jamk.fi

Enhancing Cyber Security for SME organizations through self-assessments

How self-assessment raises awareness

Tarmo Hassinen

Master's Thesis
April 2017
School of Technology
Master´s Degree Programme in Information Technology
Cyber Security

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

jamk.fi

Description

Author(s)	Type of publication	Date
Hassinen, Tarmo	Master's thesis	10.04.2017
		Language of publication: English
	Number of pages: 52	Permission for web publication: x

Title of publication

Enhancing Cyber Security for SME organizations through self-assessment

Degree programme

Master´s Degree Programme in Information Technology, Cyber Security

Supervisor(s)

Mika Karjalainen, Jari Hautamäki

Assigned by

Marko Koukka, Telia Finland Oyj

Abstract

This thesis primarily studied the importance of self-assessment in increasing business organizations' cyber security awareness of their ICT environment. The secondary studied item was the relevance of self-assessment in detecting new business potential while understanding ICT environment changes. The self-assessment is based on FINCS, the Finnish basic level cyber security certificate launched in December 2016. FINCSC consists of physical and management security, ICT service and system security as well as risk management. Behind FINCSC there is e.g. ISO/IEC 27001 information security standard.

The study uses explanatory research methodology to conduct the research, and the method of the research is survey. The participants to the survey were persons from SME business organizations that participated to the pilot of the FINCSC development. For the survey, Webropol portal was used. The survey was conducted in two phases: before and after completing the FINCSC self-assessment. This was mandatory in order to study the change of the awareness before and after the self-assessment. For the results of the survey, inductive and hermeneutic analyses were used.

Based on the results of the survey, self-assessment helps the organizations to acknowledge the impact of the different parts of cyber security to the business. Especially, for the awareness of the current state of the business ICT environment, the self-assessment is valuable. Otherwise, from business prospect's perspective, direct benefits were not found with the self-assessment.

Keywords (cyber security, self-assessment, SME, business, ICT service, FINCSC)

jamk.fi

Kuvailulehti

Tekijä(t)	Julkaisun laji	Päivämäärä
Hassinen, Tarmo	Opinnäytetyö, ylempi AMK	10.04.2017
		Julkaisun kieli Englanti
	Sivumäärä 52	Verkkojulkaisulupa myönnetty: x

Työn nimi

Enhancing Cyber Security for SME organizations through self-assessment

Tutkinto-ohjelma

Master´s Degree Programme in Information Technology, Cyber Security

Työn ohjaaja(t)

Mika Karjalainen, Jari Hautamäki

Toimeksiantaja(t)

Marko Koukka, Telia Finland Oyj

Tiivistelmä

Opinnäytetyössä primääristi tutkittiin itsearvioinnin merkitystä kyberturvallisuuden ymmärryksen kasvattamisessa yrityksen liiketoiminnan ICT-ympäristön osalta. Toissijainen tutkittava asia itsearvioinnin merkityksestä oli liiketoimintamahdollisuuksien kartoittamisessa liiketoiminnan ICT-ympäristön ymmärryksen muuttuessa. Itsearviointi perustui Suomeen joulukuussa 2016 lanseerattuun kyberturvallisuuden perustason sertifikaattiin FINCSC:hen, joka koostuu fyysisen, hallinnollisen, ICT-palvelujen ja järjestelmien tietoturvallisuuden sekä riskienhallinnan osa-alueista. FINCSC:n taustalla on mm. ISO/IEC 27001 tietoturvallisuuden hallinnan standardi.

Tutkimus oli luonteeltaan kartoittava ja suoritettiin kyselytutkimuksena FINCSC-pilottihankkeeseen osallistuneiden yritysten kesken. Kysely suoritettiin Webropol-portaalin kautta kahdessa osassa: ennen ja jälkeen FINCSC itsearvioinnin suorittamisen. Tämä siksi, että tutkimuksen mittaamista varten tarvittiin tilanne liiketoimintaympäristön nykytilan ymmärryksestä ennen itsearviointia. Kyselytutkimuksen tulosten analysointi suoritettiin induktiivista sekä hermeneuttista analyysiä hyödyntäen.

Kyselyiden tuloksien perusteella itsearviointi auttaa yrityksiä tunnistamaan kyberturvallisuuden eri osa-alueiden vaikutuksia yrityksen liiketoimintaan. Näistä etenkin liiketoimintaympäristön ICT-palveluiden nykytilan kartoittamisessa itsearvioinnilla on selvästi hyötyä. Muutoin esimerkiksi liiketoiminnan edistämisen näkökulmasta ei itsearvioinnin ja sen myötä parantuneen kyberturvallisuuden nähty tuovan merkittävää etua.

Avainsanat (cyber security, self-assessment, SME, business, ICT service, FINCSC)

Content

Content **1**

1 Introduction **4**

1.1 Background of the study 4

1.2 SME segment's role in cyber resiliency 4

1.3 Cyber Scheme Finland project 6

1.4 Goal of study and researched problem 7

2 The background and basis of the research **8**

2.1 Research questions 10

2.2 Definition of SME organization and its role in economy 11

2.3 What is cyber and what belongs to cyber space? 12

2.3.1 Trendsetter organizations affecting to international cyber discussion 14

2.3.2 How prepared are we for cyber threats in the EU and in Finland? 15

2.4 SME segment's financial role and cyber awareness in UK 17

2.5 National and international standards for Cyber Security 18

2.5.1 Risk management practicies (ISO 30001) 19

2.5.2 KATAKRI 2015 19

2.5.3 VAHTI 20

2.5.4 ISO/IEC 27001 Information Security Management System 20

2.5.5 ISO/IEC 27002 Information Security Controls 21

2.5.6 ISO/IEC 27032 Cyber Security 22

2.5.7 Payment Card Industry Data Security Standard (PCI DSS) 22

3 Research **23**

3.1 Research methodology 23

3.2 Survey-study process 25

3.3 Research questions and categories 27

3.4 Research: structures of the organizations 28

3.5 Comparable other studies 29

4 Evaluation of the results of the surveys 32

4.1 The research: current understanding of the business environment 32

4.2 The research: current understanding of the processes 36

4.3 Research: future development 40

4.4 Research: change from the points of view of processes 43

5 Conclusions and discussion 48

References 53

Appendices 56

Appendix 1.The first survey 56

Appendix 2.The second survey 67

Figures

Figure 1. Network readiness index over EU in 2014 16
Figure 2. Sections of ISO/IEC 27002 standard (SFS-ISO/IEC 27002:2013) 21
Figure 3. 10 Steps to Cyber Security 29

Tables

Table 1. Statistics of Finnish enterprises in 2015. 11
Table 2. Fields of industries of organizations participating in the Cyber Security Finland project. 28
Table 3. Business environment awareness, the first survey (N=18) 33
Table 4. Business environment awareness, the second survey (N=12) 35
Table 5. Current state of understanding of the processes (N=18) 37
Table 6. Current state of understanding of the processes, the second survey (N=12) 39
Table 7. Current state of future development (N=18) 41
Table 8. Current state of future development, the second survey (N=12) 42
Table 9. Business management point of view after the self-assessment (N=12) 44
Table 10. Continuity management point of view after the self-assessment (N=12) ... 44
Table 11. Risk management point of view after the self-assessment (N=12) 45
Table 12. Security management point of view after the self-assessment (N=12) 46
Table 12. Service management point of view after the self-assessment (N=12) 47

1 Introduction

1.1 Background of the study

This study aim to understand Finnish SME business organizations' awareness on their dependency of ICT services and solutions. The thesis also wants to raise the acknowledgement of these organizations' decision makers and information management staff on importance of decent cyber security level in their business environment. The studied phenomena relate to the complexity of cyber space and how SME organizations balance between the threats, risks and possibilities in the cyber space related to their business. The main research question is whether an SME organization will increase their awareness of business related cyber space when they complete a self-assessment?

One part of the study was to estimate whether the SME organizations' investments in their employees' cyber security awareness will bring a business advantage for them.

SME organizations often adopt modern information technology services since they often are cheaper and more flexible than conventional services. The conventional services here refer to more private and company specific services, whereas the new technology services relate to internet based services, which means the modern information technology services have different and even new kinds of threats and risks, however, they also possess possibilities not really understood by the companies yet.

1.2 SME segment's role in cyber resiliency

Based on the European Union's (EU) statistics 99.81% of all businesses in the EU area belong to the SME category (SME Performance Review 2016).

This means that increasing the awareness of cyber security to SME organizations diminishes the possible business losses because of poor cyber security planning and deployment (What is an SME? 2016).

In addition to possible risk of business loss for SME organizations, the SME segment often provides services for large and governmental enterprises and organizations. The vulnerabilities in SME organizations' business environment might open doors to even more critical environments for the evil doers.

Nevertheless, the overall security from a nation's perspective relies on security and safety authorities who, in addition to the other governmental regulatory organizations, make sure the nation is safe. They also make sure a nation's international cooperation with other nations, regulatory organizations and organizations is implemented in accordance with the nation's policy.

A nation's internal safety and security beneath governmental authorities is divided into separate groups from the security of supply perspective, which in Finland is controlled by the National Emergency Supply Agency. The National Emergency Supply Agency's main duty is to maintain the society's basic economic functions. The responsible party for the security of supply is a governmental authoritative, however, the parts within the security of supply are individual organizations, either private or public depending on the field of industry. Here the public-private partnership is the key to success. The organizations providing basic economic functions are, for instance, from fields of energy (heat and electricity) and food production, traffic in all terms, financial, health care and ICT services. In these fields, there are plenty of SME organizations providing their services as subcontractors to the providers of the critical service, and thus they constitute a very important part of a nation's security and safety as well. The chain of services or organizations is as strong as its weakest link. The same applies to national cyber security preparedness and awareness as well.

The SME organizations are close to individual consumers from their behavior in business environment perspective. More likely it is the SME entrepreneurs that spread the cyber awareness around them than national authorities. Therefore, the better SME organizations take care of their cyber security aspects and manage the threats and possibilities in cyber space, the more each individual will learn what is important and what is not that important in cyber space. If SME organizations can protect

themselves from cyber-attacks, maintain and develop their business despite the disturbance, the more confident the individual citizens are about the meaning of decent security.

Albeit, being a very important piece of puzzle in national cyber resiliency, business development and awareness, the SME organizations do not widely understand their importance and possibly therefore are according to studies not handling their cyber security and business continuity properly. Some of these studies are discussed more in detail in Chapters 2 and 3 of this study.

The study bases its points of view on few ICT security standards. The main standard and the one that covers the majority of ICT security aspects is ISO/IEC 27001. The national Finnish security frameworks KATAKRI 2015 and VAHTI guidance have been taken into account as well. All of these are discussed in further chapters of this thesis later. The technology standards (such as IEEE) are not within the scope of the study, since the focus of the work is on common practices, not on technology.

Since the organizations for this research are Finnish, the assumption is that they follow Finnish rules and regulations, which is the reason why the implications of rules and regulations in details have not been taken into the scope of this research.

1.3 Cyber Scheme Finland project

The study and its research work were mainly done as a part of a project that developed and introduced a basic level cyber security certificate for SME business organizations in Finland called ‘Cyber Scheme Finland’. The certificate was later on named FINCSC (Finnish Cyber Security Certificate). The certificate has been planned to be a self-assessment tool for an organization to prove their basic level cyber security capabilities (Cyber Scheme Finland 2015). 22 SME organizations from a wide spectrum of industries and sizes participated in the pilot phase of the project, the smallest ones being organizations with five users and the biggest with just about 250 users. Another aspect of the project was to use such common items in the certificate process that would be possible to copy and use widely in other countries as well. The interna-

tional point of view will be interesting, especially when SME organizations see business opportunities abroad either directly providing services or buying services. When SME organizations internationally were able to prove their cyber security capabilities in the same guided framework, it most likely would help to build up trust between parties. That means the focus of the questions of the self-assessment is on the basic level ICT environment items such as password policy, physical access control, user guidelines and policies and for instance basic security controls of perimeters of the business networks. All of these are part of the scope of the ISO/IEC 27001 standard (SFS-ISO/IEC 27001:2013).

A similar process is already available in the UK, called 'Cyber Essentials' (Cyber Essentials Scheme, 2014), which was partially used as an example for Finnish version.

In this sense, the self-assessment questionnaire is nothing new and there are various tools already created for such a purpose, but none of them is aiming for a certification approved by Finnish CERT.

1.4 Goal of study and researched problem

The behavior of an SME organization concerning information technology services is close to behavior of consumers and they do not have too much resources, neither people nor money, to spend on information security. At the same time, it is the biggest business organization segment with approximately 99% coverage in the EU area, which raises the question of how well they are prepared for cyber threats to sustain continuity in business, which provides the question of this study.

The goal of the study is understand the impact of self-assessment on SME organizations' cyber security and business continuity awareness focusing on the problem described above.

2 The background and basis of the research

Based on the nature of this study, it is a qualitative research; however, some data in the study can be treated as quantitative study information. What makes this more a qualitative study is the fact that from the cyber security perspective, in any organization there is no one single truth. This is why the researched phenomena of cyber space dependencies to business environment have been approached from a global perspective, narrowing the research to the viewpoint of Finnish SME organizations (Hirsjärvi, Remes & Sajavaara 2004, 152). The focus in the study is to understand the importance of self-assessment in the enhancement of understanding and awareness of cyber security for business organization.

The SME organizations in Finland face quite easily issues when talking about cyber space or cyber security, e.g. they may not understand the scope of what belongs to cyber space and therefore to cyber security. They tend not to have answers to questions what all aspects needs to be considered what it means for their business etc. The SME organizations cannot be blamed for this since already the terms 'cyber' and 'cyber security' are ambiguous. If the point of view is widened to concern a global perspective and it is studied how the terms have been defined internationally, it can be noticed that the work has not been completed yet. However, cyber security has generally been understood as technology and technique in SME organizations, which is one of the aspects this research is focusing on. The following paragraphs go through the structuring of cyber space pointing out its relevancy for SME organizations.

The cyber security awareness of SME organizations has been studied by security appliance manufacturers, security service providers, different enterprises, authorities and academies quite widely, therefore, there exists a great deal of material about this already. The material provides a good basis for this research as well, and some of it is discussed later on in this thesis (Aho & Nevala, 2016, 16; Kivikoski & Kauppinen, 2016, 48). The majority of these studies states that the cyber security situation in SME organizations is not at an optimal level, neither in Finland nor in other countries.

As an example, the study of Prior Konsultointi Oy for Finnish SME segment organizations' digitalization and information security states that only very few (3%) of the organizations know their business ICT environment has suffered from a security breach, and at the same time, about 5% of the organizations see the information security threats notable for them. The same study reveals that only 13% of entrepreneurs familiarize their employees the information security policies of the company. The study also clarifies the differences between the business areas in behavior for information security, where the healthcare and social services, information management, communication as well as business services are handling the information security in the most versatile ways from the scope of the organizations (Kivikoski & Kauppinen 2016, 48.).

One detail worth mentioning from the study mentioned above as well is that the General Data Protection Regulation in the EU countries, which will be enforced on 25th of May 2018 will hit heavily the majority of the SME organizations, since only 1% of them knew well the requirements of the regulation (Kivikoski & Kauppinen 2016, 50). The ones who knew the requirements and were prepared for the majority of them were from healthcare and social services segment, where there are already quite strict regulatory requirements for the ICT environment.

Then again, the usage of the personnel's own equipment for business purposes in SME business segment is relatively high (31%), which may also be a risk for the business. At the same time, 66% of the respondents state that there are no dedicated personnel for information security. The duties of information security are responsibilities in addition to other duties. (Aho & Nevala 2016, 16, 19.)

TeliaSonera Finland Oyj committed a survey related to information security in SME organizations in February 2016. When asked how the unavailability of the data connections affect the business, 24% of the respondents state their business will stop completely. An interesting finding in the survey was that 13% of the respondents say they have never paid attention to the information security of the company. Three per cent (3%) of the respondents claim they have not protected their business related

data at all, and two percent (2%) state they are not prepared to information security threats. (Sonera tietoturva 2016, 3, 5, 6, 7).

Martti Lehto, Professor of Practice from the University of Jyväskylä states in an article of Keskisuomalainen that too often information or cyber security related threats are not relevant for individuals and are still seen to be far away. At the same time, Lehto states the biggest lack in management of cyber security of Finnish SME organizations is the preparedness for network incidents. This is because of the lack of understanding and know how. 'Not in my back yard' and negligence attitude is one of the reasons for these shortages (Suihkonen 2016).

Negligence on events in cyber space and especially in security might be something that is common for all the above-mentioned studies. SME organizations tend to think and behave quite the same way as individual consumers or citizens.

