OULU UNIVERSITY OF
APPLIED SCIENCES

Sami Pohjolainen

INFORMATION SECURITY IN FINNISH SMALL AND MEDIUM ENTERPRISES

Current state and future trends

INFORMATION SECURITY IN FINNISH SMALL AND MEDIUM ENTERPRISES

Current state and future trends

Sami Pohjolainen
Bachelor's thesis
Spring 2013
Business Information Technology
Oulu University of Applied Sciences

ABSTRACT

Oulu University of Applied Sciences
Business Information Technology

Author(s): Sami Pohjolainen
Title of Bachelor's thesis: Information Security in Finnish Small and Medium Enterprises – Current state and future trends
Supervisor(s): Anu Niva
Term and year of completion: Spring 2013 Number of pages: *47 + 5 appendices*

The purpose of this study was to examine the current state and future trends of information security in small and medium enterprises in Finland. The research was a part of a pan-European research program and was commissioned by a local company in Oulu.

The research task was completed in two main parts. Preliminary research was conducted as a secondary research and included examination of previous research done in Finland and familiarization with the subject matter through books and other sources. Primary research included data collection, analysis and summary. The data was collected with an online survey that was sent out to 3800 unique enterprises from which 157 responded.

The main conclusion from the survey was that enterprises currently have a positive, but somewhat inflated view, of their information security when compared with the actual steps they have taken to improve it. Another conclusion was that many enterprises are planning to develop and invest in their information security in the next few years.

Keywords: Information Security, InfoSec, Market Research, Information Security Management, SME, Small and Medium Enterprises

CONTENTS

1 INTRODUCTION

The landscape of information security related threats is changing. New types of devices, services and criminals are forcing organisations to adopt stricter and flexible security policies. All size of organisations are vulnerable and need to protect their information assets. Particularly vulnerable are those small and medium enterprises (SMEs) who do not have proper security controls in place and do not see information security as a problem.

There are readily available sources of information that provide guidance for smaller enterprises that are looking to improve their information security. Unfortunately, the number of studies done to understand the needs of SMEs is not as exhaustive. This could indicate that their needs are not properly understood, as studies tend to focus on larger organisations.

The objective of this study was to provide answers to research questions for the commissioner, Net Man Ltd (Net Man). The study was a part of a pan-European research program that included many organisations across Europe. One of the goals of the research program is to be able to offer better security products and services for smaller organisations.

The research task for this study was defined using specifications from the commissioner. The specific task was to examine the current state and future trends of information security in Finnish SMEs. There was added emphasis on administrative security as it was one of the focus areas of the pan-European program.

Research was completed in two parts. Preliminary research was conducted in order to gain theoretical understanding on the subject and ability to formulate good questions for the questionnaire. Primary research included data collection, analysis and summarisation. Online survey was chosen as the method that would best gain answers to the research task. The survey was sent out to 3800 unique enterprises in Finland. It was answered by 157 decision makers in those enterprises. The findings were first reported to the pan-European research program and later included to this thesis.

There are few notable limitations to this study. Micro enterprises with fewer than 10 employees were excluded. Although, there are many of them, they have very basic IT needs. Also, the sample was selected from a database but included judgement based sampling. Judgements were based

on the type of industrial sectors, as the goal was to select information intensive sectors and other sectors that use information systems. The aim was to choose those respondents that are decisions makers and in charge of information security in their enterprises. This was also based on available information and judgment. There is also a risk that some respondents may not have taken the survey seriously and affected the results.

Net Man Ltd

The thesis was commissioned by Net Man, as a part of a work for the Predykot project (Predykot). Net Man is a Finnish ICT and business technology service provider. It was founded in 1992 and is currently privately owned. The company offers flexible, efficient and professional information management services for enterprises and other organisations (Net Man Oy 2013. date of retrieval 12.4.2013).

Net Man currently employs around 30 people and made just over 3.3 million euros in revenue in 2012. The company is a part of the Predykot consortium that consists of 16 expert organisations from all over Europe.

ITEA2 and Predykot

Predykot is an ITEA2 project. ITEA2 stands for Information Technology for European Advancement. The goal of ITEA2 is to stimulate and support innovative, industry-driven, pre-competitive research and development projects. The aim is to contribute research excellence to Europe's competitive software-intensive systems and services sector. (ITEA2 2013. date of retrieval 12.4.2013)

Predykot stands for 'Policy Refined Dynamically and Kept On Track'. The project aims to provide an innovative, modular and consistent ecosystem of software modules to dynamically improve a security policy and keep it on track. The project also examines appropriate parts of security management standards, such as ISO 27001.

The project brings together major European industrial actors in the information security field. These companies and organisations will gain tangible outcomes from the project in their respective business areas. One of the tasks of Net Man was to conduct market research on the SME sector in Finland. Other Finnish participants in Predykot include Oulu University, Nixu and Pohto. (Predykot-ITEA2 2013. date of retrieval 14.4.2013)

2 INFORMATION SECURITY FOR ORGANISATIONS

The purpose of this chapter is to go through the basics of information security and familiarise the reader with the key concepts used in this study. The focus is on organisational information security. This is not meant as a comprehensive guide on information security, but should provide substance to those less familiar with the topic.

2.1 Information security is a part of corporate security

Information security is essentially a part of corporate security, as seen in figure 1. The purpose of corporate security is management of security, continuity and safety of an organisation. The parts that need to be taken into account can vary greatly between organisations, but security governance as a whole is an important aspect of organisational management, as it protects staff, reputation, data, assets and environment where the organisation functions. Different sections of corporate security have overlap. For example, information security can have overlap with all sections. (Confederation of Finnish Industries 2013, date of retrieval 10.4.2013.)

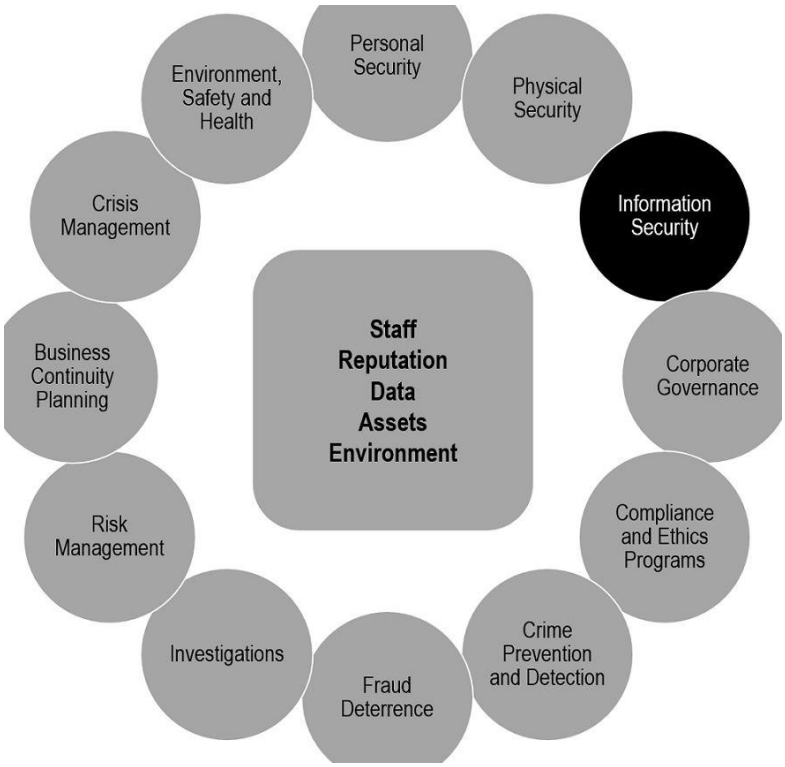

FIGURE 1. Sections of corporate security (Confederation of Finnish Industries 2013, date of retrieval 10.4.2013)

The role of information security is to keep data and systems protected from natural disasters and those who would seek to exploit or misuse them. This is accomplished by supporting organisational needs and by meeting both internal and external requirements. The requirements should become evident in a risk assessment process. (Laaksonen, Nevasalo & Tomula 2006, 17.)

Information security needs to take into account a broad range of potential risks and to provide means to protect and secure against them. Today, risks are not solely on physical things like computing hardware or networks, but also on intellectual property, such as source code or data. Threats can be both external and internal. While attacks can include things like theft or vandalism, good security also takes into account things like natural disasters and power failures. (Andress 2011, 2.)

2.2 Principles of information security

The CIA triad (figure 2) is a common security model used to discuss information security or identify problem areas and find solutions. The triad is considered common knowledge and is required understanding in security policy development. It consists of three parts that should be guaranteed in any kind of secure system: confidentiality, integrity and availability. If any part of the triad is breached, there can be serious consequences. The parts have been explained in this chapter. However, the triad is not without its critics, as it is seen as a limited view of looking at information security, but it is a good starting point. (Andress 2011, 4–6.)

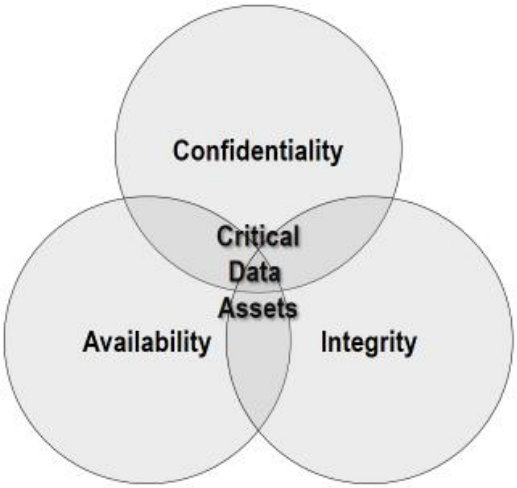

FIGURE 2. The CIA triad (Andress 2011, 4–6)

Confidentiality

Confidentiality is about protecting the privacy of information and it may be applied at many levels of a process. Confidentiality is breached when somebody intercepts information not meant for them. Such breaches can occur when somebody sees a person typing a password or someone steals a laptop. It can also include unintended breaches like when an email is sent to a wrong person. (Andress 2011, 4–5.)

Managing confidentiality is usually a task of Information Security Management System (ISMS). Tasks commonly include management of file permissions, access controls, and file and volume encryptions. (Perrin 2008, date of retrieval 10.4.2013.)

Integrity

Integrity is about managing the data by preventing it from being changed without authorization. It also means that data should be protected from authorised, but undesirable change or deletion. A well-managed information system should contain capacity to restrict access and actions from unauthorised users and feature an ability to reverse undesirable changes from authorised users. (Andress 2011, 5.)

Common technical level solutions to integrity issues include limited file permissions to key files, read-only flags for files, version control systems and backups. A typical attack could be interception of a file and making changes to it before passing it to the intended receiver. (Perrin 2008, date of retrieval 10.4.2013.)

Availability

Availability is about being able to access the data when needed. The task of Information security is to ensure access to data located in a system when something goes wrong. This can mean that customers are able to access the website even when it is suffering from a denial of service attack. It can also mean that employees have access to enterprise data when there is power loss or one of the application servers is down. (Andress 2011, 6.)

For example, high availability systems are designed so that there is limited disruption to the system access when an unwanted security event occurs. Those organisations that need a high uptime for their information systems can benefit from additional security measures that ensure rapid recovery

and high availability at all times. (Perrin 2008, date of retrieval 10.4.2013.)

2.3 Security threats

SMEs face both external and internal threats just like larger organisations. Unfortunately, most SMEs keep up only with the most basic level of information security unless required or mandated otherwise (PCToday 2012, 18). The basic level usually means having an anti-virus and a firewall. However, SMEs need to take care because the security landscape is constantly changing and becoming increasingly more threatening (GFI Software 2010, 2).

