Petri Keltanen (1704104, CSKT17SY)

Measuring outsourced Cyber Security Operations Center

Thesis
Master's Degree Programme in Cybersecurity

2019

South-Eastern Finland
University of Applied Sciences

Kaakkois-Suomen ammattikorkeakoulu

Author (authors)	Degree	Time
Petri Keltanen	Master's Degree Programme in Cybersecurity	November 2019

Thesis title

Measuring outsourced Cyber Security Operations Center

49 pages

Commissioned by

Elisa Oyj

Supervisor

Vesa Kankare

Abstract

Organisations have noticed the importance of cyber security in today's threat landscape. There can be situation where organisations realise that their knowledge about cyber security is not enough, so they bought outsourced Cyber Security Operations Center, CSOC. Organisations usually want to know how their outsourced Cyber Security Operations Center is operating. That is the reason why metrics are needed. The main object of this study is research how outsourced CSOC can be measured. Objective was combining the qualitative and quantitative methods of the measure.

The purpose of this research was to study how can outsourced Cyber Security Operations Center use customer survey as one metric and how customer survey can be created. There were also research how different metrics can be combined. There were also research how choose right metrics. Unfortunately, field study is missing from this study. This research has also best practice to implement a project to create metrics.

Because shortcoming of the field study, in this research peer review was made. Responders were professional team leaders and they had experience about cyber security. Feedback from peer review was positive, but there was also some criticism.

Keywords

CSOC, cyber security, metrics, Cyber Security Operations Center

Kaakkois-Suomen ammattikorkeakoulu

Tekijä	Tutkinto	Päivämäärä
Petri Keltanen	Master's Degree Programme in Cybersecurity	Marraskuu 2019
Työn nimi		49 sivua
Measuring outsourced Cyber Security Operations Center		
Toimeksiantaja		
Elisa Oyj		
Työn ohjaaja		
Vesa Kankare		

Tiivistelmä

Viime vuosina yritykset ovat heränneet tarpeeseen suojata heidän tietoverkkonsa ja päätelaitteet rikollisten verkkohyökkäyksiltä. Samalla yritykset ovat havainneet, että heidän omat taitonsa ja aika ei välttämättä riitä kaiken epäilyttävän tietoverkko- ja päätelaitetoiminnan seuraamiseen. Näin ollen yritykset ovat alkaneet kartoittaa Cyber Security Operations Center-palvelun (CSOC) hankkimista ulkoistettuna palveluna. Koska CSOC ulkoistettuna palveluna on vielä uutta, niin yrityksillä on vaikeuksia hahmottaa palvelun toimivuutta. Tätä ongelmaa ratkoo CSOC-palvelua tarjoavan yrityksen tuottamat mittarit. Tämän työn tavoitteena oli selvittää millä tavalla CSOC-palvelua voi mitata. Tavoitteena oli yhdistää laadullinen ja määrällinen mittaaminen.

Tässä tutkimuksessa selvitettiin miten asiakaskyselyä pystyisi käyttämään CSOC-palvelun yhtenä mittarina. Samalla mietittiin myös keinoja yhdistää eri mittareita yhdeksi mitattavaksi asiaksi. Tutkimuksessa myös tutkittiin, millä keinoilla voisi erilaisia mitattavia asioita laittaa tärkeysjärjestykseen. Ikävä kyllä työstä jäi puuttumaan käytännön toteutus, joten sen puutetta paikattiin vertaisarvioinnilla. Tutkimuksessa on myös selvitetty parasta käytäntöä toteuttaa projekti, jossa suunnitellaan yrityksen mittaristo.

Koska tutkimus ei edennyt käytännön osuuteen mittariston luomisesta, tehtiin korvaavana tutkimuksena vertaisarviointi, jossa kyberturvallisuuden parissa työskennelleet esihenkilötason johtajat kertoivat näkemyksensä esitetystä tavasta mitata CSOC-palveluita. Vertaisarvioinnin tulos oli positiivinen, vaikka haastatellut henkilöt esittivät myös kritiikkiä. Organisaatiomuutosten takia työn hyöty työnantajalle on selvittämättä.

Avainsanat

CSOC, kyberturvallisuus, mittarit, Cyber Security Operations Center

CONTENTS

1 INTRODUCTION

Organisations have noticed that they need to protect cyber assets and are ready to invest in cyber security. After some large cyber-attacks, organisations have realized that they have lost money and a brand reputation, because of being victims of a data leak (Coughlin, 2017). The worst-case scenario is that organisations might lose business opportunities, because some of their customers think they are not reliable business partners.

There is also some regulation from governments which gives a cause to protect critical assets. If organisations fail to meet the governmental regulations and there is a data leak of sensitive customer data, there is a legal action and economic sanctions for organisations. In directive 95/46/EC (General Data Protection Regulation) European Union has decided that a fine can be up to 10 000 000 euro or 2% of the total worldwide annual turnover (Official Journal of the European Union, 2016.).

Some organisations outsource their Cyber Security Operations Center and they need a way to measure how cyber security companies produce their service. As Flyktman (2016, 31) states, a growing number of outsourcing put some pressure against companies that offer cyber-security services. Also, upper management wants to know how their employees succeed. These are the reasons for measure metrics in cyber security.