2.1 Research questions

The main research question is:

- Will cyber security self-assessment increase understanding and awareness of the importance of it to a business organization?

This question is supported by some additional questions approaching the studied phenomena from slightly different angles. These again will help to understand better what is important for the business units and what their maturity level on cyber security is. Additional questions for the whole thesis are:

- What is the impact of cyber security self-assessment to an SME organization's business environment?
- Will cyber security self-assessment improve the awareness of the business critical ICT components and ICT processes?
- Will cyber security self-assessment help the SME organization to invest in ICT security and security related processes?

These are the main questions trying to provide a conclusion for the all phenomena of cyber security and preparedness of an SME organization. The main questions and the answers for them are discussed more thoroughly later in the subsection 3.3 on the

Research questions and categories, and in Chapter 4 Evaluation of the results of the surveys as well as in Chapter 5 Conclusions and discussion.

2.2 Definition of SME organization and its role in economy

An organization belongs to SME category if its staff headcount is less than 250 and if the annual turnover of organization is equal or less than 50M Euros (What is an SME 2016).

According to the statistics of the European Union from 2016, 99.81% of all businesses belong to SME category. In slightly more detailed figures, it means about 23 million SME organizations, generating about 3.9 trillion Euros net contribution of the company to the economy and employing about 90 million people. The majority of SME organizations in EU area employ 10 or less (SME Performance Review 2016.).

In Finland, according to the Bureau of Statistics (Tilastokeskus) in 2015 (Table 1.) there were 363 587 companies out of which 363 004 belong to the category of SME organization. This means 99.8% of the Finnish companies were in the SME category in that year. From financial perspective, SME organizations provided 56.7% of the annual turnover which is over 200 000 million Euros (Statistics Finland, Enterprises 2016.).

Table 1. Statistics of Finnish enterprises in 2015.

	Enterprises		**Staff count**		**Turnover**	
		%	**1 000**	**%**	**M €**	**%**
Staff count per enterprise						
0–4	325 057	89,4	269	18,7	43 172	11,2
5–9	19 414	5,3	125	8,7	20 627	5,3
10–19	10 209	2,8	136	9,5	27 634	7,2
20–49	5 770	1,6	172	12,0	41 737	10,8
50–99	1 657	0,5	113	7,9	34 353	8,9
100–249	897	0,2	136	9,5	51 455	13,3
250–499	305	0,1	105	7,3	30 631	7,9
500–999	159	0,0	105	7,4	37 374	9,7
1 000–	119	0,0	273	19,0	98 913	25,6
In total	**363 587**	**100**	**1 434**	**100**	**385 897**	**100**
SME in total	**363 004**	**99,8**	**951**	**66,3**	**218 978**	**56,7**

Thus, from the financial as well as from employer perspectives SME organizations have a significant role in the EU's and Finland's wellbeing. Individual citizens are either directly or indirectly much closer to SME organizations than large enterprises. Therefore, the importance of cyber security and business continuity in SME organizations has an extremely important role in increasing the awareness and preparedness on phenomena in cyber space.

2.3 What is cyber and what belongs to cyber space?

The term 'cyber' is known to refer to computer, electronic based technology, information technology and virtual reality. The origin of the word 'cyber' is in cybernetics, which again means joint co-operations between man and machine, either a machine acting like a human or human acting as a part of some machine. Afterwards 'cybernetics' developed into 'cyborgs' and the prefix 'cyber' began to mean communication, control and co-operation of man and machine. Today 'cyber' is anything that is related to connecting any kinds of machines to any kinds of networks.

The forthcoming sections from 2.3 to 2.5.7 explain roughly what all belongs to cyber domain, what kinds of activities have taken place there, and how the cyber domain gets organized. These are meant to give an overview where all cyber related requirements originates from and what still might lie ahead. All of these give an insight to what eventually will be relevant for SME organizations as well.

Today, several instances are trying to generalize and define what is cyber space, what are the common terms to be used and the norms that would frame the rules on how to operate in the cyber space. The issue with the generalizing the definitions is that the viewpoints of different instances may vary a lot. Even though the situation of the international law may not sound ideal, it is anyway on its way to improve. The communities actively updating their own terminology and norms can be considered as laboratories of best practices which eventually help the global definitions and the law enforcement.

United Nations (UN) as an international community has the obligation to set the international laws for global domains. The international law for information security

and later for cyber security has been on the table on discussions since late 1990s, however, without significant success. Currently the international law including norms and terminology have, for instance, been set over Space (United Nations Convention on the Law of Outer Space) and Sea (United Nations Convention on the Law of the Sea). Cyber, being a global domain, should also have its own set of global rules, norms and terminology, which have not been defined yet. The main forum leading the discussion and decision making for international information security on information and telecommunication globally is the UN Group of Governmental Experts (UN GGE).

As an example of the lack of norms and terms is the usage of the term ‘cyber war’. Where has it been stated when to use term ‘cyber attack’ and when ‘cyber war’? Or has it been defined when a ‘cyber war’ begins, when it ends and as post activity, how to disarm one from cyber weapons? Were the attack to Ukrainian power grids in December 2015 a cyber attack in terms of war, or was it just ‘cyber sabotage’. Or, what does this mean for non-military organizations? Was Sony hack in late 2014 an act of war, sabotage or just a well targeted ‘cyber hack’? There are no definite and clear answers for these questions.

The definitions of norms and terms are getting crucial as time goes by. In the near future, one of the main issues that are needed is the ‘code of conduct’ of cyber space or cyber domain. For instance, the Internet of Things as phenomenon will bring, according to Gartner, an estimation of 25 billion connected devices by the year 2020. How many of these devices are making decisions based on the data of other devices? What will be the criteria of those decisions? The criteria of decisions have to rely on norms and code of conduct that need to be common and agreed upon.

Another aspect is due diligence in cyber space. Due diligence answers to the question ‘what are the necessary actions to fulfill the requirements’. The requirements can be based on international law, national law or just the policy on a specific enterprise. If there is no defined ‘due diligence’ in cyber space, the possible international law becomes just a guidance. Tallinn Manual, Rule 5 states that "A state shall not knowingly

allow the cyber infrastructure located in its territory or under its exclusive governmental control to be used for acts that adversely and unlawfully affect other States" (Schmitt, 2013, 26). This rule is the base of Tallinn Manual based on a statement of International Court of Justice on states' responsibilities.

Then again, if independency of a state from territorial perspective is undisputed, how is the situation from cyber space perspective? From the perspective of physical borders it is illegal to intrude to another country's territory, however, what do physical borders mean in cyber space? For instance, SME organizations in Finland, even though providing services and products to Finnish customers and partners, quite often utilize international cloud services for processing their data.

Whenever there is some international agreement for all of these questions, it will have an impact to every one operating in the cyber space. Therefore, these are very important for SME organizations to understand as well, even though they might appear not to concern them. All this just proves the fuzziness of the cyber space and the rules how to play there.

2.3.1 Trendsetter organizations affecting to international cyber discussion

Since there is no international law for cyber space, there are no definitive norms around cyber space either. The international law for cyber space is relevant for the states to operate there congruently, just the way they do in sea or air domains.

When the norms have not been agreed upon globally, what does it mean for the global standards of cyber space? At the moment, it means there are various regional or environment specific standards available for cyber space.

The North Atlantic Treaty Organization (NATO) agreed to recognize cyberspace as a domain next to air, space, sea and land in Warsaw Summit on July 8 and 9 in 2016 (Warsaw Summit Communiqué, 2016). It means that NATO will raise the focus on cybersecurity and will require a raised focus from its member states. It remains to be seen if NATO will now be able to influence the United Nation's (UN) definitions for terminology and norms. Nevertheless, NATO is only one of the many coalitions which create definitions from their own point of view.

Shanghai Cooperation Organization (SCO) is a coalition led by China and Russia who have been very active in defining norms and terminology for cyber domain and information security, however, their proposals have not been accepted as such in the UN. The reason for this have been the proposals' restrictions to open and free internet data transmission and communication, which have been seen to be deviations from some western countries' perspective. However, within SCO, the countries have signed the Yekaterinburg Agreement in 2009 where the main principles and cooperation processes related to international information security were introduced (Yekaterinburg Declaration of the Heads of the Member States of the Shanghai Cooperation Organisation, 2009). It, however, forms a basis for the UN's 'International Code of Conduct for Information Security'.

The Organization for Security and Co-operation in Europe (OSCE) is a coalition of 57 countries from Europe, North America and Central Asia, thus, for instance Russian Federation and United States are members of this group (Participating States, 2017). Within OSCE, it has been agreed on some specific confidence building measures in 2013. The agreement includes, for instance, communication and information sharing mechanisms such as defining the contact points of ICT incident handling and consultancy between member states.

Then there are for instance G8 and G20 countries as well as enterprises such as Microsoft who have their own points of view and requirements for the international law of cyber space.

2.3.2 How prepared are we for cyber threats in the EU and in Finland?

However, when the cyber security awareness and capabilities are studied globally it can be seen that the overall situation in the EU and in Finland is relatively good. In December 2014, the EU Institute for Security Studies released a study relating cyber development to human development. This study consisted of e.g. country specific figures about the amount of internet users and mobile / fixed line subscriptions, number of top global ICT companies, network readiness, usage of internet and skill level on computer / internet and prediction of probability of cyber threats. According to this study, the EU countries are doing well, and Finland is one of the highest

ranked countries in the world in these categories (Pawlak 2014, 83 - 85.). Figure 1 shows the network readiness index over EU countries.

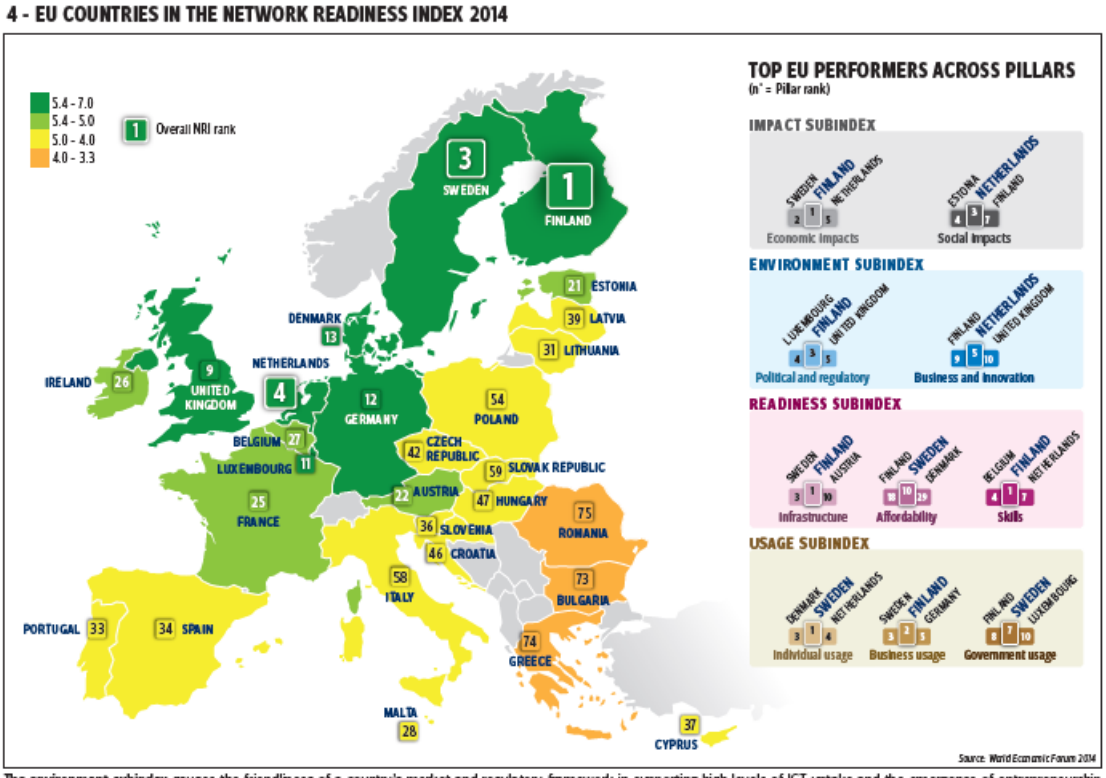


Figure 1. Network readiness index over EU in 2014

In 2016, the EU put Network Information Security (NIS) directive into operation. This means some more obligations for information sharing of cyber security incident for organizations in a certain role. NIS directive does not have obligations for SME organizations, however, it mandates organizations providing critical infrastructures or services. In chains of services where SME organizations are a part of services of critical infrastructures, the directive most likely means more attention to cyber security for the whole chain.

In May 2018, the General Data Protection Regulation (GDPR) is to be adopted in the EU countries. This means quite a big step for all organizations in the EU area to enhance the security of the information and privacy.

In addition to this, according to the Security Intelligence Report (SIR) published by Microsoft, Finland is one of the countries that have the least amount of malware in

its networks. The reports also states that Finland is one of countries with the lowest number of infected computers (FICORA's Cyber Security Review 1/2014).

From Finnish SME organizations' perspective, the term 'cyber' is ambiguous. Still today too often it turns to technique and technology, how to protect business environment from threats of the internet. According to one study, 90% of the respondents believes their firewalls and anti-virus software are up to date, however, 20% believed the information security guides and policies were in place. Only 13% claim to familiarize their personnel with information security (Kauppinen, Kivikoski 2016, 5).

2.4 SME segment's financial role and cyber awareness in UK

According to the report of Dept. for Business Innovation & Skills (BIS) "Business population estimate for the UK and regions: 2015 statistical release" in UK, the amount of SME organizations of all private sector business was 99.3%. In addition, SMEs contribute £1.8 trillion, which means 48% of all UK private sector turnover. From the figure's (Figure 1) perspective UK is quite close to Finland what comes to the importance of SME business.

Based on this, Ponemon Institute in the UK analyzed the state of cyber security in SME organizations, and found that only 14% of the companies rated their ability to mitigate cyber attacks as highly effective (Ponemon Institute, 2016 State of Cybersecurity in Small & Medium-Sized Businesses (SMB), 6). At the same time, the security breaches to SME organizations had increased by 21% in a year. During the same time period in the large segment business organizations the increase of security breaches was 11% (BIS, Information Security Breaches Surveys 2015)

UK Government BIS have published a guide for SME organizations to clarify the ambiguousness of cyber security (BIS/15/147, Small businesses: What you need to know about cyber security, 2015). It has a section "Train your staff" which is linked to free online training courses. These kinds of guides in addition to the self-assessment tools are welcome to Finland as well.

Another study from Feb 2015 in UK states that SME organizations seem not to understand the threat of losing business (Bradley & Vaizey, 2015). According to the study

SME organizations put almost a third (32%) of their revenue at risk because of believing they are protected, that they cannot get hit by cyber criminals or just because of some other misconception.

According to the UK government's Information Security Breaches Study the average cost of the security breach is somewhere between £65,000 and £115,000 and can put business out of action up to ten days, although at the same time, 24% of the SME organizations claim it costs too much to invest in cyber security (Bradley & Vaizey, 2015).

So far the same kind of study has not yet been found in Finland, however, the same kind of behavior can be found in Finland as well. The SME organizations do not believe they are the targets of the criminals, or that they would be under a big risk to lose revenue because of security breaches.

However, what seems to be common in studies related to SME organizations and cyber security is that the SME organizations need to balance between organizational, technical and psychological aspects in order to respond to keeping their cyber protection high.

2.5 National and international standards for Cyber Security

Open standards create the basis for the digital infrastructures now and in future, and they are so necessary for organizations to be able to operate in cyber space. Despite the lack of international laws for cyber space, the standards – international, national and industry specific – however, support each other quite well and have many similarities.

The active organizations in standardization of cyber space internationally have been for instance International Organization for Standardization (ISO), International Electro-Technical Commission (IEC) and International Telecommunications Union (ITU). On more technical specific matters, The Institute of Electrical and Electronics Engineers (IEEE) and Trusted Computing Group (TCG) are active and often referred to in technical standards. As a proof for similarities in international standards, ISO and IEC

have combined the ISO/IEC 27000 family of standards for information security and management.

Some international standards such as Control Objectives for Information and Related Technologies (COBIT) and Information Security Forum Standard for Good Practice (ISF-SOGP) relate heavily to ISO / IEC 27000 family of standards; but to others as well.

From industry specific standards, one of the most often referred standard in ICT services is Payment Card Industry – Data Security Standard (PCI-DSS).

National standardization organizations and active members are then for instance American National Standards Institute (ANSI), British Standards Institution (BSI), Deutches Institut für Norming e.V. (DIN) and Finnish Standards Association (SFS). The national standards, however, differ quite often from each other, which is also why the international standards are normally referred to as the standards for cyber space.