Security threats are increasing rapidly. For example, zero day viruses, that are previously unknown computer viruses or other malware with no antivirus signature available, have increased from a few thousand just a decade ago to hundreds of thousands. The volume of attacks is continuing to increase at an exponential rate. The positive news is that while the number of attacks has increased the actual types of threats have stayed pretty similar. (PCToday 2012, 12–13.)

Network related threats include spam, phishing, viruses, rootkits, and other types of malware. The difference today comes from the sophistication of attacks and the number of devices and services that are affected. Malware in particular has become a serious problem because of the multitude of devices that can be taken over or infected. Those responsible for these threats have also changed. In the past, hackers were often motivated by recognition. Today, cybercriminals are focused on economic benefits and are increasingly more organised. The level of organisation is a major concern, as resources of such organisations can be vast. (PCToday 2012, 12–19.)

Different type of attacks

The CIA Triad (figure 2) is also useful when looking at security threats in general. Different types of attacks can occur at different points of the triad. These attacks can be represented in four categories: interception, interruption, modification, and fabrication (Andress 2011, 8–9). Some of these can occur at more than one point of the triad as seen in table 1. The table shows type of attacks and what are the typical methods for that particular type of attack. It also shows what point of the CIA triad is affected by what type of attack and its methods.

TABLE 1. Type of attacks based on the CIA triad (Andress 2011, 8-9)

Type of attack	Typical methods	Triad point affected
Interception	▪ reading email ▪ eavesdropping ▪ unauthorised file viewing and copying	▪ Confidentiality
Interruption	▪ denial of service ▪ loss and corruption of data	▪ Integrity ▪ Availability
Modification	▪ asset tampering ▪ data alteration	▪ Integrity ▪ Availability
Fabrication	▪ generate undesirable data, processes or communications	▪ Integrity ▪ Availability

Most serious security attacks are often based on social engineering and people's willingness to trust each other. Social engineering means that people are manipulated to perform actions or give out confidential information. For example, a phishing email that is clicked by an employee can be used to spread malicious content. However, the most damaging security breaches often come from disgruntled employees or from industrial espionage. A disgruntled employee can steal valuable data and sell it to the highest bidder. Avoiding these types of attacks require an enforced security policy, access limitations and most importantly security awareness amongst employees. (GFI Software 2010, 3–5.)

2.4 Vulnerabilities

As information security is a part of the corporate security framework, it has a direct relationship with the organisation and its performance. Breaches in security can affect the image or cause financial problems. (Laaksonen et al. 2006, 19.) These problems are generally well-known and understood in larger organisations, but SMEs often lack required resources or expertise to implement appropriate measures.

In order to assess the impact, organisations need to understand threats, vulnerabilities and risks that they face. Risks can be understood by analysing the potential threats and whether the organisation is vulnerable to those. Once the risks are understood the potential impact for the business can be assessed and appropriate controls can be put in place. (Andress 2011,10–11.)

2.5 Information security controls

Organisations can mitigate risks by using security controls. Controls related to information security fall under three domains: administrative, logical (technical) and physical. (Andress 2011, 11-12.) These information security control domains have been explained in the next few sub chapters.

Administrative security

This control essentially defines how the information security organisation is run and managed. Administrative security includes policies, procedures, standards and guidelines that inform people how the organisation is supposed to be run on daily basis. It also defines responsibilities, tasks and forms the basis for other information security controls.

The types of administrative controls vary depending on the need and resources of the organisation. It is also important to measure how compliant the organisation is. If the policies and procedures are not followed, even a well-written security policy can have very little impact. Therefore, it is vital that policies are enforced and monitored with appropriate resources. (Andress 2011, 11-12.)

Technical security

Technical controls are probably the most well-known information security controls. These controls include things that many people deal with on daily basis, such as firewalls, encryption, passwords, and intrusion detection systems. The goal of technical controls is the prevention of unauthorised access to networks and systems. This means that intruders are not able to access organisation's networks or data. (Andress 2011, 11.)

Technical controls can be divided into three categories; preventive controls, wireless access controls and remote access security. Preventive controls include access controls software, malware solutions, passwords, security tokens and biometrics. Wireless access controls focus on limiting access to wireless networks, and encrypting and monitoring traffic. Remote access security is about providing external access to networks and systems, while protecting them from malicious use. (Olzak 2010, date of retrieval 10.4.2013.)

Physical security

Physical security is about protecting environments. It means protecting IT assets, such as servers and computers, from unauthorised access and other hazards. Without good physical security, the other security controls can become vulnerable and even meaningless. Physical controls include basic security measures such as fences, locks, gates, guards and cameras. One aspect of physical control is division of tasks and roles to ensure that the security is not dependant on a single person. (Andress 2011, 11.)

Physical controls can be divided into three parts; deterrent, detective and preventive. Deterring focuses on discouraging people from violating security controls such as signs and warnings. Detective controls on the other hand focus on detecting and reporting on violations. Detecting measures include systems like cameras and smoke detectors. Preventive methods can include anything from simple locks to high fences that prevent unauthorised access to certain areas. (Andress 2011, 100–101.)

2.6 Governance, risk management and compliance

While organisations need to understand security related risks, they are also required to comply with many direct and indirect requirements (Laaksonen et al. 2006, 18). The term used to describe this is compliance. It means that organisations need to conform, submit, or adapt as required or requested usually by a third party such as a business partner or government. It is also closely related to risk management and governance. Compliance requirements can help risk management to identify what security controls are needed and at what level. (Weiss & Salomon 2011, 8-9.)

Governance, risk and compliance (GRC) is an umbrella term used to describe a process that helps organisations to put in place policies and controls to address compliance related issues and also to gather information about the business. The goal of a GRC is to help manage an organisation more effectively (King 2012). What this means to information security is that risk management and compliance needs drive application of security controls, while a proper governance ensures that risks are managed in the right way by supporting the operational or business goals of the organisation.

Compliance requirements can come from various sources and can be internal or external. Requirements can also be mandatory or optional. Internal requirements can for example be about

how the organisation manages to conform to its information security policy. External requirements can be related to business practises or contracts, industry regulations, laws, standards or other practises that require an organisation to take steps to comply. Mandatory requirements are those that the organisation must fulfil, while optional ones can be adopted if assessment deems them appropriate or sensible. (Weiss & Salomon 2011, 8.)

Customers and business partners may also have requirements that must be complied with before starting to work with them. For example, a supplier may require a certain level of security before allowing a connection to their information systems. A typical example is the payment card industry that has developed its own security standards and also provides self-regulation. Any organisation who wants to take payments from the payment cards must comply with the Payment Card Industry Data Security Standard (PCI DSS). (Weiss & Salomon 2011, 8.)

Laws and regulations

Organisations have to comply with many laws and norms when operating in Finland or internationally. Figure 3 shows the landscape of Finnish legislations and some of the international norms that need to be considered. Impact on different parts of organisation's activities can vary. The figure is not an exclusive collection, but should provide an indication on how daunting the legislative landscape can be, especially for a SME. (Laaksonen et al. 2006, 21–23.)

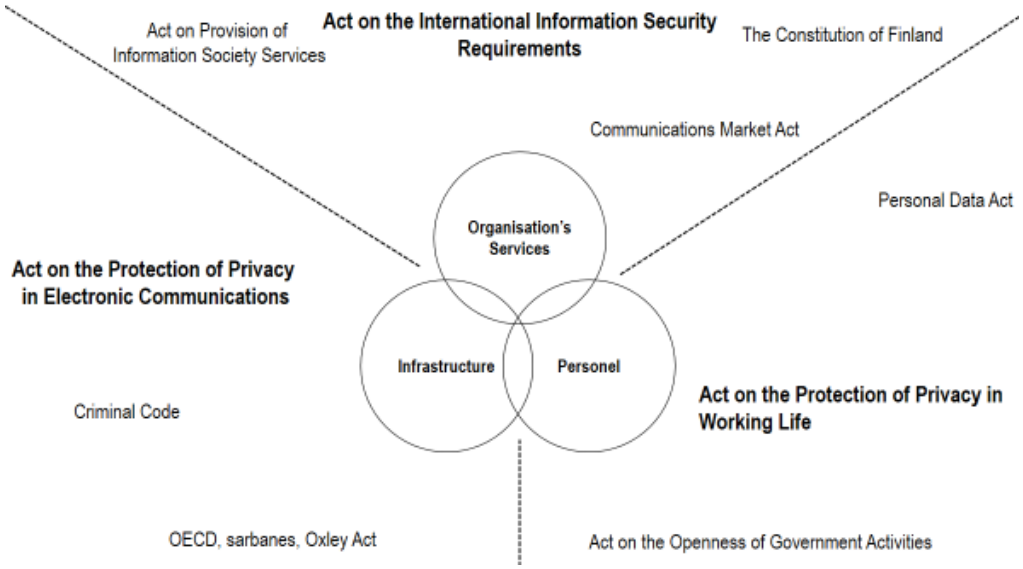

Figure 3. Finnish legislations and international norms related to Information Security (Laaksonen et al. 2006, 21–23)

Another major concern for organisations is the changing security landscape. Legislation also impacts this. For example, in 2013 the EU proposed a new Cyber Security Strategy for European Union, which would have an impact on many requirements at national, EU and international level. (European Commission 2013.)

Frameworks, models and standards

The legislative framework typically provides the foundation for information security policy development on the organisational level. In addition many frameworks, models and standards have been developed that can be used to help develop and manage information security needs. Not all models are suitable for all organisations, as some have been designed for specific purpose, industry or process, but there are more universal models that are also suitable for SMEs. (Laaksonen et al. 2006, 83–85.)

Organisations can also apply for certificates to that will help identify their level of information security. These certificates can be applied to services, products, systems and personnel. When organisation is looking at suitable certificates, they should consider how well-known they are and whether the enterprise will actually benefit from them. (Laaksonen et al. 2006, 84.) Applying for a security standard can create an image of trustworthiness, but it can also be very costly to upkeep. Many SMEs will have to assess the cost of any security standard against potential benefits. However, certification may be mandatory in some cases. (Laaksonen et al. 2006, 107.)

A well-known information security standard is the ISO/IEC 27000-series, which will be the focus of the next sub-chapter and has also been used as a framework in the research for this thesis. Another well-known standard of good practice for information security is provided by Information Security Forum (ISF), but it is mostly used by larger organisations and therefore does not apply to this thesis.

Control Objectives for Information and Related Technology (COBIT) is a well-known framework and Information Technology Infrastructure Library (ITIL) is often referred as a good model. The former is a toolset that can help managers to manage control requirements, technical issues and business risks at the organisational level. The latter is a collection of best practises related to IT service management that aims to align IT services with the needs of business. (Laaksonen et al. 2006, 92, 95.)

2.7 Information Security Management Systems

The role of Information Security Management System is to protect critical information assets and data (figure 1) from threats to availability, integrity and confidentiality (King, 2012). ISMS brings information security controls under the same management system, as these are typically disorganised or disjointed. The ISO/IEC 27001 provides specification for such system, as it is a formal specification it mandates specific requirements (ISO 27000 2013, date of retrieval 14.4.2013).

Requirements of ISO/IEC 27001

The ISO/IEC 27001 requires that the management conducts a risk assessment of the information security risks, designs and implements appropriate security controls, and adopts a management process that ensures that the information security controls continue to meet organisation's needs. The standard uses the plan-do-check-do (PDCA) cycle to manage its process (figure 4). (Moen & Norman 2011, date of retrieval 10.4.2013.)

