Procurement and supply of cyber security consultant services

Interview-based case study

Lasse Kurkela

Master's thesis
May 2020
School of Technology
Master's Degree Programme in Information Technology
Cyber Security

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

jamk.fi

Description

Author(s) Kurkela, Lasse	Type of publication Master’s thesis	Date May 2020
		Language of publication: English
	Number of pages 45	Permission for web publication: x

Title of publication

Procurement and supply of cyber security consultant services

Degree programme

Master’s Degree Programme in Information Technology, Cyber Security

Supervisor(s)

Saharinen Karo, Hautamäki Jari

Assigned by

Telia Inmics-Nebula Oy

Abstract

Cyberthreats have been rising as one of the major concerns in organizations throughout the world and different types of information security incidents are making it into news headlines more often than ever. This has made organizations more aware of the need for information security regardless of the type and line of business the organization presents. Many companies provide different types of information security services to provide protection against these emerging threats and new businesses are started every day.

Each organization has their own specific needs depending on multiple factors such as type, size, age, line of business, people working in these organizations and clients they have. Companies selling their products and solutions also differ from each other by their technological approach, methodologies they have used and people who adapt these to the needs of the client. As the number of these combinations is almost infinite, the technical success rate and people's opinions from these implementations vary highly.

The research was conducted by interviewing people from different types of organizations to get their opinions about the kinds of information security services they have procured and how they see these services have met their needs and expectations.

The results provide more understanding what the needs and expectations of different types of organizations are, and through this research the offering of security services can be profiled better to meet the needs of a client and also to find the gaps in the offering that the next generation needs.

Keywords/tags (subjects)

Consultancy, procurement, supply, services, information security

Miscellaneous (Confidential information) jamk.fi

Kuvailulehti

Tekijä(t) Kurkela, Lasse	Julkaisun laji Opinnäytetyö, ylempi AMK	Päivämäärä Toukokuu 2020
	Sivumäärä 45	Julkaisun kieli Englanti
		Verkkojulkaisulupa myönnetty: x

Työn nimi

Kyberturvallisuuden konsulttipalveluiden myynti ja hankinta

Tutkinto-ohjelma

Master´s Degree Programme in Information Technology, Cyber Security

Työn ohjaaja(t)

Karo Saharinen, Jari Hautamäki

Toimeksiantaja(t)

Telia Inmics-Nebula Oy

Tiivistelmä

Kyberuhat ovat nousseet yhdeksi merkittävimmäksi riskiksi organisaatioissa kautta maailman samalla, kun erilaisista tietoturvauhkista kirjotetaan mediassa useammin kuin aikaisemmin. Tämä on saanut organisaatiot, koosta ja toiminnastaan riippumatta, panostamaan enemmän tietoturvaansa. Yritykset ovat tuoneet markkinoille erilaisia ratkaisuja ja palveluita näiden uhkien torjuntaan, ja uusia tuotteita ja yrityksiä tulee markkinoille lähes päivittäin.

Jokaisella organisaatiolla on omat yksilölliset tarpeensa, jotka vaihtelevat organisaation tyypin, koon, iän, toimialan, työntekijöiden sekä asiakkaiden mukaan. Myös tietoturvapalveluita tarjoavat yritykset eroavat toisistaan tuotteidensa, menetelmien ja palveluita toteuttavien ihmisten osalta. Näiden yhdistelmistä saavutetaan lähes rajaton määrä yhdistelmiä, jolloin toteutusten onnistuminen teknisesti ja käyttäjien näkökulmasta vaihtelee äärilaidasta toiseen.

Tutkimuksessa haastateltiin henkilöitä useista eri tyyppisistä organisaatioista. Heiltä kysyttiin omakohtaisia kokemuksia ja mielipiteitä, kuinka eri tyyppisten palveluiden hankinta on onnistunut ja ovatko ne lopulta vastanneet tarvetta.

Saatujen tulosten perusteella voidaan arvioida erilaisten organisaatioiden tarpeita ja odotuksia palveluiden suhteen. Tulokset voivat myös auttaa paremmin profiloimaan palveluiden tarjontaa erilaisiin asiakassegmentteihin sekä tunnistamaan mahdollisia puutteita tarjonnassa.

Avainsanat (asiasanat)

Konsultointi, hankinta, tarjonta, palvelut, tietoturva

Muut tiedot Salassa pidettävät liitteet tulee merkitä. Merkinnästä tulee käydä ilmi, mitkä liitteet ovat salassa pidettäviä, mihin salassapito perustuu ja mikä salassapitoaika on. ***Esimerkiksi: Liitteet 1,4 ja 7 ovat salassa pidettäviä, jotka on poistettu julkisesta työstä. Salassapidon peruste Julkisuuslain 621/1999 24§, kohta 17, yrityksen liike- tai ammattisalaisuus. Salassapitoaika viisi (5) vuotta, salassapito päättyy 18.5.2022.***

Contents

Figures

Tables

1 Introduction

1.1 Motivation

Gartner (2018) estimated that worldwide information security expenditure will have exceeded 124 billion US dollars in 2019. In this estimate, the value of services accounts for about half of it being about USD 64 billion. Table 1 shows Gartner's figures for security spending by segments worldwide for years 2018-2019 in millions of USD (Gartner 2018). Unfortunately, the table and report do not go into more details about how the services are divided further between consulting and other types of managed services.

Table 1. Worldwide Security Spending by Segment

Market Segment	**2017**	**2018**	**2019**
Application Security	2434	2742	3003
Cloud Security	185	304	459
Data Security	2563	3063	3524
Identity Access Management	8823	9768	10578
Infrastructure Protection	12583	14106	15337
Integrated Risk Management	3949	4347	4712
Network Security Equipment	10911	12427	13321
Other Information Security Software	1832	2079	2285
Security Services	52315	58920	64237
Consumer Security Software	5948	6395	6661
Total	**101544**	**114152**	**124116**

CGI has created polls 2016 (CGI 2016) and 2018 (CGI 2018) to Finnish companies about how they will address the emerging cyber threats. Based on those polls the share of procured cyber security services shows an increase from 34% in 2016 to 38.3% in 2018. Also 47.5% of the companies are investing on improving their security mechanisms. Figure 1 shows the responses from the latest poll on how organizations prepare themselves against cyber threats (CGI 2018, 10). Based on this, it can be estimated that the value of sold consultancy services is rising in billions of dollars per year making it a very lucrative market.

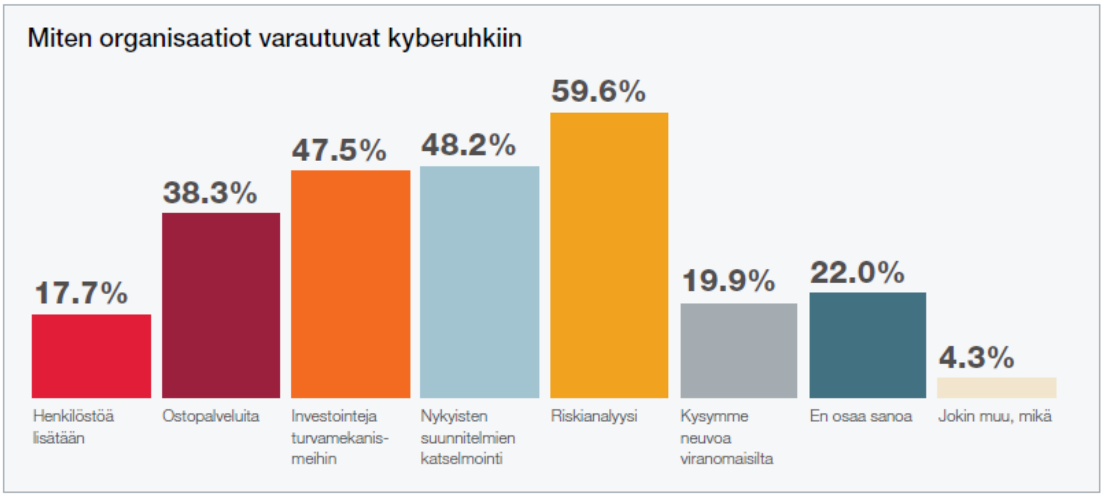


Figure 1. How organizations are preparing for cyber threats

In the discussions with the people buying and selling consultancy services to companies it has been identified that selling administrative consultancy services not involving physical goods or clearly measurable objectives, e.g. certification or testing, is very difficult. Such services would include e.g. preparing or enhancing cyber security risk management processes or security policies to improve the state of a company’s cyber security posture.