From Finland's perspective to cyber space, the main standards most often referred to are ISO / IEC 27000 family and national criteria and guides KATAKRI and VAHTI. KATAKRI and VAHTI are collections from global standards (i.e. ISO / IEC 27000, COBIT, PCI-DSS, ISG-SOGP) and national requirements and regulations.

2.5.1 Risk management practicies (ISO 30001)

Risk management is one part of the problem discussed in this study. SME organizations might be operating with only few persons, and they have considered business impacts of physical threats. For those they normally have insurances to mitigate the risk. From cyber space point of view, they may not have anything in place.

ISO 30001:2009 provides principles and guidelines for managing the risk (SFS-ISO 31000:2009). Some parts of this standard have been taken into account in the Cyber Scheme Finland-project as well as in the survey questionnaire for this study.

2.5.2 KATAKRI 2015

KATAKRI 2015 – National Security auditing criterion - are Finnish national security criteria created by Ministry of Defence, and they are meant for auditing organizations'

preparedness for securing important assets. KATAKRI 2015 can be used as a security management framework when planning and organizing security controls for an environment that is known to have relations to higher security class organizations or environments (Ministry of Defence, Katakri 2015).

KATAKRI 2015 consists of a set of minimum requirements that are based on national and international regulations and standards. It is nowadays a 'de facto' framework for ICT environments of public authority in Finland.

For SME organizations, KATAKRI 2015 as such is too demanding framework for ICT services. Some parts of KATAKRI 2015 are also covered within Cyber Scheme Finland project. The survey questionnaire of this study also includes some requirements of KATAKRI 2015.

2.5.3 VAHTI

VAHTI provides the guidelines and policy for Finnish governmental organizations in information and cyber security. VAHTI guidance is created by Ministry of Finance.

VAHTI guidance has quite an extensive set of instructions and guidelines, which as such can be used for instance for SME organizations as well, however, since it has been created for government organizations, it not all relevant for SME organizations, because it is too heavy and demanding. VAHTI guidance consists of about 1,200 couples of requirements (Ministry of Finance, VAHTI, 2015). Probably that is why it is undergoing quite an extensive renewal work, which will most likely be ready during year 2017.

The study and the research questions are covered within VAHTI.

2.5.4 ISO/IEC 27001 Information Security Management System

ISO/IEC 27001 standard is an international standard for information management (SFS-ISO/IEC 27001:2013). To it belongs information technology, security techniques and management and information management requirements. The main thing for SME organizations in ISO/IEC 27001 standard is the Information Security Management System (ISMS). It pretty well covers risk management related ICT environment,

but it has the same issues with SME organizations as the other main standards. It is too time and resource consuming to follow it exactly.

For this study ISO/IEC 27001 has some similarities with ISO 30001. The differences have not been specified separately. The items that have been raised in the questionnaire of this study are partially the same as in a normal ISMS process.

2.5.5 ISO/IEC 27002 Information Security Controls

ISO/IEC 27002 is an international standard for ICT security. It also provides a guidance for good practices from information security perspective such as VAHTI. From an organization's perspective if ISO/IEC 27001 provides the ISMS to it, the ISO/IEC 27002 provides the security controls for the ISMS, which is why they are quite often paired.

For SME business organizations, ISO/IEC 27002 provides a good set of technical requirements or guidelines on how to set up the ICT environment, however, as with the other large national or international standards, this is quite heavy for them to be certified (SFS-ISO/IEC 27002:2013). However, ISO/IEC 27002 has all the same parts as FINCSC has (see Figure 2.). So if an organization applies for FINCSC certificate, it is one step closer to ISO/IEC 27002 certificate.

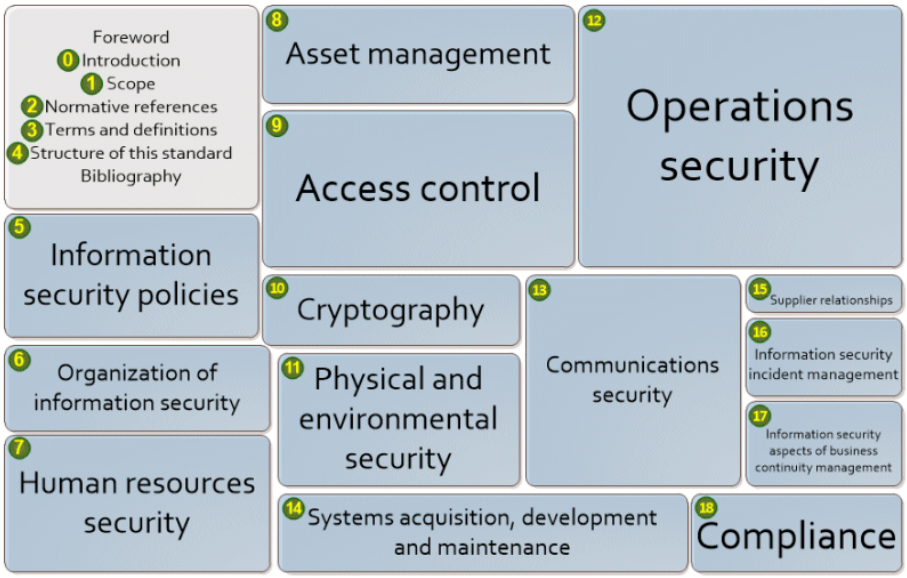


Figure 2. Sections of ISO/IEC 27002 standard (SFS-ISO/IEC 27002:2013)

2.5.6 ISO/IEC 27032 Cyber Security

ISO/IEC 270032 provides the requirements and guidelines for cyber security. Or like it is said in the standard itself, “Cyberspace security”. The focus is with the internet security. This is also one of the standards that have definition to word ‘cyberspace’ (ISO/IEC 27032:2012):

> *“the complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form”.*

This standard is not much referred to in this study nor in the FINCSC certificate. The reason for this is that the focus of the study is on SME organizations’ ICT environment, and only one part of it was the assessment of the internet border security.

2.5.7 Payment Card Industry Data Security Standard (PCI DSS)

Payment Card Industry (PCI) is a global organization, which elaborates the safety of the payment cardholders data by requiring all the entities involved with the payment card data transaction to fulfill the security requirements framework (Data Security Standard) it has developed.

PCI DSS aims to help businesses and financial sector to make sure they have protected the data of the cardholder and the systems the data is stored to (Security Standards Council, 2016). These requirements also follow technology vendors and service providers; basically, the whole chain of services involved with the flow of the data of the cardholder.

PCI DSS requirements apply to quite many SME organizations, however, like with the other standards, only some parts of it are used for the basic level cyber security assessment.

3 Research

This study aims to understand the importance of self-assessment of an SME organization in increasing awareness on cyber security. The survey study method was used to conduct the research. Because of the ambigousness of cyber space and subjective reflections of each respondent to the research questions, this research will be treated as qualitative research. In addition the amount of respondents to the surveys were rather small, which meet better the requirements of qualitative research than quantitative. However, the study has some parts that have quantitative features, which appear in the survey phase and in the analysis of the results. The study does not try to prove propositions, instead it points out facts and realism, which are common nominators for qualitative research (Hirsjärvi, Remes, Sajavaara, 2004, 152).

When thinking about the research plan of this study it can be seen there has not been such in the beginning of the study. There actually has not been a firm research plan for this study throughout the whole study. The research itself has developed and changed according to the circumistances, and the process has been flexible, which is also common for a qualitative study (Hirsjärvi, Remes, Sajavaara, 2004, 155).

3.1 Research methodology

This study uses explanatory research methodology to conduct the research, and the method of the research is a survey study. In addition, when investigating the results of the survey, inductive and hermeneutic analyses have been used to point out the findings.

Hermeneutic analysis is in this study used to gain understanding on human behavior. The language used in the survey study may not be understandable for all of the participants, mainly because of the ambiguousness of cyber security and its terminology. Some of the answers of the surveys are then analyzed based on hermeneutic approach (Anttila, 2014, Tutkimisen taito ja tiedon hankinta., 7.3.2 Hermeneuttinen

kehä), combining questions into groups and trying to understand as well as decode the answers.

The frames for the inductive analysis are provided in section 2, Background. The questions created to the surveys of this study are conducted from these frames, so also the answers of the respondents reflect on the frames (Hirsjärvi, Remes, Sajavaara, 2004, 155; Anttila, 2014, Tutkimisen taito ja tiedon hankinta., 7.1 Tieteellisen päättelyn logiikat).

Survey study was selected to be the method because of few reasons. First, the studied samples of business organizations were pre-defined to be the pilot organizations of the Cyber Security Finland project. It was much easier for the author as well as for the respondents to commit a survey instead of, for example, an interview. Moreover, since the survey was committed twice, other methods would have required even more time, efforts and arrangements. Second, the research question and the supporting questions are more aiming to point out human factors of the studied phenomena (e.g. thoughts, feelings or even believes). According to Hirsjärvi, Remes and Sajavaara (2004, 129), these are typical for survey method study. And third, the comparison of before and after self-assessment was easiest to carry out with survey-method.

Because of these human factors, the results of the study and the surveys are subjective to each respondent. For instance, each respondent's working history and experience, knowhow of ICT and business and status in organization have an impact to the results. These are some of the factors why inductive analysis and hermeneutic analysis were used as research strategy (Tuomivaara, 2005, 29).

The survey method has some disadvantages as well. Since the respondents of the surveys are individuals, there are some human factors affecting the results: have the surveys been committed seriously, have all the questions been understood, are the questions relevant for each respondent, how quickly were the answers given. There are plenty of questions that put the survey study in shallow and modest light (Hirsjärvi, Remes, Sajavaara, 2004, 184), although some of these are answered in the

hermeneutic analysis. One of the issues with this study is that the sample of each survey is relatively small.

3.2 Survey-study process

As mentioned before, the study was committed as part of the Cyber Security Finland project in which twenty-one organizations participated. The project aimed at creating a self-assessment tool for a business organization to prove that they have the basic cyber security controls, guides and processes in place. Because this research is aiming to understand the importance of self-assessment in increasing awareness and understanding of cyber security, the survey of this study had two phases: before the self-assessment and after the self-assessment. This way it was possible to get a 'before' and 'after' view from each respondent. The first survey is in Appendix 1 and the second in Appendix 2.

A Webropol survey study tool was used to conduct both surveys. For the assessment of the surveys, a Likert scale was used to measure the like-mindedness of the respondents, on a scale one to five from "completely disagree" to "completely agree", although zero was "not applicable".

The questionnaires to the SME organizations were aimed at persons who have an overview of the business organization. Important was that the persons responding to the surveys of the study were the same ones who responded to the Cyber Security Finland project's self-assessment. The titles of the participants from the business organizations varied a great deal. The majority of the participants were CEOs, then there was one CIO and few business and service managers.

The first phase of the survey consisted of a set of questions, which aimed to provide and rate the participant organizations' understanding of their current work environment. How well they know and manage the main risks related to their business or for instance, how well do they think their business related ICT services are monitored and managed? The first phase of the survey consisted of 36 questions.

The first survey was sent out to all twenty-one participants on the 10th of March, 2016. After a reminder note on the 20th of March, 2016 eventually answers from eighteen participants were received on the 23rd of March, 2016.

It is important to notice and mention that the answers for the first survey had to be given before the organizations began to answer the certificate questions. Otherwise, the responds would not have been authentic.

Then, during April 2016 the participating organizations committed the self-assessment of Cyber Security Finland project. It appeared that during the self-assessment phase five organizations dropped out from the pilot project, which means only seventeen organizations were left. The reason for leaving the pilot is not known. Nevertheless, this is worth to notice as the reason might be the same as TeliaSonera Finland's study pointed out: cyber security is not seen a risk for 13% of the business organizations (Sonera tietoturva 2016, 3). Or it can even be the negligence in attitude mentioned by Lehto (Suihkonen 2016).

The second survey began right after the last organization had completed the self-assessment of the Cyber Security Finland project. The questions during the second phase concentrated more on studying the change on the awareness of the business environment. Considering the second phase questionnaire as a whole, the main question would be 'how much more you know now than before the self-assessment certification of your business environment and its relation to cyber space'. Have they changed or will they change their ways of working after completing the certification self-assessment? The survey of the second phase had altogether 38 questions and one open question for feedback of the pilot project.

The second survey was then sent out to the rest of pilot project organizations on the 18th of May, 2016. Two reminder notes were sent to the respondents, the first on the 29th of May and the second on the 20th of June, 2016. The end-result was twelve answers. From that perspective, not all the findings of the research can be generalized.

3.3 Research questions and categories

The surveys are divided into two parts, 'before' and 'after' the self-assessment. Therefore, the questions in the surveys have a slightly different weighting in what angle they approach the studied phenomena. The first survey, the 'before' the self-assessment, will have more weighting on the current state of awareness of the overall situation in the business and ICT environment. The second survey has then more weighting on change of the awareness after the self-assessment. Does the world look any different from what it used to be after a basic level cyber security self-assessment?

The main question for the whole study is:

- Will a cyber security self-assessment help to increase understanding and awareness of the importance of it to a business organization?

This can be answered when both surveys and their results are analyzed.

The supporting questions are following:

- What is the understanding of the current situation of the business ICT environment?
- What is the current situation of the business ICT environment from security perspective (people, processes, technology)?
- Future development of the business ICT environment (people, processes, technology).

And

- Will cyber security self-assessment improve the awareness of the business critical ICT components and ICT processes?
- Will cyber security self-assessment help the SME organization to invest in ICT security and security related processes?

Based on these questions, both of the surveys will have a point of view for basic processes of business and ICT services:

- Business management
- Continuity management
- Risk management
- Security management
- Service management

3.4 Research: structures of the organizations

The organization participating in the Cyber Security Finland project pilot belonged to the SME category, both from revenue as well as from headcount perspectives. The headcounts within the organizations varied a great deal, which was also intentional when selecting the organizations to the pilot. The smallest ones had less than five employees and the largest about 250. This way the self-assessment process could be tested from both ends of the SME category. At the same time, the ground for this research is to be fertile enough to provide some findings.

As mentioned earlier, the employees attending the surveys of this research were the same ones who committed the self-assessment. There were 18 employees to respond the first survey. Ten of them were CEOs or Entrepreneurs, five CIOs, COOs or Business Directors. Three respondents were Engineers or Service Managers.

The second survey comprised twelve respondents, out of which eight were CEOs or Entrepreneurs, two CIOs or Business Directors and two Engineers or Service Managers. Thus, respondents mainly consisted of decision makers.

The fields of industries of the organizations are shown in the Table 2 below. The fields are in accordance with the Standard Industrial Classification described by Statistics Finland (Statistics Finland, Standard Industrial Classification TOL 2008).

Table 2. Fields of industries of organizations participating in the Cyber Security Finland project.

Standard Industrial Classification TOL 2008	**Amount of organizations in Cyber Security Finland project**
Science, Technology and Information Society	2
Information and communication	10
Financial and insurance activities	1
Construction	1
Electricity, gas, steam and air conditioning supply	2
Manufacturing	2
Human health and social work activities	2
Public administration and defence; compulsory social security	1
Wholesale and retail trade; repair of motor vehicles and motorcycles	1

3.5 Comparable other studies

In the UK, there has been a basic level cyber security self-assessment system for SME organizations, called Cyber Essentials, in production since 2014. Cyber Essentials is supported by The Government Communications Headquarter (GCHQ) of UK, the centre for Her Majesty's Government's Signal Intelligence. Cyber Essentials was produced by Information Assurance for Small & Medium Enterprises (IASME), Information Security Forum (ISF) and British Standards Institution (BSI) (Department for Business, Innovation and Skills, 2014, Cyber Essentials Scheme, 4).

One of the main purposes in Cyber Essentials was to raise the awareness of cyber threats in general. CESG (the information security arm of GCHQ) developed a "10 Steps To Cyber Security: At-a-glance" graphic (Department for Business, Innovation and Skills, 2014, 10 Steps: Summary) that defines well all the basic elements of cyber security shown in Figure 3.