Figure 4. The PDCA cycle (Moen & Norman 2011, date of retrieval 10.4.2013)

The PDCA cycle is a commonly used on-going management process. The plan stage establishes the ISMS with policy, objects, processes and procedures needed for risk management and development of information security. In the do stage policy, security controls, processes and procedures are actually implemented. Monitoring and review of the ISMS is conducted in the check stage and in the final act stage, updates and improvements are applied. (ISO 27000 2013, date of retrieval 14.4.2013)

ISO/IEC 27001 is a certifiable standard for an ISMS and many accredited registrars can be hired to audit and award a certificate. Just like with most ISO standards there is a three-stage audit process that needs to be passed. (ISO 27000 2013, date of retrieval 14.4.2013)

Code of practice for information security management

The ISO/IEC 27002 is often used together with ISO/IEC 27001. It outlines twelve sections of the ISMS standard that need to be addressed based on security controls and their objectives. Each section contains best practices for achieving good results. Section references and what they contain can be found in appendix 1 and are numbered according to the official standard. (IsekT 2013, date of retrieval 13.4.2013.) The sections should provide an idea of the complexity of ISMS. For example, the first section that is risk management contains processes like risk assessment, risk analysis and risk mitigation.

3 OUTLOOK FOR THE INFORMATION SECURITY MARKET

This chapter provides a brief look at the information security market and particulars of the Finnish market. A number of different perspectives have been provided, but the main goal was to outline the key features that relate to the research task and research questions.

3.1 Security infrastructure market

Gartner, an IT advisory company, estimates that despite the economic downturn the worldwide security infrastructure market will grow 8.4 percent year-on-year in 2012. This includes security software, services and appliances used to secure enterprise and consumer IT equipment. The total market is estimated to reach 60 billion dollars by 2013 and 86 billion dollars by 2016. (Gartner 2012, date of retrieval 14.4.2013.)

The growth is estimated to be high because information security has become critical for businesses. The threat landscape is changing, as malware and criminals are becoming more sophisticated. Mitigating risks and reducing security vulnerabilities has become one of the top priorities. (Gartner 2012, date of retrieval 14.4.2013.)

A survey by Symantec, a major security company, indicated that most SMEs believe that security is critical to their success and brand. In contrast, two-thirds of SMEs are not concerned about information security threats. This is a major problem, as almost 40 percent of the one billion cyber-attacks prevented by Symantec in the first quarter of 2012 were targeting enterprises with less than 500 employees. (Symantec & NCSA 2012, 3 - 9.)

3.2 Business outlook for Finnish SMEs

According to a recent study of Finnish SMEs, enterprises remain modest with their business outlook and expect to act more cautiously with their investments in the next twelve months. The modest outlook is attributed to the European sovereign-debt crisis and weakening local demand. (Federation of Finnish Enterprises, Finnvera, & Ministry of Employment and the Economy 2012.)

Regardless of the outlook, nearly 40 percent of the SMEs expect to see revenue growth. These expectations were more positive with the larger SMEs. In contrast, only every fourth SME expects to see improved profitability in the next twelve months. In normal economic conditions, nearly half

of the Finnish SMEs would expect to see improved profitability. The industry and services sector have the most positive outlook in terms of profitability. (Federation of Finnish Enterprises et al. 2012.)

The uncertain economic climate is likely to postpone investments in the next twelve months with only the services sector looking to increase their investments. The most significant reductions are in the trade sector and the industry's subsector, construction. (Federation of Finnish Enterprises et al. 2012.)

3.3 Use of information technology in Finland

All enterprises with more than ten employees use computers in Finland. Around 72 percent of all employees who work in enterprises use computers in their work. (Statistics Finland 2011a, date of retrieval 14.4.2013.)

Broadband access to the internet was used by 99 percent of Finnish enterprises in 2011. This included both fixed and wireless broadband connections. Across all enterprises, around 65 percent of employees used computers with access to the internet. In some sectors, like information and communication, the internet was used by almost all employees. (Statistics Finland 2011a, date of retrieval 14.4.2013.)

Finland is far above EU averages when it comes to the use of e-commerce by enterprises, as seen in table 2. Around 46 percent the enterprises make purchases electronically and around 15 percent receive orders from the internet in Finland. The EU averages for these numbers 19 percent and 4 percent, respectively. In Finland, enterprises with more than 100 employees are most active in this space, but even smaller enterprises are far above the EU average. This indicates that Finland is far ahead of most EU countries in adoption of e-commerce.

TABLE 2. Enterprise e-commerce by enterprise size in 2011 (Statistics Finland 2011a, date of retrieval 14.4.2013)

Number of Employees	Orders received from the internet %		Orders received from Electronic Data Exchange (EDI) %		Purchased made electronically %	
	Finland	EU	Finland	EU	Finland	EU
10 – 19	13	3	4	1	42	14
20 – 49	14	3	9	1	48	20
50 – 99	16	4	15	3	48	23
100+	27	11	24	10	64	37
All enterprises	15	4	8	2	46	19

E-business practices and systems have been widely adopted by Finnish enterprises, with over half of them using systems like Enterprise Resource Planning (ERP), Customer Relations Management (CRM), electronic invoicing or Radio Frequency Identification (RFID). (Statistics Finland 2011a, date of retrieval 14.4.2013.)

Outsourcing is also very common in Finland. Over two-thirds of the enterprises have outsourced at least one development task to a third-party. While half those that employ ten or more, have outsourced some of the following; website development and administration, application development and administration, IT infrastructure and administration, end-user support, or development of information systems. (ibid. 2011a.)

3.4 Key information security issues for SMEs

There seems to be a disparity amongst SMEs between how information security is perceived and how it is practiced. Symantec's survey revealed that 87 percent of the SMEs do not have a formal information security policy. Most even lack a policy for the use of social media, which is an increasingly popular for phishing attacks. Surprisingly 86 percent report that they are satisfied with their information security. (Symantec & NCSA 2012. 4). This creates concern, as they seem to lack even the most fundamental levels of administrative security. This concern is supported by data from Visa, which states that small businesses represent more than 90 percent of the payment data breaches (Fontana 2012, date of retrieval 10.4.2013).

Clearly one of the biggest problems for SMEs is that they have inflated view of the state of their information security, while lacking proper policies, plans and often have not conducted a proper risk assessment (Symantec & NCSA 2012, 3-4). The other major challenges today include cloud security, regulation compliance, education and training, SME standards, and of course the changing threat landscape (chapter 2.3) (Kelly 2011, date of retrieval 14.4.2013).

While security threats are the same for SMEs, they are different from large organisations. They often lack resources, like knowledge, motivation and funds, to implement proper measures, but also do not necessarily need complex solutions offered to larger organisations. The issue for SMEs is to find appropriate solutions when considering their size and growth expectations. (Kelly 2011, date of retrieval 14.4.2013.)

4 METHODOLOGY AND DATA COLLECTION

This chapter provides the details about the methods used to gain answers to the research questions. Research process has been illustrated and how the problem was defined during the initial research. The research process used can be seen in figure 5.

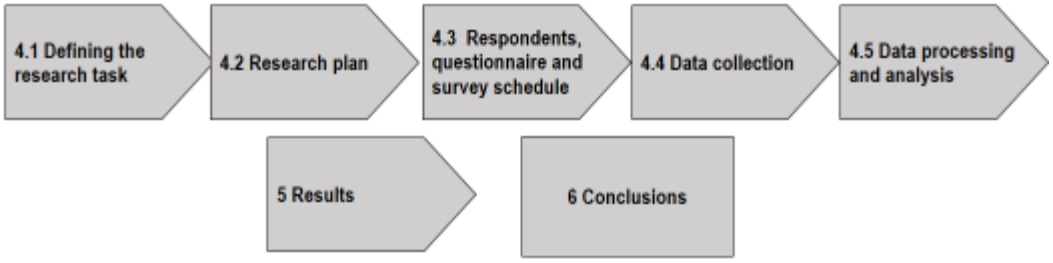

FIGURE 5. Research Process Model

The research process was divided into seven steps. Each step had specific tasks to complete and because this was commissioned research, some of the tasks were required by the commissioner. The goal of the research task was defined by Predykot, but how and by which methods the research task was completed was defined during the research process.

4.1 Defining the research task

Net Man was tasked to conduct a specific part of research for Predykot. The research task was to gain understanding about the current state and future trends of information security in Finnish SMEs with a focus on administrative security. The commissioner wanted to conduct this research as an online survey.

Preliminary study was conducted as secondary research. This could also be defined as an exploratory research phase. The starting materials and basic resources were provided by Predykot and Net Man. However, majority of sources used to formulate the theoretical foundation were from external, publicly available sources, referred to in chapters 2 and 3. Based on the preliminary study, the research task was divided into two research questions:

1) What is the current state of the information security in the Finnish SMEs?
2) What are the information security development and investment plans of the Finnish SMEs in near future?

During the preliminary study, potential survey questions were considered and formulated. The basis for these questions was previous research done in Finland and specifications from Predykot. The questions were presented to Net Man for a final approval before the research plan was written.

4.2 Research plan

The research plan was written in June 2012 and it was based on the project outline and findings from the preliminary study. Outline was for the research task and requirements, why the research was necessary, what research methods were going to be used and why. The plan also included a preliminary schedule, a budget and other financial considerations, and ethical principles. The research plan has not been included for the thesis as it was written in Finnish, but key parts have been explained briefly in this chapter.

The research task and requirements were explained in chapter 4.1. Necessity for the research was covered in the research plan and included many of the sources used in chapters 2 and 3. Chosen research methods, the preliminary schedule, the budget and ethical principles have been described briefly in this chapter.

Research methods

The original plan was to conduct two surveys. The smaller survey would have been conducted as Telephone interviews for around 30 – 50 people while the bigger survey would have been done as Internet survey for around 2000 – 3000 enterprises. After further consideration, it was decided that Internet survey alone would provide enough data for the purposes of the project.

Few other factors supported the choice of an online survey. The commissioner had an account with Webropol, an online survey and analysis software that is popular in Finland. Most Finnish people also use computers in their work (Statistics Finland 2011a, date of retrieval 14.4.2013). Lastly, there were time constraints because of the summer holiday season and the October deadline for the project report.

Population and sample sizes

Respondents for the survey were selected from Finnish SMEs. European Commission recommendation concerning the definition of micro, small and medium-sized enterprise was used when determining the size categories used in this study (European Commission 2005, 14).

The selection excluded most micro-enterprises with fewer than ten employees and large enterprises with more than 250 employees as seen in table 3. It should be noted that while micro enterprises represent 94 percent of all enterprises, they employed only 28 percent of the workforce and generated 17 percent revenues in 2010. Most of the micro enterprises only have one or two employees.

The total population of SMEs that were considered in this research amounted to 17 180 and are categorised in table 3. Both small categories and the medium category were included in the population. The population represents 35 percent of enterprise employees in Finland and amounts to 33 percent of the total revenue generated in 2010.

TABLE 3. Population of SMEs considered in this research (Statistics Finland, 2011b, date of retrieval 17.9.2012)

Categories	Enterprises	%	Employees	%	Revenues (1000€)	%
0-9 (micro)	301 155	94,4	408 573	28,3	62 565 394	17,4
10-49 (small)	14 825	4,6	285 379	19,8	61 814 342	17,2
50-99 (medium)	1 504	0,5	102 654	7,1	25 012 961	7,0
100-249 (medium)	851	0,3	130 338	9,0	32 671 504	9,1
250+ (large)	616	0,2	517 086	35,8	176 844 524	49,3
Total	318 951	100,0	1 444 030	100,0	358 908 725	100,0
Population (SMEs)	17 180	5,4	518 371	35,9	119 498 807	33,3
Others	301 771	94,6	925 659	64,1	239 409 918	66,7

Some enterprises were excluded based on the industrial classification, such as those operating in agriculture, forestry, and fishing. While some were excluded based on the services they provide and have very limited need for information technology, such as hairdressers and funeral services.

