more specifically its second largest city named Kosice (Eastern Europe). According to Borbás (2014) Slovakia's performance within European Union (EU) single market is above EU average due to its geographical location and openness in economic sense which adds an extra dimension to understand decision making about cyber security measures in this country. It also has to be mentioned that this study is time limited due to it is a study and an integral part of a master program in information systems. Also the number of SMEs available to participate in this study is limited.

The scope of this study will specifically focus on how organizational, technological and psychological aspects are brought into consideration when IT staff in SMEs decides about creation of cyber security measures. Further, this study focuses on understanding why IT professionals in SMEs use their particular cyber security measures for organizing and protecting ISs from cyber-attacks in their organization. While defining the research problem it was addressed that Julisch (2013) proposes four cyber security anti-patterns that are covered by psychological, technological and organizational aspects. However, the psychological aspect will not be taken from Julisch (2013) but from Cohen et al. (2011) and Cohen, Panter and Turan (2013) by adapting their theory of counter productive work behavior (CWB) and guilt and shame proneness. The reason for not taking the psychological aspect from Julisch (2013) but from Cohen et al. (2011) and Cohen, Panter and Turan (2013) is supported in the chapter of theoretical framework of this thesis (Ch. 3). Further, two Julisch's (2013) anti-patterns are adapted for this study that are covered by two aspects i.e. technological and organizational. The technological aspect is adapted by being limited only to foundational cyber security measures and Julisch (2013) refers to it as *"Leaving cracks in the security foundation"*, while organizational aspect is limited only to IT staff responsibilities and rights allocation that Julisch (2013, pp. 2206-2207) refers to it as *"Weak security governance"*. Additionally, the organizational aspect will be supplemented by SMEs use of any international, national or EU standards.

It is also important to point out that this study focuses on IT professionals in SMEs who are responsible for security issues. However, due to the small size of sample organizations used for this study, some of their IT professionals are responsible for the whole ICT activities in their company. Despite their overall responsibility of the whole ICT in their organization, we focused only on their responsibility of cyber security.

Further delimitations of this study are that it does not focus on impact assessment and risk evaluation of cyber-attacks, cost analysis and investment decisions about CS strategy implementation. The term "information security" is considered to be an integral part of cyber security which is explained in details in the next chapter. Finally, this study does not tend to define and explore the term "cyber-crime" because "crime" is object to different definitions in different countries' legislations but it focuses on any kinds of attacks and dangers that come from the cyber space.

1.6 The Thesis Structure

There are eight chapters in this master dissertation. The second chapter describes the research motivation of this study being conducted. The third chapter provides the theoretical framework where the choice of theoretical framework is argued and a new theoretical framework is proposed. The research methodology is presented in the fourth chapter where the research strategy is described with the inclusion of the ethical considerations. The chapter five represents the study of empirical findings and in the chapter six data analysis and results are provided. Finally, the discussion is given in the seventh chapter while the chapter eight represents conclusions with the future research included.

2 Research Setting – Concepts and Definitions

In this chapter, a definition and role of SMEs is given, literature review concepts and definitions are provided as well as standards and trends of cyber security are presented. Later on, previous cyber security studies are introduced.

2.1 Small and Medium Enterprises

SMEs are the group of enterprises that need to fulfil two requirements. First of these requirements is the number of employees and second the financial balance. Number of employees must be less than 250 and the financial annual turnover must not exceed 50 million euro (European Commission, 2003). More specifically, in the group of small enterprises belong the enterprises that employ less than 50 employees and with a financial annual turnover less than 10 million euro and in the group of the medium enterprises belong the enterprises that employ less than 250 employees and their financial annual turnover does not exceed 50 million euro (European Commission, 2003). According to Ayyagari, Beck and Demirguc-Kunt (2007) SMEs are a core sector element for fostering the growth of economy, increasing employment and alleviating poverty. On the global level, SMEs perform more than 90 percent of the worldwide business economy (Vives, 2006). Therefore the importance of researching SMEs requires a high attention among researchers due to the fact that this group of enterprises represent a backbone of the global economy.

2.2 Cyber Security History, Concepts and Definitions

Although the cyber security and its concepts change over the time, it is worth saying that it was mentioned first time in Computer Science and Telecommunications Board's report: "*Computers at Risk: Safe Computing in the Information Age"* (CSTB, 1991) which defined this term as: ‘‘protection against unwanted disclosure, modification, or destruction of data in a system and the safeguarding of systems themselves’’ (CSTB, 1991, p. 2). When defining CS, Nissenbaum (2005) refers to three categories. Firstly, protection from dangerous, antisocial and disruptive communications and organizations that come from computer networks, secondly, protection for societal infrastructures such as for example banks, healthcare, communication media and government administration and lastly, protecting ISs from being partially or completely disabled.

However, the term "cyber security" consists of two words, so the word "cyber" needs to be first explained. According to Hunton, (2009) the word "cyber" refers to describing virtual environment which is in a strong association with the Internet. Guariniello and DeLaurentis (2014) to the word "cyber" add the word "space" so they define cyberspace as "the interdependent network of information technology infrastructures and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries". From aforementioned arguments we can understand that the word “cyber” refers to the environment or space that can be “moved through” and accessed by the Internet. On the other hand word “security” can be generally referred to protection from something but Ng, Kankanhalli and Xu, (2009) refer to it as protective technologies. However, for this study the word “security” is referred to as protective measures.

Therefore, from the previous definitions the conclusion can be drawn that the term “cyber security” is referred in this study as protective measures created for the space that can be accessed by the Internet.

When it comes to protective or cyber security measures this study considers how they are created towards organizational, technological and psychological aspects (Julisch, 2013). According to Julisch (2013) the organizational aspect represents decisions about security priorities and roles and in this study it refers to national, international and EU cyber security standards, written cyber security policy and their usage in practice, information value prioritization, system access permissions, cyber-attack measures, cyber-attack analysis and informing stakeholders about cyber-attacks. The technological aspect in this study implies using cyber technology protection tools such as system logs analysis, hardware and software inventory list, system backups, antivirus threat analysis, advanced password rules and internet firewall rules. The psychological aspect considers taking in relation counter productive work behavior with the level of guilt and shame in IT professionals as well as distinguishing guilt from shame proneness.

According to Hathaway et al. (2012) cyber-attacks target computer network over the Internet but it is important to emphasize that the final target beside desktop and laptop computers can be devices controlling traffic lights, elevators, mobile phones, washing machines, televisions (for example in smart homes and cities) and any other assets that can be accessed over computer network. Not a long time ago cyber-attacks could be only performed by computer geniuses called “hackers” but as the technology has been improving, there are tools that can even be purchased online for this purpose and an individual who wants to perform an attack of this kind does not have to have an expert knowledge to be successful in this aim (Potts, 2012).

According to Von Solms and Van Niekerk (2013) it is important to distinguish the terms of information security and cyber security because information security is concerned with information availability, confidentiality and integrity while the term cyber security beside information, encircles ICT infrastructure and humans as part of the society.

2.3 Cyber Security Standards and Trends

2.3.1 Cyber Security Standards

When it comes to international cyber security standards it would be hard not to mention International Organization for Standardization (ISO). This organization has published numerous security standards since 1980s but the most famous publications related to cyber security are marked as ISO 27001 followed by ISO 27002 and ISO 27005 (Infosec and ISO, 2013). These three standards belong to the family of information security management standards and under the general title of *Information technology – Security techniques* (ISO/IEC, 2014). ISO 27001 encompasses the requirements for information security management systems, ISO 27002 relates to code of practice for information security controls and ISO 27005 emphasizes information security risk management (Infosec and ISO, 2013). Although, these three ISO standards more refer to the term of information security, ISO 27032 encompasses cyber security guidance and covers four domains namely *information security, network security, internet security and critical information infrastructure protection* (ISO/IEC, 2012).

European Council adopted a directive to confront cyber-attacks against information systems as a part of Digital agenda for Europe in 2020 initiative (European Commission, 2014). This directive emphasizes the importance of information systems in European Union (EU) and points out that cyber-attacks can be critical to both, private and public sector in EU (European Parliament, 2013). Beside this directive EU also established European cybercrime platform, work with global stakeholders against computer-based security attacks and supports EU wide cyber security preparedness exercises (European Commission, 2013).

According to Rezek et al. (2012, p. 9) there is “no state-sponsored institution in Slovakia specialized exclusively in the whole spectrum of cyber security issues”. They continue by explaining that cyber security is dispersed among Slovak National Accreditation Service, National Security Authority, Ministry of Interior, Ministry of Defense, Ministry of Finance and Personal Data Protection Office. However, the Ministry of Finance of Slovak Republic has established so called *Computer Security Incident Response Team* that is in charge to protect critical information and communication infrastructure (CSIRT, 2009).

It remains being a question how many SMEs in Slovakia really use these or any other cyber security standards to protect their ISs but this question we categorized into organizational aspect of cyber security and asked our IT professionals that we interviewed.

2.3.2 Cyber Security Trends

While reports from 2011 and 2012 showed that SMEs were target to 50% of all cyber-attacks, the report from 2013 shows that this number increased to 61% (Symantec Team, 2014, p. 30). One of the reasons that attacks in the cyber space are concentrated on SMEs in this proportion is that the majority of big organizations have already developed and implemented advanced cyber security measures for their ISs, which is not the case with SMEs so attacking them represents a lower risk for cyber attackers to be revealed in their actions (Verizon Risk Team, 2012, p. 20). According to Verizon Risk Team (2012, p. 17) there is a possibility of SMEs being more often object to cyber-attacks because they are a part of supply chain or are business partners of big enterprises so perpetrators find easier to get to the big organizations through the small ones that are less well protected. This is why some large organizations approach SMEs and offer them help to deal with security in the cyber space (Gostev, 2012).

However, as previously mentioned, despite of awareness for increasing trends of cyber-attacks on the global level, it is not easy to verify their number through the real statistics due to firms' reluctance to report them fearing to compromise themselves either in front of their clients or disbelieving these attacks are enough serious and dangerous (Byres and Lowe, 2004; Choo, 2011).

2.4 Analysis of Previous Cyber Security Research

There have been a lot of studies conducted in cyber security field since this term appeared for the first time. At beginning of the cyber era Loch, Carr and Warkentin (1992) performed a study where they identified four dimensions of IS cyber-attacks. First dimension is distinguished by source of attack which can be internal and external. The second dimension represents sorts of perpetrators which can be human or non-human. The third dimension is classified by intention of attack that could be either accidental or intentional and finally the fourth dimension reflects the consequences of attacks such as information system modification, destruction, disclosure and denial of use. Batsell, Rao and Shankar (2005) developed a framework for detecting new cyber-attacks for information systems by creating measures of real-time detection and a recent study shows that cyber security threats can be categorized according to adversary goals where they can be classified according to attack techniques and attack goals (Jouini, Rabai, and Aissa, 2014). These cyber-attack categorizations and classifications can help IT professionals to improve cyber security measures in their organizations. However, this study adapts and uses Julish's (2013) proposal of why cyber security often fails in organizations despite investing enough resources where technological and organizational aspects are taken into consideration and from Cohen et al. (2011) and Cohen, Panter and Turan (2013) by adapting their theory of counter productive work behavior and guilt and shame proneness.

3 Theoretical framework

This chapter first reviews the current cyber security theoretical frameworks in academic literature and provides the argumentation for the choice of the theoretical framework for this thesis. After that, a theoretical framework is going to be developed for this particular paper and its model will be graphically presented.

3.1 Current theoretical frameworks review

While it is a dilemma to agree what the best decision about security strategy for a company is, there is a common existing problem in practice that organizations often underestimate organizational aspect of security strategy and overemphasize the technological aspect (Kajtazi, 2013). However, as we will see further, some researchers developed theoretical frameworks about cyber security measures creation where sometimes even organizational aspect prevails. Therefore it is important to summarize several important theoretical frameworks proposed previously, which focus on cyber security and represent their aspects.

One of the pioneering cyber security frameworks was represented by Ban and Heng (1995) in their article "*Computer security issues in small and medium-sized enterprises*". They proposed how to create security measures in SMEs and defined them like tasks namely to be: (i) issue a computer security policy statement; (ii) assign responsibilities and accountabilities for security; (iii) educate all staff on security issues; and (iv) establish a simple enforcement plan and a follow-up strategy to monitor security compliance (Ban and Heng, 1995, p. 23). Security policy statement is meant to be conveyed to all organization's employees and also represents legal evidence. Responsibilities and accountabilities assignment implies allocation of corresponding security positions and roles to employees. Staff education on security issues considers raising employees' awareness on security issues in general while the last task focuses on creation of security enforcement plan that should be aligned to company's strategy. Although this particular framework was developed early on when many organizations have not even considered incorporating security strategies in their business agenda, this framework shows us that Ban and Heng (1995) put less weight on the technological aspect and no weight on the psychological aspect as opposed to the organizational aspect.

Dutta and McCrohan (2002) in their article *Management's Role in Information Security in Cyber Economy* provided a theoretical framework that entails three dimensions of a balanced approach of security for organizations. However, they argue that security is in the first place a management but not a technological issue. They propose a framework that consists of three cornerstones. The first cornerstone represents the organizational aspect that implies business structure and environment, politics and culture, operational procedures and education, for example on awareness. Secondly, there is a technological cornerstone that contains internet firewalls, password rules, detection of intrusions and secure servers. Finally, the third cornerstone is called critical infrastructure and encircles critical infrastructure protection which is usually under government's rule which leads us to conclude that organizations do not have control over this last dimension. The main components of critical infrastructure are namely critical infrastructure protection, government industry collaboration and managements' role in critical infrastructure. According to Dutta and McCrohan (2002) security must be left to senior management who must initiate and manage security policies and plans, particularly because if the security function is left with the IT staff, the technological dimension will be overemphasized. It stays unclear how the third dimension i.e. the critical infrastructure protection can be controlled by the senior management as previously mentioned, because it is under government's ownership and maintenance. Additionally, we are of opinion that all the three dimensions need to be in balance and that IT staff also has to be included when decisions are initiated and implemented.

In a case study presented by Tawileh, Hilton and McIntosh (2007), security management process creation for SMEs is conducted by soft systems methodology, which contains four stages. They emphasize the importance of flexibility while defining security goals where the minimum resource requirements are crucial for the success of their approach. Specifically, the stages they propose are goals definition, action identification, implementation and monitoring and review. In the first stage security goals need to be defined by specifying their aims and objectives. The second stage includes action determination that needs to be accomplished in order to achieve the aims and objectives of previous goals defined. In the third stage the determined actions need to be performed and the last stage should encompass changes in business environment that would then allow to know how to be respondent to the changes.

Mattern et al. (2014) propose a quite creative or better said proactive way of thinking when it comes to cyber security measures creation. They support intelligence-driven cyber security that is based on proactive measures of protection and the theoretical framework that they propose encircles three intelligence led operations. The first is proactive security posture that covers defense of network, legal efforts, public relations as well as other operations of business. The second operation is to understand threats of the environment, in a timely and accurate fashion and the last measure is to create decisions that are based on data. Mattern et al. (2014) assert that cyber security measures must be proactive but not defensive i.e. reactive because once when a perpetrator is already in the system it may be too late to react and to avoid a potential damage to organization. They state that in the essence of their framework there is importance to know what is "not known" and in that way to decrease uncertainty for professionals who make decisions which can be achieved through using data i.e. intelligence.

In his proposal for holistic approach of cyber security measures creation and while at the same time explaining why cyber security measures often fail in business organizations, Julisch (2013) identifies three aspects being crucial to consider when creating cyber security measures. As mentioned before these are organizational, technological and psychological aspects. Organizational aspect implies clear distribution of responsibilities and rights for IT staff. The aspect of technology refers of having created firm and steady cyber security measures foundation and that when IT professionals create these measures their knowledge should not rely only on security products databases as it for example is antivirus software database but also to take advantage of their knowledge acquired from other sources. Finally, the psychological aspect asserts not to rely on intuition but on statistical data of cyber-attacks like for example their nature and concentration on certain subjects.

In order to summarize the abovementioned theoretical frameworks, Table 1 is created. The table shows containing aspects of theoretical frameworks that were found while scrutinizing existing cyber security measures creation literature.

Table 1: Summary of cyber security theoretical frameworks and their aspects

	Cyber security aspects			
Author	**Organizational**	**Technological**	**Psychological**	**Critical infrastructure**
Ban and Heng (1995)	Computer security policy; responsibility and accountability assignment; all staff education; establishment of enforce plan and following-up strategy;	X	X	X
Dutta and McCrohan (2002)	Business structure and environment; politics and culture; operational procedures and education;	Internet firewalls; Password rules; detection of intrusion; secure servers;	X	Critical infrastructure protection; government industry collaboration; managements' role in critical infrastructure protection;
Tawileh, Hilton and McIntosh (2007)	Goals definition; action identification; implementation; monitoring and review;	X	X	X
Mattern et al. (2014)	Creating decisions based on data	Proactive security posture (network defense, to public relations, legal efforts, and other	Understanding threats of the environment	X

		business operations)		
Julisch (2013)	Defining clear decisions processes and rights	Security foundation to be well established (existence of Internet firewall, logs of system events, existence of hardware and software inventory list; data backup; existence of antivirus software; existence of password rules;	Over reliance on statistical and other data but not on intuition when making decisions	X

As we can see in the Table 1, it shows the summary of theoretical frameworks that are created in order to help decision making when creating cyber security measures. Organizational aspect is taken onto consideration in each theoretical framework and followed by technological aspect in its frequency. The psychological aspect is offered by Mattern et al. (2014) and Julisch (2013) while the aspect of critical infrastructure is proposed only by Dutta and McCrohan (2002). However, the aspect of critical infrastructure is not clear how to use due to organizations do not have control over it.

3.2 Argumentation for the Choice of Theoretical Framework

As we could see Ban and Heng (1995) focus on organizational aspect by proposing creation of security policy statement, responsibilities and accountabilities allocation as well as to create enforcement plan. Moreover, by proposing all organization staff education they also focus on socio-organizational aspect and we could say that the technological aspect is neglected. This is not the case with Dutta and McCrohan (2002) who strongly argue that cyber security is primarily organizational i.e. management issue due to if it is left to IT professionals, they would put more weight on technological aspect. In addition, beside organizational and technological aspects that they propose, they also add the third, as they call, cornerstone of critical infrastructure. Although Dutta and McCrohan (2002) admit that management does not have any control over the critical infrastructure, they assert that it is management's responsibility to balance these three dimensions which brings up quite a paradoxical situation. Similarly to Ban and Heng (1995) and their organizational approach of cyber security measures creation, Tawileh, Hilton and McIntosh (2007) also support more organizational than technological or any other theoretical aspect in this domain. Actually, their framework reminds us on four management functions i.e. planning, organization, leading and controlling (Robbins, DeCenzo, and Gao, 2007). They propose goals definition as the first step (planning), then action identification (organizing), afterwards implementation (leading) and finally monitoring and review (controlling). As we saw, Mattern et al. (2014) present a theoretical framework about cyber security measures creation that operates within the field of intelligence-driven cyber security and we know that decisions based on intelligence represent predicting future by analysis of data (Turban et al., 2010). Although the last measure, i.e. creating decisions based on data, is similar to Julisch's (2013) psychological aspect, Mattern et al. (2014) do not define their framework strictly but leave some gaps for readers to understand by guessing. Such an example is where they present their first operation which is proactive security posture where they number the defense of network, legal efforts, public relations as well as other operations of business but do not specify exactly which business operations they are. Finally, Julisch (2013) covers and explains three aspects that he proposes in his theoretical framework. It is a very good point to notice that when it comes to technological aspect, certain organizations invest their resources but some parts of security foundations are neglected and this directly leads to security issues. Organizational aspect must not be neglected and clear distribution of responsibilities for IT professionals such as for example, system permissions must be defined and distributed necessarily. Moreover, in his study, Julisch (2013) includes the psychological aspect where he argues that cyber security decisions should not be made intuitively but they should be based on existing data. However, although Julisch (2013) clearly describes how to measure technological and organizational aspects in his study, it remains unclear how to measure the psychological aspect i.e. if IT professionals, while making decisions about cyber security creation are led by intuition or statistical data or even both, respectively.