The traditional metrics have some disadvantage when measuring cyber security. Cyber security is somewhat different from the traditional services like the Internet connection. For example, if the Internet connection is not working an organisation can measure how fast it is fixed. In cyber security, speed is not always the right way to handle incidents. (Haaranen, 2017.)

There is also a big knowledge gap between organisations that need cyber security and companies that offer it. For instance, technical jargon and reports that are offered to organisations might be useless because nobody understands them. To make reporting easier, there should be clear metrics that are easy to read.

This research will studies methods and metrics for creating metrics for outsourced Cyber Security Operations Center. Because shortcoming of a field study this research focus to previously studies. This research also describes best practices for a design project to create metrics.

2 USED TERMINOLOGY

In this research, the word metrics refers to a unit that can be measured. Metrics can be any activity which offers information (Cambridge Dictionary, n.d.). For example, metrics can indicate how many incidents an analyst has handled per day.

Key Performance Indicators are objective values that measuring metrics produce. Usually, Key Performance Indicators measure how well an employee or an organisation has performed. (Cambridge Dictionary, n.d.) For example, if the organisation has an object that the analyst should handle ten incidents per day and the analyst handles more than that the analyst has fulfilled the requirements of Key Performance Indicators.

The Cyber Security Operations Center is a department in an organisation which handles incidents related to cyber security (Kowtha & Nolan & Daley, 2012,470). For example, if the organisation has a data breach usually Cyber Security Operations Center leads the operation that investigates how malicious and wide the breach was.

3 RESEARCH OBJECTIVES, METHODS AND QUESTIONS

This research focuses on the pragmatic methods of measuring the metrics of cyber security services. The main goal is to develop a method that can be used in measuring Key Performance Indicators. The research problem was that there was not appropriate method to measure the outsourced Cyber Security Operations Center.

The main question in this research is how the outsourced Cyber Security Operations Center can measure how it is performing. During the research process, also some additional questions have risen:

- What is the best practice for a customer survey?
- What is the best way to compare metrics and choose the right metrics?

This research also examines, how to combine good qualitative and quantitative metrics in cyber-security. What is the efficient mechanism to compare different metrics? For example, when an upper management needs to know how their team has performed, they can produce qualitative metrics from a customer survey and from some quantitative data.

This research will pay attention on the best practices in using customer surveys as a part of qualitative metrics. What kind of questionnaire produce the best answers? The idea is how the outsourced Cyber Security Operation Center can measure how it is performing.

The sources of data are collected background information from previous research and literature about metrics. Naturally, a part of the research is done with an empirical method with conversations between business units and colleagues.

Method of this research was a development research (Kananen 2011, 151) because this research was part of a development project of a Cyber Security Operations Center that Elisa corporation offers to customers.

The literature chapter has evaluated the conclusions of previous studies and literature. Also, in the literature chapter has some evaluation of how the used metrics and methods could use in the outsourced Security Operations Center.

It was noticed during the literature and research evaluation that previous studies do not match a need for modern outsourced Cyber Security Operations Center. End customers demand more qualitative reports and analyses more than traditional metrics.

In conversations between business units had an idea of using a customer survey (Ropponen, 2017). Because given reason, part of this research was studied how conduct the customer survey and implement the customer survey into the KPI-metrics.

This thesis has also a chapter about how to design a project which describes how to conduct a project regarding measuring the outsourced Cyber Security Operations Center. The chapter will help to implement created metrics and describes problems that might appears during the project.

Because organisational changes, there were no field study of this research. Peer review were conducted because there were a need for opinions about studied methods of creating metrics.

4 PREVIOUS RESEARCH AND LITERATURE

Several studies have been executed on cyber security metrics. Although those studies are valid, they presume that an organisation has the ability to measure several services in their IT-infrastructure. There is a lack of research on how the Cyber Security Operations Center can be measured.

Usually other studies and the previous literature describe the process and structure how of metrics should be build. Literature usually offers the lists of pragmatic metrics in an appendix. Those are useful metrics, but is presumed that the Cyber Security Operation Center has access to all data and rights to do necessary remediation.

There are some studies that only focus on one metric. For example, the research might only consider incident handling time or the cost of the incident. From the perspective of the outsourced Cyber Security Operations Center, looking at only one metric is not meaningful. It might lead to a situation where indicators show that everything is ok but the end-customer is not satisfied with the outsourced Cyber Security Operations Center.

Another lack of previous and literature is qualitative metrics. There are mentions that there is a possibility for qualitative metrics but there is no research that would describe good qualitative metrics.

One reason for this lack might be the nature of these metrics. Usually qualitative metrics is questions, such as customer surveys, are comprised of questions, and they are under the business secret.

4.1 Developing a Metrics Framework for the Federal Government in Computer Security Incident Response

Sritapan, Stewart, Zhu and Rohm (2011) have conducted a research about Developing a Metrics Framework for the Federal Government in Computer Security Incident response. The research mainly focuses on three types of measurement: Cost, time and quality combined with Audience Based Metrics. There are three audience groups: administrative, operational and external. Every group has its own views and needs to the metrics. Sritapan et al. (2011, 63) also add objects which need to determine by organisation itself.