The industrial classifications used in the research are based on the official industrial classification, TOL 2008 (Statistics Finland 2008, date of retrieval 17.9.2012). Previous notable research on information security in Finnish SMEs was published by Ministry of Employment and Economy (2007). However, categories used there were based on old classification and therefore are not directly comparable. Table 4 shows the classifications used in this research and also includes joined classifications used in chapter 6. Joined categories include industry, trade and services sectors.

There were only few respondents from the construction industry, so a decision was made to include it in the industry category.

TABLE 4. Industrial classifications (based on TOL 2008)

Joined classifications	Official TOL 2008 classification
Industry	▪ Manufacturing ▪ Construction
Trade	▪ Wholesale and retail trade, repair of motor vehicles and motorcycles
Services	▪ Electricity, gas, steam and air conditioning supply ▪ Transportation and storage ▪ Accommodation and food service activities ▪ Information and communication ▪ Financial and insurance services ▪ Real estate activities ▪ Professional, scientific and technical services ▪ Administrative and support services ▪ Education ▪ Human health and social work activities ▪ Arts, entertainment and recreation

The sample size was determined by using margin of error at 1.5 and confidence level of 95 percent. Based on the estimated population of 17 180 SMEs, the sample size needed to reach 95 percent confidence level was 3419. The survey was sent out to 3800 enterprises after removing from the database those enterprises that no longer existed or did not meet other requirements.

Schedule and budget

The preliminary schedule in the research plan had outlined a three month period when the research would be conducted and the report written. That schedule was amended as a decision was made to conduct the data collection for the survey in August rather than in June or July. The reason for the change was the holiday season, as the decision makers would be on holidays and not able to answer it. The data processing and analysis was pushed to early September and writing the report to the end of September.

There were no serious budgetary concerns because the research was fully funded and did not include separate costs. The only additional cost was iPad 3, which was promised as a raffle prize

for those who answered the survey.

Ethical Principles

Ethical principles section in the research plan defined the principles used when conducting the survey, analysis and reporting. The survey followed the requirements of Personal Data Act. All data was also anonymised and personal data that was collected during the survey was not used in any other capacity with exception to the raffle conducted after the survey, but respondents were given option not to participate.

4.3 Respondents, questionnaire and survey schedule

The questionnaire was designed for the Webropol application. The questions used in the survey can be found in appendix 2. The questionnaire is included in the original language for accuracy.

The design focus was on making the questions easy to understand and that answering all questions would only take about 5 to 10 minutes. It was important that respondents would feel comfortable answering the questions and it did not take too much of their time. This meant that technical jargon was reduced, only few open questions were presented and brief descriptions were given in some questions to help with comprehension.

Once the questionnaire was internally tested and approved, a survey schedule was written. Sending the invite emails was divided into multiple days in order to avoid spam. Spamming large number of emails from the same domain increases the risk of getting the company email on a black list.

The respondents were selected from a list of over 4400 candidate enterprises. Each respondent was manually selected by looking for suitable persons within the enterprise. The selection was based on the judgement. The sources included publicly available databases and the company websites.

The goal was to find people who make the decisions about information security needs in their organisation. Contacts were given priority considering their role in the organisation. Highest priority was given to chief information officers, information management officers and other type of IT managers. Available job descriptions were examined for IT responsibilities, if no such person was

found, the survey was sent to the managing director or someone in equivalent position. It should be noted that smallest enterprises seldom had a dedicated IT manager, but those tasks were usually delegated to office managers and financial controllers who were also in charge of the data.

4.4 Data collection

The survey data was collected during August of 2012. The goal was to get minimum of 100 responses, which is the minimum recommended for this type of survey (Heikkilä 2001, 45). The survey was sent out as an email with a cover letter. A single reminder, also with a cover letter, was sent out after two weeks.

Data collection included monitoring the quality of answers and any problems that might have occurred during the process. Few respondents were removed as per their request and some were removed because they were on extended holidays or had left the organisation.

4.5 Data processing and analysis

Data was processed using Excel to create frequency tables. The analysis was primarily done with quantitative methods, but qualitative analysis was also used for open questions. Cross-tabulation was done to summarise categorical data to create contingency tables. Pivot tables and charts were also used with the analysis process.

Three categories were used to analyse the questions. These were enterprise sizes, revenues and industry sectors. The focus in the results chapter was on all these categories.

5 RESULTS

This chapter has been divided to three sub chapters. The first examines the relevant survey data about respondents. The second looks at the current state of information security and the third will look at the future development and investment plans.

5.1 Summary of respondents

The survey was sent out to 3800 SMEs. It was completed by 157 respondents. This gave the survey a response rate of 4.1 percent.

Around 85 percent of the respondents identified themselves as responsible for information security in their enterprise. Entrepreneurs and managing directors represented 29 percent of the respondents. The remaining 71 percent were chief information officers, IT managers or other supervisors. About 94 percent of the enterprises had been operating for more than ten years.

Respondents by category

Table 5 shows the distribution of respondents between enterprise sizes, industry sectors and revenues in 2011. It should be noted that only seven respondents worked in an enterprise with less than ten employees. These were included in the small segment because most of them produced over two million euros annual revenue making the classification valid (European Commission 2005, 14). Only eight respondents were received from the construction industry and a decision was made to include them in the industry sector for summarisation.

Industry and services sectors received 69 and 64 responses, respectively. The trade sector only received 24 respondents, which falls slightly short from the recommended 30. The split between enterprise sizes was good. There were 73 respondents from small enterprises and 84 from medium enterprises. Only 12 percent of enterprises had revenues below two million euros 47 percent reported revenues over ten million euros in 2011. Those with below two million were included in the below ten million category.

TABLE 5. Distribution of respondents between different categories and segments

Categories	Segments	%	n
Industry	Industry	44	69
	Services	41	64
	Trade	15	24
	Total	100	157
Enterprise size	Small (10-49)	46	73
	Medium (50-249)	54	84
	Total	100	157
Revenues in 2011 (1000€)	Below 10000	54	84
	Above 10000	46	73
	Total	100	157

Respondent profiling

Table 6 collates the customer profiling based on the survey data. The profiles were done for the industrial categories. In this profile, small enterprises have 10 or over, but less than 50 employees, while medium enterprises have more than 50 and less than 250 employees.

The table 5 shows that 46 percent of respondents were from small enterprises and 54 percent were from medium enterprises. There were no significant differences between industry categories to this split. Over 94 percent of these enterprises had operated for more than 10 years. Revenues in excess of 10 million euro were reported by over 50 percent of enterprises operating in industry or trade sectors.

Around 75 percent of enterprises in the trade sector had a dedicated IT manager, but this was only true to around 40 percent in other sectors. External requirements were reported in a significant number of enterprises across all three sectors, with the services sector being highest with 88 percent.

Around 33 percent of enterprises from the trade sector are planning to make significant changes to their information systems within 12 months. Information security is included in the cost considerations in majority of enterprises. For example, this was true for 91 percent of enterprises in the services sector and the rate is not significantly lower in other sectors either.

TABLE 6. Respondent profiling (n=157)

Category	Industry n=69	Services n=64	Trade n=24
Employees	46% small, 54% medium	48% small, 52% Medium	42% small, 58 % medium
Years in operation	10+	10+	10+
Revenue at 10m €	Below 49%, Above 51%	Below 61%, Above 39%	Below 46%, Above 54%
Dedicated IT manager	43%	42%	75%
External requirements	64%	88%	71%
Significant changes to Information Systems within 12 months	10%	23%	33%
Information Security Cost Considerations	85%	91%	74%

5.2 Current state

5.2.1 Security controls

Finnish SMEs showed high-level of confidence when asked to rate their information security. Table 7 illustrates these ratings with a break down between information security controls and industry sectors. Information security controls are administrative, technical and physical. From the respondents 13 percent evaluated their security as very good, while 57 percent rated it as quite good. Only seven percent rated their information security as either slightly poor or very poor. The services sector was most confident in their security controls while the industry sector was the least.

The technical controls were considered as the best by all sectors with 19 percent rating it as very good and 59 percent as quite good. The main differences between industry sectors were with the trade and the industry. Only 10 percent, half of the average, in the industry sector rated their technical controls as very good, but this difference can be seen added to the quite good category. Notably 17 percent of enterprises in the trade sector rated their technical controls either as slightly poor or very poor.

Physical controls were just behind technical controls, as 12 percent rated them as very good and 61 percent as quite good. The services sector was by far most confident with 22 percent of enterprises claiming their physical controls as very good. In contrast, only 4 percent and 6 percent of trade and industry sectors were that confident, respectively.

The administrative domain showed the least amount of confidence. Only 8 percent claimed it as a very good, which is nearly half of the other two controls. However, just 53 percent of all sectors regarded their administrative controls as quite good, 30 percent as fair and 9 percent as slightly poor or very poor. The services sector was again the most confident and the trade sector the least.

TABLE 7. Present views on security controls by industry

Security control	Sector	Very good %	Quite good %	Fair %	Slightly poor %	Very poor %	n
Administrative	Industry	4	54	30	10	1	69
	Trade	4	50	25	17	4	24
	Services	14	53	31	2	-	64
	Total	8	53	30	8	1	157
Technical	Industry	10	67	22	1		69
	Trade	21	50	13	13	4	24
	Services	28	53	17		2	64
	Total	19	59	18	3	1	157
Physical	Industry	6	65	23	6	-	69
	Trade	4	75	17	4	-	24
	Services	22	50	25	3	-	64
	Total	12	61	23	4	-	157
Total		13	57	23	6	1	157

5.2.2 Security issues and concerns, and external requirements

Security issues and concerns

The respondents were also asked to identify the main reasons for security related issues (figure 6) and what they consider as the most significant security concern (figure 7). Other category was omitted from figure 7 as it did not contain any responses.

The biggest security issue for 41 percent of the respondents was that information security was not considered or seen as a problem in their enterprise. Other major issues were that the guidelines set for information security were not followed or that the official guidelines were of poor quality, these were reported by 32 percent and 31 percent of enterprises, respectively. In contrast, staff related issues were only reported by 5 percent.

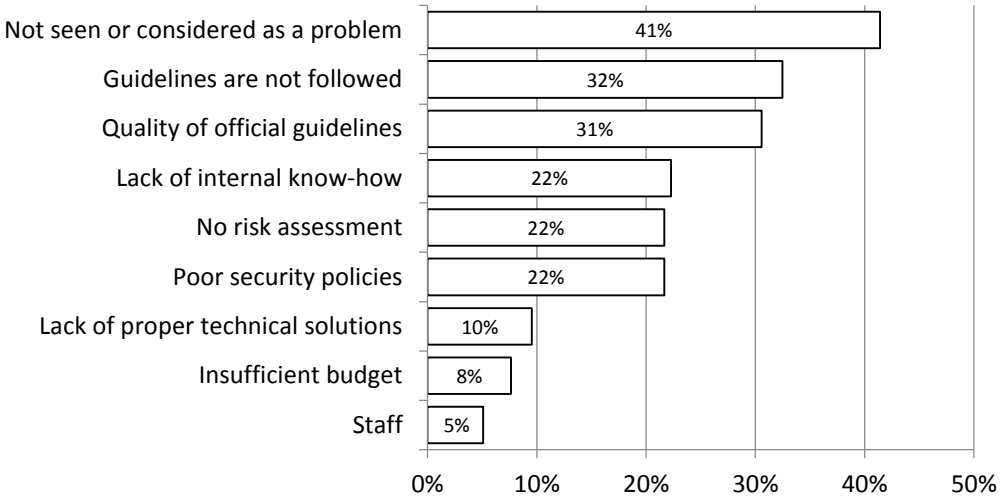

FIGURE 6. Perceived reasons for security issues (n=157)

The respondents were asked what their most significant security related concern is currently (figure 8). This was open question and it was answered by 54 enterprises and percentages are based on those rather than all survey respondents. The most significant concern was employees, as it was reported by 30 percent of the respondents. This was followed by 19 percent who were concerned about access control and 11 percent who were concerned about protection of customer data.