Changes in the legislation affect a large number of companies, and they can often be seen as spikes in the increased demand for consultancy services. The latest major effect was seen when the EU introduced General Data Protection Regulation, GDPR, in 2016, which took effect on 25 May 2018. It required companies around the globe working with personal data of EU citizens to make themselves familiar with the regulation and adjust their processes and data storage accordingly. As GDPR was a completely new regulation there were no previous rulings how different types of companies must adopt the requirements into their existing processes. Therefore, it created a huge demand for competent consultancy services to support the implementation.

By the time of writing the thesis, there are not many published figures of how much GDPR implementation has cost the companies around the world. Forbes (Smith 2018) has estimated that until the beginning of May 2018, U.S. Fortune 500 companies have spent USD 7.8 billion and in the UK FTSE 350 the companies spent USD 1.1 billion.

2 Background and research basis

2.1 Research objectives

The objective of this research is to build an understanding how the cyber security consultancy services should be packaged from buyers' and sellers' point of view to make them most interesting and simplify their procurement.

Companies' demands for cyber security are driven by the type of the company as the laws and local regulations as well as their line of business define the different levels of requirements. Small workshops that do not have an active online presence have completely different needs for cyber security to protect their customer registry than banks or insurance companies who need to safeguard their customers' personal information while still providing a service portal to allow customers themselves to access it.

This research focuses on business to business services and does not take into account the consumer-facing services due to the nature of consultancy services.

2.2 Research methods

Theme interviews were selected as the main research method to collect information. Interviews with participants produce textual material that will be analysed by means of qualitative research. Interviewing allows participants to answer questions freely, informally and express their thoughts openly about the question at hand, which allows to collect more data and build a more in-depth view and understanding on topics when analysing the collected data. With these, items that could not have been thought about beforehand can surface allowing to find new views to subjects at hand and allow an interviewer to ask more about these items. (Hirsjärvi 2015, 34-40.)

Another option would have been to create a questionnaire that would have been sent to participants to fill in. The questionnaire would have produced quantitative data for analysis; however, a questionnaire with multiple choice answer options does not allow that much of interactivity for more in-depth discussion on the questions and answers. Hence, interviews like the aforementioned could not be processed with quantitative methods, and a questionnaire would have to be the same for all participants in order to collect statistically analysable data. (Valli 2000, 81) Quantitative research gathers and analyses the statistical meaning of numerical values that are placed into a table. Researchers define the population that should be described with the results. The results are gathered from a sample group which represents the larger population and chosen by the researchers. Results from the sample group are then generalized over the entire research group in order to explain a phenomenon that is under research. (Alasuutari 2011, 26-28.)

As the aim of the research is to find reasoning behind the interviewees' choices and possible suggestions to improve the situation, it can be determined that using a questionnaire is not the best possible solution.

2.3 Literature review

To find out if there is any prior research about similar topics, searches from various academic sources were conducted. This required two main steps: the first was to build a list of possible sources to go through and the second was to build a list of search patterns to find the material from the sources.

There is no single universal place that would include all the research in the world; however, all universities and research organizations have their own processes and publication platforms of which some are public, some are open only to other academic institutions and some are behind paywall. Therefore it was necessary to build a list of sources to go through and the means to access them. Fortunately, JAMK's library services provide various methods to be able to reach also those platforms that are not completely public but allow more comprehensive research for prior research of a similar topic. As sources for national academic institutions were selected Theseus which is a repository of theses of Universities of Applied Sciences, Aalto University's Aaltodoc, Jyväskylä University's JYX, Tampere University's TuniLib. For international research, MIT's DSpace and Oxford University Research Archive were used for academic sources as well as IEEE Xplore Digital Library and Google's Scholar search that narrows searches to academic publications only.

The second task was to find most suitable keywords to bring up the relevant documents from the huge masses of research papers. For domestic sources both Finnish and English keywords were used, and in the international searches only English was used. Single keyword searches brought the most hits from the databases; however, their relevance was very low. Using multiple keywords narrowed down the amount of results; however, it did not neccessarily improve the relevance. The tool used to iterate plausible search keywords was Finto service which provides thesauruses and suggestions for other relevant keywords from multiple official ontologies and glossaries.

Searches using single keywords such as "procurement" brought results about procurement processes, "consultancy" brought mainly results about establishing consulting services. Searching "information security service" brought theses about improving the information security in the organization as the main objective of the thesis; however, iterating keywords "information security consultancy" did not bring any document matching the query. Additionally, "information security procurement" brought a paper about "The EU Defence and Security Procurement Directive" from Jay Edwards of Chatham House; yet, the actual relevance in the scope of this research was quite low.

In addition to exact prior research, research was also conducted to find similar studies but in a different context. An example of this could have been a research about selling management consultancy services or other types of information security services. In this area the most suitable paper was Tommi Metsälä's master's thesis from Tampere University of Applied Sciences "Purchase of consulting services in public entity – evaluation methods and evaluation of price and quality". (Metsälä

2012.) Unfortunately, none of the public organizations participated in the research so the results from this research could not be reflected on Metsälä's work.

3 Frameworks

3.1 Security standards

3.1.1 ISO 27000

ISO 27000 family of standards provides an overview and implementation instructions of information security management system, ISMS. Following these standards, organizations can build a framework for managing their information security and assets. The family of standards includes standards for defining the requirements of ISMS, provides guidance for the process of implementing, maintaining and improving the ISMS and addresses sector specific guidelines and conformity assessment. (ISO/IEC 27000:2018, 5-6)

ISO 27001 standard provides the requirements for the ISMS implementation. The standard is meant to be generic and applicable to all kinds of organizations regardless of their size and type as it does not mandate the used technologies or exact implementations. This standard mandates the requirements, which an organization must fulfil to be certified for the standard. (ISO/IEC 27001:2017, 6)

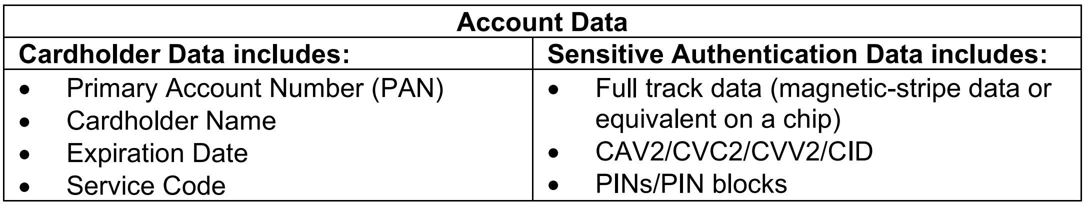
ISO 27006 standard provides guidance and requirements for the organizations providing certification and auditing for ISO 27001 based information security management systems. The standard supports the assessment, accreditation and auditing process of these organizations. (ISO/IEC 27006:2016, 6)

3.1.2 PCI DSS

The Payment Card Industry Data Security Standard (PCI DSS) is a baseline for technical and operational requirements for operations handling card payments and cardholder data. The standard is applied to all entities involved in payment processing and entities storing, processing and transmitting cardholder and authentication data. This includes merchants, card issuers, payment processors and service providers among others. (PCI Security Standards Council 2018, 5)

The standard defines account data which is divided into cardholder data and sensitive authentication data as shown in Table 2 (PCI Security Standards Council 2018, 7). Primary account number, PAN, is the key factor on cardholder data. If it is presented in the cardholder data environment (CDE) or it is processed, stored or transmitted with the cardholder name, expiration date or service code, the data must be protected according to the requirements defined in the standard. Even organizations that have outsourced payment operations to third parties may still be subject to the requirements defined in the standard and required to ensure that the third party fulfils the requirements of PCI DSS while processing and storing the account data. (PCI Security Standards Council 2018, 7)

Table 2. Account data definition



Account Data	
Cardholder Data includes:	**Sensitive Authentication Data includes:**
• Primary Account Number (PAN) • Cardholder Name • Expiration Date • Service Code	• Full track data (magnetic-stripe data or equivalent on a chip) • CAV2/CVC2/CVV2/CID • PINs/PIN blocks

3.2 Regional and line of business regulations

3.2.1 Directive on public procurement

Directive 2014/24/EU of the European Parliament and of the Council on public procurement and repealing directive establishes rules for procurement of public contracts and design contests by contracting authorities when the estimated value of the contract exceeds the defined threshold which depends on the type of the contract (Directive 2014/24/EU, Article 1). Finnish law on public procurement and license agreements (L 1397/2016) implements this EU parliament directive into the national legislation.