In general, research by Sritapan et al. (2011) recommends that there should be an object that is measured, and the results should be presented based on the audience. For example, the financial department might not be interested in how fast incidents are handled, but they want to know what the cost per incident is.

From the point of view of outsourced Cyber Security Operations Center measuring costs can be difficult. As Sritapan et al. (2011, 60) demostrate very well, a cost is easier to assign to tangible elements. In the outsourced Cyber Security Operations Center, there are tangible elements but measuring those elements is not in the focus. As described in this research, it is more important is how satisfied the end-customer is and how that satisfaction can be measured.

Because of the nature of the research by Sritapan’s et al. (2011), there are no recommendations which are the metrics that should be measured. However,

the research gives a good overall perspective to measuring security metrics and the incident handling process.

4.2 A methodology to measure and monitor level of operational effectiveness of a CSOC

The research by Shah, Ganesan, Jajodia and Cam (2017) focuses on measuring and monitoring the level of operational effectiveness of the Cyber Security Operations Center. The authors use only one metric which is the incident handling time.

Shah et al. (2017) have the development value called Level of Operational Effectiveness (LOE). The research is very mature and Shah et al. have considered very well different phases of the alert analysis, can be seen in Figure 1.

A downside of the research is the lack of other metrics, as Shah et al. concentrate on the incident handling time. As mentioned before in this research, there is a disadvantage when using the time as the only metric. It will lead to a situation where analysts do their analysing as fast as possible but in a hurry analysts might miss something important which endanger customer IT-environment.

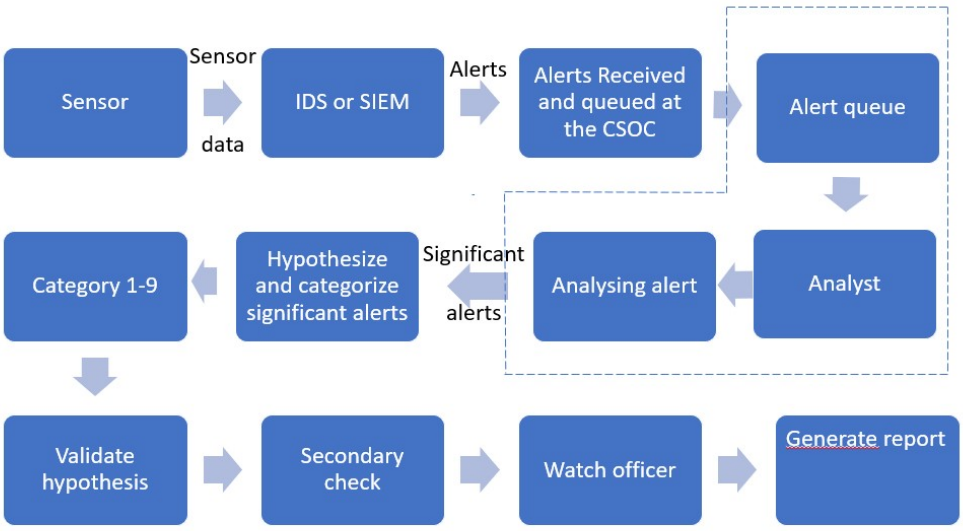

Figure 1. Alert analysis process (Shah et al. 2017, 3)

From the perspective of this research LOE could be one metric but not the only one. For example, LOE and the customer survey together would formulate KPI-metrics. This kind of a combination solve the problem that occurs when solely LOE is used as a metric.

4.3 IT Security Metrics

The strength of the Hayden (2010) book about IT Security Metrics is the information about how to build a project about security metrics. There are also good, practical hints to analyse the gathered data.

Hayden (2010) focuses on metrics at a high level. He describes very well important aspects of planning the metrics project. For example, Hayden brings forth the importance of documentation and conversation with stakeholders and employees.

The shortcoming of Hayden's book is samples of the metrics. In the book some metrics are described, but the metrics is not relevant to the outsourced Cyber Security Operations Center. It should be taken into account that the book is published in year 2010 when the cyber security was different than today. In the past, measuring security metrics concentrated more on costs than on cyber threats.

From the perspective of the outsourced Cyber Security Operations Center, the most important topic in the book is how to create the project and analyse data. After all, as the title of the book says Hayden's book is a framework for measuring security.

4.4 Pragmatic Security Metrics

A book by Brotby and Hinson (2013) offers good examples of the metrics, for instance, what to measure and how to compare the different metrics. There are also examples of the metrics to measure.

Brotby and Hinson (2013) notion is classified metrics with METAMETRIC-method. It is a good practice to decide which metrics are worth to measure. For example, if the organisation has doubts which metrics should be chosen as Key Performance Indicators, METAMETRIC-method will support choosing the right metrics.

A shortcoming of this book is that there is no mention about customer surveys. Neither are there any comments about outsourced Cyber Security Operations Center. This is not unusual in studies about security metrics. In general, the book by Brotby and Hinson is worth to reding.

4.5 SFS-ISO/IEC 27004:2016. Monitoring, measurement, analysis and evaluation.

Standard SFS-ISO/IEC 27004:2016 (2016) has been created to help organisations when they need to measure their state of the security. The standard has an appendix where example metrics are listed.