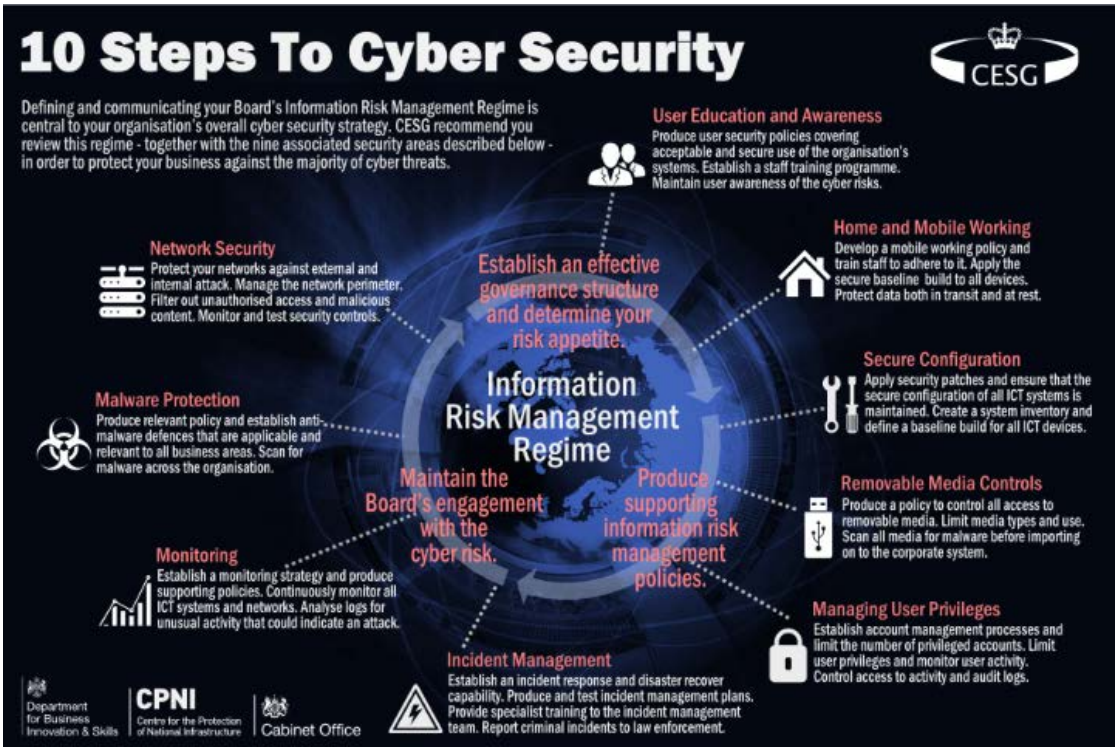


Figure 3. 10 Steps to Cyber Security

Now that the Cyber Essentials have been in production for about three years, there already is some evidence of its effectiveness. It has been proven that with Cyber Essential tools, more than 99% of the most common internet based vulnerabilities in the SMEs were mitigated (Such, Vidler, Seabrook, Rashid, 2015, CYBER SECURITY CONTROLS EFFECTIVENESS, 2), although, the study still does not highlight how much the awareness of cyber security has been increased through Cyber Essentials.

Mark Tomlin in his Master's thesis states that many of the current self-assessment tools are not targeted to SME organizations. The reason is that the maturity level of SME organizations in cyber security is on such a level that they do not even understand the self-assessment questions (Tomlin M., Advancing Small Business Cyber Maturity: An application of the NIST Cybersecurity Framework, 2015, 46-49).

The study of Aho and Nevala (2016, 4 - 5) states that the importance of individuals in maintaining cyber security level is crucial, and unawareness or negligence may have severe security impacts. Aho and Nevala in their study asked, for instance, if the respondent has acknowledged the guidance of the employee for the social media. As the answer 'Yes' was relatively high (about 67%), Aho and Nevala believe this is because there was a link to the guidance along with the question. Therefore, Aho and Nevala believe the question with a guidance motivates the respondent to find answers (2016, 15). In addition, one interesting point in their study is that nearly 20% of the respondents had not been guided on how to use the internet and its services securely, neither at work or outside work. Aho and Nevala believe that the lack of security guidance at work is a consequence of the lack of training arranged(2016, 20).

In general, the study of Aho and Nevala points out the basic level cyber security items well all as the way from password management to other technical and functional as ways to improve cyber security. This study provides important observations of awareness of cyber security perspective as well as human behavior in cyber security incidents. These are equal to what Lehto from the University of Jyväskylä states in the article of Keskisuomalainen about the negligence (Suihkonen 2016).

The study of Prior Konsultointi Oy for Finnish SME segment organizations digitalization and information security states the same observations as Aho and Nevala,

namely, that the employees are not often familiarized with the company's security policies and practices (Kivikoski, Kauppinen 2016, 48). Nevertheless, Kauppinen and Kivikoski (2016, 50) add that the organizations operating in the field of healthcare and social services, information management, communication as well as business services take care of the information security comprehensively.

All of these are items that will be reflected on in the next section of this thesis, as they all support this study, raise its reliability and are valid with its findings.

4 Evaluation of the results of the surveys

As described earlier, the material for this research was gathered in surveys conducted in two phases. The research itself is a qualitative research where some of the findings have quantitative features because of the results of the surveys. For the research strategy, inductive and hermeneutic analyses have been used to point out the findings.

Since these surveys were appointed to individuals representing their own organization, the human factor of the responses need to be taken into account. As the responses are always subjective to each respondent, the factors e.g. the personal status in the organization hierarchy, personal knowhow on ICT services or business factors, the industry and the size of the organization may have an impact to the answers.

4.1 The research: current understanding of the business environment

The research wanted to point out whether a self-assessment can help to increase understanding of the importance of cyber security. In addition, the supporting questions have been used in separating the questions into separate groups:

- What is the understanding of the current situation of the business ICT environment?
- What is the current situation of the business ICT environment from security perspective (people, processes, technology)?
- Future development of the business ICT environment (people, processes, technology).

The research has, according to the research question, been divided into three logical groups where both, ‘before’ and ‘after’ surveys are combined after which the change is reviewed. The groups are:

- Current understanding of the business environment
- Current understanding of the processes
- Future development

Both of the surveys, the ‘before’ and ‘after’ the self-assessment are found in the Appendices of this thesis. The first survey in Appendix 1 and the second in Appendix 2.

The first survey consisted of 36 propositions from different angles of business and ICT environment. Its intention was to enhance understanding on the current state of each respondent's awareness of their own business environment, policies, processes, procedures and services.

Table 3 below describes the current state of awareness of the business environment.

Table 3. Business environment awareness, the first survey (N=18)

The current state during the first survey was relatively optimistic. Only the amount of staff in maintenance and development functions of ICT services would have some enhancement needs.

Another interesting point here is that the respondents are more or less confident they know the requirements of regulations for their business environment. This question should have been defined more precisely to point out, for instance the requirements of GDPR to their business. Now the question leaves slightly open what the respondent understands with the question.

An example of human factor can also be seen in question 'digitalization adds value to your business' as digitalization as a term is undefined; however, still ubiquitous. The same actually applies to the term 'cyber security'. It is also used everywhere and its description is not very accurate. However, when in the future development section it was inquired whether the respondents 'believe cyber security will bring advantage to your company', only six respondents agreed. The answers are based on the respondents' feelings, beliefs or thoughts.

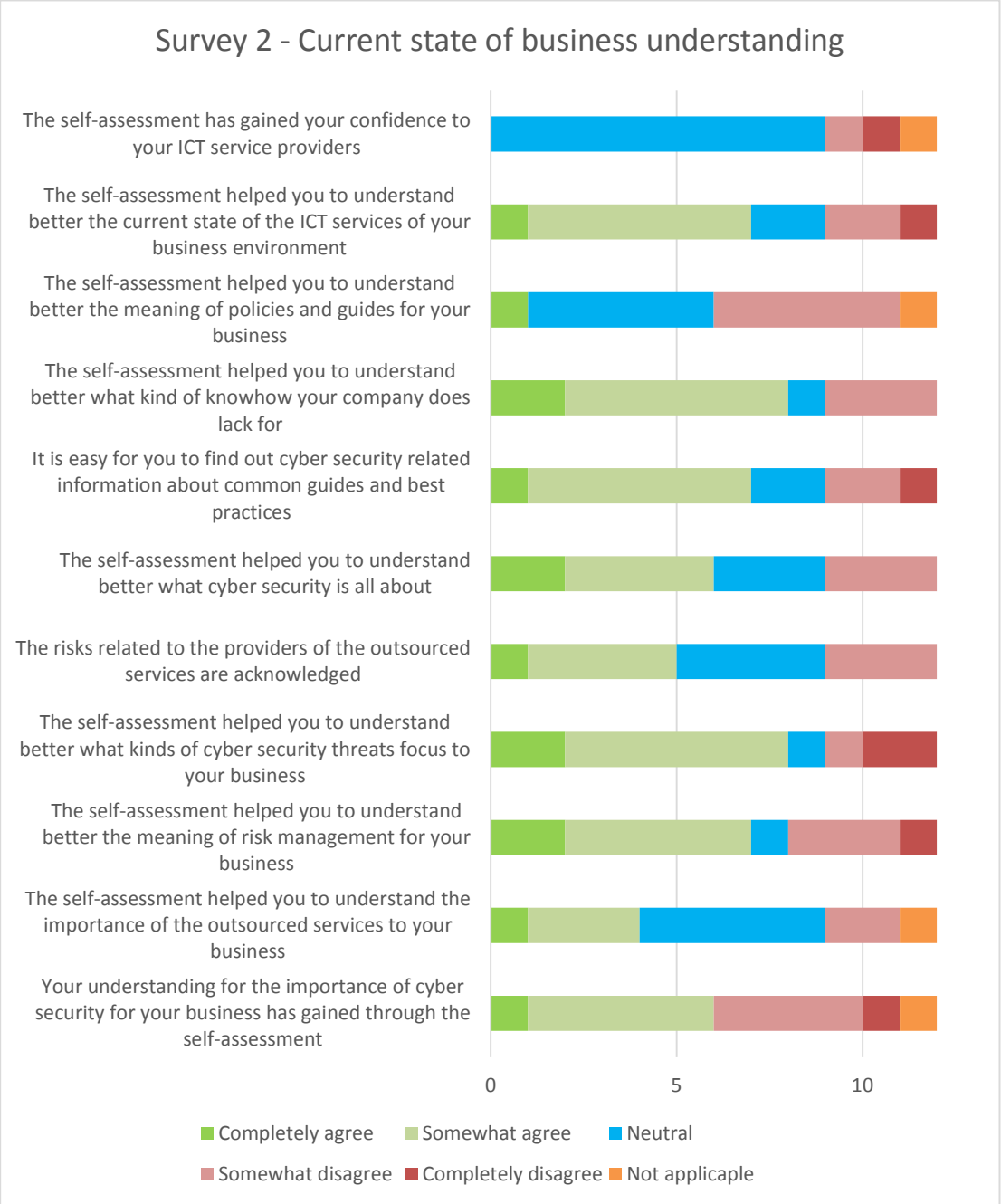
The second question of the survey provides the change of the awareness of cyber security in business environment after the self-assessment in Table 4. Half of the respondents (six) either completely or somewhat agreed, four either completely or somewhat disagreed. One stated the question not to be applicable for them. The answers of the individuals as well as the open comments of the second surveys business environment awareness related questions reveal that the ones who did not see any increase in awareness were organizations that already have a high maturity level in cyber security, either at organizational or personal level. The differences between the answers cannot be explained based on the industry or respondents' roles.

Concerning the statement, 'you have a clear figure of your ICT environment', thirteen of the answers were completely or somewhat agree, which indicates, especially remembering the statuses of the respondents, a really high value. However, when the same statement was raised in the second survey, after the self-assessment, the responses point out in quite many respondent states that the self-assessment helped

them to get a better picture of their environment. Again, however, it is more about how the respondents' feelings and beliefs instead of hard facts.

The second survey pointed out the respondents experience on the change of the awareness of the business environment and cyber security understanding as illustrated in Table 4.

Table 4. Business environment awareness, the second survey (N=12)



When comparing the question ‘it is easy for you to find out cyber security related information about common guides and best practices’, the answers state no big change in awareness, although, in the open comments of the second survey one respondent states that sharing basic cyber security information e.g. examples and best practices free of charge would be important especially for the small companies.

Then, the statements about self-assessment gaining awareness of cyber security and its importance to the business, threats against their business, lack of knowhow and risk management seem, according to the second survey, to provide positive results. Mainly the respondents state the awareness and understanding has enhanced through the self-assessment process.

One open comment states that the self-assessment raised points of view they had not much considered such as physical information security and backup personnel. Another open comment stated that self-assessment tools are needed in order for the organizations to know what to ask from service providers or where in cyber security they can ask for advice.

In the questions related to the outsourced services, their service providers and the risks related to the outsourced services, the responses have a slight variation. For the statement, ‘the self-assessment has helped to increase your confidence to your ICT service providers’, the answers either neutral or disagreeing. This can be interpreted so that the situation with the service providers has remained the same, and self-assessment did not change the understanding. One open comment stated that for SME organizations it would be beneficial, if there were a framework, a standard guidance or a tool how to purchase ICT services remembering good practices of cyber security. Nowadays, SME organizations do not have such a framework. This is true, even though plenty of information about the topic is available. The frameworks, tools and guides are currently the bread and butter of many consultancy companies.

4.2 The research: current understanding of the processes

The current understanding of the processes focuses on the current ways of working and operating processes. Since the self-assessment for the Cyber Security Finland

project concerned cyber security, the security has quite a big weighting in these surveys.

The first survey focuses on the current state of the ways of working and processes, whereas the second survey on increase of the understanding after completing the self-assessment. Table 5 shows the responses for the first survey.

Table 5. Current state of understanding of the processes (N=18)

From the current state perspective before the self-assessment, the questions are related to information and incident management, current policies and guidance, continuity management aspects and training.

According to the survey, the basic processes related to services and their management are generally in good shape. Business critical services are managed, controlled and monitored. Regarding the awareness of the fault tolerance of the business critical systems four respondents disagreed and nine agreed. However, when asking about fault tolerance tests for these systems seven out of 18 respondents disagreed and four agreed, which might raise the quite common issue with the backup systems for the critical services: they do exist; however, they have not been tested nor proven to work. Yet again, the responses are from individuals, which means they may not know the current situation exactly.

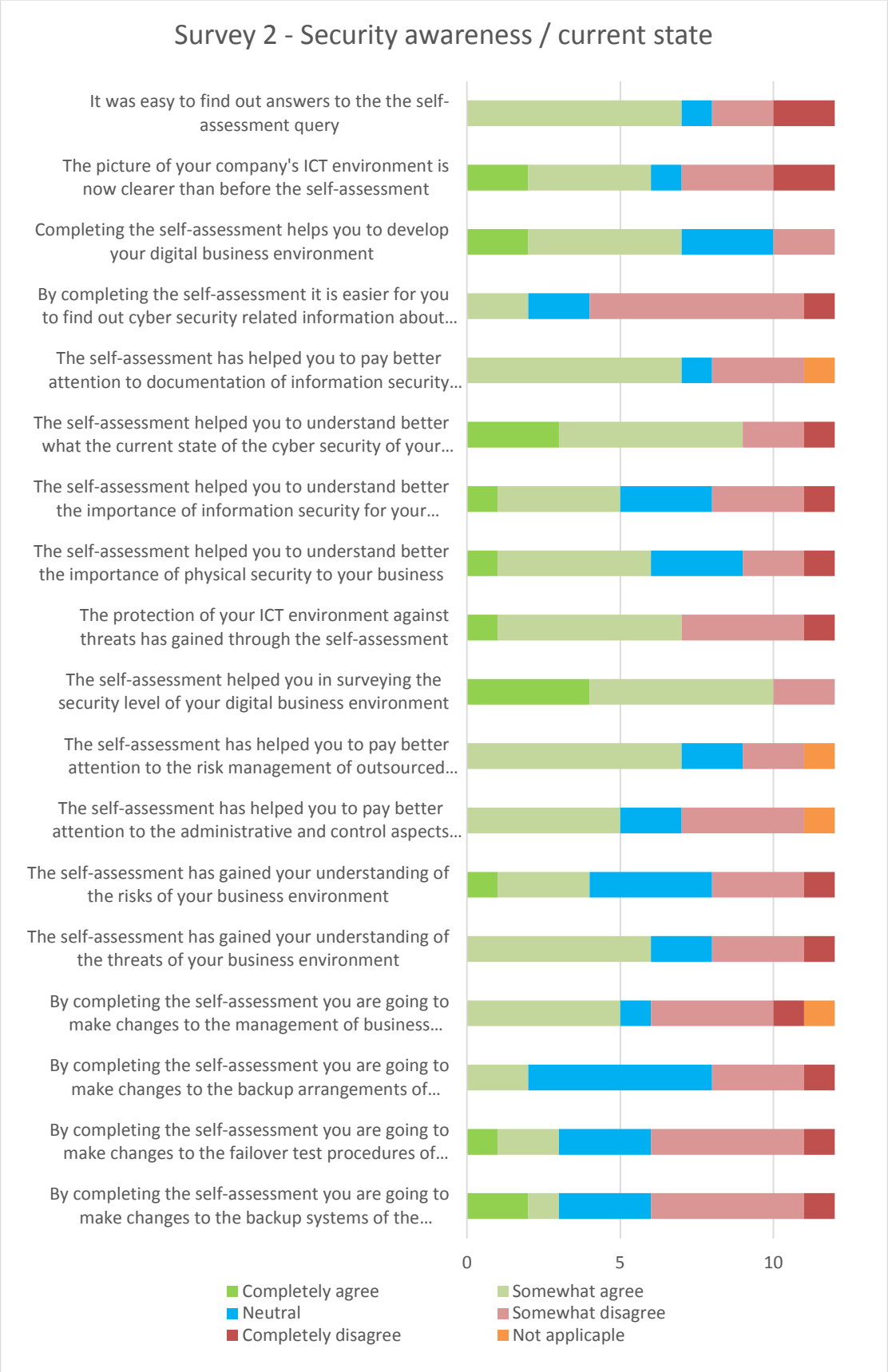
From the information security perspective, the availability, confidentiality and integrity of the information are important for the respondents. The availability of the information is, according to the survey, the most important.