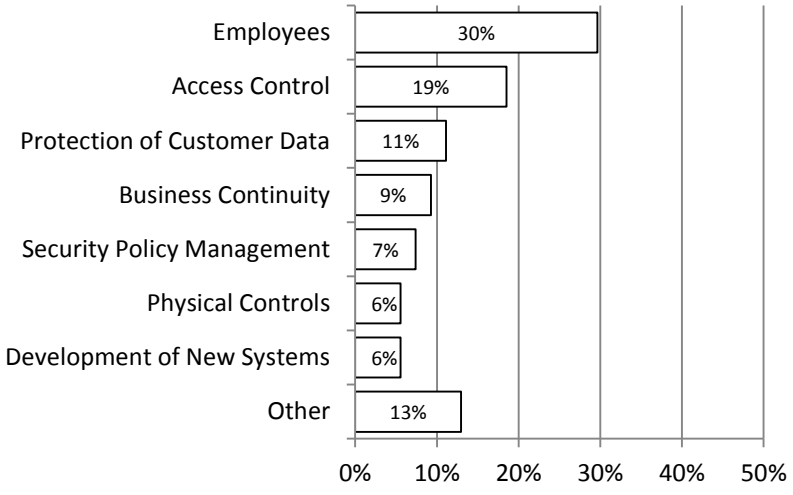

FIGURE 7. Most significant security concern (n=54)

External requirements

Most of the Finnish SMEs reported having to fulfil external requirements for information security (figure 8). Customers, local legislation, and authorities were the top three external requirements. Half of the enterprises point to customers, while 35 percent and 25 percent indicated local legislation or public authority, respectively. Implemented standards added requirements to 18 percent of enterprises. However, just 10 percent reported having to deal with foreign legislative issues.

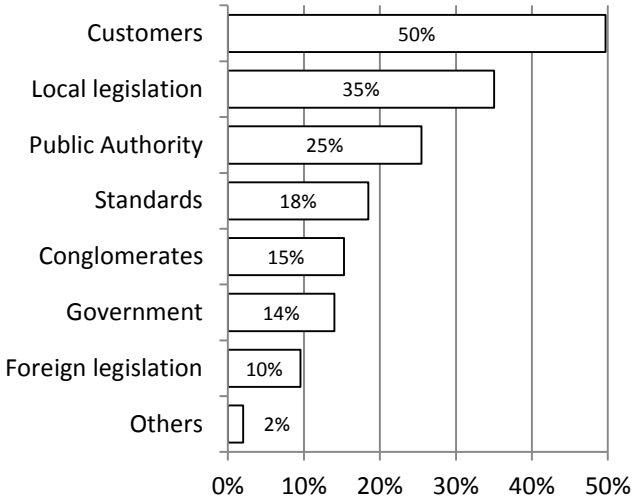

FIGURE 8. External requirements for SMEs (n=157)

5.2.3 Administrative security issues and controls

Respondents were asked whether they have properly managed their administrative information security issues and controls in their enterprise. Figure 9 provides a top level summary of the analysis and it has been ordered by the most positive results.

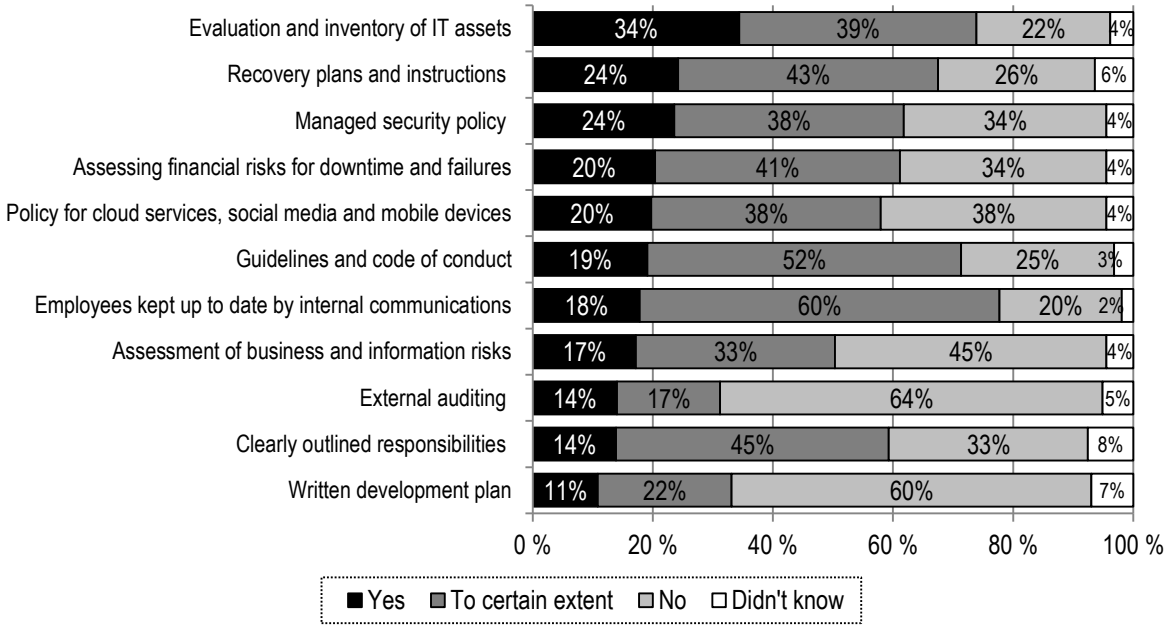

FIGURE 9. Management of different administrative information security issues and controls (n=157)

To some extent, Finnish enterprises have managed their administrative security issues and controls (figure 9). However, the degree of between sections varied from 11 to 34 percent for those who had done them sufficiently and 17 to 60 percent for those who had completed them to certain extent. Those who had not completed them at all varied between 22 to 64 percent. It should be noted that only between 17 to 24 percent of enterprises had the base administrative controls sufficiently in place. The base controls include security policies, risk assessments, guidelines and recovery plans.

The top three controls that had been completed at least to certain extent were internal communication about information security issues by 78 percent, evaluation and inventory of IT assets by 73 percent, and guidelines and code of conduct had been put in in place by 71 percent. Policy for social media, mobiles devices and cloud services was done to at least certain extent in 58 percent of enterprises.

The most poorly managed aspects were external auditing and written development plan, as these had been completed at least to certain extent by only 31 percent and 22 percent of enterprises, respectively. It should be noted that external auditing is not needed by all enterprises.

Each section was also analysed in more detail based on enterprise sizes, industry sectors and revenues. This analysis included two assumptions. Firstly, medium enterprises were expected to

have slightly better administrative security and this was confirmed. The analysis did not produce substantial differences. Secondly, enterprises with higher revenues were also expected to have done more towards security. This assumption was also confirmed, but there were few interesting data points that were included. It was also expected that most noteworthy differences appear between industry sectors, which was also confirmed. Conclusions from significant differences have been described and illustrated in this chapter, while appendix 3 contains the analysis summary indicating categories where differences occurred (refer to table 5 for exact number of respondents in each category).

Managed security policy

Enterprises were asked whether they have a proper security policy to manage their information security. There was a significant difference between enterprises based on their revenues (figure 10). Around 37 percent of enterprises with revenues over ten million reported that they have a proper security policy in place. In comparison, this was only 12 percent with enterprises who had below ten million revenues.

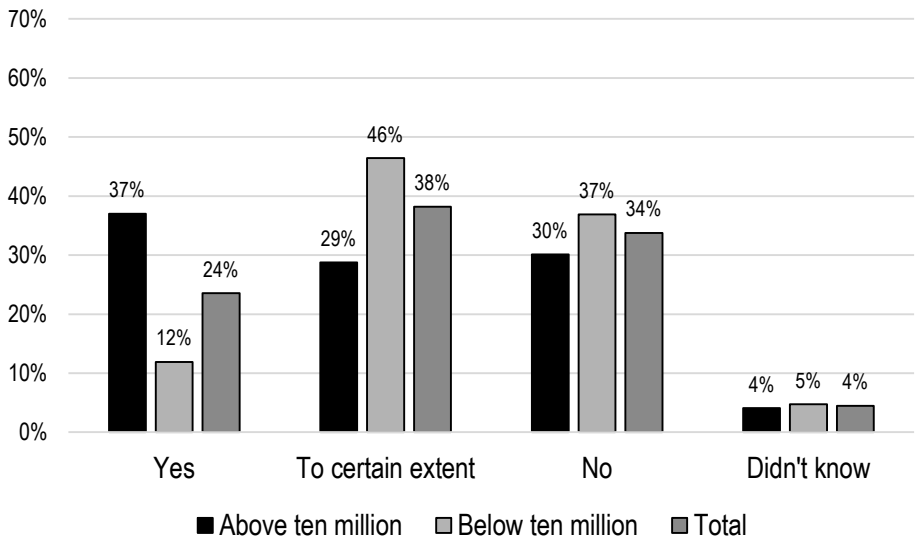

FIGURE 10. Managed security policy by revenues (n=157)

There were also differences between industry sectors, as seen in figure 11. In the services and industry sectors, 69 percent and 59 percent had a security policy in place at least to certain extent, respectively. This was lowest in the trade sector at just 50 percent with 42 saying that they do not have it at all.

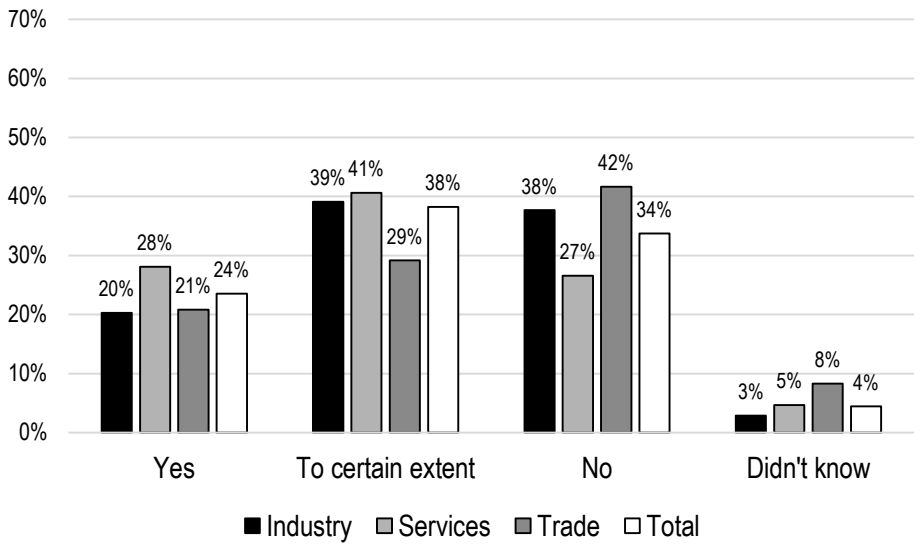

FIGURE 11. Managed security policy by industry sectors (n=157)

Assessing financial risks for downtime and failures

There were differences between industry sectors on how well they had assessed the risks for downtime and other failures, as seen in figure 12. The most noticeable difference was that 50 percent of enterprises in the trade sector reported that they have not done the analysis at all. This is much higher than the 31.5 percent average between other two sectors. The industry sector was best prepared in overall, as 65 percent either had done it or had done it to certain extent.