The standard is useful especially when the organisation is about to achieve the standard ISO/IEC 27001. The requirement for monitoring security is a part of the standard ISO/IEC 27001.

Since the standard is made for organisations directly, there is no part for outsourcing. The Outsourced Cyber Security Operations Center can use metrics that are mentioned in the appendix but generally there is no mention or metrics about outsourcing.

Of course, it is good practice to understand the basics of the standard. For example, there might be a situation where an end customer is applying standard ISO/IEC 27001 and therefore the outsourced Cyber Security Operations Center needs to meet the requirements of the standard ISO/IEC 27001.

4.6 Cyber Resiliency Metrics

Bodeau, Graubat, LaPadula, Kertzner, Rosenthal and Brennan (2012) made a publication about cyber security metrics to Mitre. Their publication is like SFS-ISO/IEC 27004:2016.

As Bodeau et al. describe (2012,1) their goal was to create metrics which help a wide scale of experts. That is the reason why there are many examples of what can be measured in the cyber security.

As the publication of Bodeau et al. (2012) is comprehensive there are some metrics that should be considered to the outsourced Cyber Security Operations Center. Those metrics are related to the incident handling time. For example, Bodeau et al. suggest that there is a chance to measure time when the incident has occurred and when it has been noticed (2012,18.).

Bodeau et al. (2012) do not mention a customer survey as a potential metric. They refer to a qualitative value scale (2012,4), but there is no research on the actual qualitative metric. The reason probably is that the Mitre is a state-aided institution and its main purpose is to offer assist to the United States government (Mitre,2019).

4.7 Performance Measurement Guide for Information Security

Chew, Swanson, Stine, Bartol, Brown and Robinson (2008) have conducted a comprehensive study about implementing security measurements into the agencies of The United States. Because of the nature of the NIST as a state-aided institution there are lots of references to laws and standards of The United States government. In general, the Cyber Resiliency Metrics by Mitre is more comprehensive.

Chew et al. (2008) have described very well measurement processes in details. Their publication is more to the head of an agency or to upper management since there are not so many technical observations. Instead, the focus is on processes.

Chew et al. 2008) also underline that when the organisation has the first results there should be a project to improve results as described in Figure 2. The processes studied by Chew et al. (2008) are good to know when designing cyber security metrics measurement for the outsourced Cyber Security Operations Center. The process is roughly the same kind when talking about a governmental agency or a private sector company.

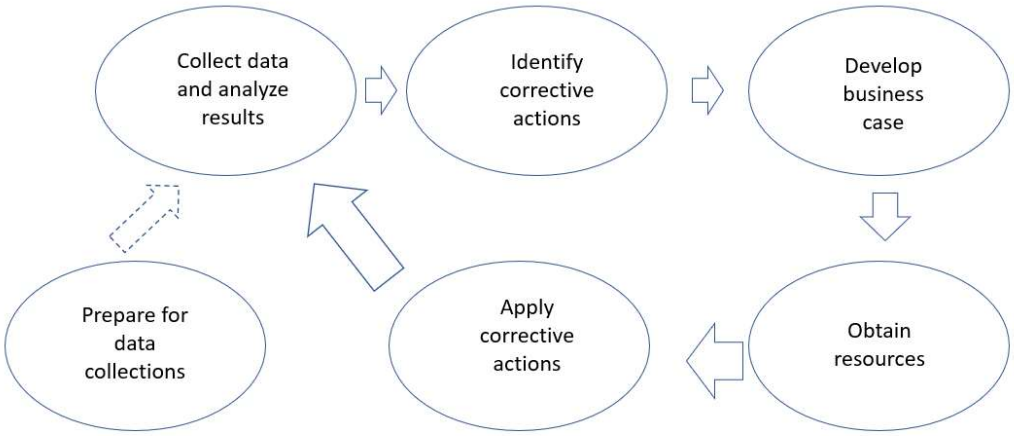

Figure 2. Information Security Measurement Program Implementation Process (Chew et al., 2008,35)

The main disadvantage of the publication of Chew et al. (2008) is lack the of pragmatic metrics examples. There are some, but they are not good for the outsourced Cyber Security Operations Center. However, it must be remembered that the publication has been done for the agencies of The United States.

4.8 Security Metrics: replacing fear, uncertainty, and doubt

The book Security Metrics: replacing fear, uncertainty, and doubt by Jaquith (2007) is slightly different than other books about the security metrics. Jaquith has a descriptive style. There is no list of the possible metrics but Jaquith tells what can be measured. There are also good points about the visualization of the measurement report.

Jaquith (2007) has raised some issues about a customer survey which is more than other literature concerning security metrics. Also, Jaquith has good points about the methods of analysing data.

It can be said that Jaquith describes what metrics should measure and how he would design them. Should also remembered that the book has been written in 2007 and the cyber security landscape is now different than those days.

4.9 A survey on systems security metrics

Pendleton, Garcia-Lebron, Cho and Xu (2016) have done research on security metrics. The main idea of the study is to divide measuring security metrics in four sub-categories: the metrics of system vulnerabilities, the metrics of defence strength, the metrics of attack/threat severity, and the metrics of situation understanding. The sub-categories are described more detailly in a Table 1.