Contracting authorities are defined in the directive (Directive 2014/24/EU, Article 2) as state, regional or local authorities, bodies governed by public law or associations formed by one or more authorities or such bodies governed by public law. A public contract is defined as a financial contract between the contracting authority and one or more economic operators, a natural or legal person, in order to provide work, products or services.

The directive is applied to public supply, service contracts and design contests exceeding EUR 134 000 when procured by central government authorities or EUR 207 000 when procured by sub-central authorities. For public works contracts the threshold is 5 186 000 euros. (Directive 2014/24/EU, Article 4)

3.2.2 GDPR

General Data Protection Regulation, officially EU regulation 2016/679 on the protection of natural persons regarding the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation) came into operation on 25 May 2018. (Regulation 2016/679.) Finnish law on data on data protection (L 1050/2018) implements and amplifies the EU regulation as part of national legislation.

Regulation defines rules to protect natural persons respecting their personal data and their right to the protection of their personal data. It applies to the processing of the data wholly or partly by automated means or by other means that forms a filing system. There are exceptions where the regulation does not apply, e.g. when the data is processed by a natural person for a purely personal or household activity, by authorities for the purpose of public safety or criminal investigation and prosecution and on various other specifically listed activities of EU member states. (Regulation 2016/679, Article 1-2)

The regulation defines that personal data can only be collected for specified and legitimate purposes. The data must be stored protected appropriately so that the data is protected against unauthorised processing and access. The data can only be stored for the minimum time period necessary for that storage where it permits the identification of subjects. Processing of the data is allowed only when the subject has given consent for it, the processing of data is necessary for compliance of a contract that the subject is part of or the legal obligations where the data controller is the subject. The controller must be able to demonstrate that the subject has given consent to collect and process the personal data. The subject has also the right to revoke the consent at any time. The controller is a natural or legal person who determines the purpose and means of personal data processing. The controller may use the processor to process the data on their behalf. (Regulation 2016/679, Article 5-7)

The subject also has the right to obtain information from the controller about what data has been collected and wat the purpose for the processing is. The subject can demand rectification if the data is incomplete or inaccurate. Additionally, the subject has the right to demand erasure of the personal data when the original need for processing data has ended or the consent for processing has been withdrawn, and there are no legitimate requirements that would override the right of erasure. The subject can request the controller to provide the personal data that has been stored. The controller must provide the data in a structured and machine-readable format. (Regulation 2016/679, Article 15-21)

Breach or non-compliance of the regulation, depending on the type and size of the infringement, may lead into administrative fines up to EUR 20 000 000 or up 4% of the organization’s total worldwide annual turnover, whichever is higher. (Regulation 2016/679, Article 83)

3.2.3 VAHTI

VAHTI is Governmental Information Security Management Board that works under the Ministry of Finance. Its main objective is to work as co-operation, preparation and coordination workgroup for organizations that work in development and steering of public governmental digital safety. VAHTI creates and maintains the requirement frameworks for information security and promotes digitalization of public administration through ICT security and continuity. VAHTI publishes VAHTI-instruction documentation series that guide public administration on how to implement information security. (Ministry of Finance 2018a.)

VAHTI supports decision making and preparation work in the public administration concerning digital security. Digital security enables digitalization of public administration, operational reliability, the confidentiality, integrity and availability of information and operations as well as improvement of operational quality and risk management. (Ministry of Finance 2018b, 17-20)

3.2.4 Katakri

Katakri is an audition tool for evaluating an organization's ability to protect officially classified information. It is based on local and international regulations and obligations and it does not define any additional requirements. (Ministry of Defence 2015.)

Katakri can be used as an auditing tool for evaluating organizations security arrangements in corporate security clearance and evaluating security of authorities' systems. The use of Katakri is to ensure that organizations do possess adequate security controls in security management and to protect the classified authorities' information from unauthorized access in the environment they are being processed. (Ministry of Defence 2015.)

The main source for regulations in national legislation is Council of State's enactment of information security in civil service (L 681/2010) that contains the requirements for protecting national and international classified information. The main international source is EU Council's decision on security rules for protecting EU classified information (EU Regulation 2013/488/EU). (Ministry of Defence 2015.)

Katakri's requirements are divided into three sections. The first part handles security management and aims to make sure that an organization has readiness and ability to maintain and deploy the security standards in use. The second part handles physical security for the environment where the classified material is handled. The third part is technical information security describing the requirements from technical infrastructure that is used for processing the material. (Ministry of Defence 2015.)

3.2.5 Capability Maturity Model Integration

Capability Maturity Model Integration is a tool to measure and improve an organization's process maturity. It was originally developed for the needs of U.S. Department of Defence for assessing software contractors but has been expanded to be applicable to any field of industry. Currently it is being administered by CMMI Institute. (CMMI Institute 2020)

Organizations will be recognized for a certain level of maturity through an appraisal program. Maturity level determines how well an organization compares to the CMMI best practices at process level. Maturity level is a value from 1 to 5 and the values are described as shown in Table 3. (CMMI Institute 2020)

Table 3. CMMI Levels

Level	**Name**	**Description**
0	Incomplete	Ad hoc and unknown.
1	Initial	Unpredictable and reactive
2	Managed	Managed on the project level
3	Defined	Proactive, rather than reactive.
4	Quantitatively Managed	Measured and controlled.
5	Optimizing	Stable and flexible.

ISACA has built a capability maturity model which grades an organization's state of security from process perspective with a scale 0-5. The description of levels at the scale are listed at Table 4. (ISACA 2012, 50-51).

Table 4. ISACA Capability Maturity Model Levels

Level	Name	Description
0	Non-existent	No recognition by organization of need for security.
1	Ad hoc	Risk is considered on an ad hoc basis—no formal processes.
2	Repeatable but intuitive	Emerging understanding of risk and need for security.
3	Defined process	Companywide risk management policy/security awareness.
4	Managed and measurable	Risk assessment standard procedure, roles and responsibilities assigned, policies and standards in place.
5	Optimized	Organization wide processes implemented, monitored and managed.

4 Execution of interview process

4.1 Interviewing process

The process was started by surveying suitable candidate organizations of interest to be interviewed. The aim was to get as diverse an interview base as possible to get the research output to be applicable as widely as possible. For this reason, there was an effort to select organizations which were from different fields of industries and different size.

After this, the next phase was to identify persons from within these in order to be able to reach out for the most suitable person whom to be interviewed. In many cases a person was able to be identified; however, when what was not successful then some common contact channel, e.g. role address or general contact form was used to try to reach out the organization in general. The initial contact with the potential interviewees was made through various means. The majority of people were contacted directly by email or by phone and some through contacts in social and professional networks. One version of the Finnish cover letter sent to the interviewee candidates is shown in Appendix 3.

During the contacting phase there was a noticeable difference in the success rate of the replies and setting up the interview between different types of contacts. All persons belonging to existing networks or who were referred to by a person from the networks accepted the invitation for the interview. Only one single person with no existing connection accepted the invitation, and very few replied to decline from the interview so the majority of the requests where completely ignored.