The backup arrangements for the key personnel were arranged for five of the eighteen respondents. The others responded either neutral (eight) or disagreeing (five). This might mean that the smaller the organization is, the less backup resources there are considered or that the respondents are not aware of the situation.

The majority of the respondents expected the self-assessment to help them to increase understanding of their current security level of the digital business environment. This already is a good statement raising the importance of self-assessment tools in enhancing awareness, even though it still based on the beliefs and feelings of the respondents.

Table 6 provides the information of security and process awareness after the self-assessment. Its statements are heavily comparing the change of the understanding to the situation before the self-assessment.

Table 6. Current state of understanding of the processes, the second survey (N=12)



For the question ‘your company has had security incidents’ the responses were either neutral (three) or disagreed (fifteen). Then again, the question ‘your ICT environment is protected against threats’ one responded disagreed, five were neutral and twelve agreed. These are quite vague questions and therefore leave a great deal for the respondents to decide what the questions exactly mean. However, one could interpret these so that there are respondents who do not know if there have been security incidents or if the protection is in place. In the second survey, it was asked: ‘the protection of your ICT environment against threats has gained through the self-assessment’, and seven out of twelve responded agreed.

For the propositions related to self-assessments’ helpfulness to increase awareness to overview and development of the ICT and business environment, information security of the outsourced services and the current state of understanding of the digital business environment were all more positive than negative, which proves that the self-assessment tool designed in the Cyber Security Finland project will help the organizations in enhancing awareness of their enviroment.

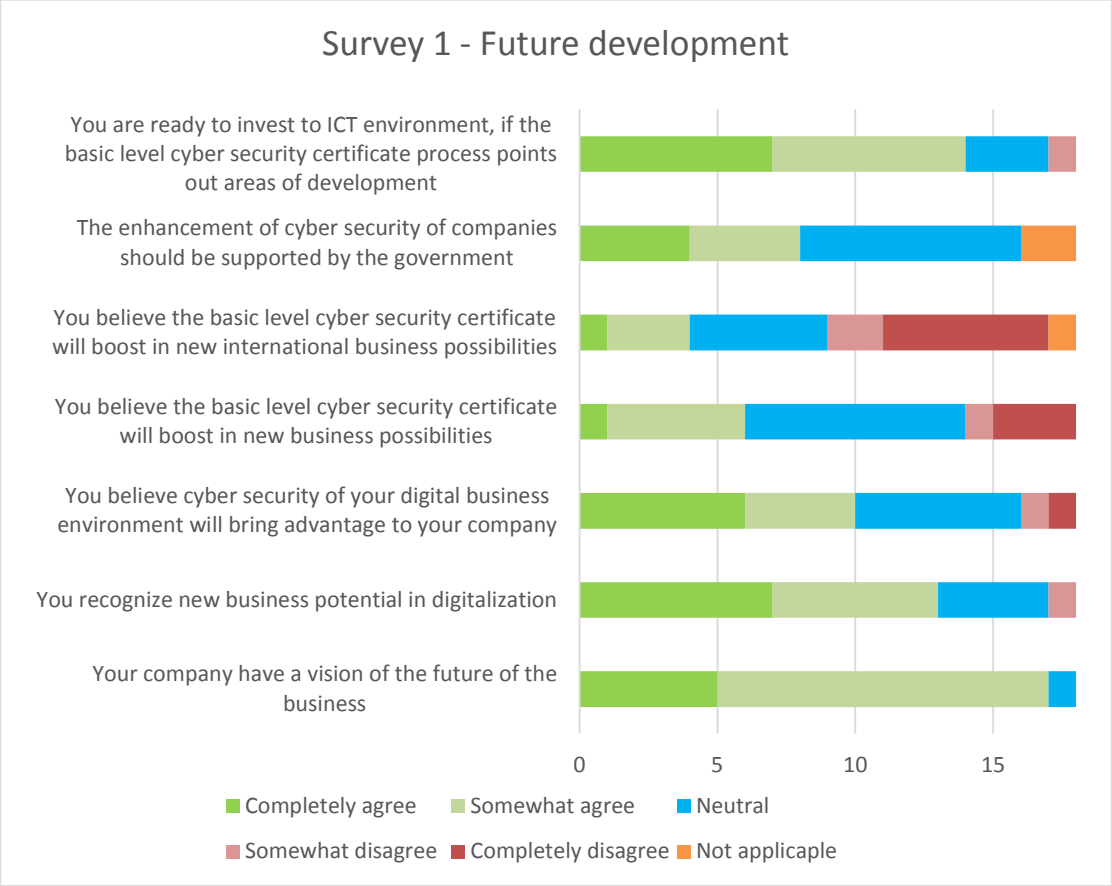
From cyber security perspective the survey shows that the self-assessment helps in increasing the overall understanding of it and additionally, issues concerned with it, meaning information security, physical security, threat management and awareness, risk management and training.

4.3 Research: future development

The future development part for the research is again divided into two parts, where the first survey focuses on the expectations and beliefs of the Cyber Security Finland projects self-assessment: how do the respondents think it will change their understanding and awareness, will it bring some business benefit and will it even help to change or adjust some services or processes?

The second part of the survey is mainly about measuring the reflections to these expectations and beliefs. Table 7. provides the responses of the first survey.

Table 7. Current state of future development (N=18)



The responses for the propositions of the first survey show that the majority of the respondents are ready to invest in their ICT environment if the self-assessment shows some development needs. At the same time, they state that digitalization provides new business potential for their company. On the other hand, quite many respondents do not see the importance of cyber security in business (six neutral, two disagreeing), which might be because of the industry they are operating in, or the level of understanding of the importance of cyber security. Nevertheless, cyber security is a crucial part for digital and information services.

Some of the respondents did not see any business potential for them by completing the self-assessment and getting the cyber security basic level certification. This question was just to point out what the expectations are for the Cyber Security Finland project and its certification.

The proposition 'enhancement of cyber security of companies should be supported by the government' is based on the process currently applied in the UK, where the

organizations applying for the basic level cyber security certification are awarded some amount money for it by the government. It is just good to know the basis in the list, however, it is still interesting to find out how the respondents seemed to hesitate in supporting this.

Table 8 illustrates the survey after the self-assessment.

Table 8. Current state of future development, the second survey (N=12)

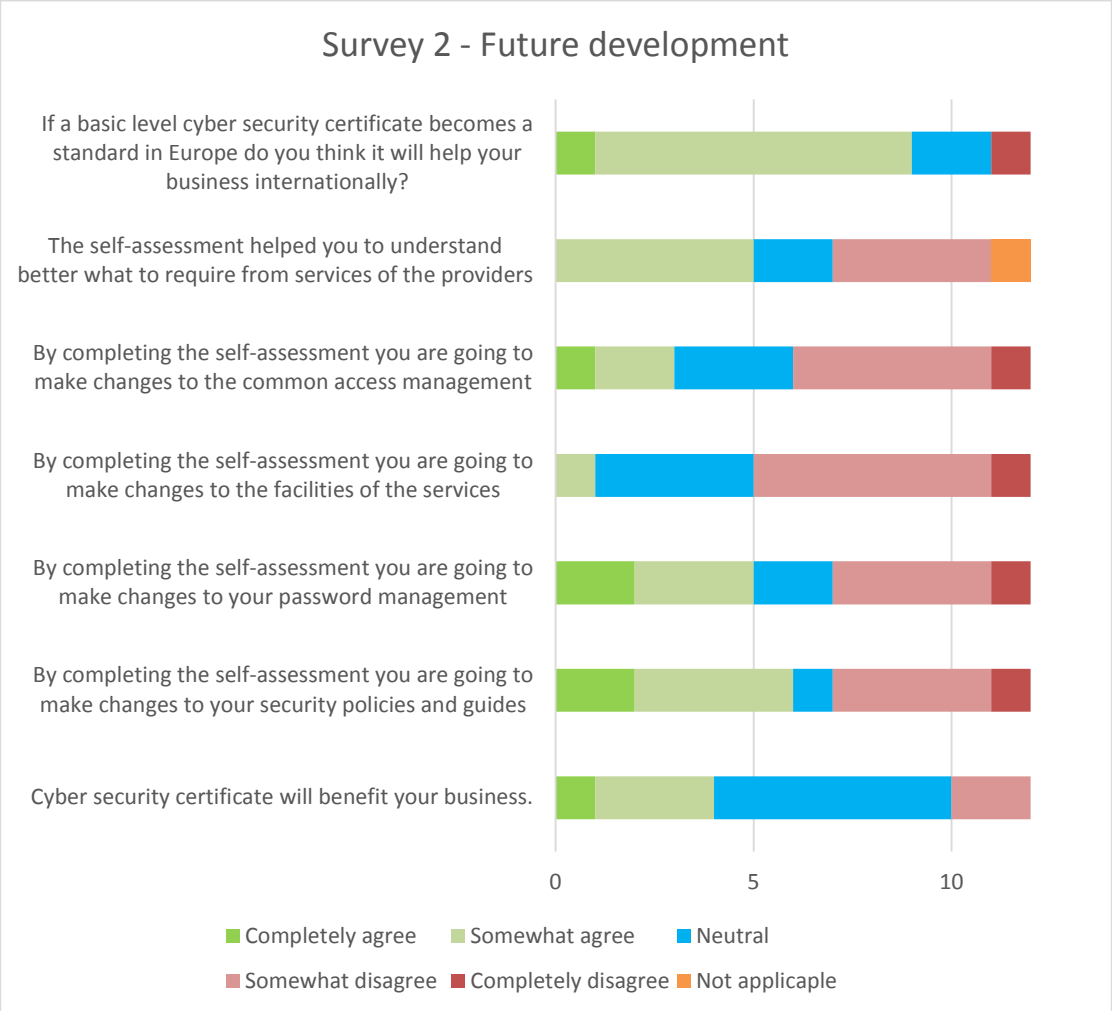


Table 8. shows that only some individuals are going to make changes to their service facilities and access management based on the self-assessment, and already that is a good change if they are enhancing the security. Regarding password management and policies and guides, more than one third of the organizations state they will make changes based on the self-assessment.

In addition, more than one third of the respondents state their understanding of requirements for the service providers has been increased through the process.

Three out of four respondents state that if the basic level cyber security certificate will become as a standard in Europe, it will help their business gaining internationally. At the same time, one third of the respondents state the certificate itself benefits their business.

4.4 Research: change from the points of view of processes

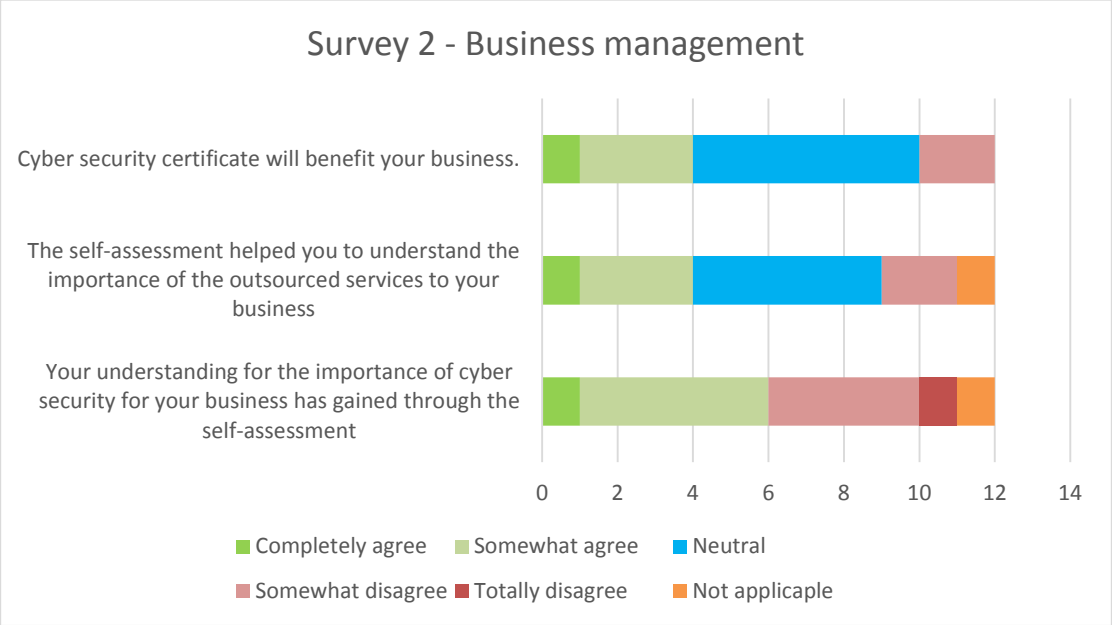
From the point of view of the processes, the research have been divided into five different processes:

- Business management
- Security management
- Risk management
- Service management
- Continuity management

The questions of the survey have been categorized regarding these processes so that one question can only be part of one category, even if it could belong to other gategories as well. This limitation is a part of scoping the research. In order to study the change of the situation from the perspective of the processes, it is necessary only to take a closer look at the results of the second survey.

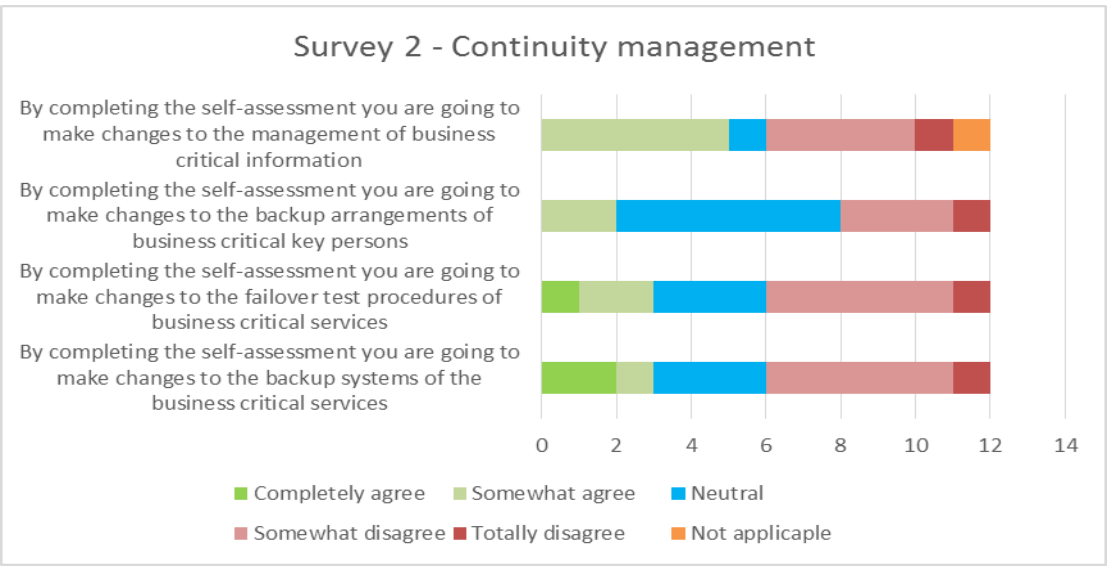
From the perspective of the business management processes, the change of the overall understanding of the importance of cyber security to the business after completing the self-assessment is positive, as shown in Table 9. Only one fourth of the respondents claim the self-assessment did not help them to understand the importance of the services they have outsourced. At the same time, 50% of the respondents state the self-assessment increased their awareness of importance of cyber security for their business.