The fact that Julisch (2013) does not pay less attention neither to organizational nor technological or psychological aspect and that he does not overemphasize any of them, is one of the reasons why this framework is the key for this study, which intends to highlight the value of all of the three aspects in creating security measures by IT professionals.

The second reason is, that Julisch (2013), after describing each aspect and identifies problems and causes of weak cyber security in organizations, also proposes how to overcome these specific problems which is not the case with the frameworks mentioned above. Being more specific, at the end of technological and organizational aspects, Julisch (2013) provides comprehensive tasks that need to be accomplished in order to close cyber security gaps which he expresses by writing in imperative grammatical mood. In his study, after presenting the psychological aspect, he does not exactly specify the tasks that need to be done but explains from a general point of view what to pay attention about and describes the most frequent cases of cyber security omissions that are also based on his personal experience.

The third reason for not taking any of frameworks mentioned above is that, as we could see Ban and Heng (1995) and Tawileh, Hilton and McIntosh (2007) mostly focus on organizational aspect where Tawileh, Hilton and McIntosh (2007) base their framework on four management functions. Further, Dutta and McCrohan (2002) advocate the idea that cyber security is primarily management (organizational) issue and assert the third aspect to be critical infrastructure over which neither organizations and therefore nor IT professionals have any influence. Finally, although Mattern et al. (2014) build their theoretical framework upon foundations of intelligence and well define their technological aspect, they fail to precisely identify their proposed dimension for operation of proactive security posture.

Despite the advantages of Julisch's (2013) organizational and technological aspects, it must be criticized that he does not clearly describe how to measure the psychological aspect that is based on intuition. In this study, if we decided to measure the psychological aspect based on intuition then the whole study would change methodologically because, the intuition, would require to be observed in a longitudinal study rather than what this study proposes. By other words, the psychological aspect would need in-depth analyses and complex methods to derive the desired results. One of these analyses is conducted by Schneier (2008) where, in order to explore psychology of security, he uses the field of neuroscience which helps intuition to be understood by exploring parts of the brain such as neocortex and amygdala that are brought in relation with thinking emotionally and intellectually. Studies that would also take this kind of psychological factor into consideration could, for instance, conduct an experiment with functional magnetic resonance imaging (fMRI) that would certainly lead to better understanding of decisions based on intuition and personal experience (Krawczyk et al., 2013; Sahito and Slany, 2012).

While this study does not propose to make such complex measurements on the psychological aspect, as a reflection to the arguments developed above, another perspective of how the psychological aspect could be analyzed in this study is described below.

3.3 Bringing a New Psychological Perspective

In their attempt to understand what drives counterproductive work behavior (CWB) among employees in organizations, Cohen, Panter, and Turan, (2013) investigated the relationships between CWB and guilt and shame proneness. Fox, and Spector (2005) and Spector, Bauer, and Fox, (2010) define CWB as behavior that is counterproductive to organizations in a way that harm employees and organizations per se. As Cohen, Panter, and Turan, (2013) identify, this kind of behavior involves intentionally doing work incorrectly, stealing employer's assets from work or writing more working hours than it was worked or abusing colleagues or intentionally wasting employer's supplies or materials. From this we can grasp that CWB is not a single behavior, but it consists of a set of behaviors. Additionally, in case of IT professionals and their responsibilities about creating cyber security measures, it would be a huge risk and potential waste of firm's resources to have a person in this role that is prone to CWB.

According to Berry, Carpenter and Barratt (2012) CWB can be measured in two ways; by observation and self-reports. However, self-reports are considered more measurement trustworthy due to employees have more knowledge about their job responsibilities and their own behavior but to achieve a full effect participants must be guaranteed complete anonymity (Cohen, Panter, and Turan, 2013).

According to Cohen et al. (2011) high level of guilt and shame proneness are directly proportional to each other but indirectly proportional with unethical making of decisions. They assert that guilt and shame proneness are not emotional state but rather an emotional trait and prior studies proved that people with higher guilt and shame proneness less likely engage in the set of behavioral activities that indicate CWB. As Cohen, Panter, and Turan, (2013, p. 6) put:

"… for guilt-prone individuals public surveillance should not be required to prevent moral transgressions; instead, their conscience should guide them in their decision making." (*Cohen, Panter, and Turan, 2013, p. 6).*

In their study, Cohen, Panter, and Turan, (2013) found that it would be wise that while making hiring decisions, employers consider guilt and shame proneness.

They measured guilt and shame proneness by conducting survey where asked their participants to imagine themselves in different kind of specific situations. Some of the questions that Cohen, Panter, and Turan, (2013) had in their survey they put as:

"After realizing you have received too much change at a store, you decide to keep it because the salesclerk doesn't notice. What is the likelihood that you would feel uncomfortable about keeping the money?" (*Cohen, Panter, and Turan, 2013, pp. 9-10).*

"At a coworker's housewarming party, you spill red wine on their new cream-colored carpet. You cover the stain with a chair so that nobody notices your mess. What is the likelihood that you would feel that the way you acted was pathetic?" (Cohen, Panter, and Turan, 2013, p. 10).

"You lie to people but they never find out about it. What is the likelihood that you would feel terrible about the lies you told?" (Cohen, Panter, and Turan, 2013, p. 10).

Although most of people use "guilt" and "shame" terms interchangeably, these words differ in their meaning. Cohen et al. (2011) explain this difference by describing two schools of thought i.e. public-private distinction and the self-behavior distinction. The public-private distinction implies that transgressions that are committed publically provoke feeling of shame but the ones that are committed privately (not in public), provoke feelings of guilt. On the other hand, in the self-behavior distinction school of thought shame focuses on one’s self where that person creates self-impression such as “I am a bad person”, while guilt emphasizes one’s behavior by creating a statement such as “I did a bad thing”. In their study Cohen et al. (2011, p. 51) found that “guilt proneness is more adaptive than shame proneness in terms of psychological functioning”. This can be explained by realizing that persons with high level of guilt proneness after making a mistake or failure are aware of that and they are motivated to make correction and to apologize while people with high level of shame proneness tend to run away and avoid coping with consequences (Tangney and Dearing, 2002). Despite these differences, as mentioned above, people with higher level of guilt and shame proneness are less likely to interfere in counter productive work behavior.

Having in consideration that the psychological aspect can be studied from a perspective other than the intuition as originally proposed in Julisch (2013), taking a guilt and shame proneness perspective would allow us to develop a new understanding on why and how IT professionals take particular decisions when choosing security measures. The latter also informs us about how IT professionals would react after they have taken decisions to incorporate security measures in their organization, which they find that it may have not been the best solution. Thus, based on these arguments it is considered that guilt and shame proneness can be used as a part of theoretical framework to understand the psychological aspect of cyber security. More specifically, as we can understand, guilt and shame proneness represents an emotional trait that can affect IT professionals’ during or post decisions making after they for example realize that a wrong decision had been made while deciding about their cyber security measures.

Having in consideration abovementioned, Figure 1 is created in order to depict the model that represents the interplay of three cyber security aspects that is proposed to be brought into this field.

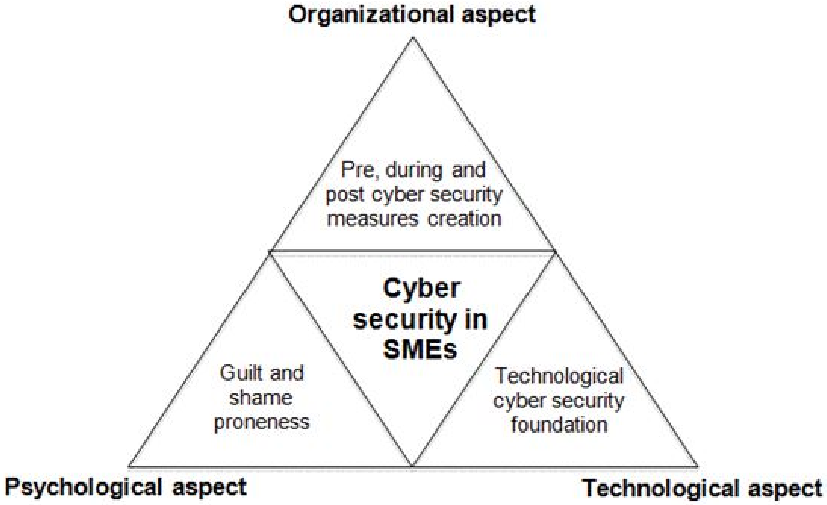
Organizational aspect
Pre, during and post cyber security measures creation
Cyber security in SMEs
Guilt and shame proneness
Technological cyber security foundation
Psychological aspect
Technological aspect

Figure 1: Cyber security aspects in SMEs

3.4 Developing the Theoretical Framework

Here we develop a theoretical framework based on two theoretical perspectives. One by Julisch (2013) by adapting his organizational and technological aspects and the other by Cohen et al. (2011) and Cohen, Panter and Turan (2013) by adapting their guilt and shame proneness i.e. psychological aspect. This blended theoretical framework is meant to help us to understand IT professionals' decission making on cyber security measures in their organizations.

3.4.1 Organizational Aspect

When making decisions about cyber security measures in organizations it is not sufficient to be limited only to technological but it is also important to develop and include organizational domain (Julisch 2013; Kajtazi 2013). It needs to be emphasized that weak governance creates gaps that leave organizations harmful to cyber-attacks (Julisch 2013). According to Weill and Ross (2005, p. 64) IT governance specifies "the decision rights and accountability framework to encourage desirable behavior in using IT". However, Julisch (2013) asserts that huge numbers of organizations do not clearly define responsibilities, rights and roles in a case of a cyber-attack occurrence in their IS.

In order to adapt and present Julisch's (2013) organizational aspect in a comprehensive manner we decided to divide organizational cyber security decision creation into three phases. The first phase represents *pre-cyber-attack organizational decision making*, the second *during-cyber-attack organizational decision making* and the third *post-cyber-attack organizational decision making.*

3.4.1.1 Pre-cyber-attack Organizational Decision Making

Under *pre-cyber-attack organizational decision making* we consider all the measures that are or could be created in order to prevent cyber-attacks. Here at the first place we would like to see if any of national, EU or international cyber security standards are adopted and used in particular organization. As mentioned and described before, these standards exist and could represent a useful security guide for IT professionals even if only partly adopted.

Although cyber security standards exist, Julisch (2013) claims that there is not a unique optimal way to deal with organizing cyber security for every organization due to each organization is object to distinct business strategy, culture and organizational structure. In order to define these specific organizational needs, cyber security policy can be created. According to Doherty and Fulford, (2006, p. 2), "information security policy provides a framework to ensure that systems are developed and operated in a secure manner".

However, despite security policy creation is an essential point in organizational cyber security, it should be ensured that it is used in the practice (Bulgurcu, Cavusoglu and Benbasat, 2010).

Governing security priorities is another important factor of organizational aspect of cyber security due to each asset in an IS has different organizational value and therefore priority which identification must be evaluated by certain processes (Julisch, 2013). Julisch (2013) adds that based on IS asset priority there must be set up system access permissions (for example, e-mail accounts, share drives) and there are usually disagreements about whose responsibility is to decide about these permissions i.e. company's management or IT professionals.

3.4.1.2 During-cyber-attack Organizational Decision Making

The consideration that is taken under this phase is the organizational decision about who and how to act in the real time of a cyber-attack. In order to specify what needs to be done in the case of such an attack organizational responsibilities and accountabilities must be made (Julisch, 2013). Some of examples of these decisions could be the roles and accountabilities such as whether the server or only Internet connection should be shut down during the attack and if yes, by who.

3.4.1.3 Post-cyber-attack Organizational Decision Making

The last phase represents the post organizational activities after a cyber-attack has occurred. Going further with organizational aspect Julisch (2013) addresses what responsibilities need to be taken after cyber-attack has occurred. Here he emphasizes the importance of deciding if the attack was an isolated case or it was a large-scale attack that is directly meant to target the current organization and how the impact of the attack that happened is assessed in order to obtain this information.

Finally, it is also important that after the attack has passed someone needs to be informed about it (for example clients, stakeholders, national cyber security body) and there should be a person who has that role (Julisch, 2013).

These are the three phases that comprise organizational cyber security aspect and decision making in organizations. Julisch (2013) does not present proposed organizational aspect in three phases but we did it in order to present this aspect more comprehensively and more easily to be understood.

3.4.2 Technological Aspect

Empirical evidence shows that most of organizations that were victims of cyber-attacks were not fully familiar with the basics of cyber security measures and that "it is still common to find organizations that lack fundamental security controls" (Julisch, 2013, p. 2206). Further, according to Verizon Risk Team annual report (2012) 80% of cyber-attacks were performed successfully only because the foundational security measures were not met in those organizations.

In his survey about computer crime and security, Richardson (2008) finds that only 50% of responders track logs in their management system. Lack of monitoring system logs in organizations represents a huge factor for successful cyber-attacks (Verizon Risk Team, 2012). From aforementioned facts it can be concluded that tracking and monitoring system logs represents one of technological cyber security foundations for ISs in organizations. Moreover, Julisch (2013) emphasizes that it is not sufficient only to track and monitor the system logs but they also need to be analyzed for successful cyber-attacks prevention.

Organizations often do not have complete and correct inventory list of their hardware and software assets that results with not knowing which devices and software are authorized in their IS (Julisch, 2013). This directly leads to firms' inability to identify software or devices that should not be authorized in their cyber space Montesino and Fenz (2011) and could be perpetrator's tools for performing a cyber-attack.

Siegel, Sagalow and Serritella (2002, p. 36) provide an extensive guidance for data backup and archival for ISs where they stress that "backups should be made regularly – as often as daily depending on the requirements of the business – and should be stored off-site to prevent loss or damage". Despite system backup is good old and proven practice in the "computer world" Julisch (2013) points out that many organizations either have incomplete backups or they are slow for retrieval.

Vulnerability scanning of ISs is a good practice to mitigate cyber-attacks but it is useless without ability of results evaluation (Julisch, 2013). Many cyber-attacks on SMEs represent so called "opportunistic attacks" that is not so difficult to prevent by using antivirus software (Maisey, 2014). Unlike targeted cyber-attacks, opportunistic cyber-attacks require much less sophistication of perpetrators (Kshetri, 2005) due to they are random and without any specific aim or purpose.

Using passwords is a well-known technique for protection in the cyber space however there are two factors addressed by Sommestad, Ekstedt and Johnson (2009). These two factors are "the strength of passwords, and if there is a limitation to the number of attempts that an attacker can try passwords using standard logon functionality" (Sommestad, Ekstedt and Johnson, 2009, p. 4). There is a frequent problem in organizations that represents intrusions thankfully to shared, default or weak passwords (Julisch, 2013) so specific character password rules as well as changing passwords over the time is a good practice that adds to cyber security foundation.

Finally, in order to prevent perpetrators' cyber-attacks organizations must install and implement internet firewall (Dimopoulos et al., 2004). However, only existence of an internet firewall does not mean automatically that the system is safe (Lopes and Oliveira, 2014). Company assets in the cyber space must be classified by its priority and accordingly internet firewall rules applied (Julisch, 2013). Otherwise the existence of the full cyber security foundation is a mere pretext.

Technological aspect of cyber security is a broad field but as we could see this study focuses on cyber security foundations such as existence of internet firewall, logs of system events, existence of hardware and software inventory list, data backup, antivirus software and password rules. More specifically, the technological aspect of cyber security foundation is applied in order to understand how IT professionals in SMEs decide to employ these cyber security measures and why they are included or some of them are not included for protection of ISs in their organization.

3.4.3 Psychological Aspect

As mentioned before there are two ways of measuring CWB i.e. by self-reports and observation (Berry, Carpenter and Barratt, 2012), where self-reports are considered to derive more reliable results due to only an employee knows the best what his/her own behavior is and what the work responsibilities require at the particular job position (Cohen, Panter, and Turan, 2013). This is the reason why interviews are chosen in order to elicit the level of shame and guilt proneness among IT professionals. Additionally, the condition of self-reports implies a full confidentiality of respondents.

Further, according to abovementioned, it is advisable for employers to take in consideration the level of guilt and shame proneness due to people with the higher level of these psychological traits are less likely to interfere with immoral and unethical actions that in short or long run would inevitably lead to CWB (Cohen, Panter and Turan, 2013). Therefore, we conclude that in the case of low level of guilt and shame proneness in IT professionals it could be risky business for organizations as during and post creation of cyber security measures some security gaps can stay open and not reported to the management. This is why, in this study we first establish the general level of guilt and shame proneness of IT staff in SMEs in Slovakia by asking first set of three more general questions in order to elicit interviewees' answers. Second, we ask them the second set of three questions related to specific area of during and post cyber security measures creation in order to understand whether these persons are more in possession of guilt or shame proneness.

The first set of questions provides us with a general level of both, guilt and shame proneness that helps us to understand whether guilt and shame proneness indicate unethical behavior in regard to their decision-making about their security measures placed in their organization. The second set of questions helps us to distinguish the guilt and shame proneness of IT staff which is meant to give us the insight whether IT professionals are likely to be prone to guilt, which would indicate they are likely to accept the mistake, apologize and correct it, or they are more prone to shame that indicates their affinity to “run away” from problem i.e. not to face the consequences and not to apply necessary corrections. In other words, people with higher value of shame proneness are more able to hide mistakes.

In overall we believe that the answers on these two sets of questions will provide us with answer if psychological traits such as guilt and shame proneness add to the fact of why SMEs are being more cyber-attacked than large enterprises.

The interview questions can be found in the interview guide in the Appendix 1 of this thesis.

4 Research Methodology

In this section, interpretive philosophical approach, qualitative research method and research strategy are introduced. Afterwards, how the data was collected, interview participants selected and how the data would be analyzed are presented. Lastly, there is a description of this research validity and reliability, ethical considerations and finally the research methodology was criticized.

4.1 Interpretive Philosophical Approach and Qualitative Research Method

There is a raising interest among researchers to use interpretive philosophical approach when it comes to researching information systems (Myers and Avison, 2002). Interpretive philosophical assumption tempts to provide understanding of human interactions and experience which represents a social phenomenon where "the researcher seeks to establish the meaning of a phenomenon from the view of participants" (Creswell, 2009, p. 22). According to Walsham (2006) interpretive research presents people as social beings and has subjective point of view that concerns the reality. Therefore this study follows interpretivism as a philosophical underpinning by tending to understand making decisions of creating cyber security measures of IT professionals when taking into consideration technological, organizational and philosophical perspectives.