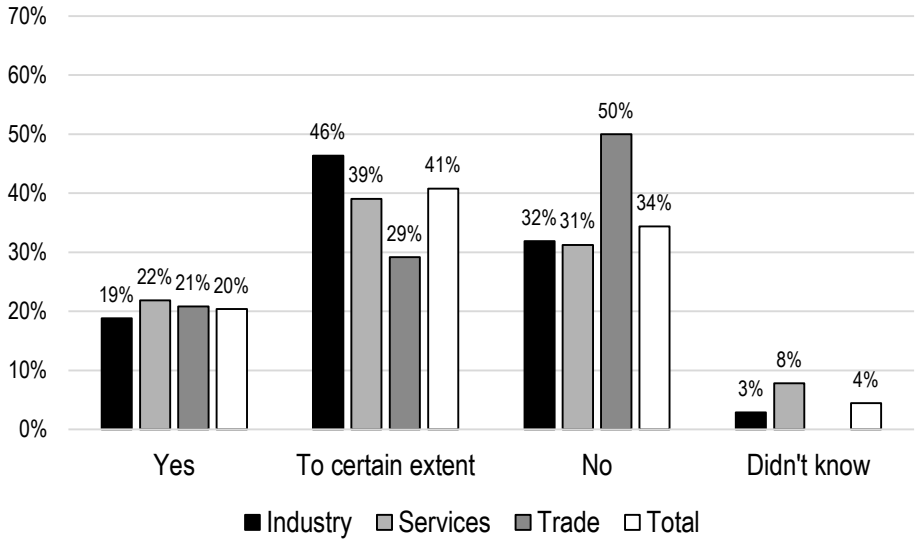

FIGURE 12. Analysing financial risks for downtime and failure by industry sectors (n=157)

Policy for cloud services, social media and mobile devices

There were clear difference between industry sectors on how prepared they are for cloud services, social media and mobile devices (figure 13). Only 10 percent of enterprises in the industry sector reported that they had a policy in place, while 43 percent said that they have no policy at all. Services and trade sectors were slightly better prepared, as 25 percent and 33 percent reported having a policy, respectively. In average, 38 percent had no policy.

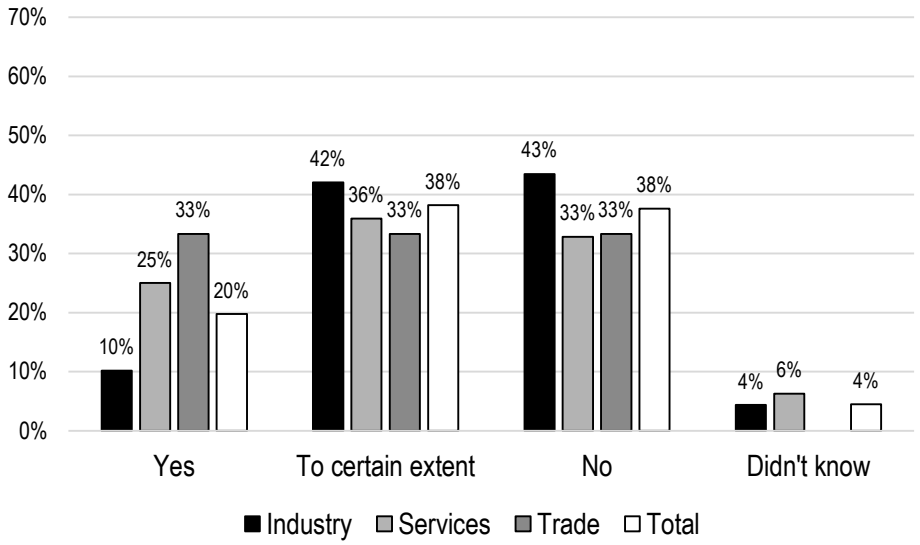

FIGURE 13. Policy for cloud services, social media and mobile devices by industry sectors (n=157)

Employees kept up to date by internal communications

From the industry and services sector 76 percent and 86 percent of enterprises stated that they keep their employees informed about information security related issues (figure 14). However, about 38 from the trade sector claimed that they do not inform their employees at all. This was 18 percent above the average. It is clear that the trade sector is not as active with its internal communications regarding information security.

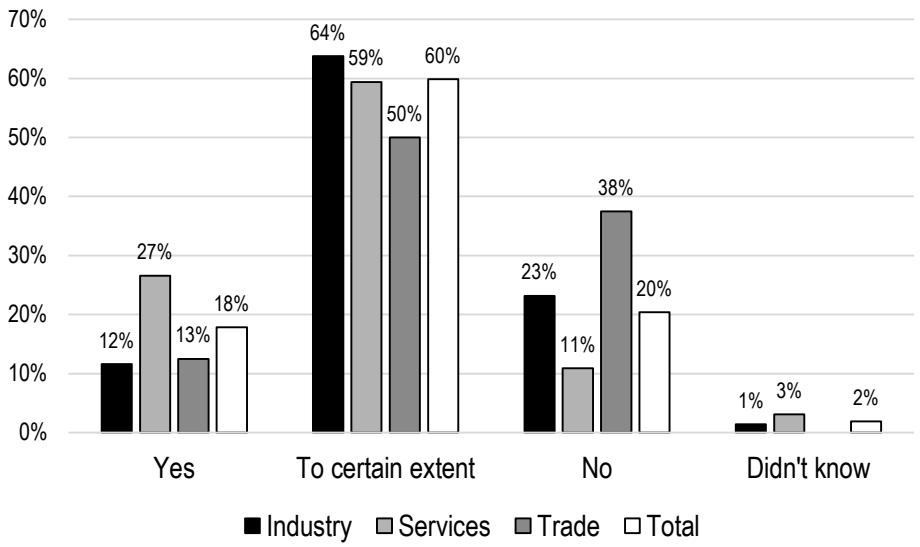

FIGURE 14. Employees kept up to date by internal communications by industry sectors (n=157)

Assessment of risks to business and confidential information

Respondents were asked whether they have assessed risks to their business and confidential information, if a security related event would incur. There was a significant difference when compared with revenues, as seen in figure 15. About 26 percent of enterprises with revenues above ten million had done risk assessment, while 56 percent of enterprises with below 10 million revenues had not.

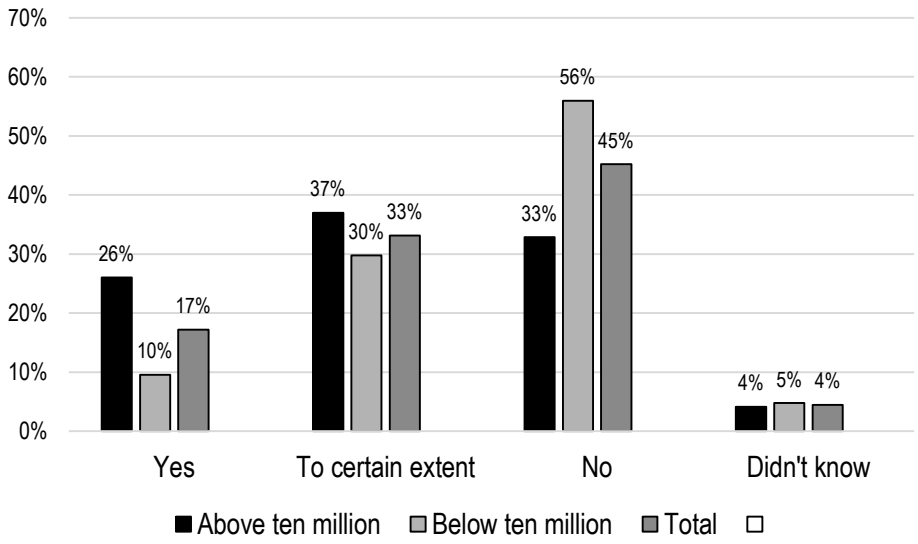

FIGURE 15. Assessment of risks to business and confidential information by revenues (n=157)

External auditing

Different sectors reported equally negative results about external auditing (figure 16). The industry sector was the weakest with only 28 percent reporting that they have had external auditing done to at least some extent. This was closely followed by the trader sector at 29 percent and services sector that had most external audits with 36 percent. There difference here are not major, but the services sector is somewhat ahead of others.

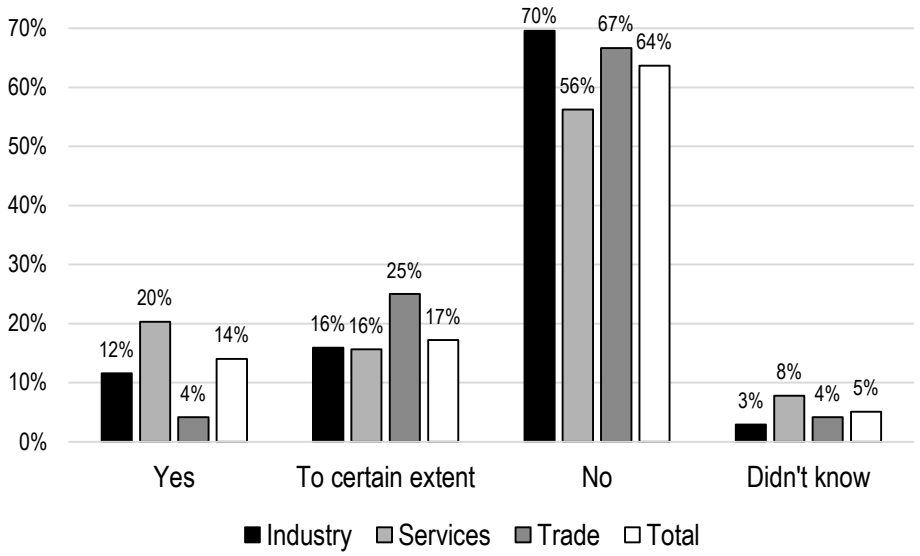

FIGURE 16. External auditing by industry sectors (n=157)

Clearly outlined responsibilities

Respondents were asked whether they had clearly outlined responsibilities related to information security. Figure 17 shows the split between industry sectors. Enterprises from the services sector seem to be significantly more prepared than the other two sectors. About 39 percent claimed that they had clearly outlined responsibilities, while 13 percent had not outlined. In contrast, only 17 percent and 22 percent of enterprises in the trade and industry sectors had done so, respectively. While 29 percent in both industry and trade sectors had not done it all, which is 16 percent higher than in the services sector.

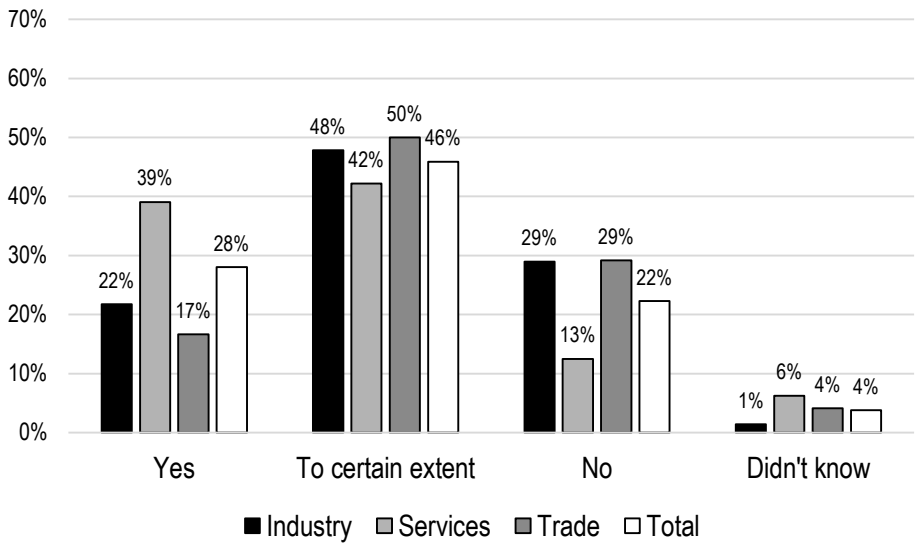

FIGURE 17. Clearly outlined responsibilities by industry sectors (n=157)

5.3 Future plans

Nearly 19 percent of enterprises are planning significant changes to their information systems in the next 12 months and another 65 percent are planning smaller changes. This means that the total of 84 percent of enterprises is planning changes to their information systems in the next 12 months.