Table 9. Business management point of view after the self-assessment (N=12)



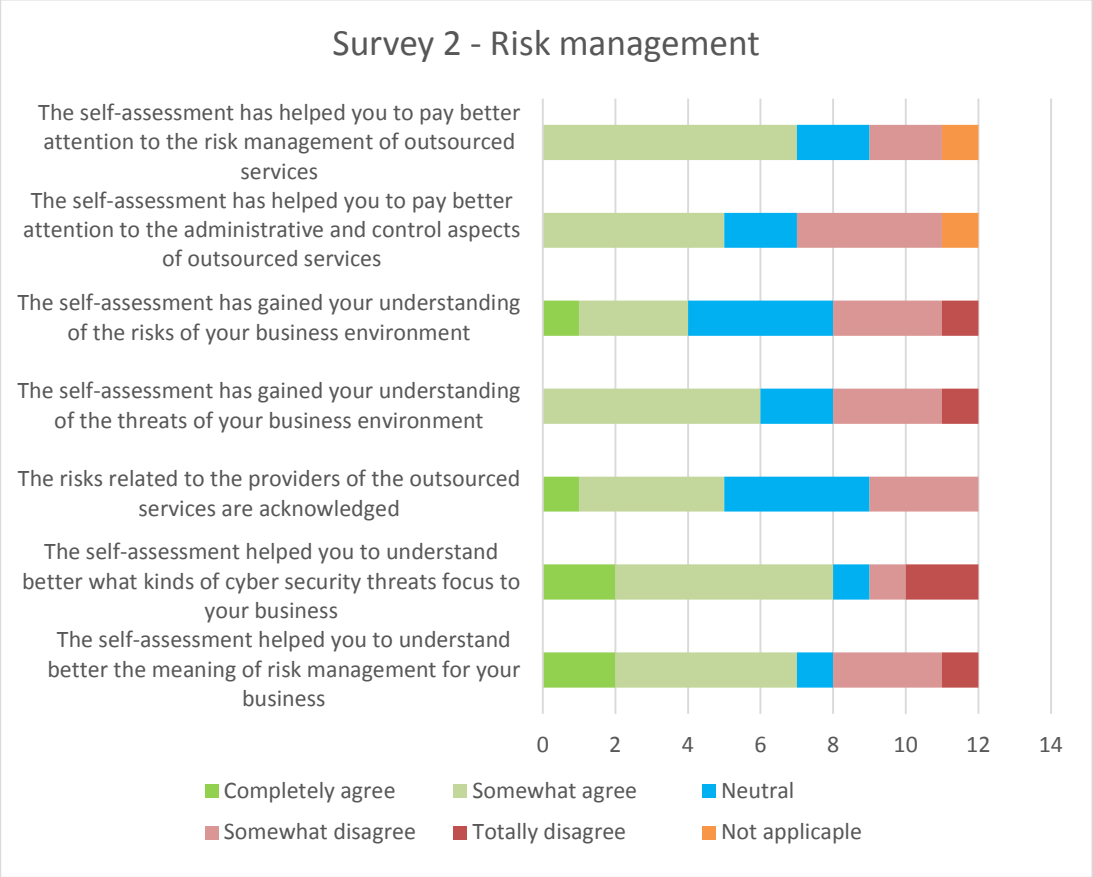
Continuity management is refers more to business continuity than to service continuity, even though in the questions on Table 10 the systems or services are often mentioned. The research unfortunately does not reveal if the respondents have considered these questions to refer only to business critical systems or services. However, according to the responds, approximately half of the respondents will not make changes to management environment, key personnel, failover tests or to backup systems that are treated as business critical, based on the self-assessment.

Table 10. Continuity management point of view after the self-assessment (N=12)



From risk management perspective, the self-assessment seemed to have a positive impact to increasing risk awareness of the business environment. Clearly, the understanding of the risks related to the outsourced services gained as well as the awareness.

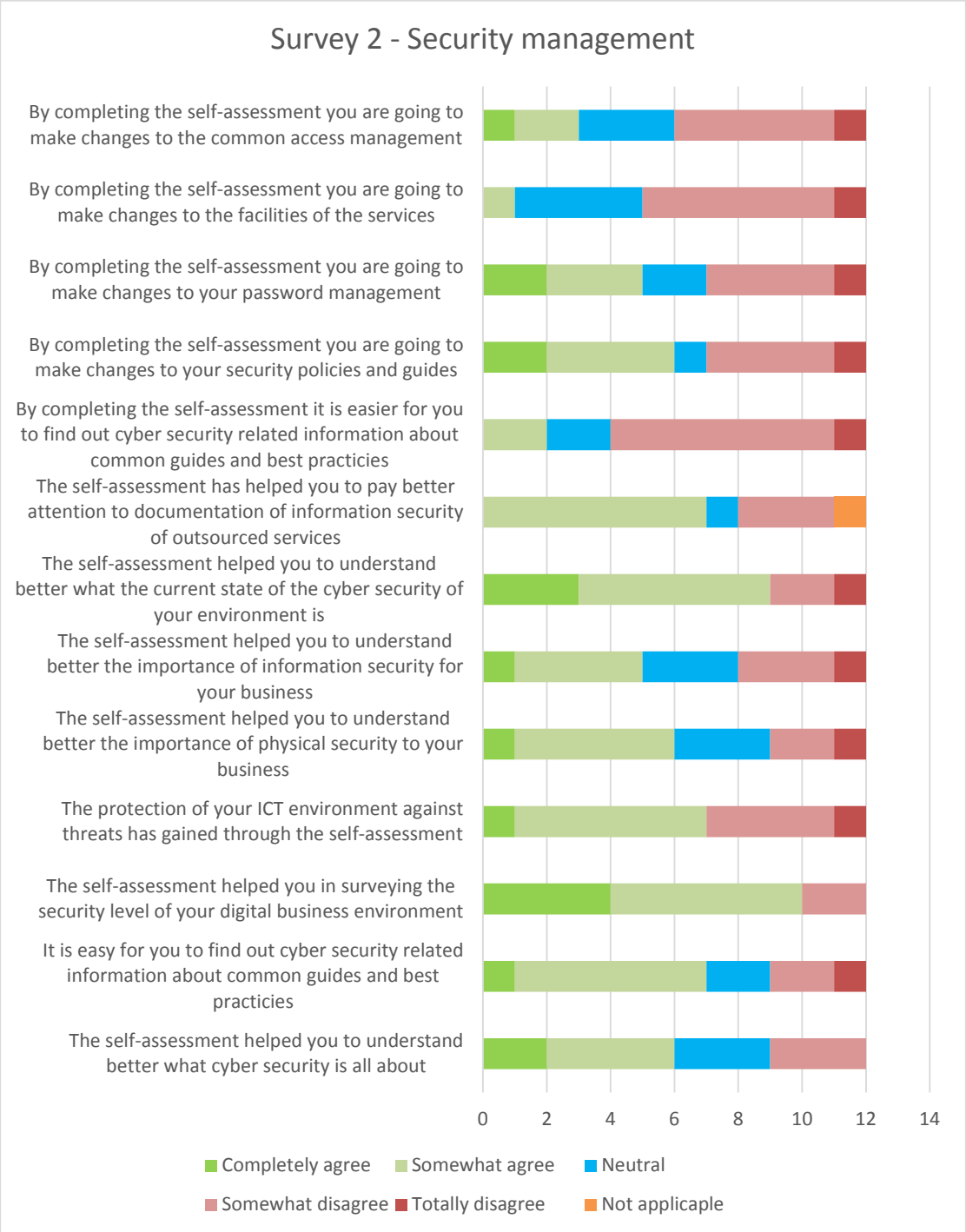
Table 11. Risk management point of view after the self-assessment (N=12)



From the security management point of view, the self-assessment was relatively successful in increasing the awareness of cyber security (Table 12.). According to the survey, the awareness of the current state of the security of the business ICT environment, including the outsourced services, improved nearly with every respondent.

From technical security point of view, the self-assessment did not impact to increase or change technical security controls or processes such as password management or facility management. Most likely these already are in good shape with the majority of the respondents.

Table 12. Security management point of view after the self-assessment (N=12)

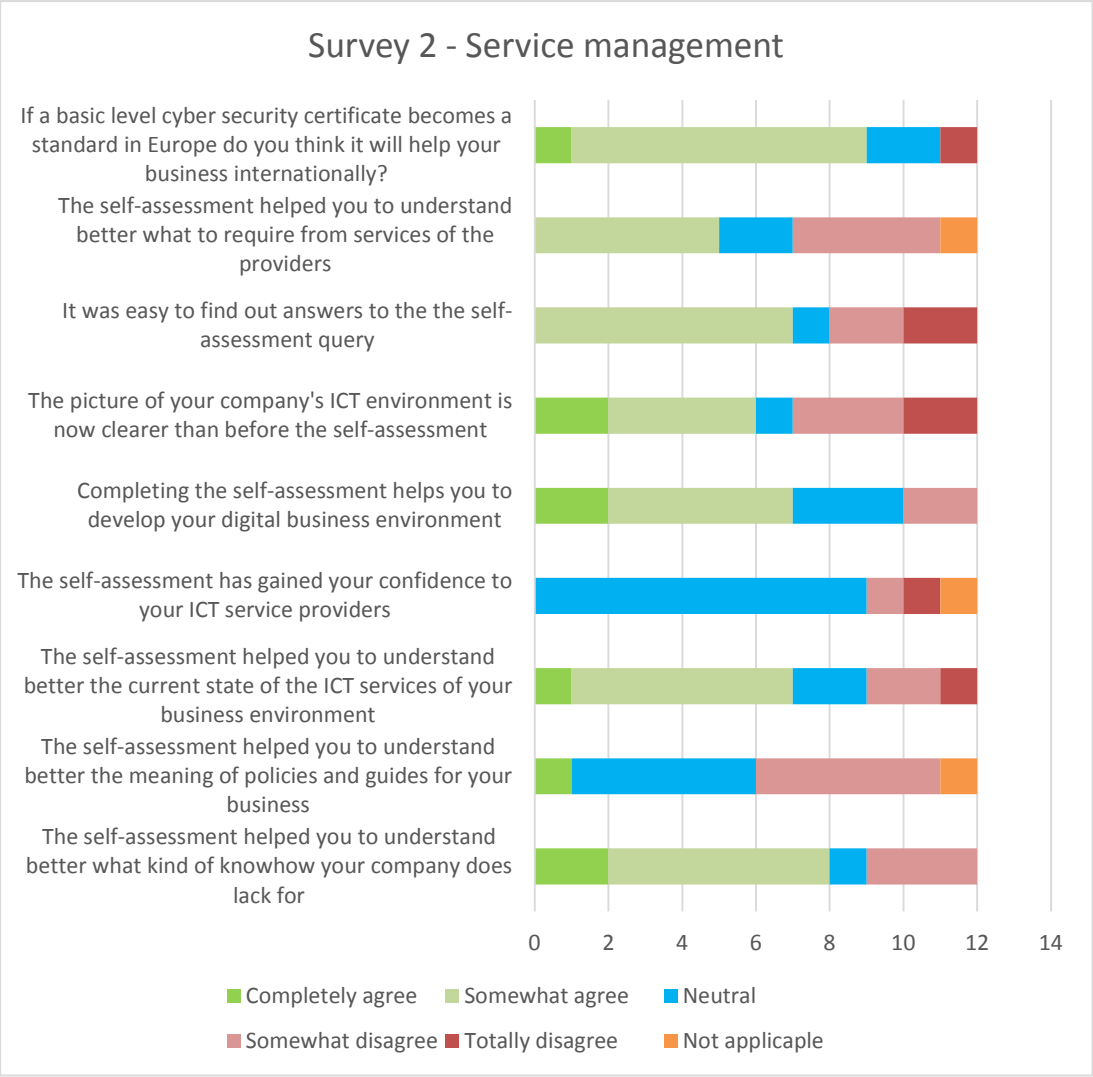


The impact of the self-assessment from the service management perspective looks more or less positive as well (Table 12.). Especially the understanding of the requirements or needs related to the ICT service providers seemed to enhance; though, at the same time the confidence with the incumbent ICT service providers

did not change to positive after self-assessment. It would be interesting to know what kinds of service providers (big or small, local or global) the respondents are utilizing since these might have an impact.

Otherwise, the survey shows that the overall understanding of the ICT services enhanced during the self-assessment. Worth mentioning is that the self-assessment for instance increased awareness of the needed experteese.

Table 13. Service management point of view after the self-assessment (N=12)



5 Conclusions and discussion

The self-assessment tool appears to be effective in increasing awareness and understanding cyber and cyber security. The phenomena of cyber and cyber security are at the same time ubiquitous and vague, but still have a big impact on current ways of working and future development, just like e.g. digitalization. This research provides the same findings as the studies committed in the UK, where the self-assessment process has been in production since 2014. There it has been studied that the self-assessment process really enhances the awareness of cyber security and protection against various kinds of threats (Such, Vidler, Seabrook, Rashid, 2015, 2) and (Tomlin M., 2015, 46-49).

In the future, cyber security as a term will need to be clarified, where most likely military industry has a significant role. When cyber will get a somewhat concrete and internationally accepted definition, the international legislation most likely will become more definitive, which again supports national players and even SME segment organizations. International legislation will also provide the support for cyber security standards that set the frameworks for good practicies in cyber domain. As long as the terms and definitions are vague, area specific directives and regulations like EU generated GDPR will raise the awareness of importance of security in ICT and enhance the security controls in organizations.

The number of items in cyber space will grow rapidly in the near future. This will also widen the playground for technologies and technical experts in cyber space meaning even more and more are people are dependent, one way or another, on cyber space. At the same time, the amount of threat vectors increases with the same cadence. The awareness of dependency to cyber space and its threats will have to grow within individuals, business organizations in all sizes and states. In order for the growth of awareness to take place smoothly and systematically, international norms and regulations have to develop into a more firm and constant format. This will most likely begin in the military field, next, turning into international consensus of norms of cyber space and then finally, into international standards. The standards then tend to guide global organizations but increasingly SME organizations as well.

Self-assessment tools provide an efficient way for any organization to increase awareness of what they have to consider to be able to maintain continuity of business. When assessment questions are considered properly, they take into account people, processes and technology. For organizations, this mean awareness of existing or needed policies and guides, technical controls and guidance, and follow-up.

The main goal of this research was to study the usefulness of one kind of self-assessment tool in increasing cyber security awareness of SME organization. At the same time, the intention was to find out whether the SME organizations are able to see any advantage to their business from enhanced cyber security. From the results perspective a surprisingly big amount of organizations states their environment to be organized and well prepared to ensure continuity of business.

To question the results of this study, two issues need to be raised at this point. Since the cybercrime is a hidden crime by its nature, the cyber security breaches will not nearly always get reported and published. For this to happen, it would require the organizations suffering from the breaches to tell openly about them. Why does this not happen too often? Maybe because of negative publicity, for the sake of their customers, or because they feel they have failed in their business. These are just guesses, however, this is how individuals tend to think at the moment, even though it would be beneficial for everyone if all of the security breaches, incidents or common vulnerabilities were to be openly published. However, the becoming General Data Protection Regulation in the EU area will raise the obligations for organizations in reporting information security breaches and breaches related to privacy. This will most likely raise the awareness for the security breaches in the whole EU area.

Another issue needed to raise to question the results of this study is the small sampling amount of organizations. The first phase consisted of 18 organizations and the second of only 12 organizations, although, the small amount of sampling was acknowledged before the study, it still raises the question if there is enough evidence to generalize the outcomes. Related to the other studies done in Finland or in the UK, the outcomes are equal. In that sense, this research was successful.

If I had a chance to conduct this research again to the same sample group, I would do two things differently. First, I would pay much more attention to grouping the assessment questions, for both parts one and two, under specific themes to explore the phenomena from as many angles as possible. During this research, I ended up creating just two lists of questions without thinking beforehand about the categories of the questions. The categories were created while the answers were studied.

Second, I would not use a faceless survey such as Webropol. Instead, I would prefer 'face to face' method. This because with a faceless survey I do not know how long it took to answer all questions, were they even considered enough, or was it just another survey that they wanted to be quickly over. With the 'face to face' method there would most likely be more discussion regarding the questions, what is behind them, and what they relate to. The 'Face to face' method would provide less impulsive answers, although, the 'face to face' method could also affect the reliability of the answers if the respondent thought more about feelings instead of just answering to the questions realistically.

Relating to this study, the awareness of cyber space dependency and security within SME organizations could be better. The becoming statements are referring to Appendices 1 and 2.