When the time and place for the interview was agreed, the interviewee was also given the preliminary list of questions to be discussed so that they could see if there were any questions they did not feel comfortable with and to give them a chance to prepare in advance. This list of the questions in Finnish is in Appendix 1.

The interviews were carried out during the year 2019. At the beginning of the interview the purpose of this research and the motivation behind it were discussed together with the interviewees. They were reminded that participation is voluntary and that they can skip any question they want without any reasoning. The notes of discussion were written down to computer simultaneously during the interview and while all participants were offered a possibility to see them during the interview, e.g. using the external screen, projector or having the notes emailed them afterwards, nobody wanted to use these options.

4.2 Interview questions

The basic set of questionnaires used in interviews is divided into three sections. The Finnish version of interview questions is shown in Appendix 1. The questionnaire was also translated into English for the non-Finnish speaking persons and can be found in Appendix 2.

The first section was for gathering demographic data about the participants. The demographic data was used for generalization of the gathered data. Generalization is a method of quantitative research in order to find similarities within a reference group (Alasuutari 2011, 180-195.). While this research is based on qualitative methods, the demographic data helps to build an understanding about the interviewed organization and to categorize the results for analysis.

The questions in the second section were used to build an understanding of the current state of information security management. As a tool for evaluation, ISACA's capability maturity model (CMM) was chosen to create comparable results. The outcome value of the organization's maturity was then used as one of the demographic values to build reference groups reaching across the organizations.

The third section of the questionnaire contained the questions about the procurement of information security services. The questions were to gather the organizations' needs for procuring services as well as types and selection criteria for vendors. After the procurement section, the questions continued with the ways how the organizations evaluate services they are procuring during and after the delivery. The interviewees were then requested to tell about their past experience with different kinds of scenarios where the procurement had failed or the procured service did not meet the expectations. The interviewees were asked to express their opinion whether good information security could provide a competitive edge to their businesses. Finally, at the end there was a chance for interviewees to freely discuss any topic they see fit related to the interview.

5 Evaluation of interview results

5.1 Gathering interview data

5.1.1 Background information

Line of business

The participating organizations were from line of businesses in education, energy, finance, insurance and healthcare. The organizations had local, national, Nordic and worldwide presence.

Company size – number of employees / economic turnover

For the demograpic data the sizes of the interviewed organization spanned from 5 to over 10,000 employees, in economic terms the turnovers were from EUR 100,000 to over 5 billion a year. The majority of interviewed persons were company owners and C-level managers – 1 CEO, 2 CIOs, 1 CISO and 1 IT managers. Also 2 system specialists and 1 network specialist were involved in the interviews to provide insight from their areas of speciality through the organization. Distribution of interviewed persons between different organization sizes can be found from Figure 2.

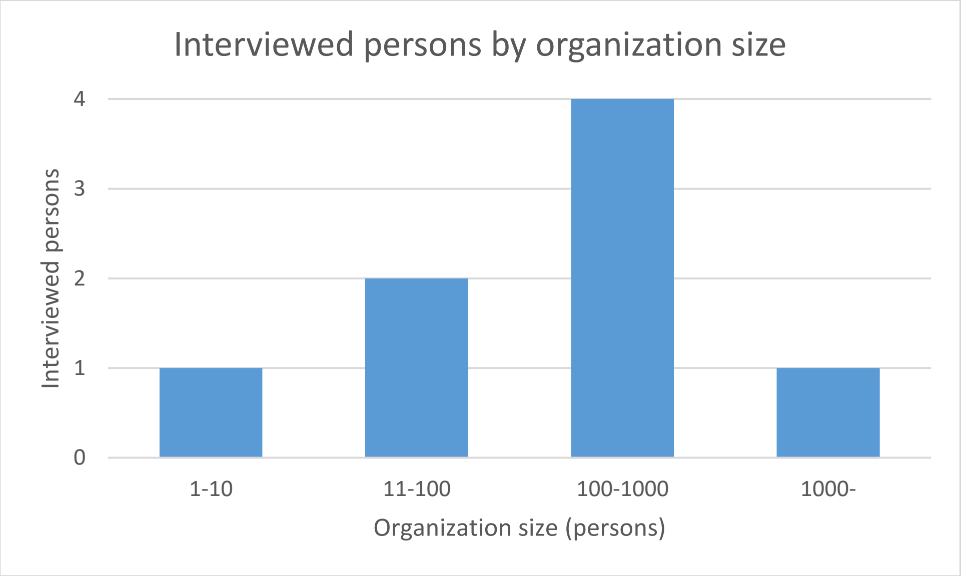


Figure 2. Number of interviewed persons by organization size

5.1.2 Internal information security management

Are you implementing any information security framework? Why has the framework been chosen for implementation?

ISO 27000 information security standard family, NIST cybersecurity framework and VAHTI regulations were listed by the bigger organizations as frameworks used for developing the organization’s information security guidelines. However, in most cases the frameworks were used as a reference documentation and were not completely implemented to full extent.

Smaller organizations did not use any of the information security frameworks as a baseline for their information guidelines; however, they had their guidelines defined through other organizational certification processes that e.g. mandate risk management procedures or through the mandatory regulations from their line of business.

How would you evaluate the current maturity level of information security within your company? Is there a nominated responsible person for information security?

Every organization had nominated a responsible person or several persons. The bigger organizations had multiple persons holding more focused roles. International organizations also had their own responsible persons for each country or region.

Do you have written information security policy?

Bigger organizations have written information security policy that the employees re also trained to as a part of the orientation process.

Smaller organizations told that they did not have an information security policy at the time of the interview; however, they were considering having one. The main reason for not having one in all cases was the trust that the organization is small enough so that each employee can be individually trained to follow the organization’s policies as part of their orientation process and to have enough knowledge to survive in their daily work as well as to be able to easily reach out for the responsible persons for help in case should something occur. Also, there were discussions about whether the written policy could be short “house rules” type of poster that could be framed and hanged on the wall or a full document with video tutorials for more inexperienced persons.

Do you monitor and process security incidents?

All interviewed organizations had some sort of a way to monitor security incidents; however, the extent and ways of the monitoring and further processing differed on the size of organization.

The smallest organizations lean on to the computer’s end-point protection software to collect security events, and the personnel may act on an ad-hoc basis upon them if and how they see fit. Incidents are not centrally collected or processed further.

As the size of organization grows, monitoring introduces more various technical methods in addition to only device monitoring. Many organizations with a single vendor for their telecommunication have bought network security services from their vendor. The vendor then analyses the network traffic for possible indicators of compromise and other unwanted traffic and then reports back and acts upon when needed. Large organizations may also have their own security operating centre, either an internal one or operated by some other organization that monitors and processes the security incidents with dedicated personnel.

Technical incidents are usually carefully logged using some sort of ticketing system or other structured database. Non-technical security incidents following from a human error or physical security issues are usually less likely to be logged at all or at the same detail as many times these are not recognized to be comparable to technical security incidents.

Do you enhance information security continuously based on the observations?

All interviewed organizations informed that they do have a procedure to improve their information security position based on the earlier observations from within the organization or information received from outside.

Organizations with a formal way to register incidents also have implemented a formal process for continuous improvement of their information security processes and procedures as they have a measurable way to observe the results from their previous actions, and they can then be reiterated when needed.

Organizations that do not have such a systematic approach on security incidents still try to find ways to improve their processes and procedures to avoid such risks in the future; however, unsystematic and unformal ways to introduce the changes - as usually these organizations also have very low amount of events - make it difficult to track the effectiveness of these changes.

Is information security a part of business management processes, e.g. risk management?

Organizations with a certified quality management system, e.g. ISO 9001, must have very detailed risk management processes including information security as a part of it.

Also, other organizations had included information security into their risk management and business continuity plans. The extent of detail, however, varied a great deal.

What security functions you do implement internally? Do you attempt to provide all the needed functions by yourself?

All organizations had chosen to implement themselves the administrative functions for defining, managing and improving the organization’s information security guidelines. The technical implementation was then more or less outsourced to some other party.