	Vulnerability metrics	**Defence metrics**	**Attack metrics**	**Situation metrics**
Measurement	Vulnerabilities of an enterprise or a computer system	Strength of defence mechanism	Strength of attacks	situation, including system's security
Target	An enterprise system or computer system	Defense mechanisms employed at systems	Attacks against systems	Evolution of situation and environment
Types	User's vulnerabilities, interface-induced vulnerabilities, software vulnerabilities	Preventive, reactive, proactive and overall defense strength	Different type of attacks, like botnets and malware spreading	Security state, security incidents, security investment

Table 1. Metrics and Measurement of Vulnerabilities, Defenses, Attacks, and Situations (Pendleton et al. 2016, 7)

Although the study by Pendleton et al. (2016) is very comprehensive, it can be questioned how pragmatic the method is for measuring cyber security. The research framework might be possible to implement into the organisation if the Cyber Security Operational Center it is managing by the organisation.

For example, Pendleton et al. (2016,8) propose that there can be measuring metrics based user behavioural or how weak passwords are. From the perspective of the outsourced Cyber Security Operational Center those metrics are not essential. Usually the outsourced Cyber Security Operational Center has nothing to do with the password policy or cannot affect how users behave e.g. visit malicious websites.

While the research from Pendleton et al. (2016) is not pragmatic, there are some suggested metrics that should be considered to be implemented. Such as like a delay in incident detection (Pendleton et al. 2016,22). The outsourced Security Operations Center should serve the end customer as fast as possible.

4.10 Model-Based Quantitative Network Security Metrics

Ramos, Lazar, Holanda Filho and Rodrigues (2017) have conducted a comprehensive study about network security metrics. As Ramos et al. (2017, 2730) states, Model-Based Quantitative Network Security Metrics are still under development. That is the reason why implementing the study of Ramos et al. (2017) to the Outsourced Security Operations Center is complicated because there are not any pragmatic examples.

Even though the research of Ramos et al. (2017) has a lack of pragmatic examples there is a good figure about security metrics which can help perceive different aspects of security metrics. As described in Figure 3, network metrics is just one target type of metrics. Outsourced Cyber Security Operation Center is more in category “organisation”.

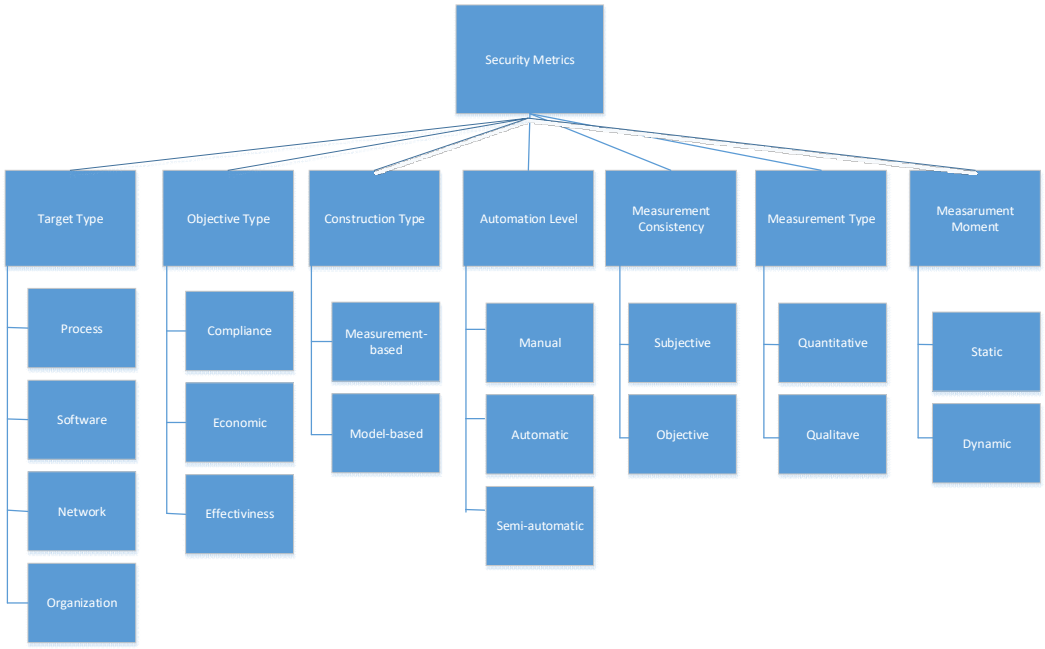

Figure 3. Classification of Security Metrics (Ramos et al. 2017,2707)

4.11 Risk analysis supported by information security metrics

Breier and Hudec's (2011) research about security metrics is a framework for controlling different metrics. As Breier and Hudec (2011, 398) mention, their research focus on a formal mode of metrics.

Research of Breier and Hudec (2011) has a good approach to measure metrics. A shortcoming of the research is there is no field study. As the research of Breier and Hudec (2011) is only theoretical there is no evidence if the formal mode of the research is working or not. Breier and Hudec (2011, 398) recognize the shortcoming of field study and suggest that future research would study how to find right metrics.