Considering the purpose of this study, the qualitative research method drives the analysis and results in this thesis. Myers and Avison (2002) assert that qualitative research method predominates in social science in order to understand complex cultural and social phenomena where interviews and observations represent some of the typical types of data sampling, where the whole research must be taken into consideration such as potential limitations, targeted objectives as well as available time and resources. According to Creswell (2009, p. 20), "qualitative research is fundamentally interpretive". Creswell (2009) explains that data interpretations are made by the researcher, which includes description development of a setting or individual where data are analyzed for categories or themes. According to Lichtman (2013) the purpose of qualitative research is to understand "the whole" (feelings and ideas) of interviewed participants in natural setting.

Due to aforementioned arguments, this study uses qualitative research method in order to achieve its overall aim in regard to technological, organizational and philosophical aspects when IT professionals make decisions about creating cyber security measures in SMEs in Republic of Slovakia. In addition, this study is therefore driven by the interpretive paradigm where the social reality is a network of assumptions (Dhillon and Backhouse, 2001).

4.2 Research Strategy

There are different types of qualitative research strategies that need to be carefully considered in relation of the nature of the study. According to Creswell (2009) some of these strategies are grounded theory, phenomenological research, ethnography, action research and narrative research. However, empirical research is taken into consideration when the real life phenomena is being investigated for acquiring knowledge of complex problems that need to be understood (Yin, 2009). The complexity of the problem introduced in this study comes from the possibility of different cyber security measures creation in SMEs where IT professionals answer interview questions based on their experience and knowledge that was gained from their everyday work setting.

This study focuses on six different SMEs and their different contexts where experience and knowledge of IT participants let us understand why they make certain choices about the security measures that are in place in their organizations. For a detailed overview of the data collection method, the section below gives a detailed introduction.

4.3 Data Collection

In this study, interviews are used as a method for data collection. Interviews mostly represent studies of an interpretive nature by accessing participants' interpretations in the research field (Walsham, 2006). In one of his papers, Walsham points out the importance of time management while conducting interviews (Walsham, 1995). While conducting interviews for this study we could experience what Walsham meant under the good time management. Firstly, most of participants, i.e. the IT professionals, were very busy with their everyday work activities and had a tight schedule so the given interview time had to be utilized very well. Secondly, at interview initiation, each IT professional was quite suspicious about this study's purpose despite when scheduling the interviews it was explained that their and the company's names would not be revealed and that the interview was completely anonymous. These two reasons were warnings to plan the time of interviews carefully. So once the interview has started there was a time needed to reassure the interviewee about the purpose and confidentiality (Walsam, 2006). This was done by explaining the study's purpose, aims, methodology and ethical considerations and this took for about five to seven minutes of each interview in order to make interviewees feel relaxed and obtain their trust.

According to Bernard (1988) semi-structured interviews are best to use when researcher knows that there will not be another chance to arrange additional time with the interviewee. As mentioned above, interviewed participants had very tight work schedule at work and hardly found time for the interviews so each interview was a unique opportunity of using their time. For semi-structured interviews, interviewer prepares interview questions in advance which is referred to as "interview guide" (Cohen and Crabtree, 2006, p. 1). According to Cohen and Crabtree (2006), ahead preparation is one of the reasons of why semi-structured interviews are favorable to be used by interviewers. Another benefit that is brought by semi-structured interviews is that they "also allow informants the freedom to express their views in their own terms" (Cohen and Crabtree, 2006, p. 1). For a detailed overview, the interview guide of this study is enclosed in the Appendix.

For the purpose of this study, the interviews were conducted in formal mode and were type recorded. Specifically, when interviews took place, as introduced earlier the researcher dedicated five to seven minutes to describe and explain the study purpose, aims, methodology and ethical considerations and then the interviewee was given the interview guide to read it through. In some cases, IT professionals asked the interviewer to send them the interview guide in advance in order to read questions ahead, which was also a practice in this study to accommodate the interviewees' needs. After the interviewee read through the interview guide, the type recording started. Type recording represents very practical way to conduct interviews because it is quite difficult for a researcher "to focus on conducting an interview and jotting notes" (Cohen and Crabtree, 2006, p. 1).

The interview guide consists from introductory text and four types of questions. Introductory words addressed the interviewees by thanking for their participation, explaining the ethical considerations and describing types of the questions used. First sort of questions are of general type and therefore were not analyzed but only presented in the chapter of empirical findings (Ch. 5.1). They are meant to elicit some answers such as general company details (number of employees, business core that the company operates within and where the company conducts its business), number of responsible people for cyber security, company's dependency of cyber space and IT professional opinion of cyber security importance for the particular firm. The second type of questions represents organizational aspect which is divided into pre, during and after cyber-attack. The *pre-cyber-attack* covers the period of decision making while cyber security measures are created by IT professionals. *During-cyber-attack* is the moment when the attack is happening. And finally the *post-cyber-attack* questions cover the actions of IT professionals after a cyber-attack happened. The third type of questions contains specific questions of cyber security from technological aspect. They cover specific questions about system logs, inventory list of hardware and software, system backups, antivirus software and firewalls and system protection passwords. The technological questions are meant to understand if the particular organizations have created foundational level of cyber security. Lastly the fourth type of questions represents psychological perspective and is divided into two sets of questions. The first part has intention to measure a general level of guilt and shame proneness of IT professionals while the second set of questions is meant to find and distinguish whether it is the guilt or the shame that is more present with IT professionals.

There were six interviews with six IT professionals from six different SMEs in Republic of Slovakia. The interviews took from 35 to 50 minutes. The main reason for some interviews took longer was that some interviewees were not fluent in English because their mother tongue was Slovak language so they spoke slower. Three interviews took place at the company's premises while the other three were taken by using online social media software such as Skype and Viber. Each interview was initiated in a more formal manner because it was noticeable that participants were a bit reserved. However, after it was carefully explained that the interview was completely anonymous and as the questions started being asked, the interviewees gradually relaxed and opened themselves. This is also the reason why some of interviews took even fifty minutes.

4.3.1 Interview participants selection

One of the critical parts in data collection that contributes to understand a research theoretical framework is data selection (Bernard, 2002). Therefore, it was carefully considered how participants for this study would be selected. The selection of the interview participants was an extensive process and it was performed by the help of Internet. While browsing the Internet, the search criteria was to find the list of small and medium enterprises in Kosice, Slovakia. Once when the SMEs' list was found, the companies were randomly chosen and their website would be visited in order to find more about each organization. According to Creswell (2012, p. 206) the intent of qualitative research "is not to generalize to a population, but to develop an in-depth exploration of a central phenomenon". This is why, although the companies were chosen from the list randomly, the purpose of the sampling was to find IT professionals who would participate in this study interviews. Being more specific, when it is referred to sampling of IT professionals in this study, it is very important to note that the main aim was to find IT professionals who are responsible for cyber security in SMEs. Therefore, the target IT professional could be a person who is responsible only for cyber security or a person who is responsible for the whole ICT in a particular SME including the cyber security.

Once the companies were selected, they were contacted by e-mail where the researcher introduced himself and explained the purpose of contacting the company. Some of companies did not reply, some of them replied with negative answers but some of them were interested to participate in this study. If a particular company expressed the interest of being a participant, the researcher would arrange a live meeting with the potential company's contact person and the IT professional. At the meeting it would be talked about the research details and some of the potential participants asked to be given the interview guide before they would accept to participate in the study.

If the company would accept its participation, the consent form was sent to the firm by e-mail and asked kindly to print it out, sign it and send it back by e-mail. Once when the consent form was signed by the company and received, the company's contact person would be contacted by phone and asked when and what time the interview would be arranged and if it would took place at the company’s premises or via social media software.

This was the standard procedure when all of the six interview participants were selected for this study.

4.4 Data Analysis Description

Although there are sources about qualitative research in abundance, the vast majority of these texts mostly do not describe in exact details how to perform data analysis or only contain one meagre chapter about it (Berg, 2004; Creswell, 2007; Shank, 2002). According to Leech and Onwuegbuzie (2007, p. 563) a lot of leading textbooks about qualitative research method “also do not provide explicit details as to how to analyze qualitative data”. However, in their article *“An Array of Qualitative Data Analysis Tools: A Call for Data Analysis Triangulation”*, Leech and Onwuegbuzie (2007) describe qualitative data analysis tools such as keywords in context, taxonomic analysis, classical content analysis, constant comparison analysis, domain analysis, componential analysis and word count. Keywords in context data analysis is suitable to use when collected data seems uninteresting or less rich in information by identifying keywords and then making list of the words that exist before and after those keywords (Leech and Onwuegbuzie, 2007). Domain analysis is found by Spradley (1979) and he suggested it to be used for pure ethnographic studies but Leech and Onwuegbuzie (2007) argue that domain analysis can be also used for understanding relationships between concepts. Taxonomic analysis represents the second step of domain analysis and it “helps the researcher to understand how participants are using specific words” (Leech and Onwuegbuzie, 2007, p. 572). Componential analysis also can be used as the second step of domain analysis but opposite to taxonomic analysis, it is used to understand how specific words are used and to understand the relationships among these words (Leech and Onwuegbuzie, 2007; Spradley, 1979). Classical content analysis is very frequently used for qualitative data analysis and it is done through looking for “which might be the most important concepts for the interviewee” (Leech and Onwuegbuzie, 2007, p.569). According to Leech and Onwuegbuzie (2007) word count is data analysis where person’s perspective can be understood by counting her words. They further refer to Carley (1993) by concluding that “underlying assumption with word counts is that more important and significant words for the person will be used more often” (Leech and Onwuegbuzie, 2007, p. 568).

Lichtman (2013) asserts that qualitative data analysis represents a practical dilemma and that there is only general information of how to perform it. However, Lichtman (2013) continues that although qualitative data analysis is a challenge without clear rules, it can be practiced, as she suggests, by using coding process. Coding process starts by organizing and categorizing for example, interview text data which is continued by analyzing and categorization this data into codes (Lichtman, 2013). Coding analysis is also referred to as *"Constant comparison analysis"*, it is most widely used in the analysis of qualitative data and it is created by Glaser and Strauss in 1967 (Leech and Onwuegbuzie, 2007, p. 565). Leech and Onwuegbuzie (2007, p. 565) describe coding analysis process as follows:

"… the researcher first reads through the entire set of data (this also could be a subset of the data). After doing so, the researcher chunks the data into smaller meaningful parts. Then, the researcher labels each chunk with a descriptive title or a "code." The researcher takes pains to compare each new chunk of data with previous codes, so similar chunks will be labeled with the same code. After all the data have been coded, the codes are grouped by similarity, and a theme is identified and documented based on each grouping" (Leech and Onwuegbuzie, 2007, p. 565).

Lichtman (2013) believes that the biggest success of coding analysis comes from systematic approach where personal discipline and creativity come into the force. Although in qualitative data analysis it can be searched for similarities, Kaufmann (2011) sees this process as rather looking for differences. All in all, qualitative data analysis represents a non-standardized process which is only limited by researcher's creativity and technology availability (Lichtman, 2013).

Therefore, coding analysis is chosen to be used for this study. All the interviews were recorded with participants' permission and transcribed into written form. For the purpose of this study these data were read and subcategorized into meaningful parts which is in this thesis referred to as themes. As Lichtman (2013) suggests, the data analysis began at the same time when the data collection started. Firstly each subcategory of data was compared and grouped into similar groups (looking for similarities) and secondly data differences were categorized. Later on, themes were identified in these groups of categories and were compared constantly and iteratively. In the part of data analysis interviewees' answers were analyzed and thereafter the themes emerged were analyzed according to the details of cyber security aspects requirements.

The findings that were considered most important were similarities and differences among the answers and themes emerged and it was spotted that IT professionals from two companies had quite similar answers while the other four were quite different which is referred in data analysis part of this study.

4.5 Research Validity and Reliability

There is a great importance for researchers to represent valid and reliable results in their research. That is also the case in this study when the data were collected from IT professionals who are responsible for making decisions about creating cyber security measures in SMEs. The collected data are either recorded or noted on the paper through the interviews with the participants. If they were recorded, they were transcribed in the written form. These data are presented truthfully and without any sophistry. Moreover, during the data analysis, the themes emerged were double checked and compared in a constant and iterative manner in order to avoid inconsistencies and deviations (Creswell, 2009). Additionally, in order to avoid inconsistencies and deviations, participant were asked to go through the interview guide once when interview was finished and to add something if they considered it important or to correct themselves if they think they did not understand some question well. This was done for the purpose of ensuring the collected data validity (Creswell, 2009).

Additionally, there was a need to be in connection with companies' owners where it was needed a patient and very careful approach due to their initial distrust. It required careful and detailed explanation and going through the consent form in details in order to gain trustful, supportive attitude and acceptance of the company's owners. This attitude was welcomed for this study due to necessary cooperation with interviewees and was a real award to the researcher due to extensive time and effort spent by explaining that participation in this study would not harm either the company's employees or the company per se.

The interview recordings were performed by researcher's laptop computer. However, after the interview was conducted, the interview recordings were copied on a universal serial bus drive (USB) in order to be backed up. Once when interviewer arrived at his home, the data were immediately transcribed to the paper. After the data were available on the paper, the recordings were deleted from the USB and researcher's laptop.

4.6 Ethical Considerations

This study is conducted by taking into account ethical considerations for participants' and business organizations' privacy and confidentiality. This primarily means that the participants' identities and all the companies' names stay anonymous and are preserved in a safe place and never are revealed by any circumstances. In order to assure the participants about this intention, the consent form was sent to them and the researcher went through all of the details of the consent form if it was needed (please see Appendix 2). Before any data collection all the participants were clearly presented about the overall aim and purpose of this study as well as why their participation was important for this study. Upon the consent form was read by a participant and the details were explained, they would be clear with that they can withdraw whenever they wished during the research process.

According to Hart (2005) it is of a high importance to have respect to others. Therefore, all the participants were treated by respect and honesty during their participation and they were asked for the interviews being recorded. If they had refused interview recording, notes would have been taken in a notebook. After the interviews, all the participants were sent an appreciation letter in order to be thanked for their time and effort in this study.

According to (Mörtberg et al., 2010, p. 106) it is very important “to be able to use intuition, judgement, and to be able to communicate with the research subjects”. Mörtberg et al. (2010, p. 106) continue that it is necessary “to perceive and to be open to the unexpected and to contradictions”. The author of this study was led by this notion and he did not react verbally negative to potential interview participants by judging their decisions of taking or not a part in this study or for instance to refuse the interview is being recorded but to be written.

There is the obligation of researchers to respect informants’ desires, values and needs (Creswell, 2009). This is the reason why the participants of this study were treated with flexibility i.e. the researcher was adapting his time in favour in theirs. This primarily means that the interviews were held when it was most convenient for them, at the place where they preferred and their choice if the interview will be held via a social media software (also which social media software) or live were always taken in consideration.

4.7 Methodology criticism

Quantitative research method data collection is conducted usually by experimental research and survey inquiries that compare variables and take into consideration the examined size of population (Creswell, 2009). This kind of research method often requires identification of predetermined variables and then the data collection can be conducted by standardized forms such as for instance questionnaires. In comparison to quantitative research method, the qualitative research method, as abovementioned, is to understand the feelings and ideas in the natural setting of interviewed participants Lichtman (2013) and in this study this has meant to be achieved through semi structured interviews in order to understand the interviewed participants in their complex social and cultural phenomena. Quantitative research more reflects seeking for objective knowledge which is more characteristic to positivists and according to Coombes (2001) it suits to researchers who are independent and remoted from the process of research. However, this study is based on interpretive, but not the positivist paradigm, where the social reality is more an assumption of researcher’s subjective knowledge. Additionally, and as mentioned before, “qualitative research is fundamentally interpretive” (Creswell, 2009, p. 20). The abovementioned arguments support for qualitative but not quantitative research method to be employed in this particular study.

5 Empirical Findings - Themes Classification

In this chapter, there is a short description of IT professionals and their companies provided as well as the names of the emerged themes. Then, the empirical findings were classified into the themes emerged that are described and the empirical findings presented.

5.1 General interview details and emerged themes description

The semi-structured interview data are analyzed from six interviewees' answers (IT professionals) that were conducted at six different companies, operating in the Republic of Slovakia. As mentioned before, the interviews took from 35 to 50 minutes, depending on interviewees intention to elaborate shortly or lengthy on various questions. Instead to refer to interviewees' real names, in the text they are referred to as Interviewee 1, Interviewee 2 and so on or IT professional 1, IT professional 2 et cetera. The same pattern applies in the case of companies' names where they are referred to as Company 1, Company 2 etc. The answers of the first type of questions, i.e. general questions, with a short description of interview initiation process can be found in the section 11.1 of this thesis. However, general data of interviews' details and companies are summarized in the following table (Table 2):

Table 2: General details of IT professionals and their companies

Company	Interview date	Company's business activity	Company size/number of employees	Interviewee's expertize	Communication
Company 1	01/04/2015	Import and distribution of children's garment	Small/25	General IT professional	In company's premises
Company 2	02/04/2015	Import/export of construction materials	Medium/70	Cyber security professional	In company's premises
Company 3	03/04/2015	Cooperative for ethical finance	Small/15	General IT professional	Viber
Company 4	04/04/2015	Restaurant and food delivery	Small/11	General IT professional	Skype
Company 5	06/04/2015	Point of sale terminal deployment	Medium/56	Cyber security professional	In company's premises
Company 6	07/04/2015	Assembly line production	Small/18	General IT professional	Skype

Firstly, the answers from the general questions with the interview initiation process can be found in the Appendix 3. Secondly, the themes that emerged were complete awareness (CWA), high unawareness (HUWA), lack of resources (LOR), negligence (NGL), lack of empowerment (LOE), predominant technological aspect (PTT) and partial compliances (PTC). The emerged themes description is presented in this chapter but the complete presentation of the themes that emerged from the participants' answers is provided in the chapter of data analysis in the tables 3, 4 and 5.

The questions provided by IT professionals on organizational, technological and psychological aspects are taken into consideration about making decisions of cyber security measures creation in SMEs by IT staff in Republic of Slovakia.