The more complex implementations like SIEM and SOC functionalities requiring 24/7 operations were more likely to be completely procured as a service than implemented in-house. Also, network monitoring to recognize patterns of malicious traffic, and end-point security that tries to detect anomalies from the normal usage, are also usually procured as a service as these require plenty of attention and dedicated personnel to work on them. Centralization provides the advantage of being able to apply and share patterns over a larger user base.

Less complex and non-timing critical processes such as backup and patch management were more likely to be implemented by in-house functions as these are usually very automated processes once they have been set up and most of the time they require little effort on monitoring in case issues should arise.

How do you ensure adequate internal competence?

The most common way was to provide internal training based on the individual's position to raise the awareness of possible, most likely threats to face them. Intranet, emails and similar ways were as well used to notify employees if something had happened or if some significant threats, e.g. targeted phishing attempts or special malware, were noticed.

In addition to general awareness, in most organizations people with specific roles had the possibility to attend courses on information security and get certified on their area of specialization.

Some organizations procured consultancy from a third party to help them with a specific need in a manner that helps them not only to solve the issue once but also provide training allowing the organization to solve the similar issues in future either independently or at least partially, depending on the complexity of the topic.

How do you think information security impacts your business?

All organizations see information security as an asset for their businesses and told that there has been a change into a more positive way during the last few years from how information security previously has been thought as a preventer of the ways of work.

Everybody underlined the negative impact that poor security would introduce to their business if any incident were to occur. A smaller incident would cause more inconvenience to the daily work by hindering or preventing people from working, e.g. if employees were not able to read their emails or access information they need in order to work. Major incidents could lead to a permanent loss of data or exposure of confidential information, which would damage the reputation of the organization and/or cause financial losses that could affect the organization’s ability to continue their business.

On a positive note, good information security was seen as an enabler that allows new ways of working. Technology allows people to work securely using different types of devices and to have access to data regardless of the time and place as communication channels and data can be transferred and stored encrypted to ensure the confidentiality and integrity of the data. Effective tools, processes and procedures lighten the burden from administration and allow employees to work more effectively.

5.1.3 Procurement of information security services

What or for what purpose do you procure information security services from external vendors?

External vendors were used to complement the resources and knowledge that organizations have. All organizations have acknowledged that it is not practical and cost effective to try to produce all resources and knowledge inside the organization. Organizations commonly held information security management and development tasks to themselves and procured services that require infrequently needed but highly technical skills like security and penetration testing and very resource intensive operations such as 24/7 SOC function.

How often do you procure these services?

Apart from continuous services like SOC function and network monitoring, the services are mostly procured with on-demand basis where the frequency of the need for a specific service may be one-time, e.g. consulting for procurement process or verification of an application environment installation, to more repetitive tasks like periodical vulnerability assessment of a specific system.

On what basis do you choose vendors? What are the selection criteria? How do you run the bidding competition?

Major factors in the vendor selection and listed by all organisations were price, reputation and references. Regulations on the geographic area or in the field of business also might introduce requirements to the criteria when selecting vendors for specific tasks.

Some organizations have their own short list of preferred vendors that they are used to working with and have a good standing based on their track record from previous assignments with the organization. Many organizations had their preferences as for the type and size of the vendor to be somehow similar to their size and type, e.g. smaller organizations preferred smaller and local vendors whereas bigger organizations were comfortable working with large multinational vendors.

As part of the procurement process, all organizations have a competitive bidding to find the most suitable vendor for the assignment at hand. During this phase organizations evaluate a vendor’s offering and references concerning the given price to verify that the offered solutions fit the need and the price also meets the budget and quality of the service. Smaller organizations often favour price over quality and the scope of the service, whereas bigger organizations have the possibility to reduce the effect of the price in favour of quality.

How do you evaluate the quality of services? During the project / delivery? After delivery / during the use?

The main evaluation criteria for the organizations are that the agreed tasks are fulfilled during the delivery and possible acceptance testing shows that the requirements are met.

For services affecting multiple users directly, e.g. endpoint protection, the feedback is gathered from the end users to receive their viewpoint about the service.

Have you encountered situations where the service does not fulfil the need?

Most of the organizations stated that they have been in a situation where the delivered service did not meet their expectation. In those cases, most of them could have been avoided by paying more attention to the procurement process. In some cases the product or service quality was not considered to be worth of the price paid for it. Cases where the actual delivery was a failure were very minimal.

One of the major hurdles during the procurement process is that the selection is made by non-technical people based on the very detailed and technical presentations and many times also the procurement is carried out component by component over the longer timeframe. This easily leads to a situation where the services overlap with each other providing an unnecessary double protection (with double costs) on some areas while still easily leaving blind or dark spots in between. Separate components might not integrate into the existing frameworks and into each other making it difficult to get consolidated visibility over the monitored entities. Some organizations brought up that they would like to be able to consolidate their procurements to one vendor that would then have the responsibility for component level selection based on the organization's needs to make sure that the components would integrate into each other and the existing frameworks in a cost-effective way.

Other frequently encountered problem is that the needs brought up by business users are very specific and product centric. These are then often required by the same user to be solved using a specific product that they have in their mind while raising the issue. While this often works with that one specific issue, the resolution usually is not generic and compatible with the existing framework allowing it to be consolidated or to be used for similar issues with other products within the organization.

It was also brought up that the modern services components have multiple ways to integrate with each other but if the organization has legacy software or hardware? This might present issues and hinder the compatibility with modern components and the ability to use all the functions that the services could present.

Have you chosen not to complete the procurement because there has been no suitable service / product or vendor, the price has been too high or the benefit from the service could not be justified?

All organizations have been in a situation where they have decided not to proceed with the planned procurement after a closer evaluation. Basically, most of the times this has been due to the fact that the benefits from the service could not be justified against the price they would need to pay for it, especially when the solution could be overlapping with existing solutions or lack something required, which would lead to the need for another procured service or product. However, when it comes to regulatory demands, the organizations have been required to pay the price for the services regardless how high it has been, in order to be legally compliant with the running of their business.

Small organizations have very limited resources and budgets to carry out projects and investments, so they need to emphasize heavily on the price tag of the procurement and still require the vendor to provide a turnkey delivery, which narrows down their options in the markets. Bigger organizations usually have bigger budgets and more resources to engage into the projects allowing them a wider selection to evaluate and to choose the most suitable one.

While the procurement budget increases, the vendors usually become more willing to provide customized solutions with additional services and help from vendor side for the implementation, and sometimes they even create a completely new product or service. This helps big organizations to get what they want as long as they are willing to pay the price for it. On the small organization side this means that they mostly need to make a selection from basic off-the-shelf products and try to find if one or more of them cover their needs while still meeting the acceptable price point.

Are there offerings that you could use missing from the market?

The smallest organizations were interested in a service package for information security that would work in a similar way as externalized accounting and payroll services. The vendor would work as a CSO/CISO and help to create processes and risk management, help with training and awareness raising and look after IT assets to make sure they work effectively and are sufficiently protected. These organizations also recognized that this kind of service would be difficult to be priced in a way that it would be attractive to both sides as the workload would vary a great deal from time to time.

Also, the smallest organizations were interested in pursuing entry level information security training for a non-technical audience. Most of the employees have vocational education in such an area that does not include more than very basics of information technology and very little in information security if at all, depending on the time of education, on the information technology; hence, they do not have basics of information security and there are very few opportunities for self-education.

The bigger organizations were quite content with their current state of offerings and their possibilities to affect the supplied services.

Many organizations recognized that the rapid pace of development in many areas will soon start to present issues that are not yet recognized and that need to be solved in some manner. AI and machine learning were mentioned as such areas which grow rapidly and are in adoption; however, the implementations are very proprietary and algorithms are confidential so it is very hard to proactively analyse which kinds of threats they will face and how to protect against them. For example, can the self-learning algorithms be contaminated to make the whole system work inconsistently and make it to choose wrong decisions or can an algorithm crash the system in destructive way when correctly crafted data is parsed to system?