The research of Breier and Hudec (2011) is worth consideration. Especially the idea of about using weight with different metrics is interesting and should be studied further. There is also a possibility that the whole formal mode as described in the re-search of Breier and Hudec (2011) would work on the outsourced Cyber Security Operations Center. The interesting part of the research of Breier and Hudec (2011,396) is how to implement a company size

and an annual budget into the formal mode. Because the nature of this research is theoretical there is no opportunity to continue the research of Breier and Hudec (2011).

5 BACKGROUND OF THE METRICS

5.1 Cost based metrics

One way to measure the success of cyber security services is financial more accurately the relation between costs and benefits (Brotby&Hinson 2013, 33-34,94). Although giving numbers to upper management is easy it tells quite little from the technical perspective. Particularly, if the goal is to measure cyber security in a more complex way.

For example, an organisation may invest in an antimalware software and count how much money it has used per cleaned file. This is a totally fine method, if the organisation wants to measure how the antimalware software works. However, in depth it does not measure technical readiness to prevent cyber-attacks in depth. Antimalware detections are more reactive so there should be proactive methods (Ranne 2018).

There is always a risk that cost metrics give misleading results (Brotby&Hinson 2013, 95). This can be demonstrated with antimalware detections: What if there are no infected files? Is the conclusion that we do not need the antimalware software because costs versus detections benefits are poor or is the antimalware software broken?

5.2 Metrics based on Service Level Agreement

In an agreement between a customer and a service provider is specified how fast, for example, a broken service is fixed. This is called Service Level Agreement (SLA). In cyber security SLA is justified in fast reaction. Some indicators are so strong that fast reaction is justified (Haaranen 2017). For example, some IP addresses are malicious and when there is data traffic to malicious IP address automated alert is triggered.

There might be an issue with SLA metrics when measuring incident handling time from start to the end. Sometimes there are long time periods when analysts follow data traffic and analyse if the first indicator is false positive or if a threat is real.

In the worst-case scenario, SLA metrics may lead to poor management of an incident. Analysts know that they have, for example, eight hours to analyse and remediate alert from the Security Information and Event Management (SIEM). Because of a hurry, analysts might close the incident with close code “False positive” because they want to stick into a timeframe of the SLA. The worst-case scenario in this case: is that the incident was not false positive and an organisation becomes a victim of the data breach.

It is not good either if there are too many false positive incidents which go to field engineers or end customers. It damages the credibility of Cyber Security Operations Center. A great number of false positives possibly causes a delay in incident handling when field engineers prioritize their daily jobs. They might think: “It is again one false positive” and ignore the incident.

5.3 Problems with traditional metrics

As described in the previous paragraphs, there are some problems with the most used traditional metrics. Those metrics do not fit in the modern, possibly outsourced Cyber Security Operations Center. Traditional metrics are generally matched to a situation where all information technology is controlled by a single company. In the modern business model it is a rare situation. Because IT-infrastructure is decentralized measuring just one service is not useful.

Because of outsourcing there might be a situation, where a customer has two or more vendors from which they have bought their IT-infrastructure. In the described situation, there is a possibility that the outsourced Cyber Security Operations Center analyst notices an incident and reports it to the customer. Because the customer company does not have visibility or technical knowledge it forwards the incident to a third party. The whole process takes time and if the

outsourced Cyber Security Operation Center has a total incident time from alert to resolve as SLA it gives wrong metrics because the analyst handled the incident and reported it to the customer.

It should be remembered that good metrics should not be easy to create. It is easy to create metrics but are the created metrics useful? There might be a situation, where metrics are indicating a positive signal but when an organisation inspects what this the metrics really measure they are not useful or measure the wrong things.

A problem of outsourced Cyber Security Operations Center is handling a repetitive incident. There might be a situation, for example that the same Intrusion Detection System alert gives a signal. A cyber security analyst knows it is critical and needs to be taken care of. For some reason, a customer does not take care of it. The customer might think it is not so critical. If metrics are related to Intrusion Detection System alert they give a wrong result. Of course, there should be some actions for metrics and disperse Intrusion Detection System alert from metrics.

One reason for the cyber security knowledge gap between organisations is the lack of skilled employees. An organisation might want to build Cyber Security operations Center but cannot find employees. (Oltsik, 2019.)

Because of the reasons discussed above, there is a need to provide reliable, easy to understand metrics for the Cyber Security Operations Center. Good cyber security metrics gives confidence to all, from upper management to a customer that cyber security services are doing what they are supposed to do.

5.4 Creating metrics

When planning measuring metrics one task is choosing how many metrics are intended to use. There should be a conversation with stakeholders, such as an end customer or an upper management, concerning their need for information given by metrics.

Sometimes on upper management is more interested in allocation of a cost than how some technical service is working. On the other hand, from the customer perspective it is more interesting to know how the outsourced Cyber Security Operations Center is technically working and helping them.

Naturally, there is a chance to offer the same metrics to a customer and an upper management, as described in Figure 4. It is also time saving method for instance whom management metrics. It all depends a need for different stakeholders.