5.2 Complete Awareness Theme (CWA)

Only two IT professionals in SMEs show complete cyber security awareness in considering the organizational, technological and psychological aspects. Those are IT professional 2 and IT professional 5. Here is especially interesting that any of the other companies uses cyber security standards and written cyber security policies which indicates their low awareness of these four companies. IT professional from company 5 provided the following answer about the international cyber security standard that his company implemented:

> *"We have implemented ISO 27001 which is related to information security management systems. This is for us very important because we work with serious computer software which is of a high value to our customers. I am also trying to persuade the management to invest their resources to implement ISO 27002 and I think I am on the good road to succeed in this."*

IT professional 5 here shows quite high awareness because he is trying to persuade the management in his company to implement an additional international cyber security standard i.e. ISO 27002. Although Company 2 does not have an international cyber security standard implemented, there is implementation of a national cyber security standard in this organization. There is also such a case where these two companies that belong to this theme show a complete awareness in the technological aspect which is excluded in the rest of other participants. This can be seen in their analysis of the threats identified by antivirus software. On this question IT professional 2 replies with explaining why this analysis is important to him:

> *"Certainly, we use the antivirus software and I analyze the each identified threat. It is very important to analyze the*

> *threats due to this approach increases the chances to find out what is out there on the Internet that can endanger us.“*

In the psychological cyber security aspect only these two IT professionals comply with the high level of guilt and shame

Beside of more IT professionals of the six companies possess a high level of guilt and shame proneness, only IT professionals 2 and 5 distinguish themselves in possessing the trait of guilt. This shows their awareness of being ready to face cyber security issues and problems that emerged by their mistake. Moreover, IT professional 5 is ready to go beyond confession to the management of his mistake but he also already has a proposal about how to solve this problem that has emerged by his mistake. This can be especially understood when he is answering the last interview question about reporting his wrong estimation and the need of additional company investment:

> *“I would immediately inform the management about the issue and make the vendor to take all the responsibility of this problem. If the vendor would not want to take the responsibility of this problem, I would propose to sue them in front of the court and plus, if we experience any damage in our system because of their mistake, to incur them all the costs of that damage in front of the court .”*

The IT professionals 2 and 5 complied with all the three aspects completely which made them the most aware about the cyber security and to belong to the theme of complete awareness.

5.3 High Unawareness Theme (HUWA)

To the theme of high unawareness belong IT professionals who for example show some kind of lack of knowledge which leads to them of being unaware of cyber threats that come from the cyber space. Other examples of IT professionals being unaware is when they say that they are too busy to respond to some cyber security requirements but they do not know that complying with these requirements does not really take much time or they simply overlook the compliance of most cyber security requirements. The lack of time is expressed in the case of IT professional 4 in the organizational aspect when he is not able to list any cyber security standards although this information could be quickly acquired by browsing the Internet:

> *“… (uncomfortably sighing) we are very busy with our business in order to bother with that. I cover all the IT aspects in the company so I do not have time to go into cyber security details and finding out about the standards”.*

His answer shows a high unawareness of cyber security because even he is very busy at work, he could get at least informed about the cyber security standards names.

One of the best examples of IT professional's lack of knowledge that endangers his company tremendously is IT professional 3. While saying that his company does not use an antivirus software, he provides the following explanation why this software is not included as a part of technological cyber security measure in the business organization he works for:

> *"There is no need for antivirus software in our company because we use Linux operating system. There are no viruses made for Linux* (with a pleasurable smile on his face).*"*

The abovementioned statement indicates a high level of technological cyber security unawareness and later in the discussion we refer to sources that prove that viruses can highly endanger Linux operating systems.

When it comes to the psychological aspect of cyber security there is an interesting finding that isolates IT professional 6 from the other persons employed in this role. All the IT professionals would spend some additional time at work in order to solve out an accidentally emerged minor cyber security issue which is not the case with IT professional 6. This IT professional would not stay at work for this purpose and this is how he supports his decision:

> *"… if this that you are saying would be really just a minor issue I would leave it for tomorrow. There are always some minorities present in the system that do not require an immediate attention and we are a really small and not so important company on the market that someone would take us as a target so that I would have to be more cautious."*

IT professional shows lack of knowledge by saying that the company he works for is too small and important in order to be cyber-attacked but he is not familiar that the main targets of perpetrators nowadays are SMEs as the trends show.

5.4 Lack of Resources Theme (LOR)

As previously mentioned, the lack of financial resources is one of the most prominent findings that previous studies refer when tackling the question of why SME's are more exposed to cyber-attacks than large enterprises. This theme also emerged in this study in the organizational and psychological but it was interestingly missed from the technological cyber security aspect. Company 4 was among these organizations that showed this problem when its IT professional expressed the lack of resources in order to make a deeper analysis of cyber-security threats that endanger this company. This is how he describes the reason of not analyzing the cyber-security threats:

> *"… to be straight, we are a too small company and with too scarce resources to be able to allocate them for threats analyzes that are identified by our antivirus program. Honestly, I am aware this would be a good practice but this company is just not able to achieve such a proactive security approach."*

As we said before, the lack of resource allocation also emerged in the psychological aspect of cyber security. Specifically, it was the case with Company 3 and Company 6 when it was to understand the level of guilt and shame proneness of their IT professionals. IT professional 3 here expressed this issue by saying that:

> *"If the management requires that something need to be achieved in the scope of certain budget then I have to achieve that however I know. I would just ask them if they were aware of the potential consequences but I am sure they would already know about the matter while doing the cyber security budget allocation…, our budget is quite scarce."*

The situation in Company 6 is even worse due to this IT professional explained that the company he works for does not even have enough financial resources to pay for the proprietary software applications. This situation looked quite natural to him and he explained it as:

> *"The situation you are asking about is currently the case in our company. We do not have enough money to pay for all the software licences when it comes to security so I use some open source software in order to keep the cyber security level to a reasonable extent."*

Having this theme emerged explains one of the reasons for SMEs vulnerability in the cyber space and at the same time shows why these organizations a more often the subjects to cyber-attacks then the big enterprises.

5.5 Negligence Theme (NGL)

The negligence is an unexpected but quite interesting and important finding of this study. There are two kinds of forms of negligence emerged. The first form emerges when IT professionals are aware that they could do something in order to improve the cyber security measures in their organization but they simply do nothing about it. The second form of negligence emerges when IT professionals make excuses of why they do nothing in order to improve their cyber security measures and one of such excuse is that they simply state that nothing has been done for the measures improvement because they are happy about the cyber security level in their company. The certain level of negligence is noticed in all the three cyber security aspects.

The first form of negligence can be seen in IT professional 4 where he explains why the company he works for does not have a written cyber security policy by saying that:

> *"We do not have any written policies about cyber security and the employees are generally familiar what they should or should not do* (pause and laughter) *…everyone is too busy to think about breaking the rules. The load of work is unbearable."*

However, when asked whether cyber security policy was important for SMEs he answered:

> *"…it depends … if a specific company's business depends and relies on the cyber space it is highly important to create one."*

From IT professional's last statement it can be understood that he supports having a written cyber security policy created only in business organizations that depend and rely on the cyber space but the company he works for does not have a policy written. From this it can be concluded that Company 4 does not depend and rely on cyber space which is opposite to what IT professional 4 stated while answering the general questions where he clearly explained that the business activities of Company 4 rely on the cyber space by saying that:

> *"We have a software application for food online orders that is web-based and where our customers can pay online via that application or to pay when the food is delivered. We use another application in the restaurant for food orders, payments and table booking that can be accessible via the internet and from this point we can say that we rely our business activities on the cyber space pretty much."*

The first form of negligence also was present in the psychological cyber security aspect when IT professionals answered the question about postponing the regular system security scan in the favour of doing an important administrative work. Although some IT professionals are aware about the importance of the regular system scans, they would postpone it in the favour of the important administrative work. This was the case with IT professional 1 that explained:

> *"…regular system scans usually do not require my close attention while they are performed. Anyway, if the administrative work would be so important, I would see what I could do about it and probably postpone the system scan for a while."*

And this was also the case with IT professional 3 who explained:

> *"If they would ask me to do some administrative work, it would be probably something with a high priority so I would accept to finish with that and then later I would perform the security system scan."*

The second form of negligence that emerges when IT professional make excuses such as being happy about the cyber security level in their organization was provided in the cases of absence of cyber security standard implementation and hardware and software inventory list. For instance, this kind of excuse is expressed by IT professional 3 while he was explaining why Company 3 does not have any cyber security standards implemented. This is how he explains this absence:

> "*We do not have any standards implemented in our firm and we think we still do not need them because we are happy with our security level."*

The same IT professional made another kind of excuse when he was answering the absence of procedures about the roles and accountabilities assigned in the occurrence of a cyber-attack. This time he says that he does not believe an attack would happen in his company by saying that:

> *"Hmm, let me think a bit…, err we do not have such kinds of procedures. We have never had such a delicate situation. We have the firewall and antivirus software which are under my strict control so it is unlikely to happen here… "*

This form of negligence also was found in IT professionals 4 and 6 in the technological aspect of cyber security. More specifically, IT professional 6 just simply states the absence of such a list while IT professional 4 even admits that having a complete list of hardware and software is good to have but its absence is a lack of responsibility of creating one. IT professional 4 says:

> *"I understand your point and I agree we should have one but unfortunately we do not. Frankly speaking, I do not know… maybe just a lack of responsibility."*

According to above presented, we can see that the negligence theme is quite a strong emergence among the IT professionals in SME's which even brunches off into two different forms.

5.6 Lack of Empowerment Theme (LOE)

This theme emerges when IT professionals would like to create and implement some particular cyber security measures but they do not have their management support. Such cases consider the management being an obstacle but not the IT professionals due to IT professionals are not in power i.e. they are not empowered to perform their cyber security decisions into the force. These cases mostly emerged and were spotted in the aspect of the organizational cyber security and most frequently found as an answer provided by IT professionals about why any of cyber security standards are not implemented in their organization. One of the IT professionals that are found to be in the lack of empowerment by the management is IT professional in Company 1. This is how he explains himself being limited to implement any cyber security standards:

> *"None of mentioned cyber security standards in your question are implemented in our company. I am familiar that ISO cyber security standards exist out there, …but the management consider these standards still not necessary to be implemented because they only want to have a general/basic protection."*

The similar situation is found in Company 2 where its IT professional explained that despite of already having a national cyber security standard implemented, he would be eager to have implemented an international one. IT professional 2 expresses the lack of being empowered in the following way:

> *"I would like to use international cyber security standards in our company such as ISO but there is not management support for that."*

When it comes to the system access permissions IT professional 1 feels the lack of empowerment partly due to only sometimes he is being asked for advice but this asking for advice more sounded like to be asked about something unofficially which practically does not allow him to make these kinds of decisions. Here is an excerpt from his answer:

> *"…only the company's owner decides about the system access permissions strictly, …the company's owner must*

> *decide about the permission but in some cases, the company's owner* (mild smile), *…approaches me, …he asks for advice from me* (feeling important).*"*

However, there is also the lack of empowerment, or we could better say, some kind of concordance, from IT professional 4 where he would give up his professional responsibility to the management in a certain circumstances. This was noticed during the psychological cyber security aspect where IT professional 4 explained that he would give up his responsibility to the management in the following way:

> *"I would ask them if they were sure they wanted me to create the cyber security measures with the resources available and if they would reply positively I would create them. They are the management and they pay me so I would obey what they require from me to do but it would be their responsibility because they made the decision.*"

The decision given by this IT professional shows a low level of guilt and shame due to his readiness to easily give up his responsibility and to be disempowered.

5.7 Predominant Technological Aspect Theme (PTT)

The last theme that was clearly emerged was a dominance of complying with the technological aspect by IT professionals when comparing to the organizational and psychological cyber security aspect. This dominance was shown by realizing that all the companies comply with system log analysis, system backups, advanced password rules and Internet firewall rules i.e. with the two third of the technological fundamentals of cyber security. This finding is quite disturbing due to, in this way, SMEs cannot cope with the cyber security threats that would be prevented by the other two aspects and therefore stay open for being harmed from the cyber space. For example, the dominance of the technological aspect developed so far that some of the IT professionals even created some sophisticated techniques for password rules where a software application generates advanced passwords for the employees. This is a case in Company 3 where its IT professional explained this feature in the following way:

> *"We use a strong password generator software application that generates alpha-numeric passwords for our employees where every employee has his or her personal password …the passwords are changed every three months."*

Further, even the system logs analysis is mostly done manually, all IT professionals from the six companies perform it regularly and in a timely manner. Moreover, if an additional system log analysis is needed, some of the IT professionals spend their extra effort to dedicate their time to this action. Such an example represents IT professional from Company 6 who explains doing the system log analysis as follows:

> *"I follow the logs regularly which means once a week and doing this manually. If I doubt there were some suspicious activities then I perform the analysis more often."*

Another interesting finding in the predominant technological cyber security aspect among the IT professionals is that all of them besides using Internet firewall, they also adapt the firewall rules to the needs of their organizational business needs. According to IT professional 1 the firewall rules are applied and used as it is stated:

> *"We use the firewall …it is a need to use all the time because it does its job very well. Our needs are to use the port 80 and it is always open but if there is a need for some applications to use some others, then I open them according to these needs."*

As we mentioned above, this theme that was labeled as the predominant technological aspect takes its wide primacy among the IT professionals across SMEs.

5.8 Partial Compliances Theme (PTC)

In the theme of the partial compliances are categorized all the IT professionals or firms that only comply with some of the organizational, technological and psychological cyber security aspects. That is, they show compliance but it is minor when considering the whole of any of these three cyber security aspects. One of the examples is the IT professional from Company 4 where it was realized that in the organizational aspect he complies with using cyber security policy in practice requirement, information value prioritization requirement and during cyber security measures requirements. Aforementioned requirements represent only three from the eight requirements of the organizational aspect and the similar cases exist in the other two cyber security aspects with other IT professionals as well. However, this is how IT professional 4 shows his compliance with using cyber security policy in practice by saying:

> *"…as I said we do not have a cyber-security policy created but everyone in the company is aware that they have to focus on their work activities and not to do Facebooking at the worktime."*

When it comes to information value prioritization requirement, IT professional 4 complies with it by explaining:

> *“…we are a very small company and our most valuable asset is prices of company’s services. We offer different prices to different clients so if this information would be revealed, the company would lose its reputation with the clients and the competition could take advantage of that.”*

Further, the compliance with during cyber security measures requirements is answered as follows:

> *“Certainly, certainly, if I or anyone of the employees notices some strange and unusual activity, I shut down the internet connection straight away. From my logic and personal experience, I think this the best and the most effective way.“*

Therefore, the partial compliance theme emerges in all of the three cyber security aspects where IT professionals mostly party comply with the cyber security requirements.

6 Data Analysis and Results

In this chapter, the analysis of the data from empirical findings classification chapter of the six IT professionals is presented in regard to organizational, technological and psychological aspects. The organizational aspect is analyzed by taking into consideration the three phases of cyber security i.e. pre-cyber-attack, during-cyber-attack and post-cyber-attack cyber security measures. The technological aspect is analyzed by bringing up the importance of achievement of the basic cyber technological security measures. Finally, the psychological aspect is analyzed by presenting the empirical findings that take into consideration the general level of guilt/shame and later to distinguish which one from these two dominates in the interview participants. In order to make this analysis achievable, the constant comparison analysis tool was used from Leech and Onwuegbuzie (2007) where the answers of IT participants and the emerged themes from empirical findings chapter were analyzed.

6.1 The Analysis of the Organizational Aspect

There were eight questions created in order to elicit the IT professionals' answers. These eight questions were divided into three phases. In the first phase that represents the period of the *pre-cyber-attack*, five questions were included that addressed the cyber security standards, written cyber security policies, the rules used in practice, information value prioritization and the system access permissions. The second phase contained only one question that related the period of *during-cyber-attack* and examined whether some measures exist in the case of a cyber-attack. The third phase that relates to *post-cyber-attack* security measures, contained two questions that researched the potential presence of cyber–attack analysis and the procedure about how to inform clients and other stakeholders.

Due to extensive amount of empirical findings that were elicited from the six IT professionals, their interview answers were categorized into the themes emerged. These themes were placed and presented in Table 3.

Table 3: Organizational aspect interviewees' answers with the themes embedded

No	Phase	Questions	Firm 1	Firm 2	Firm 3	Firm 4	Firm 5	Firm 6
1	Pre	Standards	LOE	**CWA, LOE**	NGL	HUWA	**CWA**	LOE
2		Written cyber security policy	HUWA	**CWA**	HUWA	NGL	**CWA**	HUWA
3		Rules used in practice	PTC	**CWA**	PTC	PTC	**CWA**	PTC
4		Information value prioritization	PTC	**CWA**	PTC	PTC	**CWA**	PTC
5		System access permissions	LOE	**CWA**	PTC	HUWA	**CWA**	PTC
6	During	Measures	PTC	**CWA**	NGL	PTC	**CWA**	PTC
7	Post	Cyber- attack analysis	PTC	**CWA**	HUWA	LOR	**CWA**	HUWA
8		Informing clients	NGL	**CWA**	NGL	NGL	**CWA**	NGL

6.1.1 Pre-cyber-attack Security Measures

As we can see from the table above, the first question was intended to elicit if any cyber security standards are used in the organizations that participated in this study, and to see if the IT professionals are familiar with them. The empirical findings of this part showed that only Companies 2 and 5 have implemented some kind of standards. More precisely, Company 2 has implemented the national cyber security standard and Company 5 has implemented an international cyber security standard, namely ISO 27001. The IT professionals from these two companies also expressed their familiarity with cyber security standards while the IT professionals from other four companies were not able to number any of them. The empirical findings also show that Companies 1, 3, 4 and 6 do not have any cyber security standards implemented in their organization. While the IT professionals from Companies 1 and 6 explained the absence of standards was due to the management's decision, the IT professionals from Company 3 said that he was happy with their cyber security level. The IT professional from Company 4 tried to support the fact of not having any standards implemented in their company because of extensive load of work and therefore being too busy to do anything for the standards initiation.

When it comes to companies' cyber security policy, only two companies fulfill this requirement. These two companies are Company 2 and 5. The IT professionals from these two companies say that these policies were created by them and the management and that it is necessary to have these two sides involved in this process due to on one hand, the management is familiar with the business of the company but on another, the IT professionals can assist with providing them with system possibilities and options available. They also added that this policy has to be read and signed by each employee. The IT professionals from Companies 1, 3 and 6 explained that they do not have a written cyber security policy in the companies they work for but expressed that there are unwritten agreements and rules about what things the employees are not allowed to do at work. They explained that these unwritten rules were created in cooperation with the management and the IT professionals. In opposite, the IT professional from Company 4 explained that his company does not possess any written cyber security policy and that it is not needed because the employees know what activities are not allowed to be performed and that even if they wanted to do them, they would not be able because everyone is very busy at work. Interestingly, this IT professional expressed that it is important to have such a policy but only for companies whose business highly depends on cyber space. The IT professionals from Companies 1 and 6 stated that it is not very important to have a written cyber security policy due to small companies do not employ many people so these rules can be easily communicated between them while the IT professional from Company 3 said that this kind of document is needed only to satisfy the legal point of view.

When the IT professionals were asked if the cyber security policy is used in practice, they responded quite differently. The IT professional from Company 1 was pretty self-confident that the so-called unwritten policy agreement is used in practice. The IT professional from Company 2 said that the rules are generally obeyed although there were some cases when some employees were caught not being compliant with the policy. He also explained the procedure that if the rules are broken, the employees are warned not to do it again but if they continue doing this they are reported to the management. It seems that IT professional from Company 3 believes the unwritten policy is used in practice because the employees know they would be fired if not complying with it and the IT professional from Company 4 stated that the employees in the company he works for are aware what they should not do although any kind of policy exists. The IT professional from Company 5 explained that proxy settings are set in the way that the workers cannot access any external websites that are not related to work activities and this was the reason why he believes the compliance with the policy exists. Finally, the IT professional from Company 6 provided a positive answer from the reason of existence of two additional computers where if needed, employees could use them for their personal purposes.