According to this study, the awareness and preparedness for business continuity of an organization depends a great deal on the part of business organization that these questions are asked . IT staff and CIOs have a good visibility to technical controls and instructions whereas the CEO level and business representatives have a better view on plans of the future business and risk management. Nevertheless, these cannot be generalized as such since such a small group of companies participated in the surveys in this study, and the variation between their sizes was quite big.

What can be emphasized about this study is that by completing a simple self-assessment, an organization will enhance their awareness of the security on the digital business environment. 83% of the pilot organizations state that this was helpful. At the same time, 67% of the pilot organizations claim to increase knowledge of the different kinds of threats towards their business.

From future business perspective, 75% of pilot organizations saw the business potential of a basic level cyber security certificate if the model of the certificate would be standardized, for instance within European countries. Based on this, the SME organizations see cyber security to bring advantage to their business. This is interesting, as in the first phase of the survey, the pilot organizations did not see that much business potential for them in cyber security. Only 33% of the organizations considered basic level cyber security certificate as an asset for them. And, when asked about international business potential in the first phase, the figure was only 22%. However, the sample of the organizations within the pilot and this study is rather narrow, therefore, the results should not be generalized. Nevertheless, the understanding of the business benefit from investing to understanding of cyber security of business ICT services would be another interesting topic to be studied.

From common cyber security awareness, acknowledgement and information sharing perspective, less than a half of the responders says it is easy for them to retrieve generic guides and good practices for cyber security. It would be an interesting topic to study how the information sharing could be enhanced.

This study would have been more informative if the amount of sample organizations had been larger. Though, already with this amount of companies, a variation between the knowledge and awareness can be pointed out. If the basic level cyber security certificate were to be adopted rapidly and largely to SME segment organizations, the same kind of study with the twist to survey their preparedness for the future would be interesting.

Another aspect for the future researches of self-assessment tools and certificates such as FINCSC is their effectiveness in partner and sub-contractor management. Especially the organizations within the SME segment operate to a great extent with other organizations. They are subcontractors for the larger organizations and they have partners. How are these interfaces managed and operated from security perspective? Do they follow some common guidance or is each interface defined separately?

The fact is that even the large and from security perspective, mature organizations such as NATO increases its power by collaborating with others, especially the small ones. For sure NATO has defined the rules and processes for the interface to be highly secured, however, it indicates anyway they need others in order to success in their targets. In digitalizing the business environment, the field of subcontractors and partners increases a great deal, and there most likely will be different kinds of eco-systems where help, support and collaboration are ordered whenever needed. The processes will be quick and co-operating parties will come and go. How will the cyber security be managed in these ecosystems sufficiently without jeopardizing its members' business assets and important data? Will there be a framework for cyber security management which would fit for everyone but which would not require too much money or other resources to fulfill? Most likely in future we will see frameworks like FINCSC or Cyber Essentials appear elsewhere as well.

References

10 Steps: Summary. 2014. Department for Business, Innovation and Skills. Accessed Feb 14th 2017. Retrieved from https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility/10-steps-summary

2015 UN GGE Report: Major Players Recommending Norms of Behaviour, Highlighting Aspects of International Law. 2015. NATO Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia. Accessed 20th Sep 2016. Retrieved from https://ccdcoe.org/2015-un-gge-report-major-players-recommending-norms-behaviour-highlighting-aspects-international-l-0.html

Aho, Jouni, Nevala, Jarmo. 2016. *Keskisuomalaisten yritysten kyberturvallisuus.* Jyväskylä. Oct 2016. Principal Regional Council of Central Finland and Jyväskylän koulutuskuntayhtymä. Accessed 20th Dec 2016. Retrieved from http://edu360.fi/wp-content/uploads/2016/08/Yrityspuolen_kybertutkimus-FINAL-20160829.pdf

Anttila, Pirkko. 2014. *Tutkimisen taito ja tiedon hankinta*. Accessed 28th Feb 2017. Retrieved from https://metodix.fi/2014/05/17/anttila-pirkko-tutkimisen-taito-ja-tiedon-hankinta/

Cyber Essentials Scheme. 2016. The IASME Consortium Ltd. Accessed Aug 2016. Retrieved from https://www.iasme.co.uk/cyber-essentials-scheme/

Cyber Essentials Scheme. 2014. Department for Business, Innovation and Skills. Accessed Feb 2017. Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/317480/Cyber_Essentials_Summary.pdf

Cyber Scheme Finland - pilot. 2015. Accessed Aug 2016. Jyväskylä: Jyväskylän Ammattikorkeakoulu / JYVSECTEC

Enterprises 2015, 2016. Statistics Finland. Accessed Sep 2016. Retrieved from http://tilastokeskus.fi/tup/suoluk/suoluk_yritykset.html

FICORA's Cyber Security Review 1/2014. 2014. Accessed 18th Jul 2016. Retrieved from https://www.viestintavirasto.fi/attachments/cert/tietoturvakatsaukset/Cyber_review_Q1_2014_EN.pdf

General Assembly, United Nations. 2015. *Developments in the field of information and telecommunications in the context of international security*. Jan 2015. Accessed Sep 17th 2016. Retrieved from https://ccdcoe.org/sites/default/files/documents/UN-150113-CodeOfConduct.pdf

Hirsjärvi S., Remes P. & Sajavaara P. 2010. *Tutki ja kirjoita.* Helsinki: Tammi.

J.M. Such, J. Vidler, T. Seabrook, A. Rashid, *Cyber Security Controls Effectiveness: A Qualitative Assessment of Cyber Essentials.* Technical Report SCC-2015-02, Security Lancaster, Lancaster University, 2015. Retrieved from http://eprints.lancs.ac.uk/74598/4/SCC_2015_02_CS_Controls_Effectiveness.pdf

Ministry of Defence, Finland. 2015. *Katakri 2015 – Tietoturvallisuuden auditointityökalu viranomaisille*. Accessed Sep 12th 2016. Retrieved from http://www.defmin.fi/puolustushallinto/puolustushallinnon_turvallisuustoiminta/katakri_2015_-_tietoturvallisuuden_auditointityokalu_viranomaisille

Ministry of Finance, Finland 2015. *VAHTI* . Accessed Sep 12th 2016. Retrieved from http://vm.fi/dms-portlet/document/0/432775

Kauppinen, Tatu, Kivikoski, Jouni. 2016. *Tutkimus suomalasten PK-yritysten digitaalisuudesta ja tietoturvasta.* Helsinki. Sep 2016. Principal Elisa Oyj and Yrittäjäsanomat. Accessed 24th Sep 2016. Retrieved from http://hub.elisa.fi/download/9327/

Participating States. 2017. Organizations for Security and Co-operation in Europe. Accessed Mar 2017. Retrieved from http://www.osce.org/states

Pawlak, Patryk. 2014. *Riding the digital wave. The impact of cyber capacity building on human development.* Dec 2014. EU Institute for Security Studies, 2014. Published by the EU Institute for Security Studies and printed in Condé-sur-Noireau (France) by Corlet Imprimeur. Retrieved from http://www.iss.europa.eu/uploads/media/Report_21_Cyber.pdf

Saaranen-Kauppanen A., Puusniekka A., Kuula A., Rissanen R. & Karvinen I.. 2009. *Menetelmäopetuksen tietovaranto KvaliMOTV*. Yhteiskuntatieteellinen tietoarkisto, Tampereen Yliopisto. Accessed 28th Feb 2017. Retrieved from http://www.fsd.uta.fi/fi/julkaisut/motv_pdf/KvaliMOTV.pdf

Schmitt, Michael N., 2013, *26 TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE.* Cambridge University Press. Accessed 30th Jan 2017. Retrieved from https://www.peacepalacelibrary.nl/ebooks/files/356296245.pdf

Security Standards Council. 2016. Payment Card Industry (PCI) Data Security Standard, v3.2. *Requirements and Security Assessment Procedures.* Accessed Sep 20th 2016.

SFS-ISO/IEC 27001:2013. *Information technology — Security techniques — Information security management systems — Requirements*. 2017. Accessed Aug 20th 2016. Retrieved from http://www.iso27001security.com/html/27001.html

SFS-ISO/IEC 27002:2013. *Information technology — Security techniques — Code of practice for information security controls.* Accessed Sep 12th 2016. Retrieved from http://www.iso27001security.com/html/27002.html

SFS-ISO/IEC 27032:2012. *Information technology — Security techniques — Guidelines for cybersecurity.* Accessed Sep 12th 2016. Retrieved from http://www.iso27001security.com/html/27032.html

SFS-ISO 31000:2009. *Risk management – Principles and guidelines*. 2009. Accessed Sep 12th 2016. Retrieved from https://www.iso.org/iso-31000-risk-management.html

SME Performance Review. 2016. European Commission. Accessed Feb 2017. Retrieved from http://ec.europa.eu/growth/smes/business-friendly-environment/performance-review-2016_en

Sonera tietoturvatutkimus. 2016. Lean Service Creation - tietoturva, TeliaSonera Finland Oyj. Accessed 7th Nov 2016.

Standard Industrial Classification TOL 2008, 2016. Statistics Finland. Accessed 7th Feb 2017. Retrieved from http://www.stat.fi/meta/luokitukset/toimiala/001-2008/index_en.html

Suihkonen, Rai. 2016. *Tuhoa rakkauskirjeet, äläkä usko joka soittajaa.* Keskisuomalainen Oyj. Accessed 3rd Jun 2016. Retrieved from http://www.ksml.fi/arkisto/?tem=archivechart&id=1811342

Tomlin M, (supervisor: C. Ciechanowicz), *Advancing Small Business Cyber Maturity: An application of the NIST Cybersecurity Framework*. Master's thesis, Royal Holloway, University of London, 2015. Retrieved from https://www.linkedin.com/in/marktomlin

Tuomivaara, Timo. 2005. *Y125 Tieteellisen tutkimuksen perusteet*. Accessed 7th Jan 2017. Retrieved from http://www.mv.helsinki.fi/home/ttuomiva/Y125luku6.pdf

von Heinegg, Wolff Heintschel, 2013. *Territorial Sovereignty and Neutrality in Cyberspace*. U.S. Naval War College. Accessed Jan 30th 2017. Retrieved from https://www.usnwc.edu/getattachment/ff9537ce-94d6-49a8-a9ef-51e335126c1e/von-Heinegg.aspx sivu 135

What is an SME? 2016. European Commission. Accessed 14th Feb 2017. Retrieved from http://ec.europa.eu/growth/smes/business-friendly-environment/sme-definition_en

Warsaw Summit Communiqué. 2016. North Atlantic Treaty Organization. Accessed 30th Sep 2016. Retrieved from http://www.nato.int/cps/en/natohq/official_texts_133169.htm

Yekaterinburg Declaration of the Heads of the Member States of the Shanghai Cooperation Organisation. 2009. Accessed Nov 14th 2016. Retrieved from http://en.kremlin.ru/supplement/66

Appendices

Appendix 1.The first survey

Tutkimus liittyen kyberturvallisuuden perustason sertifikaatin pilotti-hankkeeseen.

1. Yhteystietonne *

Etunimi _____

Sukunimi _____

Sähköposti _____

Yritys / Organisaatio _____

Titteli / Toimenkuva _____

2. Digitaalisuus tuo liiketoiminnallenne lisäarvoa. *

◯ 0 - En osaa sanoa

◯ 1 - Ei ollenkaan

◯ 2 - Vähän

◯ 3 - Jossakin määrin

◯ 4 - Melko paljon

◯ 5 - Hyvin paljon

3. Yrityksenne ICT-ympäristön kokonaiskuva on selkeä. *

◯ 0 - En osaa sanoa

◯ 1 - Ei ollenkaan

◯ 2 - Vähän

◯ 3 - Jossakin määrin

◯ 4 - Melko hyvin

◯ 5 - Erinomaisesti

4. ICT-ympäristönne on suojattu uhkia vastaan. *

◯ 0 - En osaa sanoa

◯ 1 - Ei ollenkaan

◯ 2 - Vähän

◯ 3 - Jossakin määrin

◯ 4 - Melko hyvin

◯ 5 - Erinomaisesti

5. Yrityksenne johto seuraa digitaalisen liiketoimintaympäristönne toimintaa. *

◯ 0 - En osaa sanoa

◯ 1 - Ei ollenkaan

◯ 2 - Vähän

◯ 3 - Jossakin määrin

◯ 4 - Melko hyvin

◯ 5 - Erinomaisesti

6. Yrityksenne johto seuraa digitaalisen liiketoimintaympäristönne kehitystä. *

◯ 0 - En osaa sanoa

◯ 1 - Ei ollenkaan

◯ 2 - Vähän

◯ 3 - Jossakin määrin

◯ 4 - Melko hyvin

◯ 5 - Erinomaisesti

7. Digitaalisen liiketoimintaympäristönne riskit, uhkat ja kehityskohteet ovat tiedostettu. *

◯ 0 - En osaa sanoa

◯ 1 - Ei ollenkaan

◯ 2 - Vähän

◯ 3 - Jossakin määrin

◯ 4 - Melko hyvin

◯ 5 - Erinomaisesti

8. Digitaalisen liiketoimintaympäristönne riskit, uhkat ja kehityskohteet ovat hallittu. *

◯ 0 - En osaa sanoa

◯ 1 - Ei ollenkaan

◯ 2 - Vähän

◯ 3 - Jossakin määrin

◯ 4 - Melko hyvin

◯ 5 - Erinomaisesti

9. Yrityksellänne on visio liiketoimintanne tulevaisuudesta. *

◯ 0 - En osaa sanoa

◯ 1 - Ei ollenkaan

◯ 2 - Vähän

◯ 3 - Jossakin määrin

◯ 4 - Melko hyvin

◯ 5 - Erinomaisesti

10. Tunnistatte uusia liiketoimintamahdollisuuksia digitalisoituvassa maailmassa. *

◯ 0 - En osaa sanoa

◯ 1 - Ei ollenkaan

◯ 2 - Vähän

◯ 3 - Jossakin määrin

◯ 4 - Melko hyvin

◯ 5 - Erinomaisesti

11. Koette digitaalisen liiketoimintaympäristön kyberturvallisuuden tuovan liiketoimintaetua yrityksellenne. *

◯ 0 - En osaa sanoa

◯ 1 - Ei ollenkaan

◯ 2 - Vähän

◯ 3 - Jossakin määrin

◯ 4 - Melko hyvin

◯ 5 - Erinomaisesti

12. Yrityksellänne on korkean turvallisuustason vaativia (kuten turva- tai rahaliikenteen aloilla toimivia) asiakkaita tai kumppaneita. *

◯ 0 - En osaa sanoa

◯ 1 - Ei ollenkaan

◯ 2 - Vähän

◯ 3 - Jossakin määrin

◯ 4 - Melko hyvin

◯ 5 - Erinomaisesti

13. Yrityksenne henkilökunnalla on hyvä ICT-osaamisen taso. *

◯ 0 - En osaa sanoa

◯ 1 - Ei ollenkaan

◯ 2 - Vähän

◯ 3 - Jossakin määrin

◯ 4 - Melko hyvin

◯ 5 - Erinomaisesti

14. Yrityksellänne on riittävästi henkilöstöä yrityksenne tietojärjestelmien ja palveluiden ylläpitoon ja kehitykseen. *

◯ 0 - En osaa sanoa

◯ 1 - Ei ollenkaan

◯ 2 - Vähän

◯ 3 - Jossakin määrin

◯ 4 - Melko hyvin

◯ 5 - Erinomaisesti

15. Yrityksenne käyttämät ICT-palvelut / laitteet / sovellukset ovat tunnistettu ja listattu. *

◯ 0 - En osaa sanoa

◯ 1 - Ei ollenkaan

◯ 2 - Vähän

◯ 3 - Jossakin määrin

◯ 4 - Melko hyvin

◯ 5 - Erinomaisesti

16. Yrityksenne liiketoiminnan kannalta **kriittiset** tietojärjestelmät, palvelut ja sovellukset ovat **tiedossa**. *

◯ 0 - En osaa sanoa

◯ 1 - Ei ollenkaan

◯ 2 - Vähän

◯ 3 - Jossakin määrin

◯ 4 - Melko hyvin

◯ 5 - Erinomaisesti

17. Yrityksenne liiketoiminnan kannalta **kriittisiä** tietojärjestelmiä, palveluita ja sovelluksia **seurataan ja valvotaan**. *

◯ 0 - En osaa sanoa

◯ 1 - Ei ollenkaan

◯ 2 - Vähän

◯ 3 - Jossakin määrin

◯ 4 - Melko hyvin

◯ 5 - Erinomaisesti

18. Yrityksenne liiketoiminnan kannalta **kriittisten** tietojärjestelmien, palveluiden ja sovellusten häiriönsietoisuus on **selvitetty ja tiedossa**. *