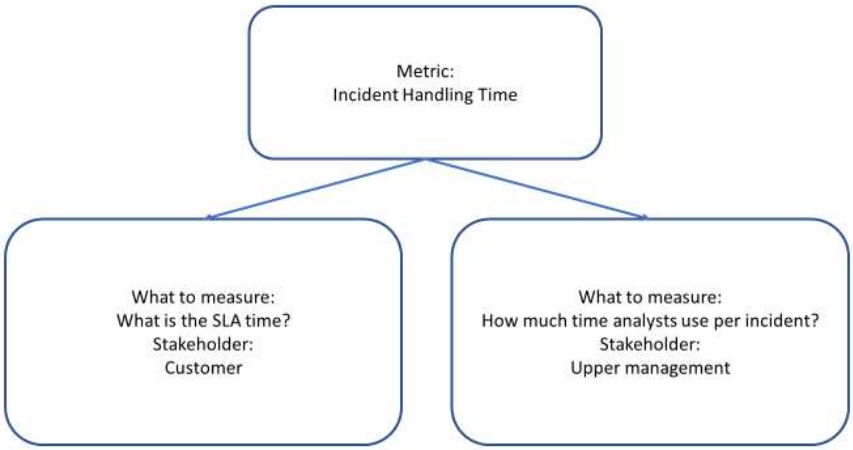

Figure 4. Using same metric for different stakeholders

Stakeholders should give clear indicators what they want to measure. After getting indicators from stakeholders, an organisation should formulate metrics. Goal-Question-Metric -method, also known as GQM, is a simple process to improve or develop organisation metrics. As Hayden (2010, 38) describes, the first step is set-up goals that are not measurement goals. Based on those goals more specific questions should be asked. Final step is identifying how an organisation can produce metrics that answer those specific questions. In Figure 5. there is an example of GQM-process.

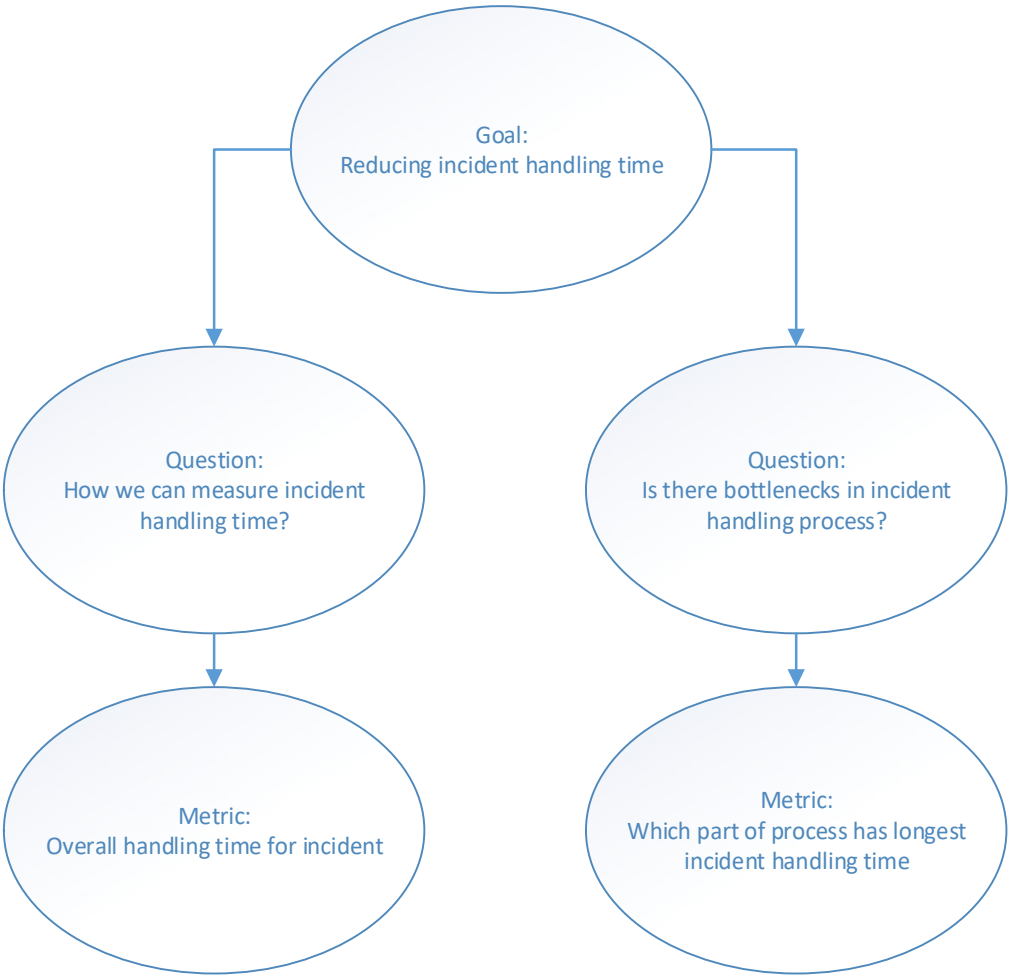

Figure 5. GQM-method (Hayden 2010, 37)

It should also be noted that there is a possibility for qualitative metrics. Qualitative metrics are more demanding than quantitative. In some cases, qualitative metrics are based on customer surveys. Questions in customer surveys should be easy and quick to answer.