The fourth question in the organizational cyber security aspect is about prioritization of information assets, who decides about these priorities and what is the process of this decision. Interestingly, all the companies have the prioritization of information assets. However, in the Companies 1, 2 and 6 these priorities are set strictly by the management and the prioritization process is not known by IT professionals. The IT professional from Company 5 said that the priorities are decided by him, management and the ISO standard and the IT professional from Company 3 stated that these are decided between him and the management. This IT professional also added that the priorities come from his manager but also explained that the manager sometimes asks his participation in how to prioritize these data by saying that there are three data classes i.e. the most valuable data, data of medium importance and the information of less confidentiality and importance. Company 4 has only one priority in their information assets and it is the price list of services they provide to the customers as they consider it highly and most important.

All IT professionals except the IT professional from Company 4 expressed the existence of system access permissions in their organizations. The argument of IT professional 4 was that the system access permissions are not needed due to all the employees are able to do each-others' work so it is taken as an advantage by IT professional from this company. Also all the IT professionals' opinion except the one from Company 4 was that the system access permissions decisions must be decided together i.e. between the management and the IT staff. Among these five opinions only IT professionals from Companies 5 and 6 supported the reason for their answers. They said that the decision making on this issue must be made between the management and IT staff due to the management has business but IT professionals the ICT expertize. However, while the practice of mutual system access permissions creation applies in Companies 3, 5 and 6, the IT professionals from Companies 1 and 2 stated that the management tends to take a complete control over this responsibility. Despite this being the practice in these two organizations, the management sometimes still asks for opinion and consultation of these two IT professionals when it comes to creating decisions of the system access permissions.

While analyzing the answers of IT professionals in the phase of the pre-cyber-attack decision making five different themes came into the spot. Here we could realize the presence of CWA in the two companies which will be recurrent in IT professional 2 and 5 as they completely comply with all the requirements in all the three aspects and the theme of PTC emerged ten times in the rest of the four companies. The occurrence of PTC of the four companies in comparison with CWA in Companies 2 and 5 explains that a low presence of cyber security awareness exist in the most of IT professionals that participated in this study. The low awareness of IT professionals in the pre-cyber-attack phase is also reflected by the emerging HUWA theme five times which can be seen in the Table 3. In this phase there is also a significant influence of the management to IT professionals because the LOE theme emerges four times and it is most dominant in the requirement of cyber security standards implementation where the IT professionals expressed their empowerment to bring their decisions into the force. Lastly and interestingly, the least emergent theme is NGL but although it appears only two times, its significance is very important for this study's findings.

6.1.2 During-cyber-attack Security Measures

The question about existence of *during-cyber-attack* measures elicited the following interviewees' answers. Opposite to Company 3 that does not have any *during-cyber-attack* security measures, due to belief that the internet firewall and antivirus software represent an absolute protection, all the other IT professionals stated that they have a procedure in the case of a cyber-attack happens. In Company 1 the measures reflect the decision to turn off the Internet server because all of company's data are stored at that place. Additionally, if the employees in this organization notice any strange cyber activities, they notify their IT professional. This measure is different in Companies 2, 4 and 6 where in a case of the cyber-attack, IT professionals turn of the Internet access. This situation slightly differs in Company 2 where employees, if they cannot find their IT professional, they have the right to turn off their computers by pressing the power button for a longer period than usual. However, the IT professional from Company 5 seems to be most cautious when it comes to organizing measures against the cyber-attack occurrence. In the case of such an event, IT professional 5 firstly turns of the Internet and secondly the Internet server. He explains that the Internet server also needs to be shut down due to not knowing if some virus or malware is already placed in the system.

The dominant theme in this phase is PTC that shows that most of IT professionals have created the organizational cyber security measures that are to be employed in the case of cyber security occurrence. In addition, there are Companies 2 and 5 with their CWA. However, the NGL theme emerges in one company, more specifically in IT professional 3 and it was present in the pre-cyber-attack phase in this IT professional as well.

6.1.3 Post-cyber-attack Security Measures

When IT professionals are asked to explain how they analyze whether, after being cyber-attacked, that was an attack directed straight against their organization or it was an isolated random attack, we realized that 50% of participants even do not perform this kind of analysis. Such analysis is conducted by Companies 1, 2 and 5 but not by Companies 3, 4 and 6. IT professional 3 says that this kind of analysis would be too complex, time consuming and if they really wanted to be provided by this information, they would ask their Internet provider to support them in this matter. Interestingly, IT professional from Company 6 stated that such analysis is not necessary because the company he works for is too small and not an interesting target that could attract cyber-attackers' attention. Finally, although the IT professional from Company 4 thinks that analyzing cyber threats would be a good practice, he supported his opinion by too scarce company's resources in order to invest in this action. IT professionals from the companies that do the analysis of cyber threats, employ different practices of doing this process. While in Company 1, IT professional tries to find some patterns in internet firewall and system logs, the IT professional in company 2, besides reading the system logs, also waits to see if the particular cyber-attack will reoccur. However, IT professional in Company 2 responds that this could be a long time process due to waiting for a threat rehearsal sometimes requires a long time period. Besides confirming the presence of threat analysis, IT professional 5 also described what indicators he considers important when conducting such an analysis. First, he fortifies what types of data was targeted by the perpetrator. Second, he estimates the level of data damage. Finally, depending on the results, he makes an assumption if the particular attack was targeted straight against the company or it was just an accidental random cyber-attack.

The last question that regards informing cyber security body and stakeholders after a cyber-attack has happened elicited different answers from the IT professionals. Only Companies 2 and 5 would inform the stakeholders, cyber security body or police but firstly referring and discussing the issue with the management. IT professional from Company 2 believes that the stakeholders should be informed because they are a part of business and IT professional from Company 5 adds that they do not inform anyone in a case of minority such as if the antivirus software identifies a single threat in the system. Further, Company 1 would not inform anyone because of disbelief that it could be of any help to someone in such a situation and Company 4 would not inform someone because this issue should stay strictly confidential between the IT staff and management as they are both fully responsible for it. IT professional from Company 3 does not see any need to report this kind of problem to stakeholders by supporting his answer that the stakeholders should not get upset while IT professional from Company 6 would only inform the management due to he simply does not see the reason why anyone else would be informed in this matter.

When comparing the PTC theme with the theme of NGL, it does not have a significant presence. However, the NGL theme seriously predominates in the post-cyber-attack phase. Looking at Table 3 this predominance is obvious due to its presence in all the IT professionals except in IT professionals in Company 2 and 5 where the CWA theme is recurrent. The LOR theme has its presence which proves the previous studies findings of why SMEs being more often attacked than large enterprises while HUWA continues its presence like in the two previous phases analyzed.

In the next subchapter the analysis of technological cyber security aspect is presented.

6.2 The Analysis of the Technological Aspect

The empirical findings from the cyber security technological aspect contain six questions that according to Julisch (2013) support technological foundation of cyber security. The integral parts of the technological cyber security foundation are system logs analysis, the presence of an updated software and hardware inventory list, performing system data backups, analyzing the threats identified by antivirus software, using the advanced password rules as well as the application of internet firewall rules.

In order to summarize the answers elicited from IT professionals in six companies, Table 4 was created and patterned in the same fashion like Table 3 that was presented in the organizational aspect analysis above.

Table 4: Technological aspect interviewees' answers with the themes embedded

No	Questions	Firm 1	Firm 2	Firm 3	Firm 4	Firm 5	Firm 6
9	System logs analysis	PTT	**CWA**	PTT	PTT	**CWA**	PTT
10	Inventory list	NGL	**CWA**	PTT	NGL	**CWA**	NGL
11	System backups	PTT	**CWA**	PTT	PTT	**CWA**	PTT
12	Antivirus threat analysis	HUWA	**CWA**	HUWA	LOR, PTC	**CWA**	HUWA
13	Advanced password rules	PTT	**CWA**	PTT	PTT	**CWA**	PTT
14	Internet firewall rules	PTT	**CWA**	PTT	PTT	**CWA**	PTT

The log analysis is performed in all the six companies but their recurrence and methods differ from company to company. When it comes to the frequency of log analysis, Companies 3 and 6 perform it once a week but also more frequently if it is needed. In Company 1, the log analysis is limited to be done only once a week, in Company 4, on an occasional basis, while in Company 2 it is conducted three times a week but if it is known that there is a new tread in the cyber space, it is done more often. The only company that performs the log analysis on a daily basis is Company 5. IT professionals in Companies 1, 3, 4 and 6 analyze the logs manually while in Company 2, besides the manual log analysis, there are automatic e-mail notifications about the error logs that IT professional 2 receives in his electronic mail account. IT professional in Company 5 also receives the error logs in his e-mail account but immediately performs the analysis of them when they are received. Additionally, he explains that he divides the system logs into three groups, namely error, debug and information that help him to perform their analysis hierarchically.

Complete and up to date inventory list of hardware and software exists in 50% of sampled companies. That is, the Companies 2, 3 and 5 have such a list but the rest of them do not. IT professional 3 states that he has such a list and that it is always updated. In Company 2 the media access control addresses of hardware devices are tracked through the system logs. The IT professional from Company 5 provided the most thorough answer. He explains that the list is always up to date and it is used for the purposes such as to replace old fashioned hardware with the new one, to keep the software license always up to date and to authorize the company's hardware and software in their information system. As aforementioned, Companies 1, 4 and 6 do not have such a list but IT professionals from these companies provided different reasons for this. IT professional 1 says that he creates the hardware authorizations while installing the new devices, IT professional 4 agrees that such a list should be created but guesses that the lack of responsibility may be the reason of not having it. Finally, IT professional from Company 6 does not provide any reason for not possessing the list but admits that it is a good idea to have one created.

System backup is the activity that is performed by all the six IT professionals. More specifically, Companies 1, 2 and 4 back up their data on a daily basis while IT professional from Company 2 added that beside the daily backup, all the company's data are backed up twice a week. In Companies 3 and 5, the complete data backup is done once a week with addition that in Company 5, this activity is also performed on a regular daily basis. IT professional 6 stated that all the data created on a daily basis are saved at two places at the same time i.e. at two hard discs but all the company's data are saved every night. There is a different length when it comes to data storage. Company 1 stores the backed up data for a month, Company 3 never deletes them and Company 4 stores its data until the next backup. Company 5 stores its data for ten and Company 6 for three years. However, in Company 2 the daily data are stored for two years but the complete backed up data is preserved until the next backup. In the case of data damage, IT professionals 1, 2, 3, 4 and 5 can retrieve their data minimally after from 20 minutes until 2 hours. More specifically, Companies 1 and 3 can retrieve their data after 1 hour, Company 4, from 20 to 25 minutes, Company 2, after 30 minutes and Company 5 can restore its data after one to two hour time. According to IT professional 6, this process takes quite a time which is data retrieval after from 4 to 6 hours.

Compared to companies 1, 2, 4, 5 and 6, the Company 3 does not have an antivirus software application implemented in its information system. IT professional 3 explains that they do not need such an application because they use operating system on their computer called Linux for which, as he self-confidently explains, computer viruses do not exist. However, as our main point was to see if IT professionals analyze the threads identified by antivirus software we focused on those answers as a priority. From that perspective, Companies 1, 4 and 6 do not do the threat analysis because, as they argue, they pay for the licence for the antivirus software and the whole responsibility belongs to the vendor who they bought the software from. That is not the case with Companies 2 and 5. IT professional 2 analyzes the threats identified due to, as he says, importance to gain wider knowledge and obtain more familiarity with the threats which can lead to better knowing what he has to fight against. Finally, IT professional 5 beside the threat analysis against their antivirus software vendor's database, he also performs the analysis by comparing others' vendors' antivirus software databases.

Surprisingly, all the companies use advanced password rules and there are no shared passwords amongst their employees but only the personal ones. IT professionals from Companies 1, 2, 4 and 5 say they use alphanumeric password rules which require that their passwords must contain from letters and numbers. In Company 3, IT professional explains that they have strong password generator software that generates alpha numeric passwords for their employees while IT professional 6 responds that their password rules consist of password requirements such as having eight characters that must be set up in a case sensitive manner. When it comes to the frequency of passwords change, the employees in Companies 2, 3, 4 and 6 are required to change their passwords every three months but in Company 1 they have to perform this activity twice a year. IT professional 5 has a software application that every 85 days reminds the employees to change their passwords. If they do not change it within the window period of 5 days, then they have to ask him for help and explain why they have not changed it by then.

The last question that considers the technological cyber security aspect is Internet firewall rules and what rules are applied against. All IT professionals stated they the Internet firewall is used in their cyber security system. IT professionals 1, 3 and 4 answered that the port 80 is opened by default but if some others ports need to be also opened then they open them. Companies 2 and 6 apply the internet firewall rules according their company's business needs and IT professional 5 explained that the firewall rules are applied for in-band and out-band connection as well and that the rules are decided by the management. He also added that if there are some firewall rules exceptions needed, then he informs the management and then they discuss together about the further decisions in this matter.

From the Table 4 it can be clearly understood that the theme of PTT plays a dominant factor which indicates the biggest awareness of the technological aspect in IT professionals in comparison with the organizational and psychological aspects. The CWA theme is constantly present in the same companies but the LOR theme appears only once. This single appearance of the LOR theme indicates the readiness of SMEs to invest into the technological aspect which does not seem to be the case with the psychological aspect. In addition to the LOR theme, it seems that the theme of HUWA appears quite rarely in the technological cyber security aspect. However, despite of the highest awareness level in the technological aspect of cyber security in IT professionals, comparing to the other two aspects, the NGL theme still emerges in this aspect and remains to keep your presence, as we will see, in all the three aspects of the cyber security.

In the following section the analysis of psychological cyber security aspect is presented.

6.3 The Analysis of the Psychological Aspect

The psychological aspect empirical data analysis is conducted by analyzing the interview participants' answers elicited from six questions. The six questions are divided into two sets of questions. The first set of questions has aim to ascertain the existence of a general level in guilt/shame proneness amongst the IT professionals. However, the second set of questions, that otherwise considers during and post cyber security creation, is aimed to distinguish whether the IT professionals are specifically prone to guilt or to shame.

The Table 5 below represents the summary of IT professionals' answers and it is created as in the same fashion as the previous two tables (Table 3 and Table 4) in previous two subchapters.

Table 5: Psychological aspect interviewees' answers with the themes embedded

No	Aim	Questions	Firm 1	Firm 2	Firm 3	Firm 4	Firm 5	Firm 6
15	Guilt/shame general level	Postponing important administrative work in favour of regular system scan	NGL	**CWA**	NGL	PTC	**CWA**	PTC
16		Staying at work longer because of discovery of minor security issue	PTC	**CWA**	PTC	PTC	**CWA**	HUWA
17		Extensively explaining hesitation of creating deficient CS measures	PTC	**CWA**	LOR	LOE	**CWA**	LOR
18	Guilt or shame	Reporting the lack of expertize to the management and discussing the issue	PTC	**CWA**	HUWA	HUWA	**CWA**	HUWA
19		Reporting solved data leakage despite no one knows about it	HUWA	**CWA**	HUWA	HUWA	**CWA**	HUWA
20		Reporting the wrong estimation and the need of additional investment	HUWA	**CWA**	HUWA	HUWA	**CWA**	HUWA

6.3.1 The First Set of Questions – General Level of Guilt/Shame

When IT professionals from Companies 1 and 3 were asked whether they would postpone an important administrative work in favour of the regular system scan or *vice versa*, their responses were that if the administrative work was so important they would postpone the regular system scan for a while. Different from this claim, IT professionals 2, 4, 5 and 6, answered that they would postpone the important administrative work in the favour of the regular system scan. IT professionals 4 and 6 explained that their main responsibility and what they are paid for is to primarily take care of security, IT professional from Company 2 was assertive that his priorities are based on security as well and the IT professional 5 explained that the only exception to postpone the regular system scan would be if the company is under a current cyber-attack which we consider as not postponing the regular system scan.

Most of the IT professionals would stay at work in a case they spot a minor security problem in their system in order to dedicate their time to fix the issue. However this is not the case with IT professional 6. The IT professional from Company 6 states that there are always some minor problems in the system and that the company he works for is too small and unimportant to be attracted by cyber attackers. IT professionals from the rest of companies provided different arguments why they would stay at work and fix the minor security issue. That is, IT professionals 1 and 5 explained that they would not leave their work until the issue is fixed because most of big problems start developing from the minor ones. IT professional from company 2 explained that the cyber security job position sometimes requires solving tasks that are out of working hours and IT professional from Company 3 said he likes to leave work clear minded and not to think there are unfinished tasks after he left. Finally, IT professional from Company 4 supported his argument of staying additional time at work by being paid to take care of security and therefore it implies his responsibility.

When it comes to the way of dealing with creation of cyber security measures with insufficient budget, 50% of participants would create the measures without hesitation and 50% would hesitate and put additional effort in order to overcome this problem. More specifically, IT professionals 1, 2 and 5 would strive by every means to reassure the management to create such insufficient cyber security measures while IT professionals from Companies 3, 4 and 6 would create such cyber security measures without any hesitation. IT professional 1 would explain the management that he would not want to be a part of such insufficient security measures because he would not feel empowered enough to do his job properly. IT professional from Company 2 expressed that he is opened for facing challenges but that in this particular situation he would not see how to deal with the situation because if financial resources are needed for example to buy a software application license, he does not see the other way out than to pay for it. In comparison to IT professionals from Companies 1 and 2, IT professional 5 seemed to be most organized and assertive while answering the question. He was organized because he would first create a list with missing parts needed in order to satisfy the minimum requirements of cyber security with the prices; then he would create a PowerPoint Presentation where he would present the dangers to the management if the financial resources are not allocated in the amount of that price; then he would explain that if the management is not ready to invest that amount of money, the organization would not need a cyber-security professional employee. Moreover, this IT professional assertively stated that if the management would not accept to invest sufficient resources into cyber security domain, he would quit his job due to inability to see how he would build his future business career in that organization. As we mentioned before, the other 50% of interviewed IT professionals would react oppositely in this type of situation. So IT professional from Company 3 says that he would rely on such management decision but he would ask them if they would be aware of the potential consequences anyway. If they would answer positively, he would create such cyber security measures despite being aware that they would be insufficient. This IT professional also noted that the budget in his company is scarce. IT professional from Company 4 explained that the management pays him the salary to be responsible for cyber security but he would ask them if they were sure they want him to create such measures and if their answer would be positive, he would create them. Additionally, he stated that the management's positive answer would automatically mean that they would become responsible if something goes wrong in the future in this domain. Finally, IT professional from Company 6 stated that the cyber security measures with insufficient budget allocation already exist in this organization. He explained that he already uses some open source software in order to somehow close the security gap in the system.

When it comes to the themes, the LOR theme emerges two times which shows the lack of ability of SMEs to invest into cyber security but the theme of LOE also shows its presence. It is interesting to notice that the LOE theme shows up in the psychological and organizational aspects but not in the technological aspect of cyber security. The HUWA theme emerges only once which looks encouraging but the theme of NGL is also present in this aspect. However, the theme of PTC remained its emergence due to it shows the partial compliance with the level of guilt/shame in the IT participants. Finally, the presence of the theme of CWA is constantly present in Companies 2 and 5.