Figure 18 show that there were major differences between industry sectors. Notably 33 percent of enterprises in the trade sector are planning significant changes, while only 10 percent were planning to do so in the industry sector. In overall, all sectors are looking to do at least some change, as only 14 percent in average are not planning to change their information systems at all.

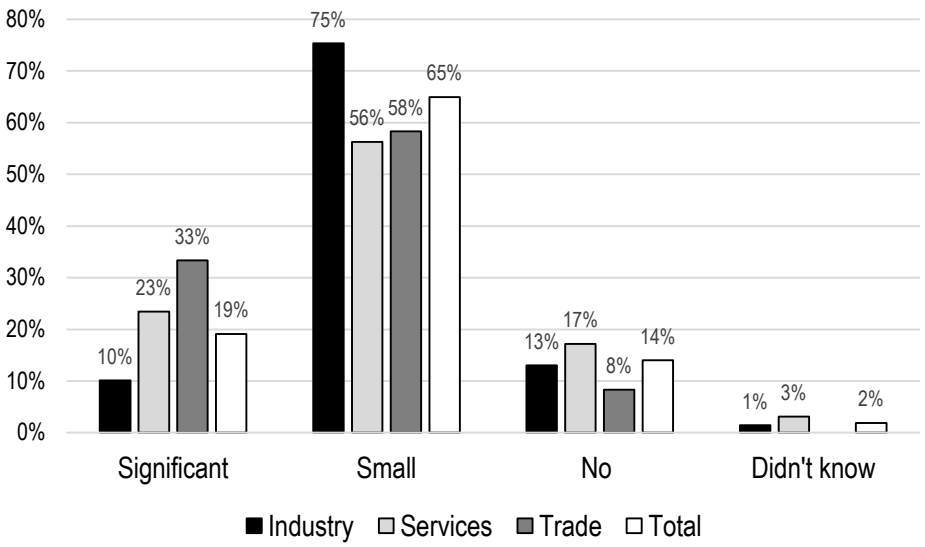

FIGURE 18. Planned changes to information systems in next 12 months (n=157)

5.3.1 Development and investment plans

The Finnish SMEs were also asked whether they have needs to develop or invest on information security in the near future. Around 55 percent indicated that they have needs in the next few years. From those, 24 percent stated that they are planning to do so in the next 12 months. However, 33 percent were not planning to develop or invest either because they did not need to or they thought that their security was good enough.

Table 8 provides a summary on what kind of development or investment needs enterprises have in overall and at what time frame. The sections were based on the ISO/IEC 27002 standard and are presented in natural order also found in appendix 1.

In the next 12 months, 19 to 29 percent of enterprises have development or investment needs in information security, while between 25 to 40 percent have needs afterwards. In average, 57 percent enterprises have needs in the next few years. Many sections with high level of needs included administrative controls. Business continuity managed was listed by 29 percent of enterprises, while security policy, security governance and communications each were listed by 26 percent. Another section with a high percentage was information systems acquisition, development and maintenance, which was at 28 percent. This indicates that many are planning information security as a part of their information system development.

Access control was reported by 35 percent as being good enough, which was well above the 22 percent average. Also, 10 percent on average thought that they had no develop or invest needs. This percentage could be explained by the fact that some of the enterprises could have outsourced their information security management to a third party.

TABLE 8. Developments and investments plans by ISO/IEC 27002 sections (n=157)

ISO/IEC 27002 Section	Within 12 months %	After 12 months %	No, good enough %	No, not needed %	Didn't know %
Risk management	24	43	15	10	10
Security policy management	26	32	18	11	13
Governance of information security	26	37	17	9	11
Asset management	24	36	16	12	12
Human resources security	22	34	24	8	11
Physical and environmental security	25	30	24	8	12
Communications and operations management	26	27	27	10	10
Access control	22	25	35	11	8
Information systems acquisition, development and maintenance	28	26	24	11	11
Information security incident management	20	40	17	10	12
Business continuity management	29	32	24	6	9
Compliance	19	31	26	9	15
Total	24	33	22	10	11

5.3.2 Categorical findings for development and investment plans

This chapter describes and illustrates key findings from the categorical analysis of different sections of ISO/IEC 27002. Instead of focusing on the time frame this part concentrated whether enterprises have needs or not. The analysis was done with enterprise sizes, industry sectors and revenues categories.

This analysis included three assumptions. Firstly, medium enterprises were expected to have more needs than small enterprises. This was confirmed, as the analysis did not produce significant differences. Secondly, enterprises with higher revenues were also expected to have more needs. This was also confirmed. Lastly, it was also expected that most noteworthy differences were from industry sectors, which was also confirmed. Appendix 4 includes a summary of these categorical findings.

The analysis did not produce noteworthy differences or significant findings for enterprise sizes and revenues categories. There were significant differences between industry sectors. Only two sections produced homogenous data. These were business continuity management and to lesser extent information security inducement management. Table 9 summarises the key finding for the other sections by giving range of percentages for each section by category. There was no need to separate these, as the same differences were visible throughout the data set.

The trade sector had the least amount of needs, as between 46 to 71 percent indicated that they had none, most sections were well above 50 percent in the no category. Similarly, the services sector had the most needs with values falling between 17 to 33 percent. Most values were above 20 percent and only risk management notably lower at 9 percent. The industry sector had more varied results, but they were also most likely to have needs at least to certain extent with values well above 40 percent with the exception of few sections.

TABLE 9. Summary of categorical analysis by industry sectors (n=157)

Category	Industry n=69	Services n=64	Trade n=24
Yes	7 – 20 %	17 – 33%	5 – 25 % One above -17%
To certain extent	28 – 52 % One below 33%	28 - 47%	17 – 38% Mostly above 25%
No	16 – 42% Mostly around 30%	22 – 32% Mostly around 30%	38 – 71 % Mostly around 50%

(Didn't know - category was omitted, but the range was averaging around 9-12% for each section)

Overall analysis of the sections yielded very little interesting data, but the differences between industry sectors were noteworthy. It was clear that the services sector had the most development and investment needs, followed by the industry sector. The trade sectors had the least needs, but it should be noted that this category only had 24 responses.

6 CONCLUSIONS AND DISCUSSION

The information security landscape is changing. Cloud services, social media and mobile devices bring new challenges to enterprises. Criminals threatening enterprises are becoming more sophisticated and organised, while external requirements force increased security even in smaller enterprises. Smaller enterprises and those with below ten million in revenues seem to be falling behind of bigger enterprises. However, they still need to tackle the same information security related concerns.

The results of the study show that most decision makers in SMEs are aware that they need better information security and have relatively good idea of the issues and threats they are facing. The study also shows that many have somewhat inflated view of the quality of their information security. However, there is disparity between how they see their own security and what they have actually done to improve it.

Overall level of information security was regarded as quite good by majority of respondents. Administrative security was seen as the weakest and technical security as the strongest. However, when asked about specifics details, it became apparent that many enterprises did not have even the most basic security controls in place. They had not done risk assessments, nor did they have written security policy or appropriate guidelines and instructions to manage one. Administrative security controls seem to be a major concern for many enterprises, especially to the smaller enterprises.

In the next few years, SMEs will be busy with changes to their information systems. Over half of the enterprises specified that they have development and investment needs for information security. These needs are likely to increase with many changes seen in the horizon. However, SMEs need better processes, policies and technologies to help secure their information assets against threats. This study shows that SMEs are vulnerable because they often lack resources and expertise to implement and maintain complex information systems. Another problem is with the current breed of technology and services, as they tend to be tailored for larger organisations making it impractical and costly for SMEs to adopt them. Increased availability of managed security solutions would be beneficial to many smaller enterprises.

Any future study on the subject would benefit from a higher response rate. The ideal number of responses would be around three hundred. The sample size for the survey was appropriate, but some segments did not get enough responses, such as the trade sector. This could be increase with interviews or sending additional reminders. Also, getting more respondents from enterprises that have operated for less than ten years would be beneficial. Start-ups would be a particularly interesting category.

7 REFERENCES

Andress, J. 2011. The Basics of Information Security. Waltham, USA: Elsevier.

Confederation of Finnish Industries. 2013. Yritysturvallisuuden osa-alueet. Date of retrieval 10.4.2013, http://www.ek.fi/ek/fi/tyomarkkinat_ym/Yritysturvallisuus/osa-alueet/Osa-alueet.php.

European Commission. 2005. The new SME definition. Enterprise and Industry Publications.

European Commission. 2013. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. Publications of the Digital Agenda for Europe.

Federation of Finnish Enterprises, Finnvera, & Ministry of Employment and the Economy. 2012. Barometer of the Finnish SMEs. Publications of the Finnish Information Processing Association.

Fontana, J. 2012. On cybersecurity, small businesses flirting with disaster, survey finds. Date of retrieval 10.4.2013, http://www.zdnet.com/on-cybersecurity-small-businesses-flirting-with-disaster-survey-finds-7000005891/.

Gartner. 2012. Gartner Says Worldwide Security Infrastructure Market Will Grow 8.4 Percent. Date of retrieval 14.4.2013, http://www.gartner.com/newsroom/id/2156915.

GFI Software. 2010. Security Threats: A guide for small and mediun enterprises. Publications of GFI Software.

Heikkilä, T. 2001. Tilastollinen tutkimus. 3rd edition. Helsinki: Oy Edita Ab.

IsekT. 2013. ISO/IEC 27002:2005 Information technology — Security techniques — Code of practice for information security management. Date of retrieval 13.4.2013, http://www.iso27001security.com/html/27002.html.

ISO 27000. 2013. An Introduction to ISO 27001. Date of retrieval 14.4.2013, http://www.27000.org/iso-27001.htm.

ITEA2. 2013. About ITEA2: Information Technology for European Advancement. Date of retrieval 12.4.2013, http://www.itea2.org/about_itea2.

Kelly, L. 2011. The top five SME security challenges. Computer Weekly. Date of retrieval 14.4.2013, http://www.computerweekly.com/feature/The-top-five-SME-security-challenges.

King, N. 2012. Governance, Risk and Compliance Handbook for Oracle Applications. Birmingham: Packt Publishing Ltd.

Laaksonen, M., Nevasalo, T., & Tomula, K. 2006. Yrityksen tietoturvakäsikirja. Helsinki: Oy Nordprint Ab.

Ministry of Employment and the Economy. 2007. PK-Yritysten Tietoturvakysely 2006. Publications of the Ministry of Employment and Economy.

Moen, R., & Norman, C. 2011. Evolution of the PDCA Cycle. Associates in Process Improvement. Date of retrieval 14.3.2013, http://pkpinc.com/files/NA01MoenNormanFullpaper.pdf.

Net Man Oy. 2013. Net Man Oy: About. Date of retrieval 12.4.2013, http://www.netman.fi/en/new-home/about.html.

Olzak, T. 2010. Administrative Security Controls. Bright Hub. Date of retrieval 10.4.2013, http://www.brighthub.com/computing/smb-security/articles/2482.aspx.