Do you see that good information security could provide a competitive edge?

All interviewed organizations were unanimous that good information security does provide competitive edge, in one way or another.

All organizations handle information about and for their customers and maintaining the trust and confidentiality of the customers is very important. If that information were exposed, it would damage the reputation, might lead into sanctions and in the worst case could lead to closure of the business. People are becoming more aware of their privacy, and organizations need to be able to convince them that they respect their privacy and have sufficient protection in place to protect the information that they have given. For example, private persons most probably do not choose a place for their healthcare based on the IT-security certifications that the organization may have but they will definitely avoid the places which are known to have issues keeping patient records confidential.

Information security certifications are often only pursued after an explicit demand due to the amount of work they need in order to fulfil the auditing requirements and even the bigger organizations may not see a need to get a hold of one without having a business need. Holding one may open completely new possibilities to organisations to provide their services to new focus areas. For example, public procurements may require the participating organizations to hold a certain level of certifications to allow the participation in the bidding process, which keeps the number of bidders low.

Certifications can also be a differentiator while looking further down the value chain. The customer of an organization may not be directly interested in the certifications the organization has; however, the client of that customer may in turn be keen to know that their vendor is using certified services to provide services to them. This way the organization can show their certification as a differentiator that will make a customer’s life easier while proving to their clients that their services are secure to use.

For the end user within the organization, the good information security allows people to work effectively with suitable tools and they do not need to make compromises between security and efficiency. When the security is a part of all development processes, the end results are often better as the user experience development goes hand in hand with the needs of security and can be worked out together with the end users to find optimal solution. If the security layers are only to be added afterwards, it usually disables or hinders existing functionalities without providing suitable replacements leading into crippled user experience and/or makes working more inefficient.

Any other experiences / topics not mentioned earlier?

The complexity of the enviroments constantly increases making it more difficult to manage the security throughly for all the components. This makes it harder to make a single pane of glass that allows one to see the status of whole environment at once. Also, this adds to the complexity to integrate things together for interoperatibility and manageability. This easily leaves some parts in gray areas that are not so effectively controlled and may lack the needed protection.

The mode of operation in security has changed from advance preparations to detection. This is a part of the rapid changes where the complexity cannot be completely known and covered; yet, new emerging threats are detected all the time by finding deviations from the baseline. Unfortunately, this does not always allow to stop the intruders at the frontline of the defences for the “patient zero” and prevent them from gaining access in the first place but allows to reduce the damage and eventually block further attempts as the new threat is analyzed and learned.

5.2 Analysis of interview data

Based on the given responses the organisations can be dived into different levels of maturity in information security using the ISACA’s maturity model described in chapter 3.2.5. The small organizations can be categorised to levels 1 and 2 whereas big organizations can be put into levels 3-5. None of the participated organizations would fall into lowest level 0.

Small organizations do have understanding about the need of information security and what they would need to do to have credible information security atmosphere. They feel that as they are so small they can promptly react on emerging issues in agile manner and walk every person through the processes and procedures one by one, they have not seen a need to write formal guidance and procedure manuals and generate a formal process documentation to handle different types of events. Small organizations see information security mainly as a technical issue. The lack of formal policies and procedures doesn’t allow these organizations to reach higher levels of the maturity model.

Big organizations have reached the size and complexity of the organization that have made them to recognize the importance of creating written policies and procedures. Size of the organization in terms of number of people and geographical locations have made it impossible to guide every person individually and to be available for them to contact in case of need. Therefore these organizations must have produced formal processes to handle issues and generated written policies and guide documents that people can examine by themselves to find answers and reach out to correct persons based on those. Having formalised processes forces organizations to define roles and responsibilities, which in turn on many cases accumulates these responsible persons to further develop processes and guidance they are responsible for. Forced formalization of the information security and the constant further development of them along other organization’s processes help big organizations to reach the higher levels in the maturity model where the process formalization is required.

Internal information security management

All interviewed organizations have nominated person that is responsible for the cyber security management and development. Not all organizations have a written cyber security policy. Only bigger organizations have one while small organizations rely on being able to communicate the needed information and guidance to the employees.

All organizations back their cyber security management guidelines into some framework. Organizations that are certified have implemented their guidance based on those certification requirements and follow them. Non-certified organizations are using frameworks as basis of their guidance and implement those on suitable parts which applies to their line of businesses.

All organizations monitor realized cyber security incidents is some way and also try to keep up with the state of threats in the surrounding world. Monitoring of the incidents in small organizations is merely based event log of laptop's endpoint security software and discussions between employees without formal written registration of events or follow-up procedure. On organizations with more formal procedures and especially those with certifications, the incidents are logged formally into centralized system and are being followed up on regular basis. These organizations will then use this collected information to enhance their guidelines and systems to be more resilient against the know threats.

Organizations manage the administrative side of the cyber security management by themselves. Automated processes like backups and patch management are also commonly implemented by organizations if they have their own ICT personnel. Cyber security related software and technical implementations for things that require extensive in-depth knowledge and operations around the clock like firewalls, SIEM and SOC are the most commonly procured as a service from external vendors to utilize organizations resources more effectively.

Organizations give basic security awareness training through internal training methods. These methods do vary based on the size and type of the organizations ranging from one-to-one discussions to formal classroom training alongside with e-learning systems for self-paced training.

Good security is seen as an asset on all organizations. It helps organizations to work more effectively without compromising the security and help organizations to meet their requirements to protect their and their customer's data.

Procurement of information security services

Main reason for organizations to procure services from external vendors is to complement organization's own resources to fulfil the needs that organization has in a cost-effective way. All functions are not useful to try to be implement by hiring enough competent persons to work within the organizations to implement said functions. Especially on small organizations benefits from the ability of having these functions as a service instead of implementing these by themselves. This way organizations can concentrate on their own core business instead of managing the IT.

Services are procured when the need is identified and no organization was able to mention that they would have identified and specific cycle on their procurement behaviour.

Vendor selection is most commonly done based on the bidding competition results where the price is one factor but also vendor's reputation and references can influence on decision making. Commonly organizations do have some preferences over the list of vendor or products which may affect on their decision and on whom they are requesting bids from. Also on the opposite side, the vendors have their preferences to whom they are targeting their services for and based on that make choices to which organizations they are making the sales efforts.

On regulated businesses and geographic regulations may affect the decision-making process as these regulations may narrow down the number of allowed vendors or the means of implementation that makes the costs higher.

Main evaluation criteria for the service quality of procured services is that the agreed tasks are fulfilled in time and that the acceptance criteria are met during the testing. Most of the organizations agreed that they have been in the situation where the expected evaluation criteria are not met after the delivery. Majority of these cases were recognized to have failed already during the procurement phase and more careful preparation would have prevent these from happening. In addition to that, some services or products had been identified only at the production phase to be not worth of the paid costs.

Most common root causes for these occurrences were identified to be origin from the situations where the evaluation and decisions had been made by the people not holding enough understanding about the subject and use-case where it was intended for. Also it was identified that sometimes when the business users were involved in the decision making process, the decisions were made in product centric way which diverted the evaluation process from complete overall enterprise architecture point of view into a single product or system making the procurement result less effective.

All organizations have decided not to procure services they originally intended to. Most common reason was the price that the organization was not able to justify comparing to the received benefits. Lack of features in products or services was rarely a reason for dropping a procurement process. Large organizations do hold budgets big enough to allow vendors for tailor services and products for these organizations while small organizations do not have such luxury due to the lack of budget.

For the same reason big organizations find it possible to find products and services they need as vendors have ability create such services from scratch if they do not have one already and they see others could buy as well. Small organizations do not have same options as building a service or product is often a costly project where usually a buyer bears all development costs alone. These organizations have to choose from mass marketed options.

All interviewed organizations see that good information security could provide competitive edge. Modern days customers are more aware and demanding of their privacy. Certifications can be used to show to customers the organizations abilities as well as allow organizations to pursue different types of deals where the certifications are explicitly required.