6.3.2 The Second Set of Questions – Distinguishing the Guilt and Shame

6.3.2.1 During CS Measures Creation

According to IT professionals' replies, Company 1, 2 and 5 would report their lack of expertise and try to find a solution by discussing the issue with their management, while IT professionals from Companies 3, 4 and 6 would try to find this problem solution in some other resorts. IT professional from Company 3 would rely on knowledge resources from the Internet and ask friends and colleagues from previous work for help, while IT professional 6 would purely rely on the Internet information sources as this is already his practice exercised for dealing with this issue. Similarly, IT professional 4 would consult people from his field of work and ask for help due to, as he says, he would also help them in return. When it comes to IT professionals who would discuss this issue with the management, IT professional from Company 1 answered that there is no person who knows everything and that everyone sometimes needs an advice; IT professional from Company 2 said that he is not ashamed of not being perfect and that no one is. Finally, IT professional from Company 5 explained that according to his experience, it is the best practice to inform the management as they represent the most responsible body in organization and are always supposed to provide problem solutions.

Three themes emerge in the phase of the during cyber security measures creation in the second set of questions of the psychological aspect. They are PTC, CWA and HUWA. Beside the CWA theme that is constantly present in IT professionals 2 and 5 there is also the PTC theme emerged. The theme HUWA takes more than fifty percent in this part that indicates quite a high cyber security unawareness among the IT professionals.

6.3.2.2 Post CS Measures Creation

After the interviewees were asked to respond if they would inform the management their company's important data leakage to the Internet but being able to solve the problem, IT professionals from Companies 2 and 5 provided positive answers. To be more specific, IT professional 2 expressed that from his point of view, it is regardless whether the management finds or not about what had happened, they are supposed to know the truth because the data are the most important asset of this organization and if the data are endangered so the company as well as IT professional's job position is. IT professional 5 explained that he would immediately inform the management as he could not be sure if someone has already stolen the data by copying them from the Internet and that by reporting this incidence, he would also protect his working position to a certain extent. Oppositely, IT professionals from Companies 1, 3 and 6 do not see the reason for informing the management if the damage has been fixed because they would not want to upset and make them worry in that case. IT professional from Company 4 was a bit undecided and said that he might have reported the major data leakage but for sure not the minor one. When asked to explain why, he explained that if something like that happened, the management would lose trust in him and it will be difficult to regain it back.

When answering the question about reporting to management their wrong estimation and therefore additional costs arose, IT professionals from Companies 2 and 5 answered they would, but IT professionals from Companies 1, 3, 4 and 5 would not inform their management about the infant issue. More precisely, IT professionals 1 and 6 would provide their management with false information that the additional costs came from some other issues because they would like to protect their reputation and their work position. IT professional from Company 3 would ask for a professional advice from his friends who work in the same field of work but anyhow, he would not report the issue to the management because they would lose their trust in him. In Company 4, IT professional would try to solve this issue with the vendor from whom the cyber security software/system was bought due to according to his opinion it is their responsibility to solve this problem and he added that probably there are more IT professionals who would approach to the vendor with the same problem so they would have to solve it anyhow. However, as aforementioned, IT professionals 2 and 5 would report the issue and act in the following way. IT professional 2 would inform the management, would be ready to suffer all the consequences and would make a plea to the vendor to close the gap. He would also include his management in this conversation. Finally, IT professional from Company 5 after reporting this issue to his management would make the vendor to take all the responsibility for what has happened. As he further explained, if there would be a negative response from the vendor, he would propose to sue him and if meanwhile some damage would occur with the company's data, the vendor would be made to reimburse the full cost of it.

In the IT professionals' answers that are meant to distinguish their guilt and shame proneness only two themes emerged. The first theme is CWA that is present only in two companies, as previously mentioned and the second is HUWA. The presence of the HUWA theme is very disturbing because it shows the high unawareness in all the IT professionals, except in the two ones with CWA. Such amount of HUWA indicates a very high level of IT professionals' unawareness in the psychological aspect of cyber security and represents an important finding in this study.

In the chapter that follows, we discuss the data that were acquired from our analysis.

7 Discussions

This section starts with a general discussion and then the implications to research and practice follows. At the end of this chapter the strengths and weaknesses are described.

7.1 General discussion

The theoretical framework that is brought in this thesis emphasizes the importance of treating the field of cyber security in SMEs from organizational, technological and psychological aspects. However, it is insufficient only to have these three aspects considered in SMEs but it is very important to stress and to keep in mind that these three aspects must be taken into consideration with the same attention i.e. they must be treated equally and any of them can be neglected. Therefore, only and just only if all the three aspects are fulfilled completely, there could be a cyber-security equilibrium achieved. However, it must be understood that achievement of this equilibrium does not guaranty an absolute cyber security with a hundred percent of safety but it just minimizes the possibilities for SMEs to be harmed to the extent of the existing cyber-attacking trends among SMEs. That is, the cyber security must be treated seriously and an overall cooperation between the management and the IT staff must permanently exist when the cyber security measures are being decided and created. This mutual cooperation between the IT staff and the management is necessary due to it brings an opportunity for cyber security alignment with organizational business goals which improve company's business development and therefore strengthens its sustainable competitive advantage on the market.

7.2 Implications to research and practice

Further, by comparing the dealing of the three cyber security aspects from our proposed theoretical framework among IT professionals, we saw that the awareness of the organizational aspect comes after the technological aspect that the IT professionals are most aware about. Here we came across the fact that why the lack of financial investments as described in the study by Rodriguez and Martinez (2013) is taken as the strong argument of why SMEs are being more frequently cyber-attacked than the large enterprises as the theme of LOR emerged in all of the three cyber security aspects. Aside from IT professionals 2 and 5 who we already seen being fully aware of all the requirements in all the three aspects which also emerged in the theme of CWA and aside from the lack of financial resources that is indicated by the theme LOR, from the rest of IT professionals' answers we could identify unawareness, negligence and in some of the cases even the lack of IT professionals' empowerment by their management.

One of the key points that have to be mentioned here is that despite the third pillar of '*Europe 2020 strategy*' represents the trust and security (European Commission, 2013), four out of six SMEs in this study do not have implemented and are not able to list any of international, national or EU cyber security standards. Moreover, these SMEs also do not have written internal cyber security policies but rely on, as they call, *unwritten rules and agreements communicated with the employees*. Although the Republic of Slovakia belongs to European Union, different themes emerged as to show why there is a very slow response across the IT professionals in this country about written cyber security policies and cyber security standards implementation. The reasons for the low cyber security response to this cyber security requirements emerged through the themes such as LOE and HUWA. However, when it comes to written cyber security policy creation the theme of NGL emerges which implies the IT professional's awareness of advantages of having a written cyber security policy but simply doing nothing in order to create or at least to initiate the creation of such a document with the management. Moreover, the NGL theme emerges as a very frequent theme and requires our attention to be identified.

Also, the study shows that one third of IT professionals are not empowered by their management to apply some cyber-security standards. Specifically this happens in Companies 1 and 6 where the management simply decided not to implement any standards. Therefore, the aforementioned argument helps us understand that there is also a presence of the lack of IT professionals' empowerment by their management and we add this as a contribution to SMEs being more exposed to cyber-attacks than the large enterprises. The additional argument is especially provided by the emergent LOE theme in the organizational and psychological cyber security aspects. Additionally, the theoretical framework according to which this study was conducted elicits empirical data that reveal interesting patterns. Here we must distinguish Companies 2 and 5 because they are compliant with all of the three aspects proposed without any exceptions and this is an emergent theme that we labeled as CWA. It is very important to recall about two points.

First, these two IT professionals are educated in the field of cyber security and opposite to the other interviewees who are general IT professionals, these two interviewees are cyber security professionals (please see Table 2). Second, compared to other companies which employ general IT professionals these two cyber security professionals are only responsible for the field of cyber security in the companies they work for. The first fact can make us assume that low awareness of the organizational, technological and psychological aspects of cyber security in SMEs may come from the reason that, at least in this study, most of SMEs employ general IT professionals. Additionally, the general IT professionals are in charge of the whole ICT in those organizations which is not the case with the cyber security professionals who have to deal only with the cyber security and not with the general field of ICT. Therefore we could link the first reason of low awareness as being the lack of appropriate education but the second maybe the lack of financial resources to employ a person who would only be responsible for cyber security. Although the results of the first reason are well supported by this study, we can only guess that participated SMEs do not have additional person for cyber security employed because of the lack of financial resources so we will keep it as a finding that the lack of the proper education may be the reason of SMEs being more attacked than the large enterprises.

Another thing that comes into the fact is that, as we could see, IT professionals are most aware of the technological aspect because they fully satisfy four out of the six organizational aspect components. This was realized by the PTT theme emergence that shows a special IT professionals' dedication to the technological cyber security aspect. This finding tends to agree with Kajtazi (2013) who points out that organizations often underplay organizational aspect of security strategy and overplay the technological aspect. However, remaining two technological components that are unfulfilled show that only two out of the six companies possess the technological cyber security foundation. The reasons of the two remaining technological components being unfulfilled are emerged through the themes of NGL, HUWA and LOR. Therefore, IT professionals' negligence, their high unawareness and the lack of resources are the main contributors that the technological foundation cyber security aspect is not fulfilled. This finding pretty much justifies Verizon Risk Team's report from 2012 where it is stated that 80% of successful cyber-attacks come from the reason that SMEs do not have established the basis of the technological cyber security aspect. For instance, we could see that Company 3 is not in a possession of the antivirus software because its IT professional believes that there are no viruses produced for Linux operating system. This is of course a fallacy because a whole an array of studies refer to issues with viruses in Linux operating systems (Harrison, 2005; Mateti, 2006; Safford and Zohar, 2005; Schmidt et al., 2008; Van Oers, 2000). Further, IT professionals 1, 4 and 6 do not analyze the threads that are identified by antivirus software due to they believe that once the antivirus licence is paid, the whole responsibility belongs to the antivirus vendor. This is technically maybe correct but this also shows IT professionals' low awareness or as it was originally emerged, the theme of high unawareness.

If we go back to negligence that emerged through the NGL theme, we could spot that when IT professionals 4 and 6 say that they are not in possession of the hardware and software inventory list because they are happy about the cyber security level in their organization, it shows they neglect to establish the technological cyber security foundation and therefore their happiness is of a subjective nature. Additionally, the lack of appropriate education i.e. to be educated specifically in the cyber security field again comes to the fore. Precisely, IT professionals 2 and 5, who are at the same time cyber security professionals, use the most sophisticated log analysis system of general IT professionals. As mentioned before, it is automatic e-mail notifications about the error logs that they receive in their electronic mail account. This automatic alert method could be something that these cyber security professionals learnt in their conventional education or they were educated how to search for some easier methods in order to improve the cyber security. Here we could see that the theme of CWA in aforementioned IT professionals supports the argument of the lack of appropriate education of IT professionals because they show complete cyber security awareness in all of the three cyber security aspects.

A new insight in the field of cyber security that is brought by this thesis inevitably represents the psychological aspect in our theoretical framework. As it was mentioned earlier, it is based on the level of guilt and shame proneness and their relation to CWB. It is assumed that the persons with a high level of guilt and shame proneness less likely involve into CWB. According to the findings presented in this thesis, the IT professionals are the least aware of this aspect. More precisely, two third of IT professionals do not comply with the components of this aspect where one third has a low level of guilt and shame and one third has a high level of guilt and shame but they are more prone to shame than to guilt. As it was previously explained, it is advised to have employed people with a higher level of guilt and shame but while people with the high level of guilt is more likely to report the issue, apologize and tend to correct their mistake, the ones with the higher level of shame are less ready to report their mistake and confront the problem. For example, IT professionals 1 and 4 show high level of guilt and shame but they are more prone to shame due to they fail to report important security issues to their management which tells us that if there is an important security issue caused by their mistake, they would try to avoid to admit what happened i.e. to confront with the problem and to look for its solution together with the management. Generally, their excuses not to report their mistakes mostly reflected the fear of losing the trust from the management which would be difficult to gain back as well as that their job position would be endangered. As it was seen through the themes emerged in this study, while the low level of guilt/shame proneness was characterized by the NGL, HUWA, LOR and LOE themes, there was an extremely amount of HUWA theme emerged when guilt and shame was to be distinguished. IT professionals from Companies 3 and 6 expressed the lack of investments and this is especially the case in Company 6 where the cyber security measures are created without sufficient financial resources so the IT professional in this company uses some open source software for which the company does not have to pay as it is reflected by the theme LOR. The negligence comes into the play in Company 6 where the IT professional would leave his work at the end of the work time despite knowing that there is a cyber-security issue in the company's system. The negligence also comes to the play when IT professionals 1 and 3 would postpone the regular system scans in the favour of important administrative work which shows that for them, security is a secondary but not the primary issue. The both examples are realized by the theme of NGL. However, it is worth noting that there are IT professionals 2 and 5 who show that they are in possession of high level of guilt which emerges in the themes of CWA. As abovementioned, the high level of guilt refers to confronting with the reality of situation i.e. with reporting the mistake to the management and working together on the issue solution.

7.3 Strengths and weaknesses of the thesis

One of the weaknesses of this thesis represents the emergence of dealing with the psychological aspect of cyber security due to this master thesis is a part of master program of information systems which belongs to the field of informatics but not to the field of psychology. Psychology is not one of the subjects of this particular master's program requirements although it can be found in the fields of informatics and information systems (Gregor et al. 2014; Shaw, Ruby, and Post, 1998). Moreover, despite that the author of this study read the literature of psychological nature, he is neither a student nor an expert in the field of psychology. However, one of the strengths of this study is that it confirms the significance of psychology by finding that it plays an integral part of cyber security and by showing that it must be treated with the organizational and technological aspects equally.

The another weakness of this research is that the interview questions were not primarily created based on the overall aim of this study but on the theory which can give the reader a hint that it is more of a positivistic nature. Therefore, the theoretical framework played a dominant role against the study participants. However, this study holds a philosophical approach of interpretivism that aims to elicit participants' personal views in their everyday work settings which are empirically supported based on their professional and working experience. Thereafter, the participants' answers were recorded, transcribed and interpreted in the researcher's subjective manner by using coding analysis.

Although new insights of cyber security were brought into the organizational and psychological aspects by the theoretical framework of this study, it is failed to bring new insights into the technological aspect of cyber security. The new insights of organizational and psychological aspects are presented in the conclusion section of this thesis but one of the insights of the organizational aspect is that some of cyber security standards are recommended to be implemented by SMEs. However, even if SMEs had higher awareness about this, they might be unable to perform such an implementation due to the lack of financial resources which is referred to in the previous studies.

Finally, this study is conducted only on the territory of Republic of Slovakia, more specifically in its eastern part in the second largest city by the name Kosice. This is a weakness due to the findings are referred only to this particular city. However, the strength of this master dissertation is that its theoretical framework can be applied to any other city in any other country and therefore to gain new results and findings that could be of a significance source of knowledge in cyber security.

.

8 Conclusions

In the world of business, it is well known that SMEs represent the backbone of global economy but at the same time we know that they are much more vulnerable to cyber-attacks than the big enterprises are. In order to decrease their vulnerability, the theoretical framework that focuses on cyber security decision making by IT professionals was created with the overall aim.

The overall aim of this master's dissertation is on organizational level and it was to bring new insights about organizational, technological and psychological aspects in cyber security and to understand their influence on cyber security on SMEs. It must be admitted that no new insights were brought to the technological aspect except that at least the cyber security foundation must be met in order to decrease success of cyber perpetrators in their harmful aims. However, two new insights of organizational aspect were brought to the surface. The first one is that any of cyber security national, EU or international standards are highly recommended to be applied due to they represent a useful security guide for IT professionals even if only partly adopted. The second insight is that organizational aspect can be divided into three phases in order to be easier to tackle which are namely *pre, during and post-cyber-attack decision making.* When looking from an organizational perspective, these three aspects have a huge influence on cyber security in SMEs due to they take into consideration organizational tasks that tackle cyber security in three different phases as mentioned above; technology which is the tool for tackling the cyber space; and psychology that tackles IT professionals' traits that come into play when making cyber security decisions.

The organizational, technological and psychological aspects have a low awareness on SMEs when looking at it from IT professionals' perspective. This argument can be supported by the fact that only two out of six IT professionals fulfilled all the aspects' components. The rest of IT professionals were most aware about the technological, then there was a medium awareness about the organizational and lastly, the lowest awareness level was about the psychological aspect. This is quite a disturbing finding due to according to Julisch (2013), these three cyber security aspects must be treated equally in order to minimize the dangers that come from the cyber space.

This thesis confirmed two arguments about why SMEs are in general more frequently cyber-attacked than the large enterprises. The first is the lack of financial investments in cyber security in SMEs (Rodriguez and Martinez, 2013) and the second is that IT professionals often do not satisfy the cyber security foundation of the technological aspect (Julisch, 2012; Verizon, 2012). However, there are additional reasons found by this study. First, only two out of six organizations fully comply with all of the components of the three cyber security aspects and these two organizations employ specifically cyber security experts i.e. the employees who are educated in the field of cyber security. Additionally, these two employees are strictly responsible for and dedicated to cyber security but not any other tasks. These findings helped us conclude that SMEs should employ people who are educated in the first place in the field of cyber or at least information security in order to improve their cyber security level. If it would be difficult to find these experts on labour market then these organizations could motivate their general IT professionals to improve their knowledge in this field through attending some cyber security certifications. Second, SMEs are not fully aware that any of the organizational, technological or psychological cyber security aspect must not be overemphasized but all the three aspects must be treated equally and considered with the same attention due it leaves additional gaps that open a gate for cyber perpetrators to achieve their aims. Third, there is a certain level of negligence of IT professionals which was found when certain IT professionals (IT professionals 1, 3 and 4) were aware that by employing some particular actions, the cyber security could be improved in their organization but they simply do not do anything about it. And finally fourth, it is found in some organizations (Companies 1 and 6) that the absence of cyber security standards comes directly from management decision, so despite of the IT professionals' awareness on this issue, these standards cannot be deployed. This finding is defined as the lack of IT professionals' empowerment.

Once we have achieved to complete the overall aim abovementioned, that is considered to be a part of tactical level, it is easier to answer the research questions that are more of strategic nature and to draw the final conclusions.

Research question 1

What is the awareness level of IT professionals among SMEs for dealing with cyber security measures creation from technological, organizational and psychological aspects?

The awareness level of IT professionals among SMEs for dealing with cyber security measures from technological aspect is the highest. This level is found the highest due to although only two organizations fully comply with the technological cyber security aspect, all the companies comply with four out of six components of this aspect (Table 3). There is the medium awareness of IT professionals of organizational cyber security level because, although only two organizations fully comply with the organizational cyber security aspect, all the companies comply with two out of six components of this aspect (Table 4). Finally, the IT professionals are the least aware of the psychological aspect of cyber security due to only two companies out of six fully comply with the components of this aspect and IT professionals from other organizations would not report the mistake they created which refers to low level of guilt or shame or only the high level of shame proneness (Table 5). However, in overall, this study found that awareness level of IT professionals in SMEs is low due to despite the IT professionals are most aware of the technological aspect, even this aspect's components are not fully met by four out of six employees.