PCToday. 2012. The Enterprise Threat Landscape - Everyone is a target. PCToday 10(5), 12-19.

Perrin, C. 2008. The CIA Triad. TechRepublic. Date of retrieval 10.4.2013, http://www.techrepublic.com/blog/security/the-cia-triad/488.

Predykot-ITEA2. 2013. Predykot Itea2 - 10035. Date of retrieval 14.4.2013, http://www.itea2-predykot.org/index.php.

Statistics Finland. 2008. Standard Industrial Classification TOL 2008. 17.9.2012, http://www.stat.fi/meta/luokitukset/toimiala/001-2008/index_en.html.

Statistics Finland. 2011a. Use of Information Technology in Enterprises. Date of retrieval 14.4.2013, http://www.stat.fi/til/icte/kat.html.

Statistics Finland. 2011b. Finnish enterprises. Date of retrieval 17.9.2012, http://www.tilastokeskus.fi/til/syr/index_en.html.

Symantec, & NCSA. 2012. National Small Business Study. Publications of the National Cyber Security Alliance 2012.

Weiss, M., & Salomon, M. G. 2011. Auditing IT Infrastructure for Compliance. Sudbury, USA: Jones & Barlett Learning.

8 APPENDICES

SECTIONS OF THE IEC/ISO 27002 STANDARD

APPENDIX 1

Section	Contains
4. Risk management	▪ Risk assessment ▪ Risk analysis ▪ Risk mitigation
5. Security policy management	▪ Principles and axioms ▪ Policies ▪ Standards ▪ Guidelines & procedures
6. Governance of information security	▪ Structure ▪ Reporting ▪ Liaison
7. Asset management	▪ Inventory ▪ Classifications ▪ Ownership
8. Human resources security	▪ Joiners ▪ Movers ▪ Leavers ▪ Awareness, training & education
9. Physical and environmental security	▪ Physical access ▪ Air conditioning ▪ Fire & water safety ▪ Power
10. Communications and operations management	▪ Archives ▪ Backups ▪ Logs ▪ Patching ▪ Monitoring ▪ Configurations
11. Access control	▪ Physical ▪ Network ▪ Systems ▪ Applications ▪ Functions ▪ Data
12. Information systems acquisition, development and maintenance	▪ Requirements ▪ Design ▪ Develop/acquire ▪ Test ▪ Implement ▪ Maintain & support
13. Information security incident management	▪ Prepare ▪ Identify ▪ React ▪ Manage & contain ▪ Resolve ▪ Learn
14. Business continuity management	▪ Resilience ▪ Disaster recovery
15. Compliance	▪ Audit, SOX, & Basel II ▪ Policies ▪ Laws & regulations ▪ 3rd parties

QUESTIONNAIRE APPENDIX 2

Kyselylomakkeen malli **1/3**

Q1) Mikä on teidän asemanne organisaatiossanne?
1 = Yrittäjä/toimitusjohtaja
2 = Muu johtaja/päällikkö/esimiesasema

Q2) Oletteko hallinnollisesti vastuussa organisaationne tietoturvasta?
1 = Kyllä
2 = En
3 = En osaa sanoa

Q4) Mikä on organisaationne päätoimiala?
1 = Teollisuus
2 = Rakentaminen
3 = Kuljetus
4 = Majoitus- ja ravitsemistoiminta
5 = Palvelut liike-elämälle
6 = Henkilökohtaiset palvelut
7 = Kauppa
8 = Muu, mikä?
9 = En osaa sanoa

Q5) Kuinka monta vuotta organisaationne on toiminut?
1 = 0-3 vuotta
2 = 4-9 vuotta
3 = 10+ vuotta
4 = En osaa sanoa

Q6) Keskimäärin kuinka monta henkilöä työskentelee organisaatiossanne (sisältää myös osa-aikaiset)?
1 = 0-9
2 = 10-49
3 = 50-99
4 = 100+
5 = En osaa sanoa

Q7) Yrityksenne liikevaihto vuonna 2011 (1000 euroa)?
1 = Alle 200
2 = 200 - 399
3 = 400 - 999
4 = 1 000 - 1 999
5 = 2 000 - 9 999
6 = 10 000 -
7 = Ei vastausta

Q8) Huomioidaanko organisaatiossanne kustannukset tietoturvan osalta?
1 = Kyllä
2 = Jossain määrin
3 = Ei
4 = En osaa sanoa

Q9) Miten arvioisitte organisaationne tietojärjestelmiin toteutettavat muutokset seuraavan 12 kuukauden aikana?
1 = Merkittäviä muutoksia
2 = Pieniä muutoksia
3 = Ei muutoksia
4 = En osaa sanoa

Q10) Jos organisaatiossanne on puutteita tietoturvan tasossa niin mistä arvioisitte niiden johtuvan? (multiple choice)
Organisaatiossa ei riittävää osaamista
Tietoturvaa ei koeta ongelmana
Sopivien teknisten ratkaisuiden puute
Sopivien toimintatapojen puute
Ohjeistuksen puute
Ohjeistusta ei noudateta
Henkilökunnan puute
Riittämätön budjetti
Ei ole suoritettu riskikartoitusta
Muita syitä, mitä?: (open question)

Q11) Miten hyväksi arvioisitte organisaationne hallinnollisen tietoturvan tason?

1 = Erittäin hyvä

2 = Melko hyvä

3 = Ei hyvä, eikä huono

4 = Ei kovinkaan hyvä

5 = Ei lainkaan hyvä

6 = En osaa sanoa

Q12) Onko organisaatiossanne hoidettu seuraavia hallinnollisia tietoturva-asioita?
1 = Kyllä
2 = Jossain määrin
3 = Ei
4 = En osaa sanoa
Q12a) Tehty virallinen linjaus tietoturvan tavoitteista, vastuista ja toteutuskeinoista (ns. tietoturvapolitiikka)
Q12b) Tietoturvan parantamiseksi on olemassa kirjallinen kehityssuunnitelma
Q12c) Tietoturvaan on riittävä ohjeistus ja toimintaohjeita
Q12d) Tietoturvaan liittyvät vastuut on määritelty selkeästi
Q12e) Liiketoimintaan ja luottamuksellisiin tietoihin liittyviä tietoturvariskejä on selvitetty (esimerkiksi riski-analyysillä)?
Q12f) Tietojärjestelmien toimimattomuuteen liittyviä menetyksiä on arvioitu
Q12g) Henkilökunta pidetään ajan tasalla tietoturvaan liittyvistä riskeistä
Q12h) On olemassa toimintaohjeita ja toipumissuunnitelmia katastrofi- ja ongelmatilanteiden varalta
Q12i) Organisaatiossa on suoritettu ulkopuolinen tietoturva-auditointi
Q12j) Organisaation IT-omaisuus ja tiedot on arvioitu sekä luetteloitu
Q12k) Tietoturvasta on linjaus pilvipalveluiden, omien laitteiden, mobiililaitteiden ja sosiaalisen median osalta?

Q13) Onko organisaatiollanne ulkoisia vaatimuksia tietoturvan suhteen?
1 = Kyllä
2 = Jossain määrin
3 = Ei
4 = En osaa sanoa

Q14) Miltä tahoilta on tullut erikoisvaatimuksia tietoturvan suhteen?: (multiple choice)
Valtionhallinto
Viranomaiset
Kotimainen lainsäädäntö
Ulkomainen lainsäädäntö
Konsernit
Asiakkaat
Standardit
Muilta?: (open question)

Q15) Miten hyväksi arvioisitte organisaationne fyysisen tietoturvan tason?
1 = Erittäin hyvä
2 = Melko hyvä
3 = Ei hyvä, eikä huono
4 = Ei kovinkaan hyvä
5 = Ei lainkaan hyvä
6 = En osaa sanoa

Q16) Miten hyväksi arvioisitte organisaationne teknisen tietoturvan tason?
1 = Erittäin hyvä
2 = Melko hyvä
3 = Ei hyvä, eikä huono
4 = Ei kovinkaan hyvä
5 = Ei lainkaan hyvä
6 = En osaa sanoa

Q17) Onko organisaatiossanne tietoturvallisuudesta johtuvia kehitys- tai investointitarpeita seuraavilla alueilla?
1 = Kyllä, mutta ei lähiaikoina
2 = Kyllä, seuraavan 12 kk aikana
3 = Jossain määrin, mutta ei lähiaikoina
4 = Jossain määrin, seuraavan 12 kk aikana
5 = Ei, koska riittävän hyvä
6 = Ei, koska ei ole tarvetta
7 = En osaa sanoa
Q17a) Riskien arviointi (fyysiset, sisäiset, ulkoiset ja muut riskit)
Q17b) Hallinnollisen tietoturvapolitiikan kehittäminen (organisaation tietoturvan selkeä linjaaminen)
Q17c) Tietoturvallisuuden hallinta (johtaminen sekä organisaation rakenteissa ja prosesseissa huomioiminen)
Q17d) Resurssien hallinta (tietoresurssien inventointi ja luokittelu)
Q17e) Henkilöstöturvallisuus (hallitaan työntekijöiden aloittamista, työskentelyä ja lopettamista organisaatiossa)
Q17f) Viestintä- ja toiminnanohjaus (teknisen turvallisuuden hallinta verkkojen ja tietojärjestelmien osalta)
Q17g) Fyysinen ja käyttöympäristön turvallisuus (laitteisto- ja tilaturvallisuus)
Q17h) Pääsyn- ja käytönvalvonta (rajoitetaan tietojärjestelmiin, verkkoihin, ohjelmiin ja tietoon pääsyä)
Q17i) Tietojärjestelmien hankkiminen, kehittäminen ja ylläpito (tietoturvan sisällyttäminen tietojärjestelmiin)
Q17j) Tietoturvatapahtumien hallinta (tietoturvaongelmien ennakointi ja niiden oikeanlainen käsittely)
Q17k) Liiketoiminnan jatkuvuuden hallinta (tärkeiden prosessien turvaaminen, ylläpitäminen ja palauttaminen)
Q17l) Tietoturvamääräysten, lakien ja sääntöjen noudattaminen (ns. compliance)

Q18) Mikä on tällä hetkellä organisaationne näkökulmasta merkittävin tietoturvaan liittyvä asia?: (open question)

ANALYSIS SUMMARY FOR ADMINISTRATIVE SECURITY CONTROLS APPENDIX 3

Sections	Enterprise size	Industry sector	Revenues
Evaluation and inventory of IT assets	-	-	-
Recovery plans and instructions	-	-	-
Managed security policy	-	Yes	Yes
Financial risks analysis for downtime and failures	-	Yes	-
Policy for cloud services, social media and mobile devices	-	Yes	-
Guidelines and code of conduct	-	-	-
Up to date internal communications	-	Yes	-
Assessment of business and information risks	-	-	Yes
External auditing	-	Yes	-
Clearly outlined responsibilities	-	Yes	-
Written development plan	-	-	-

(Yes – indicates that noteworthy differences were found in the analysis)

ANALYSIS SUMMARY FOR ISO/IEC 27002 SECTIONS APPENDIX 4

Sections	Enterprise size	Industry sector	Revenues
Risk management	-	Yes	-
Security policy management	-	Yes	-
Governance of information security	-	Yes	-
Asset management	-	Yes	-
Human resources security	-	Yes	-
Physical and environmental security	-	Yes	-
Communications and operations management	-	Yes	-
Access control	-	Yes	-
Information systems acquisition, development and maintenance	-	Yes	-
Information security incident management	-	Yes	-
Business continuity management	-	Yes	-
Compliance	-	Yes	-

(Yes – indicates that noteworthy differences were found in the analysis)