◯ 0 - En osaa sanoa

◯ 1 - Ei ollenkaan

◯ 2 - Vähän

◯ 3 - Jossakin määrin

◯ 4 - Melko hyvin

◯ 5 - Erinomaisesti

19. Yrityksenne liiketoiminnan kannalta **kriittisten** tietojärjestelmien, palveluiden ja sovellusten häiriönsietoisuus on **testattu**. *

◯ 0 - En osaa sanoa

◯ 1 - Ei ollenkaan

◯ 2 - Vähän

◯ 3 - Jossakin määrin

◯ 4 - Melko hyvin

◯ 5 - Erinomaisesti

20. Yrityksenne liiketoiminnan kannalta **kriittisten** tietojärjestelmien, palveluiden ja sovellusten **varajärjestelyt on hoidettu**. *

◯ 0 - En osaa sanoa

◯ 1 - Ei ollenkaan

◯ 2 - Vähän

◯ 3 - Jossakin määrin

◯ 4 - Melko hyvin

◯ 5 - Erinomaisesti

21. Yrityksenne liiketoiminnan kannalta **kriittisiä** palveluita on ulkoistettu *

◯ 0 - En osaa sanoa

◯ 1 - Ei ollenkaan

◯ 2 - Vähän

◯ 3 - Jossakin määrin

◯ 4 - Melko hyvin

◯ 5 - Erinomaisesti

22. Ulkoistettujen ICT-palveluiden toimittajiin liittyvät riskit on huomioitu. *

◯ 0 - En osaa sanoa

◯ 1 - Ei ollenkaan

◯ 2 - Vähän

◯ 3 - Jossakin määrin

◯ 4 - Melko hyvin

◯ 5 - Erinomaisesti

23. Yrityksenne liiketoiminnan kannalta kriittisten palveluiden laatupoikkeamia seurataan säännöllisesti. *

◯ 0 - En osaa sanoa

◯ 1 - Ei ollenkaan

◯ 2 - Vähän

◯ 3 - Jossakin määrin

◯ 4 - Melko hyvin

◯ 5 - Erinomaisesti

24. Yrityksellänne on ollut tietoturvaongelmia. *

◯ 0 - En osaa sanoa

◯ 1 - Ei ollenkaan

◯ 2 - Vähän

◯ 3 - Jossakin määrin

◯ 4 - Melko paljon

◯ 5 - Paljon

25. Yrityksessänne on määritelty tietoturvapolitiikka. *

◯ 0 - En osaa sanoa

◯ 1 - Ei ollenkaan

◯ 2 - Vähän

◯ 3 - Jossakin määrin

◯ 4 - Melko hyvin

◯ 5 - Erinomaisesti

26. Yrityksessänne on tunnistettu digitaaliseen aineistoon kohdistuvat lait ja vaatimukset esim. yksityisyydensuojan ja henkilötietojen osalta. *

◯ 0 - En osaa sanoa

◯ 1 - Ei ollenkaan

◯ 2 - Vähän

◯ 3 - Jossakin määrin

◯ 4 - Melko hyvin

◯ 5 - Erinomaisesti

27. Yrityksellenne on tärkeää, että tietojärjestelmiinne tallennettu tieto on aina ja helposti saatavilla. *

◯ 0 - En osaa sanoa

◯ 1 - Ei ollenkaan

◯ 2 - Vähän

◯ 3 - Jossakin määrin

◯ 4 - Melko hyvin

◯ 5 - Erinomaisesti

28. Yrityksessänne on varmistettu, että tietojärjestelmiinne tallennettu tieto on luotettavaa. *

◯ 0 - En osaa sanoa

◯ 1 - Ei ollenkaan

◯ 2 - Vähän

◯ 3 - Jossakin määrin

◯ 4 - Melko hyvin

◯ 5 - Erinomaisesti

29. Yrityksessänne on varmistettu, että tietojärjestelmiinne tallennettua tietoa ei muuteta hallitsemattomasti. *

◯ 0 - En osaa sanoa

◯ 1 - Ei ollenkaan

◯ 2 - Vähän

◯ 3 - Jossakin määrin

◯ 4 - Melko hyvin

◯ 5 - Erinomaisesti

30. Yrityksenne avainhenkilöiden varajärjestelyt on määritelty. *

◯ 0 - En osaa sanoa

◯ 1 - Ei ollenkaan

◯ 2 - Vähän

◯ 3 - Jossakin määrin

◯ 4 - Melko hyvin

◯ 5 - Erinomaisesti

31. Odotatte kyberturvallisuuden perustason sertifioinnin auttavan teitä digitaalisen liiketoimintaympäristönne turvallisuuden kartoittamisessa. *

◯ 0 - En osaa sanoa

◯ 1 - Ei ollenkaan

◯ 2 - Vähän

◯ 3 - Jossakin määrin

◯ 4 - Melko hyvin

◯ 5 - Erinomaisesti

32. Uskotte kyberturvallisuuden perustason sertifioinnin edistävän uusien liiketoimintamahdollisuuksien syntymistä. *

◯ 0 - En osaa sanoa

◯ 1 - Ei ollenkaan

◯ 2 - Vähän

◯ 3 - Jossakin määrin

◯ 4 - Melko hyvin

◯ 5 - Erinomaisesti

33. Uskotte kyberturvallisuuden perustason sertifioinnin edistävän kansainvälisten liiketoimintamahdollisuuksien syntymistä. *

◯ 0 - En osaa sanoa

◯ 1 - Ei ollenkaan

◯ 2 - Vähän

◯ 3 - Jossakin määrin

◯ 4 - Melko hyvin

◯ 5 - Erinomaisesti

34. Mikä maa tai alue olisi ensimmäisenä?

_____

_____

_____

35. Teidän on helppoa saada tietoa yleisistä kyberturvallisuuteen liittyvistä ohjeita ja hyvistä käytänteistä. *

◯ 0 - En osaa sanoa

◯ 1 - Ei ollenkaan

◯ 2 - Vähän

◯ 3 - Jossakin määrin

◯ 4 - Melko hyvin

◯ 5 - Erinomaisesti

36. Olette valmiit investoimaan ICT-ympäristöön, jos kyberturvallisuuden perustason sertifioinnin myötä paljastuu kehityskohteita. *

◯ 0 - En osaa sanoa

◯ 1 - Ei ollenkaan

◯ 2 - Vähän

◯ 3 - Jossakin määrin

◯ 4 - Melko hyvin

◯ 5 - Erinomaisesti

37. Valtion tulisi tukea yritysten kyberturvallisuuden tason parantamista Suomessa. *

◯ 0 - En osaa sanoa

◯ 1 - Ei ollenkaan

◯ 2 - Vähän

◯ 3 - Jossakin määrin

◯ 4 - Melko hyvin

◯ 5 - Erinomaisesti

Appendix 2.The second survey

Finnish Cyber Security Certificate (FINCSC) - pilottihankkeen tutkimus, vaihe 2.

1. Vastaajan tiedot *

Etunimi _____

Sukunimi _____

Sähköposti _____

Yritys / Organisaatio _____

Titteli / Toimenkuva _____

2. Kyberturvallisuuden perustason sertifiointi (FINCSC) auttoi ymmärtämään mistä kyberturvassa on kyse. *

◯ 0 - En osaa sanoa

◯ 1 - Ei ollenkaan

◯ 2 - Vähän

◯ 3 - Ei ole muuttunut

◯ 4 - Melko paljon

◯ 5 - Erittäin paljon

3. FINCSC auttoi teitä digitaalisen **liiketoimintaympäristönne turvallisuuden kartoittamisessa**. *

◯ 0 - En osaa sanoa

◯ 1 - Ei ollenkaan

◯ 2 - Vähän

◯ 3 - Ei ole muuttunut

◯ 4 - Melko paljon

◯ 5 - Erittäin paljon

4. FINCSC:n myötä ymmärrätte **paremmin riskienhallinnan** merkityksen liiketoiminnassanne. *

◯ 0 - En osaa sanoa

◯ 1 - Ei ollenkaan

◯ 2 - Vähän

◯ 3 - Ei ole muuttunut

◯ 4 - Melko paljon

◯ 5 - Erittäin paljon

5. Uskotte FINCSC:n tuovan yrityksellenne liiketoimintaetua tulevaisuudessa. *

◯ 0 - En osaa sanoa

◯ 1 - Ei ollenkaan

◯ 2 - Vähän

◯ 3 - Ei ole muuttunut

◯ 4 - Melko paljon

◯ 5 - Erittäin paljon

6. FINCSC:n myötä tiedostatte **paremmin**, mitä eri **kyberturvauhkia** liiketoimintaanne kohdistuu. *

◯ 0 - En osaa sanoa

◯ 1 - Ei ollenkaan

◯ 2 - Vähän

◯ 3 - Ei ole muuttunut

◯ 4 - Melko paljon

◯ 5 - Erittäin paljon

7. FINCSC:n myötä ymmärryksenne **kyberturvan merkityksestä liiketoiminnalle** on kasvanut. *

◯ 0 - En osaa sanoa

◯ 1 - Ei ollenkaan

◯ 2 - Vähän

◯ 3 - Ei ole muuttunut

◯ 4 - Melko paljon

◯ 5 - Erittäin paljon

8. FINCSC:n suorittaminen **auttaa** yrityksenne digitaalisen **liiketoimintaympäristön kehittämisessä**. *

◯ 0 - En osaa sanoa

◯ 1 - Ei ollenkaan

◯ 2 - Vähän

◯ 3 - Ei ole muuttunut

◯ 4 - Melko paljon

◯ 5 - Erittäin paljon

9. FINCSC:n myötä **ICT-ympäristönne** suoja uhkia vastaan on **parantunut**. *

◯ 0 - En osaa sanoa

◯ 1 - Ei ollenkaan

◯ 2 - Vähän

◯ 3 - Ei ole muuttunut

◯ 4 - Melko paljon

◯ 5 - Erittäin paljon

10. Yrityksenne **ICT-ympäristön kokonaiskuva** on nyt **selkeämpi** kuin ennen FINCSC:n suorittamista. *

◯ 0 - En osaa sanoa

◯ 1 - Ei ollenkaan

◯ 2 - Vähän

◯ 3 - Ei ole muuttunut

◯ 4 - Melko paljon

◯ 5 - Erittäin paljon

11. FINCSC:n myötä ymmärrätte **paremmin**, mistä **osaamisesta** yrityksessänne on puutetta. *

◯ 0 - En osaa sanoa

◯ 1 - Ei ollenkaan

◯ 2 - Vähän

◯ 3 - Ei ole muuttunut

◯ 4 - Melko paljon

◯ 5 - Erittäin paljon

12. FINCSC:n suorittamisen kautta ymmärrätte **paremmin** *

	En osaa sanoa	Ei ollenkaan	Vähän	Ei ole muuttunut	Melko paljon	Erittäin paljon
Politiikkojen ja **ohjeiden** merkityksen liiketoiminnalle	◯	◯	◯	◯	◯	◯
Fyysisen tietoturvan merkityksen liiketoiminnalle	◯	◯	◯	◯	◯	◯
ICT-tietoturvan merkityksen liiketoiminnalle	◯	◯	◯	◯	◯	◯

13. FINCSC:n myötä tietoisuutenne on **parantunut** *

	En osaa sanoa	Ei ollenkaan	Vähän	Ei ole muuttunut	Melko paljon	Erittäin paljon
Työympäristönne ICT-palveluiden **yleisestä tilasta**	◯	◯	◯	◯	◯	◯
Työympäristöönne kohdistuvista **uhkakuvista**	◯	◯	◯	◯	◯	◯
Työympäristöönne kohdistuvista **riskeistä**	◯	◯	◯	◯	◯	◯
Työympäristönne **kyberturvallisuuden tilasta**	◯	◯	◯	◯	◯	◯

14. FINCSC:n myötä olette **muuttaneet tai aikeissa muuttaa** *

	En osaa sanoa	Ei ollenkaan	Vähän	Ei ole muuttunut	Melko paljon	Erittäin paljon
Liiketoiminnalle kriittisten **palveluiden varajärjestelyjä**	○	○	○	○	○	○
Liiketoiminnalle kriittisten palveluiden häiriösietoisuuden **testauksia**	○	○	○	○	○	○
Liiketoiminnan **avainhenkilöiden varajärjestelyitä**	○	○	○	○	○	○
Liiketoiminnalle kriittisen **tiedon hallintaa**	○	○	○	○	○	○

15. FINCSC:n myötä olette **tehneet tai tulette tekemään** muutoksia *

	En osaa sanoa	Ei ollenkaan	Vähän	Ei ole muuttunut	Melko paljon	Erittäin paljon
Tietoturvapolitiikkoihinne ja -ohjeisiinne	○	○	○	○	○	○
Salasanakäytäntöihin	○	○	○	○	○	○
Laitetiloihin	○	○	○	○	○	○
Yleiseen pääsynhallintaan	○	○	○	○	○	○

16. Avoin kommentti / huomio liiketoimintaympäristöstä tai sen kartoittamisesta

_____
_

_____
_

_____
_

3000 merkkiä jäljellä

17. FINCSC:n myötä ymmärrätte **paremmin** mitä **ostettavilta** palveluilta pitää **vaatia**. *

○ 0 - En osaa sanoa

○ 1 - Ei ollenkaan

◯ 2 - Vähän

◯ 3 - Ei ole muuttunut

◯ 4 - Melko paljon

◯ 5 - Erittäin paljon

18. FINCSC:n suorittamisen myötä osaatte huomioida **paremmin ulkoistettujen palveluiden** *

	En osaa sanoa	Ei ollenkaan	Vähän	Ei ole muuttunut	Melko paljon	Erittäin paljon
Kuvaukset palveluiden tietoturvasta	◯	◯	◯	◯	◯	◯
Ylläpitoon ja hallintaan liittyvät asiat	◯	◯	◯	◯	◯	◯
Merkityksen liiketoiminnalle	◯	◯	◯	◯	◯	◯
Sisältämät riskit	◯	◯	◯	◯	◯	◯

19. Ulkoistettujen ICT-palveluiden toimittajiin liittyvät riskit on huomioitu. *

◯ 0 - En osaa sanoa

◯ 1 - Ei ollenkaan

◯ 2 - Vähän

◯ 3 - Ei ole muuttunut

◯ 4 - Melko paljon

◯ 5 - Erittäin paljon

20. FINCSC:n myötä **luottamuksenne ICT-palveluntarjoajiin** on **vahvistunut**. *

◯ 0 - En osaa sanoa

◯ 1 - Ei ollenkaan

◯ 2 - Vähän

◯ 3 - Ei ole muuttunut

◯ 4 - Melko paljon

◯ 5 - Erittäin paljon

21. Avoin kommentti / huomio ulkoistettuihin palveluihin / palveluntarjoajiin liittyen

_____

_____

_____

3000 merkkiä jäljellä

22. FINCSC-kyselyyn vastauksien hakeminen yrityksenne toimintaympäristöstä oli helppoa *

◯ 0 - En osaa sanoa

◯ 1 - Ei ollenkaan

◯ 2 - Vähän

◯ 3 - Ei ole muuttunut

◯ 4 - Melko paljon

◯ 5 - Erittäin paljon

23. Jos Kyberturvallisuuden perustason sertifikaatista tulee Euroopan laajuinen standardi, uskotteko sen auttavan yrityksenne kansainvälistymistä / kansainvälistä yhteistyötä? *

◯ 0 - En osaa sanoa

◯ 1 - Ei ollenkaan

◯ 2 - Vähän

◯ 3 - Ei ole muuttunut

◯ 4 - Melko paljon

◯ 5 - Erittäin paljon

24. Teidän on helppoa saada tietoa yleisistä kyberturvallisuuteen liittyvistä ohjeita ja hyvistä käytänteistä *

◯ 0 - En osaa sanoa

◯ 1 - Ei ollenkaan

◯ 2 - Vähän

◯ 3 - Ei ole muuttunut

◯ 4 - Melko paljon

◯ 5 - Erittäin paljon

25. FINCSC:n myötä teidän on **helpompaa** löytää tietoa yleisistä kyberturvallisuuteen liittyvistä ohjeita ja hyvistä käytänteistä. *

◯ 0 - En osaa sanoa

◯ 1 - Ei ollenkaan

◯ 2 - Vähän

◯ 3 - Ei ole muuttunut

◯ 4 - Melko paljon

◯ 5 - Erittäin paljon

26. Yleinen palaute FINCSC-pilottihankkeesta, siihen liittyneistä tutkimuksista tai muuten vain kyberturvallisuuteen liittyvistä asioista.

_____

_____

_____

3000 merkkiä jäljellä