Research question 2

What are the reasons that SMEs are more open to cyber-attacks than large enterprises?

As it is mentioned in the second aim achievement above, beside the low financial investments and unfulfilled components of cyber security technological aspect, this study found additional factors that contribute to the reasons of SMEs being more open to cyber-attacks than the large enterprises. The first contributor is the lack of appropriate education of IT professionals, the second is that IT professionals in SMEs are dedicated to the whole ICT company's sector to be responsible for but not only to the tasks of cyber security. The third contributor is that there is a low awareness of the three cyber security aspects and that they are not treated equally. The forth contributor is negligence that is identified as the awareness that something should be done but this is neglected by IT professionals and the fourth contributor is the lack of empowerment of IT professionals by their management, especially when it comes to cyber security standards implementation.

Cyber security must be considered as an important integral part of organizations' ISs which requires a complex understanding and it represents an extreme popular field nowadays. This importance particularly comes from the reason that in attempt to achieve their competitive advantage, organizations tend to find resort in ISs that find their implications trough creation and maintenance of organizations' most important asset today which is information. The complexity of cyber security implies that the creation, maintenance and information flow occurs in cyber space that requires two prerequisites. The prerequisite that includes information creation and maintenance are humans and the prerequisite that ensures the flow of information is ICT infrastructure. The popularity of cyber security arises from a straightforward reason. That is, the information, humans and the ICT infrastructure must be kept safe which is to be ensured by cyber security.

This master's dissertation primarily dealt with cyber security in SMEs and one of its limitations was that it was limited to the territory of Slovakia. However, despite being aware of national business culture, standards and legislations it is a good question if cyber security can be treated purely from a national level due to cyber space does not know for national borders. Moreover, we could see that four out of six organizations operate internationally which means that they can be cyber-attacked from any part of the world. That is exactly why the field of cyber security represents a special and interesting field for scientific research.

8.1 Future Research

This master's dissertation provides further opportunities for future research. One of these opportunities could be to apply the same theoretical framework to SMEs in the capital city of Slovakia, Bratislava as well as across the other countries in or out of EU borders. It would be interesting to see what is the level of IT professionals' awareness towards the organizational, technological and psychological cyber security aspects in the other countries and what is the level of equality that these three aspects are treated by SMEs. Moreover, there is a need to widen the depth of the new psychological aspect proposed by this study which also requires further testing. The second opportunity for future research could be to provide some new insights about the technological cyber security aspect due to this master's dissertation failed to do that but stuck with the technological cyber security fundamentals. The idea should be to go beyond these technological fundamentals and to broaden and innovate in this field. The third, as this master's dissertation presented, there are plenty of standards and initiatives for cyber and information security provided by different organizations and institutions. Some of examples are ISO standards and Europe 2020 strategy created by European Commission. So maybe it would be an interesting topic for research to explore why these standards and initiatives are mostly unknown and not followed by SMEs and whether it is a common practice among the SMEs in EU in general or it is only the case in Republic of Slovakia. The fourth opportunity for the future research is to examine the relation between the cyber security IT professionals and the level of cyber security in organization they work for and between general IT professionals and the level of cyber security in their organizations. More specifically, the aim of such research could be to examine whether it is true and to what extent that inappropriate education i.e. the education that is not related to cyber security but in some other ICT field plays a contributor for SMEs being more under cyber-attacks than the large enterprises. To more simplify, to find whether cyber security professionals are more aware about technological, organizational and psychological cyber aspects of cyber security than the general IT professionals. The fifth opportunity for a future research could be to understand what is the level of empowerment of IT staff is in SMEs and what the most frequent contributors of organizational, technological and psychological aspects are that the management wants to have a complete control over. In this thesis we saw that the management did not empower IT staff when it came to cyber security standards implementation. Therefore, it would be interesting to see if there are additional components over which IT staff has the lack of empowerment. Finally, an interesting finding of this master's dissertation is that one of important contributors for SME being more often the victims of cyber-attack is negligence of IT professionals. It would be useful to find out more about the negligence amongst the IT professionals in SMEs due to according to this master's dissertation, it plays an important finding that lowers cyber security in SMEs. For example, we can guess that IT professionals' unawareness comes from lack of appropriate education, and at the same time expecting the general IT staff to take care of cyber security which is not their professional domain. However, this is opposite to negligence that actually comes from awareness i.e. when an IT professional is aware that something needs to be done but s/he simply do not do anything about it. Therefore it should be additionally understand how negligence is connected to awareness and therefore for instance to find if the IT professionals in SMEs are negligent about applying cyber security standards because they are aware that they are not empowered by the management.

References

Anderson, E., 2015. SMEs failing to guard against cyber attacks, Government warns. *The Telegraph*, [online] Available at: < http://www.telegraph.co.uk/finance/businessclub/11430701/SMEs-failing-to-guard-against-cyber-attacks-Government-warns.html> [Accessed 8 March 2015].

Ashford, W., 2014. SMEs believes they are immune to cyber attack. *Computer Weekly*, [online] Available at: < http://www.computerweekly.com/news/2240216202/SMEs-believes-it-is-immune-to-cyber-attack-study-shows> [Accessed 8 March 2015].

Atoum, I., Otoom, A., and Amer, A. A., 2014. A holistic cyber security implementation framework. *Information Management & Computer Security*, pp. 251-264.

Ayyagari, M., Beck, T. and Demirguc-Kunt, A., 2007. Small and medium enterprises across the globe. Small Business Economics, 29(4), 415-434.

Baheti, R. and Gill, H., 2011. Cyber-physical systems. *The Impact of Control Technology*, pp. 161-166.

Ban, L. Y. and Heng, G. M., 1995. Computer security issues in small and medium-sized enterprises. *Singapore Management Review*, 17(1), pp. 15-29.

Batsell, S. G., Rao, N. S. and Shankar, M., 2005. Distributed intrusion detection and attack containment for organizational cyber security. Available at: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.105.9322&rep=rep1&type=pdf> [Accessed 25 February 2015].

Berg, B. L., 2004. Qualitative research methods for the social sciences (5th ed.). Boston: Pearson.

Bernard, H.R., 2002. Research Methods in Anthropology: Qualitative and quantitative methods. 3rd edition. AltaMira Press ,Walnut Creek, California.

Bernard, H. R., 1988. Research methods in cultural anthropology. *Newbury Park, CA: Sage.*

Berry, C. M., Carpenter, N. C. and Barratt, C. L., 2012. Do other-reports of counterproductive work behavior provide an incremental contribution over self-reports? A meta-analytic comparison. *Journal of Applied Psychology*, 97(3), pp. 1-24.

Borbás, L., 2014. Supporting SMEs in Central-Eastern Europe. *Volume of Management, Enterprise and Benchmarking in the 21st Century*, pp. 87-106.

Bradley, M., and Vaizey, E., 2015. Cyber security ‘myths’ putting a third of SME revenue at risk. *UK Government*, [online] Available at:

< https://www.gov.uk/government/news/cyber-security-myths-putting-a-third-of-sme-revenue-at-risk> [Accessed 8 March 2015].

Brooke, S., 2015. Target cyber hack shows how vulnerable smaller businesses are to digital attacks. *Real Business*, [online] Available at: < http://realbusiness.co.uk/article/29399-target-cyber-hack-shows-how-vulnerable-smaller-businesses-are-to-digital-attacks> [Accessed 8 March 2015].

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

Byres, E. & Lowe, J., 2004. The myths and facts behind cyber security risks for industrial control systems. *In Proceedings of the VDE Kongress,* vol. 116, pp. 213-218.

Carley, K, 1993. Coding choices for textual analysis: A comparison of content analysis and map analysis. In P. Marsden (Ed.), Sociological methodology, *Oxford: Blackwell*. pp. 75–126.

Choo, K. K. R., 2011. The cyber threat landscape: Challenges and future research directions. *Computers & Security,* pp. 719-731.

Cohen, D. and Crabtree, B., 2006. Qualitative research guidelines project. Available at: < http://www.qualres.org/HomeSemi-3629.html> [Accessed 04 April 2015].

Cohen, T. R., Panter, A. T., and Turan, N., 2013. Predicting counterproductive work behavior from guilt proneness. *Journal of Business Ethics,* 114(1), pp. 1-26.

Cohen, T. R., Wolf, S. T., Panter, A. T. and Insko, C. A., 2011. Introducing the GASP scale: a new measure of guilt and shame proneness. *Journal of Personality and Social Psychology*, 100(5), pp. 1-73.

Coombes, H., 2001. Research using IT. Palgrave Macmillan.

Creswell, J. W., 2007. Qualitative inquiry and research design: Choosing among the five approaches. 2nd ed. Thousand Oaks, CA: Sage.

Creswell, J. W., 2009. Research Design: qualitative, quantitative, and mixed methods approaches. 3rd ed. *Thousand Oaks,* CA: Sage.

Creswell, J.W., 2012. Educational Research. Planning, Conducting, and Evaluating Quantitative and Qualitative Research. 4th ed. Pearson Education, Boylston Street, Boston, USA.

CSIRT, 2009. Computer Security Incident Response Team. Ministry of Finance of the SR. Available at: < https://www.csirt.gov.sk/> [Accessed 25 February 2015].

CSTB (Computer Science and Telecommunications Board)., 1991. Computers at Risk: Safe Computing in the Information Age. *Washington, DC: National Academy Press*, pp. 1-320.

Dhillon, G. and Backhouse, J. 2000. Technical opinion: Information system security management in the new millennium. *Communications of the ACM*, vol. 43(7), pp. 125-128.

Dhillon, G., and Backhouse, J., 2001. Current directions in IS security research: towards socio-organizational perspectives. *Information Systems Journal*, 11(2), pp. 127-153.

Dimopoulos, V., Furnell, S., Jennex, M. and Kritharas, I., 2004. Approaches to IT Security in Small and Medium Enterprises. In AISM, pp. 73-82.

Doherty, N. F. and Fulford, H, 2006. Aligning the information security policy with the strategic information systems plan. *Computers & Security*, 25(1), pp. 55-63.

Dutta, A. and McCrohan, K., 2002. Management's role in information security in a cyber economy. *California Management Review*, 45(1), pp. 67-87.

European Commission, 2003. Commission recommendation concerning the definition of micro, small and medium-sized enterprises. *Official Journal of the European Union 2003/361/EC*. Available at: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2003:124:0036:0041:EN:PDF> [Accessed 5 June 2015].

European Commission, 2013. Digital Agenda for Europe: Trust and security - analysis and data – Pillar actions overview. European Commission. Available at: < http://ec.europa.eu/digital-agenda/trust-and-security-analysis-and-data> [Accessed 25 February 2015].

European Commission, 2014. Digital Agenda for Europe: Action 29: Combat cyber-attacks against information systems. European Commission. Available at: < http://ec.europa.eu/digital-agenda/en/pillar-iii-trust-security/action-29-combat-cyber-attacks-against-information-systems> [Accessed 25 February 2015].

European Commission, 2014. Enterprise and Industry SBA Fact Sheet 2014 – Slovakia, pp. 1-17. Available at: < http://ec.europa.eu/enterprise/policies/sme/facts-figures-analysis/performance-review/files/countries-sheets/2014/slovakia_en.pdf> [Accessed 16 February 2015].

European Parliament, 2013. Directive 2013/40/EU of the European Parliament and of the Council on attacks against information systems and replacing Council Framework. *Official Journal of the European Union.* Available at: < http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:218:0008:0014:EN:PDF> [Accessed 25 February 2015].

Fiol, C. M., 2001. Revisiting an identity-based view of sustainable competitive advantage. *Journal of Management,* 27(6), pp. 691-699.

Fox, S. and Spector, P. E., 2005. Counterproductive work behavior: Investigations of actors and targets. Washington, DC: American Psychological Association, pp. 105-107.

Glaser, B. G. and Strauss, A. L., 1967. The discovery of grounded theory: Strategies for qualitative research. *Chicago: Aldine.*

Gostev, A., 2012. Cyber-threat evolution: the year ahead. *Computer Fraud & Security,* pp. 9-12

Gregor, S., Lin, A. Gedeon, T., Riaz, A., and Zhu, D., 2014. Neuroscience and a Nomological Network for the Understanding and Assessment of Emotions in Information Systems Research', *Journal Of Management Information Systems,* 30, 4, pp. 13-48.

Guariniello, C., and DeLaurentis, D., 2014. Communications, Information, and Cyber Security in Systems-of-Systems: Assessing the Impact of Attacks through Interdependency Analysis. *Procedia Computer Science,* 28, pp. 720-727.

Hansen, L. & Nissenbaum, H., 2009. Digital disaster, cyber security, and the Copenhagen School. *International Studies Quarterly,* pp. 1155-1175.

Harrison, P. (2005). Linux quick fix notebook. Prentice Hall PTR. Chicago

Hart, C., 2005. Doing your masters dissertation. London: Sage.

Hathaway, O. A., Crootof, R., Levitz, P., Proctor, H., Nowlan, A. E., Perdue, W., and Spiegel, J., 2012. *The Law of Cyber-Attack,* pp. 1-71.

Hu, Q., Hart, P., and Cooke, D., 2007. The role of external and internal influences on information systems security–a neo-institutional perspective. *The Journal of Strategic Information Systems,* 16(2), pp. 153-172.

Hunton, P., 2009. The growing phenomenon of crime and the internet: A cybercrime execution and analysis model. *Computer Law & Security Review,* 25(6), pp. 528-535.

Infosec and ISO, 2013. INFORMATION SECURITY & ISO 27001: An Introduction. Infosec and ISO27001v3-uk. Available at:

< http://www.itgovernance.co.uk/files/Infosec_101v1.1.pdf> [Accessed 25 February 2015].

ISO/IEC, 2012. Information technology — Security techniques — Guidelines for cybersecurity. ISO/IEC27032(E). Available at: < http://webstore.iec.ch/preview/info_isoiec27032%7Bed1.0%7Den.pdf> [Accessed 25 February 2015].

ISO/IEC, 2014. Information technology — Security techniques — Information security management systems — Overview and vocabulary. ISO/IEC27000(E). Available at: < http://standards.iso.org/ittf/licence.html> [Accessed 25 February 2015].

Investment in Slovakia, 2013. *KPMG in Slovakia,* pp. 1-74. Available at: < https://www.mzv.sk/App/wcm/media.nsf/vw_ByID/ID_1822BC4B663925F9C1257AB8004F2D94_SK/$File/Investment-Slovakia-2013.pdf> [Accessed 15 February 2015].

Jee, S., 2014. SMEs often a 'weak link' for cyber attacks, experts warn. *Computer World UK,* [online] Available at: < http://www.computerworlduk.com/news/security/3583875/smes-often-a-weak-link-for-cyber-attacks-experts-warn/> [Accessed 8 March 2015].

Jouini, M., Rabai, L. B. A., and Aissa, A. B., 2014. Classification of security threats in information systems. *Procedia Computer Science,* 32, pp. 489-496.

Julisch, K., 2013. Understanding and overcoming cyber security anti-patterns. *Computer Networks,* 57, Elsevier B.V., pp. 2206-2211.

Kajtazi, M., 2013. *Assessing Escalation of Commitment as an Antecedent of Noncompliance with Information Security Policy.* Doctoral dissertation, Linnaeus University Press, pp. 1-164.

Kaufmann, J., 2011. Poststructural analysis: Analyzing empirical matter for new meanings. *Qualitative Inquiry, 17(2),* pp. 148–154.

Kindervag, J., Holland, R., Balaouras, S. and Mak, K., 2011. Planning For Failure. *Forrester Research Inc.,* pp. 1-16.

Kotter, J. P., 2012. Leading change. Harvard Business School Press, pp. 1-199.

Krawczyk, D., Bartlett, J., Kantarcioglu, M., Hamlen, K. and Thuraisingham, B., 2013. Measuring expertise and bias in cyber security using cognitive and neuroscience approaches. In *Intelligence and Security Informatics (ISI),* IEEE International Conference, pp. 364-367.

Kritzinger, E. and von Solms, S. H., 2010. Cyber security for home users: A new way of protection through awareness enforcement. *Computers & Security*, 29(8), pp. 840-847.

Kshetri, N., 2005. Pattern of global cyber war and crime: A conceptual framework. *Journal of International Management*, 11(4), pp. 541-562.

Kumar, N., Mohan, K., and Holowczak, R., 2008. Locking the door but leaving the computer vulnerable: Factors inhibiting home users' adoption of software firewalls. *Decision Support Systems*, 46(1), pp. 254-264.

Leech, N. L. and Onwuegbuzie, A. J., 2007. An array of qualitative data analysis tools: A call for data analysis triangulation. *School Psychology Quarterly*, 22(4), pp. 557.

Lichtman, M., 2013. Qualitative Research In Education : A User's Guide. Los Angeles: SAGE, pp. 1-368.

Loch, K. D., Carr, H. H. and Warkentin, M. E., 1992. Threats to information systems: today's reality, yesterday's understanding. *MIS Quarterly*, pp. 173-186.

Lopes, I. and Oliveira, P., 2014. Understanding information security culture: a survey in small and medium sized enterprises. In New Perspectives in Information Systems and Technologies, Volume 1, *Springer International Publishing*, pp. 277-286.

Maisey, M., 2014. Moving to analysis-led cyber-security. *Network Security*, pp. 5-12.

Mattern, T., Felker, J., Borum, R. And Bamford, G., 2014. Operational Levels of Cyber Intelligence. *International Journal of Intelligence and Counter Intelligence*, 27(4), pp. 702-719.

Mateti, P., 2006. Viruses, Worms and Trojans. Available at: < http://cecs.wright.edu/people/faculty/pmateti/Courses/4420/Viruses/> [Accessed 18 May 2015].

McFarlan, W. F., McKenney, J. L. and Pyburn, Philip, 1983. The information archipelago-plotting a course. *Harvard Business Review*, pp. 145-156.

Montesino, R. and Fenz, S., 2011. Information security automation: how far can we go?. *In Availability, Reliability and Security (ARES), 2011 Sixth International Conference on IEEE*, pp. 280-285.

Mörtberg, C., Bratteteig, T., Wagner, I., Stuedahl, D., and Morrison, A., 2010. Methods that matter in digital design research. In: I. Wagner, T. Bratteteig, & D. Stuedahl, (eds). 2010. Exploring digital design. London: Springer Verlag. pp. 105-144.

Myers, M. and Avison, D., 2002. Qualitative research in information systems. *Thousand Oaks, CA: Sage Publications.*

Ng, B. Y., Kankanhalli, A. and Xu, Y. C., 2009. Studying users' computer security behavior: A health belief perspective. *Decision Support Systems*, 46(4), 815-825.

Nissenbaum, H., 2005. Where Computer Security Meets National Security. *Ethics and Information Technology*, pp. 61-73.

Ponemon Institute, 2011. Second Annual Cost of Cyber Crime Study. Independently conducted by Ponemon Institute LLC, pp. 1-30. Available at: < http://www.hpenterprisesecurity.com/collateral/report/2011_Cost_of_Cyber_Crime_Study_August.pdf> [Accessed 8 March 2015].