5.3 Observations and comparison to hypothesis

Smallest interviewed organizations, micro-organizations and entrepreneur-lead organizations were the most unsatisfied both with the status of their current state of cyber security consciousness and the supply of the services targeted for their segment. These organizations have very small budgets which does not allow them to make big investments for their cyber security. Survey in 2019 at the United Kingdom, conducted by Department of Digital, Culture, Media and Sports (2019, 22), revealed that mean yearly investment for organizations at this size was £3490 while median spend was only £200. These organizations, working outside the field of ICT, very rarely can hire dedicated person to take care of their ICT but the entrepreneur, business owner or one of the employees must take care of those chores along their normal work. Usually these persons do not have appropriate, formal training but is just more tech-savvy than others and is willing to help others. This makes these organizations to be in the biggest demand of the external cyber security services and consulting but also require the lowest prices in order to make it possible for organizations to be able to procure them. Therefore the small organizations are not the most wanted target segment for sales organizations as low profit margins would require huge sales volumes without possibility to customize the services to make it worthwhile.

Most of the time these organizations were content with the off-the-shelf services that have been able to source but would hope to get more help on choosing the most appropriate ones. Usually the selections are made by asking recommendations from the peers and through the people networks and then spending few nights using Google to find out the details. They find it difficult to find suitable cyber security training that would be relevant for them.

Small organizations were against the original hypothesis interested in their state of cyber security and had willingness to improve it as much as they can within the budgetary constraints they have. The original hypothesis was based on the experience from people who work in the small and medium business sales and it was that small businesses are very reluctant to discuss about cyber security issues and are constantly telling that they have everything in order as they have installed antivirus software to their computers.

Small and medium sized organizations that are big enough to have a dedicated ICT-support person are usually quite content with their status. These organizations usually go with restricted budgets which reflects to the number of employees. Department of Digital, Culture, Media and Sports survey in 2019 (2019, 22), revealed that mean yearly investments in UK was £25100 at medium size businesses. As the number of employees is small, they must concentrate on their daily chores at wide area of responsibilities. This gives them a very little opportunities on concentrating on single area of expertise and requires them to be technically focused. Most commonly problems are solved using only technical measurements and solutions are tool oriented. While technical approach works on many issues, it usually leaves out the administrative security approach that would boost the humane effect on preventing the issues from happening at the first place and may give the wrong kind of sense of security.

These organizations have a decent amount of choices to choose from when it comes to procuring of cyber security products and they also can afford to procure services and consulting from vendors to help them out with setting up new things and solving out issues with existing infrastructure.

Observations were quite hand in hand with the hypothesis that medium sized businesses are happy with their status as there are dedicated technical persons responsible for their ICT issues while they might not be subject matter experts in the cyber security. They see cyber security as a technical issue and rely on technical measures to prevent against security incidents. In many cases processes might not be the first to think when thinking about cyber security.

Large organizations have no difficulties to improve their status of cyber security. They are usually big enough in order to hire in-house employees that will work full time on cyber security tasks. These employees can attend training and maintain their know-how on regular basis as well as work with hands on tasks to improve their practical skills.

Large organizations have usually budget big enough so that they are able to procure all the required services from the vendors which are more than happy enough to provide those. Their budgets allow vendors to use more time and effort to provide tailor made solutions to these organizations. Department of Digital, Culture, Media and Sports survey in 2019 (2019, 22) shows that large business organizations in UK invested yearly £277000 on average.

Large organizations live much up to the expectations when it comes to the hypothesis. These organizations have lived long enough to be become matured to work with processes and procedures and cyber security is not an exception to that. They have built solid foundation on cyber security processes that are part of their complete risk management suite. Incidents are handled pragmatically and continuous development is used to finetune the ways organizations work to prevent things happening over and over again. Large organizations have large budgets that makes these things possible while smaller organizations need to focus on their core business only.

6 Conclusions and discussion

When comparing the gathered results to the original research objectives, it could be concluded that best insight about how the cyber security service offering could be improved was achieved with the needs of small organizations. Interviewed people from these small organizations provided answers that did not follow the hypothesis and did not reflect the prior understanding and expectations that has been built over the years from discussions with salespersons and people from small organizations.

Results got from the interviews with bigger organization reflected quite a much about the offering how it is already done today. From this perspective the interviews did not give practically any new information that could be used to improve planning the cyber security offering that is focused on large customer sales.

While the interviewed small organizations did provide interesting information about their interest in cyber security, the number of the interviewed organizations is very low and therefore results cannot be generalized to cover every similar organization. As only a small fraction of the organizations did accept the request for interview, it can be assumed that only those organizations that are interested in cyber security topics were the ones to accept and those who declined are not. This can distort results to show organizations to be more interested in cyber security than the average organization would in reality be.

For a further study it would interesting to have a research that would concentrate only to small and micro organizations in order to see if and how the answers would change if the results could be collected from larger sampling group. The size of the sampling group in this research was very low due to the difficulties to find organizations willing to participate and as idea was to get samples from different sizes of organizations, it made the number of participating small organizations even lower. In the original research plan there was an idea to be able to compare the results with organizations of different sizes but ones with the similar line of business to each other's. Unfortunately, also this idea failed to realize due to the lack of participants. To retrieve most balanced set of results, it would need also to get some feedback from organizations that think that cyber security does not have nothing to do with their business.

References

Alasuutari, P. 2011. Laadullinen tutkimus 2.0 [Qualitative research 2.0]. Tampere: Vastapaino.

CGI. 2016. Kyberturvallisuuden tila suomalaisissa organisaatioissa 2016 [State of cyber security in Finnish organizations 2016].

CGI. 2018. Kyberturvallisuuden tila suomalaisissa organisaatioissa 2018 [State of cyber security in Finnish organizations 2018].

CMMI Institute. 2020. What is CMMI? Accessed 19 January 2020. Retrieved from https://cmmiinstitute.com/cmmi/intro

Department of Digital, Culture, Media & Sports. 2019. Cyber Security Breaches Survey 2019. Accessed 13 March 2020. Retrieved from https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2019

Directive 2014/24/EU. Directive 2014/24/EU of the European Parliament and of the Council of 26 February 2014 on public procurement and repealing Directive 2004/18/EC. Accessed 22 December 2018. Retrieved from http://data.europa.eu/eli/dir/2014/24/oj

Gartner, 2018. Press Releases - Gartner Forecasts Worldwide Information Security Spending to Exceed $124 Billion in 2019. Accessed 27 November 2018. Retrieved from https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019

Hirsjärvi, S., Hurme, H. 2015. Tutkimushaastattelu: teemahaastattelun teoria ja käytäntö [Research interview: theory and practice of theme interview]. Helsinki: Gaudeamus.

ISACA, 2012. CISM Review Manual 2013. USA: ISACA.

ISO/IEC 27000:2018. Information technology — Security techniques — Information security management systems — Overview and vocabulary. Accessed 22 December 2018. Retrieved from https://janet.finna.fi, SFS Online.

ISO/IEC 27001:2017. Information technology — Security techniques — Information security management systems — Requirements. Accessed 22 December 2018. Retrieved from https://janet.finna.fi, SFS Online.

ISO/IEC 27006:2016. Information technology — Security techniques —Requirements for bodies providing audit and certification of information security management systems. Accessed 22 December 2018. Retrieved from https://janet.finna.fi, SFS Online.

L 1050/2018. Tietosuojalaki [Law on data protection]. Accessed 7 December 2019. Retrieved from https://www.finlex.fi/fi/laki/alkup/2018/20181050

L 1397/2016. Laki julkisista hankinnoista ja käyttöoikeussopimuksista [Law on public procurement and license agreements]. Accessed 7 December 2019. Retrieved from https://www.finlex.fi/fi/laki/ajantasa/2016/20161397

Metsälä, T. 2012. Purchase of consulting services in public entity – evaluation methods and evaluation of price and quality. Master's thesis. Tampere University of Applied Sciences, degree programme in constrution engineering. Accessed 3 November 2019. Retrieved from http://urn.fi/URN:NBN:fi:amk-2012061412690.