Potts, M., 2012. The state of information security. Network Security, 2012, pp. 9-11.

Raiu, C., 2012. Cyber-threat evolution: the past year. *Computer Fraud & Security*, pp. 5-8.

Reed, R. and DeFillippi, R. J., 1990. Causal ambiguity, barriers to imitation, and sustainable competitive advantage. *Academy of Management Review*, 15(1), pp. 88-102.

Rezek, T., Szatkowski, T., Świątkowska, J., Vyskoč, J. and Ziarek, M., 2012. V4 Cooperation in Ensuring Cyber Security – Analysis and Recommendations. *The Kosciuszko Institute*, pp. 1-47.

Richardson, R., 2008. CSI computer crime and security survey. *Computer Security Institute*, pp. 1-30.

Robbins, S. P., DeCenzo, D. A. and Gao, J., 2007. Fundamentals of management. Pearson Prentice Hall.

Rodriguez, C. and Martinez, R., 2013. The Growing Hacking Threat to Websites: An Ongoing Commitment to Web Application Security. *Frost & Sullivan*, pp. 1-25.

Safford, D., & Zohar, M. 2005. A trusted linux client (tlc). Technical Paper, IBM Research.

Sahito, F. H. and Slany, W., 2012. Functional Magnetic Resonance Imaging and the Challenge of Balancing Human Security with State Security. *Human Security Perspectives*, pp. 38-66.

Schmidt, A. D., Schmidt, H. G., Clausen, J., Yuksel, K. A., Kiraz, O., Camtepe, A. & Albayrak, S., 2008. Enhancing security of linux-based android devices. *In in Proceedings of 15th International Linux Kongress. Lehmann.*

Schneier, B., 2008. The psychology of security. In Progress in Cryptology–AFRICACRYPT, *Springer Berlin Heidelberg*, pp. 50-79.

Shank, G. D., 2002. Qualitative research: A personal skills approach. *Prentice Hall.*

Shaw, E., Ruby, K. and Post, J., 1998. The insider threat to information systems: The psychology of the dangerous insider. Security Awareness Bulletin, 2(98), pp. 1-10. Chicago

Siegel, C. A., Sagalow, T. R. and Serritella, P., 2002. Cyber-risk management: technical and insurance controls for enterprise-level security. *Information Systems Security*, 11(4), pp. 33-49.

Sommestad, T., Ekstedt, M. and Johnson, P., 2009. Cyber security risks assessment with Bayesian defense graphs and architectural models. *In System Sciences, HICSS. 42nd Hawaii International Conference on IEEE*, pp. 1-10.

Spector, P. E., Bauer, J. A. and Fox, S., 2010. Measurement artifacts in the assessment of counterproductive work behavior and organizational citizenship behavior: Do we know what we think we know*? Journal of Applied Psychology*, 95(4), pp. 781-790.

Spradley, J. P., 1979. The ethnographic interview. *For Worth, TX: Holt, Rinehart and Winston.*

Symantec Team, 2012. Internet security threat report: 2011 trends. Symantec Corporation, pp. 1-52. Available at: <https://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_2011_21239364.en-us.pdf> [Accessed 15 February 2015].

Symantec Team, 2014. Internet security threat report: 2013 trends. Symantec Corporation, vol. 19, pp. 1-98. Available at: < http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf> [Accessed 15 February 2015].

Tangney, J. P., and Dearing, R. L., 2002. Shame and guilt. *Guilford Press.*

Tawileh, A., Hilton, J. and McIntosh S., 2007. Managing Information Security in Small and Medium Sized Enterprises: A Holistic Approach. Highlights of the Information Security Solutions Europe, *SECURE Conference, Warsaw*, pp. 1-11.

Turban, E. R., Sharda, D., Delen, D., King & Aronson, J. E., 2010. Business intelligence: a managerial approach. 2nd edition, Prentice Hall, pp. 1 – 292.

Van Oers, M., 2000. LINUX VIRUSES–ELF FILE FORMAT. VIRUS, 123.

Verizon Risk Team, 2012. 2012 data breach investigations report. Verizon Technical report, pp. 1-80. Available at:
< http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf> [Accessed 14 February 2015].

Vives, A., 2006. Social and environmental responsibility in small and medium enterprises in Latin America. *Journal of Corporate Citizenship*, 2006(21), pp. 39-50.

Von Solms, R., and Van Niekerk, J., 2013. From information security to cyber security. *Computers & Security*, 38, pp. 97-102.

Walsham, G., 1995. Interpretive case studies in IS research: nature and method. *European Journal of Information Systems*, 4(2), pp. 74–81.

Walsham, G., 2006. Doing interpretive research. *European Journal of Information Systems*, 15(3), pp. 320–330.

Watters, P. A., McCombie, S., Layton, R. and Pieprzyk, J., 2012. Characterising and Predicting Cyber Attacks Using the Cyber Attacker Model Profile (CAMP). *Journal of Money Laundering Control*, 15(4), pp. 430-441.

Weill, P. and Ross, J. W., 2005. IT governance: How Top Performers Manage IT Decision Rights for Superior Results. *International Journal of Electronic Government Research*, 1(4), pp. 63-67.

Yin, R., 2009. Case study research: design and methods. 4th ed. Thousand Oaks: Sage.

Appendix 1 - Interview Guide

Dear interviewee,

Thank you for accepting to participate in this study. My name is Milos Zec, acting as a researcher on this study, while currently I am a master’s student in Information Systems program at Linnaeus University in Sweden. Your participation in this interview will be completely anonymous. This means, that your name, surname and other personal details as well as the details of the company you work for will stay forever confidential. The purpose of this interview is to research how IT professionals create their decisions in small and medium size enterprises, particularly tackling the organizational, technological and organizational aspects that may influence such decisions. Therefore, I, as the researcher will ask you several questions that will not depend on correct or incorrect answers, considering that each answer depends on the context you operate within. Further, you will be kindly asked to be type recorded while answering the questions but if you are not comfortable with it, the paper notes will be taken. Additionally, if your decision to take your participation in this study is positive, you will be able to withdraw at any moment without any prior explanation.

We will first start with some general questions, followed by questions that relate to the organizational, technological and psychological aspects.

Type of questions	Interview questions
General	Could you please provide us with some general details about the company you work for (for example, number of employees, core of business, domestic or international business operations)?
General	Could you please tell us how many people are responsible for cyber security in the company you work for and are they general IT professionals or specifically educated for the field of cyber security?
General	In your opinion, how much is your company dependent on the cyber space (for example, e-mail collaboration, online money transactions such as payments, etc.)?
General	How much do you think cyber security is important for the company you work for?

Type of aspect	Period of cyber-attack	Interview questions
Organizational	*Pre-cyber-attack*	Are any of the national, EU or international cyber security standards implemented and used in your organization? Please list them. If not,

		how much you are familiar with them?
Organizational	*Pre-cyber-attack*	Is there any cyber security policy created in your organization and if there is, who created it (did you also as an IT professional take part in creation of this document; do you think it is important for small and medium enterprises to have cyber security policy)?
Organizational	*Pre-cyber-attack*	If there is a security policy in your organization, are you of opinion that it is used in practice or it only exists formally?
Organizational	*Pre-cyber-attack*	Who decides about the value of information system assets and prioritization of the information? What are the processes in order to assess these asset risk exposure?
Organizational	*Pre-cyber-attack*	Who decides about system access permissions? Is it you or management or both? What is your opinion about who should decide about this and why?
Organizational	*During-cyber-attack*	Are there any prescribed roles and accountabilities about measures if a cyber-attack happens in the real time (for example to turn off servers or the Internet connection on purpose, in order to stop the attack)?
Organizational	*Post-cyber-attack*	Please explain how is it decided whether a cyber-attack is a single isolated accident case or it is only a part of a large attack that is directly meant for this particular organization?
Organizational	*Post-cyber-attack*	Does someone from the company inform company's clients, stakeholders or for example national cyber security body if a cyber-attack occurs? Who spreads the information and in your opinion, how important is it to inform those who may be affected or who may need to record the attack)?

Type of aspect	**Interview questions**
Technological	Does your company track and analyze system logs and how the system logs are analyzed?
Technological	Is there a complete inventory list of hardware and software in order to authorize them in your information system?
Technological	Do you do system backups (how often, what data, how long are data stored in the system, how quick can you retrieve backup data)?
Technological	Does your organization use antivirus software and does it analyze identified threats?
Technological	Do you use passwords in order to protect your information system

	(password rules, frequency of changing passwords, shared or only personal passwords)?
Technological	Is Internet firewall used in your organization and what the firewall rules are applied against?

Type of aspect	**Aim, type and period of cyber security measures creation**	**Interview questions**
Psychological	*Level of guilt and shame/general type*	You are just about to run a regular IS security scan but you unpredictably receive important administrative work to accomplish. Would you postpone the regular system scan or the given administrative work? Please explain your decision on this matter and describe how you would feel after you made the decision.
Psychological	*Level of guilt and shame/general type*	At the end of your worktime you discover a minor security gap in IS. Would you leave this error to be corrected for tomorrow or you would stay an additional three or four hours needed to close this security gap? Please explain your decision.
Psychological	*Level of guilt and shame/general type*	The management in your organization requires from you to create cyber security measures but you are aware there are no enough financial resources available for that. Would you anyway create deficient measures with the resources available or you would hesitate to do so by extensively explaining all the reasons and dangers of management's requirements and try to pursue them this way to invest more?
Psychological	*Distinguishing the guilt and shame proneness/during CS measures creation*	While creating cyber security measures you realize that you are in lack of expertize in one particular domain, but no one else can realize this. Would you report your lack of expertize to the management and discuss the issue or you would find a resort in some other solution?
Psychological	*Distinguishing the guilt and shame proneness/post CS measures creation*	You discover that there is important information data leakage to the Internet from your information system. No one from the company you work for knows this has happened but will probably never find it out and you are able to correct the mistake. Would you inform the management about the accident or you would not. Please explain your decision.
Psychological	*Distinguishing the*	You realize the organization you work for would

	guilt and shame proneness/post CS measures creation	greatly benefit from buying and implementing a certain cyber security software/system, which is very costly. However, you succeed to persuade the management to invest into it. How would you feel and what would be your actions if after certain amount of time you realize that this costly investment was a wrong decision. In order to correct the mistake another 50% of overall investment on the software/system is needed to correct your mistake. Would you inform the management and explain your decision?

Appendix 2 – Consent Form

Research title: A study on IT professionals' Organizational Cyber Security Awareness while making decisions about cyber security measures across SMEs

Name of researcher, academic program, university and research info: Milos Zec, Master Program in Information Systems, Linnaeus University, mz222ch@student.lnu.se m.workplace@gmail.com

Research purpose: The purpose of this study is to understand the level of IT professionals from organizational, technological and psychological aspects when making decisions about cyber security in SMEs

Research process description: There will be an interview where you will be asked questions about how cyber security measures are created in your organization. You will be able to choose to allow the interviewer to record your answers or if you are uncomfortable with the recording, notes can be taken. Your answers will be analyzed for the purpose of this study and there is also a possibility for using them for writing scientific articles.

Research benefits: The benefit of this study is to contribute to rising of cyber security awareness of IT professionals in SMEs and in that way to help them to decrease cyber-attacks in these organizations. This study also aims to find the additional reasons of cyber security failure in SMEs that are not of financial investment nature.

Risk and discomfort: This research does not bring any discomforts to interview participants because only the questions relevant to cyber security measures creation will be asked. Your name and the name of the company you work for will be never revealed to anyone except the researcher. Only the information about the number of employees, your professional role and importance of cyber security to your organization will be exposed in the study.

Participant's rights about information: All the collected data through the interview will be available to you and your company at request at any time. You will be able to withdraw the interview process and request that the data collected not to be used for this study.

Confidentiality: The interview answers will never be shared with the third parties and will be used only for the purpose of this research and also for the purpose of writing scientific articles that could be published in scientific conferences worldwide. In the case of recordings, after they are transcribed on the paper or electronic format will be deleted so if you would wish to have the recording of your answer you can receive it after the interview.

Research inquires: If you have any additional inquires about this research you are welcome to contact the researcher on his e-mail address that is stated above. If you require to see the interview guide before the interview, feel free to contact and ask the researcher for it.

Please tick the boxes below in order to express your preferences:

- I understand this study nature and consent to take participation in it

  □ Yes □ No

- I consent for my answers being recorded

  □ Yes □ No

- I understand that my answers will be taken only for the purpose of this study and that anyone else will not have access to them except the researcher

  □ Yes □ No

- I agree that the data collected through interview with me can be used for the purpose of writing scientific articles and can be published in scientific conferences worldwide

  □ Yes □ No

- I am deeply aware that I can withdraw my participation in this study at any time and without any explanation

  □ Yes □ No

Date: ____________________

Signature of the participant: _______________________

Name of the researcher: Milos Zec

Appendix 3 - Empirical findings from the general types of questions

Company 1

The first interview of this study took place in company's premises between 10 and 10:30 o'clock, on 1st April 2015. There was a warm welcome from the Interviewee 1 who offered a cup of coffee and introduced himself. He is a general IT professional who takes care of overall company's IT activities so the cyber security is also under his responsibility. Then he explained that the company he works for operated internationally because it imports children's garments from abroad and distributes it on the domestic market i.e. the Republic of Slovakia. He continued by saying that it was a small company with 25 employees. He further expressed that *"…my company is quite dependent on the cyber space because we use e-mail correspondence with our suppliers from abroad as well as with our distributors here in Slovakia… "*, and added *"…we also use online money transactions. "*. The interviewee from Company 1 said that he considers cyber security as a very important and integral field of IT and that it is also important for his company due to mainly of sending and receiving the online payments that must be secured. He concluded his answer by saying that *"The cyber security is very important for the company I work for and I am of opinion that this importance will be growing over the time as the general ICT field is developing in an extreme pace. "*.

Company 2

The interview of Interviewee 2 took place between 12 and 12:35 o'clock in the meeting room of Company 2 on 2nd April 2015. This interview was held during the lunch time so some food was served and questions and answers were provided while having lunch. The interviewee is an IT professional who is specialized in the field of cyber security and he is the only person whose main responsibility is to be in charge of company's cyber security. The core business of this company is importing and exporting construction materials and therefore it operates internationally. It is a medium business organization that employs 70 people. When being asked about the company's dependency on the cyber space, Interviewee 2 replied *"We are very dependent on the cyber space as we collaborate with our suppliers and clients by electronic mail. Beside this, we have a web page where we advertise our business and where purchases can be made. Moreover, these purchases can be paid online which is a very sensible part of our business. "*. He also added *"Internet is very useful for our business because we use it for multiple purposes such as finding new clients and suppliers as well as making products research. "*. Interviewee 2 explained that the importance of cyber security of his company is very high because without the cyber space, they would not be able to keep pace with the competition. For the end he concluded *"We have to have a mechanism of keeping our business safe and the tool to help us do this is the cyber security. "*.

Company 3

The third interview was held on 3rd April 2015 between 18 and 18:50 o'clock via the social media software called Viber. This company is placed in the outskirts of Kosice city and after the working hours due to preoccupation of the Interviewee 3. The interviewee introduced himself and the company by saying the number company's employees was 15. Therefore we concluded that it was a small company. The company's business field is cooperative for ethical finance and Interviewee 3 is the only IT person in charge for all IT activities including the cyber security domain. The business of Company 3 is related to domestic market as well as to international due to its cooperation with some business organizations abroad. The question about company's dependency on the cyber space was answered in the following manner *"… our business is heavily dependent on the Internet because all of our transactions with clients and investors are online. We also regard our marketing activities to the internet and most of our business communication is done online via VOIP* (Voice Over Internet Protocol). *".* After Interviewee 3 explained that all of business operations of the company were performed in the cyber space, he was asked about the importance of the cyber security in his organization that he responded by saying that *"… obviously, the cyber security is a very important domain of our business when we do almost everything over the Internet. ",* and added *"It would be hard to imagine our business without the cyber security as it would be extremely endangered. ".*

Company 4

The interview with Interviewee 4 was held over the social media software called Skype because at the time of interview the IT professional was abroad. The time when the interview took place was in the late evening hours i.e. from 21:30 until 22:10 o'clock on 4th April 2015. Interviewee 4 described that the company he works for is a restaurant and also has the service of food delivery. He also said that it was a small company that has 11 employees and that it only operates in the domestic market. The interviewee is a general IT professional who takes care for all the ICT activities in the company which is also cyber security. Therefore he is not a specialized cyber-security professional. When asked to express the company's dependence on the cyber space, the interviewee responded *"We have a software application for food online orders that is web-based and where our customers can pay online via that application or to pay when the food is delivered. "*. He also added that *"We use another application in the restaurant for food orders, payments and table booking that can be accessible via the internet and from this point we can say that we rely our business activities on the cyber space pretty much. "*. The interviewee at the end concluded that *"Therefore, I am of opinion that the cyber security is quite important for our overall business and operations. ".*

Company 5

The fifth interview was held in the company's premises of Company 5 after working hours between 17:10 and 17:45 o'clock on 6th April 2015. The interviewee was a cyber-security professional with a master degree in the field of cyber security. His main responsibility in this company was to work with cyber security and he was the only person who was in charge in this field. The core business of the company is point of sale terminal deployment and it belongs to medium enterprises due to employment of 56 persons. The company operates only on the territory of Slovakia. Interviewee 5 explained that their company is highly dependent on the cyber space as they have to perform online software installations very often and also the installed software maintenance on a daily basis. He also continued by explaining that they use electronic mail and online payments which are performed in the cyber space as well. When being asked about his opinion of cyber security importance in the company, he responded "*Without cyber security our company would have been wiped off a long time ago and would not exist* (laughter). ". He continued "*All the operations that are the core of our business are crucial for our company's development and survival and these activities have to be closely watched all the time.* ". He added "*…otherwise, we could easily disappear over a night.* ".

Company 6

The last interview took place from 11 to 11:40 o'clock on 7th April 2015. The interview was held via Skype due to Interviewee 6 preferred this type of communication and the interview guide had been previously sent to him as he wanted to get introduced about the questions before the interview took place. This company operates internationally and its core business is assembly line production. It belongs to small enterprises due to it employs 18 people. Interviewee 6 is a general IT professional which means that he is only one person who takes care of overall ICT in the company where the field of cyber security is included. The interviewee 6 described that the company's information system consists from web site, VOIP, CRM (Customer Relationship Management System) and online money transactions and responded "*Our business requires many activities to be performed in the cyber space so I consider our organization has to thank for its existence a lot.* ". When being asked about importance of cyber security for his organization, Interviewee 6 replied "*I see the cyber security as an important part of our business operations because the cyber-crime has been in its increase and develops fast.* ". He then concluded "*My friends who work in this field told me some almost unbelievable stories to what extent the cyber attackers are ready to go in order to achieve their aims. I think the times are getting tougher and tougher for us who work in this field.* ".

Linnæus University
Sweden

Faculty of Technology
SE-391 82 Kalmar | SE-351 95 Växjö
Phone +46 (0)772-28 80 00
teknik@lnu.se
Lnu.se/fakulteten-for-teknik