Ministry of Defence. 2015. Katakri 2015 – Tietoturvallisuuden auditointityökalu viranomaisille. Accessed 22 December 2018. Retrieved from https://www.defmin.fi/puolustushallinto/puolustushallinnon_turvallisuustoiminta/katakri_2015_-_tietoturvallisuuden_auditointityokalu_viranomaisille

Ministry of Finance. 2018. VAHTI-toiminta [VAHTI-function]. Accessed 22 December 2018. Retrieved from https://vm.fi/vahti

Ministry of Finance. 2018. VAHTIn toimintasuunnitelma vuosille 2018-2019 [VAHTI strategy 2018-2019]. Accessed 22 December 2018. Retrieved from http://urn.fi/URN:ISBN:978-952-251-941-2

PCI Security Standards Council. LLC. 2018. Payment Card Industry Data Security Standard – Requirements and Security Assessment Procedures, Version 3.2.1. Accessed 22 December 2018. Retrieved from https://www.pcisecuritystandards.org/document_library

Regulation (EU) 2016/679. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation). Accessed 22 December 2018. Retrieved from http://data.europa.eu/eli/reg/2016/679/oj

Smith, O. 2018. The GDPR Racket: Who's Making Money From This $9bn Business Shakedown. Published on Forbes website 2 May 2018. Accessed 22 December 2018. Retrieved from https://www.forbes.com/sites/oliversmith/2018/05/02/the-gdpr-racket-whos-making-money-from-this-9bn-business-shakedown/

Valli, R. 2018. Ikkunoita tutkimusmetodeihin 1 [Windows to research methods 1]. 5th ed. Jyväskylä: PS-Kustannus.

Appendices

Appendix 1. Interview questions in Finnish

Taustatiedot

- Yrityksen toimiala
- Yrityksen koko - henkilöstön lukumäärä / liikevaihto

Yrityksen sisäisen tietoturvallisuuden hallinta

- Noudatatteko jotain tietoturvallisuuden viitekehystä?
  - Miksi kyseinen viitekehys on valittu käyttöön?
- Miten arvioisitte yrityksen tietoturvan nykytason?
  - Onko yrityksessä nimetty tietoturvasta vastaava henkilö?
  - Onko kirjallista tietoturvapolitiikkaa?
  - Miten seuraatte ja käsittelette tapahtuneita tietoturvapoikkeamia?
  - Kehitättekö yrityksen tietoturvaa jatkuvasti havaintojen perusteella?
  - Miten tietoturva on yhdistetty muihin liiketoimintaprosesseihin, esim. riskienhallintaan, jatkuvuussuunnitteluun?
- Mitä sisäisiä tietoturvatoiminteita toteutatte itse?
  - Pyrittekö tuottamaan tarvitsemanne palvelut itse?
- Kuinka varmistatte riittävän sisäisen osaamisen?
- Miten näette tietoturvan vaikutuksen liiketoimintaan?

Tietoturvapalveluiden hankinta

- Mitä / mihin tarkoitukseen hankitte tietoturvapalveluita ulkopuoliselta toimijalta?
- Mihin hankitatarpeet perustuvat?
- Kuinka usein hankitte tietoturvapalveluita?
- Millä perusteilla valitsette palveluiden tuottajan?
  - Mitkä ovat tuottajan valintakriteerit?
  - Miten kilpailutatte palvelun?
- Miten arvioitte saamanne palvelun laatua
  - toimituksen / projektin aikana?
  - käyttöönoton jälkeen?
- Onko joskus käynyt niin, että saamanne palvelu ei vastaa tarvetta?
- Onko joskus hankinta jäänyt tekemättä, koska
  - soveltuvaa palvelua ei ole ollut tarjolla?
  - soveltuvaa palveluntarjoajaa ei ole löytynyt?
  - palvelun hinta on ollut liian korkea?
  - palvelusta saatavaa hyöty ei ole mitattavissa
- Puuttuuko markkinoilta jotain teille tarpeellista palvelutarjontaa?
- Näettekö, että hyvä tietoturva voisi olla kilpailuvaltti?

Appendix 2. Interview questions in English

Background information

- Line of business
- Company size – number of employees / economic turnover

Internal information security management

- Are you implementing any information security framework? (e.g. ISO 27001, VAHTI, …)
    - Why the framework has been chosen to be implemented?
- How would you evaluate the current information security maturity level within your company?
    - Is there nominated responsible person for information security?
    - Do you have written information security policy?
    - Do you monitor and process security incidents?
    - Do you enhance information security continuously based on the observations?
    - Is information security part of business management processes, e.g. risk management?
- What security functions you do implement internally?
    - Do you attempt to provide all the needed functions by yourself?
- How do you ensure adequate internal competence?
- How do you think information security impacts your business?

Procurement of information security services

- What or for what purpose do you procure information security services from external vendors?
- What is the basis for procurement needs?
- How often do you procure these services?
- On what basis do you choose vendors?
    - What are the selection criteria?
    - How do you run the competitive bidding?
- How do you evaluate the quality of services?
    - during the project / delivery?
    - after delivery / during the use?
- Have you encountered situations that service doesn’t fulfil the need?
- Have you chosen not to complete the procurement because?
    - there has been no suitable service / product
    - there has been no suitable provider / vendor
    - price has been too high
    - benefit from the service could not been justified
- Are there offerings missing from the market that you could use?
- Do you see that good information security could provide a competitive edge?
- Any other experiences / topics not mentioned earlier?

Appendix 3. Cover letter for interview request in Finnish

Arvoisa vastaanottaja

Teen opinnäytetyötäni varten tutkimusta tietoturvapalveluiden hankinnasta, toimituksista ja niihin liittyvistä kokemuksista erilaisissa organisaatioissa. Tutkimusta varten kerään aineistoa haastattelemalla henkilöitä, jotka osallistuvat tietoturvapalveluiden hankintaan sekä niihin liittyviin projekteihin. Opinnäytetyö on osa ylemmän AMK:n Cyber Security -tutkintoa, jota suoritan Jyväskylän ammattikorkeakoulussa.

Säännöllisesti julkisuudessa esille tulevat eri yritysten tietojärjestelmiin kohdistuvat tietomurrot ja näiden seurauksena julkisuuteen vuotaneet erilaiset arkaluontoiset tiedot ovat lisänneet yritysten kiinnostusta kehittää omaa tietoturvaansa. Tietoturvapalveluiden myynti onkin kiihtyvällä tahdilla kasvava ala, josta monet yritykset koittavat saada oman osuutensa. Tutkimuksen tavoitteena on selvittää, millaisena yritykset kokevat eri palveluntarjoajien tarjonnan, näiden vertailun ja sovittamisen oman organisaation tarpeisiin.

Tutkimukseen osallistuminen on täysin vapaaehtoista ja haastateltaville toimitetaan etukäteen haastattelurunko tutustuttavaksi. Haastateltavalla on oikeus jättää vastaamatta kysymyksiin sekä kieltäytyä haastattelusta. Haastatteluista saatu aineisto on luottamuksellista ja tuloksia tullaan käsittelemään anonyymisti. Aineistoa tullaan hyödyntämään ainoastaan tutkimustarkoitukseen ja se hävitetään, kun opinnäytetyöprosessi on saatu päätökseen ja säilytystarve on päättynyt. Haastatelluilla on oikeus saada kopio haastattelussa syntyneestä aineistosta tarkastettavakseen.

Tulen mielelläni haastattelemaan teitä paikanpäälle, mutta haastattelu voidaan järjestää myös verkkotapaamisena. Haastatteluun on hyvä varata aikaa noin tunti. Toivon, että olisitte halukkaita osallistumaan tähän tutkimushaastatteluun. Voitte myös välittää tämän kutsun edelleen, mikäli koette että joku toinen henkilö organisaatiossanne olisi kiinnostunut osallistumaan haastatteluun.

Ystävällisin terveisin
Lasse Kurkela
K7416@student.jamk.fi