Jaquith (2007) gives some criticism against customer surveys. He demonstrates that answers may vary between answerers. Jaquith has a point in his critic. However, in the outsourced Cyber Security Operations Center the customer survey will be made for the end customer. Usually there is one person representing the end customer who will answer the survey. So, there is no variation in answers per end-customer.

Jaquith (2007) also notes that answerers might have biases that affect the answers. That is true, but in the outsourced Cyber Security Operations Center,

exaggerate by generalising it, can be said that “Customer is always right”. This means that if an end customer gives bad grades in a customer survey it is the truth; the end-customer is not satisfied no matter if the end-customer is right or wrong.

When transforming qualitative data into quantitative form, there should be some consideration how to rate questions. As Bodeau et al. (2012,4) describe, qualitative value scales also need to be clear or presented by examples. Otherwise, there is chance for different calculations by stakeholders.

5.5 Collecting metrics

When planning metrics, it is good to understand how the metrics are produced: How much there is automation and which system they are taken. If some metrics are reported because their measuring is easy and the upper management demands something. There is a risk that metrics produce inaccurate results (Hayden, 2010,32.). There should always be careful evaluation of the used metrics.

Log management is an important part in cyber-security. It is important in incident handling and detecting malicious activity in a network, but it is also used in measuring metrics. As standard ISO 27004:2016 (2016) describes, organisations should be monitoring produced data. As represented in Figure 6., there are many benefits which may help the upper management or specialists in decision making.

If an organisation has an incident response platform (IRP), it should be evaluating if there is a chance to produce a report about metrics. In the best scenario, the incident response platform produces the automated report with right values. On the other hand, it is possible that there is a lot of manual work in producing a report and counting values of a metric. From the company’s viewpoint, all manual work is expensive. If a team leader uses a lot of time calculating metrics with spreadsheet, the leader is not doing a core work; leading a team (Ropponen, 2017.).

Besides automated reporting, occasionally there should be manual evaluation from the results of the automated reporting. The purpose is investigating if an automated report is right or not. Manual evaluation is also important because used metrics should be transparent. For example, the organisation has the metrics for a merit pay. If a worker doubt that metrics are wrong, there should be a process to show manually how metrics are produced. This should be considered when choosing a tool and services which will produce the metrics. (Ropponen, 2017)

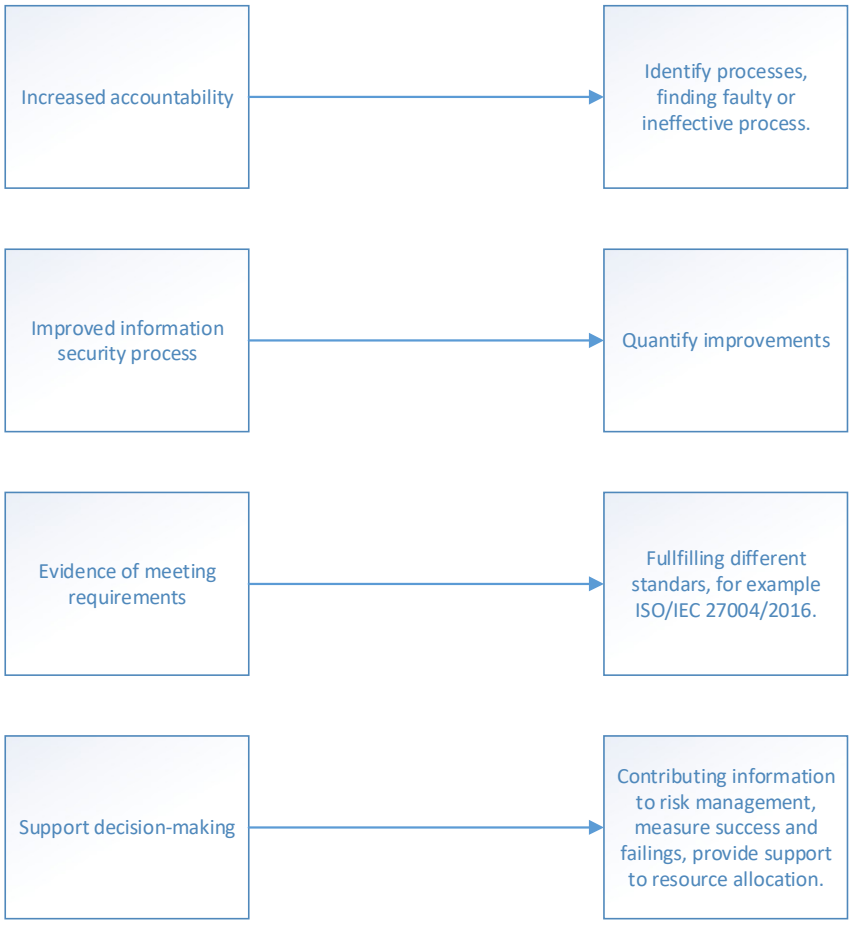

Figure 6. Benefits of monitoring and analysing produced data (ISO 27004:2016,2016,8)

6 STRUCTURE OF THE CUSTOMER SURVEY

6.1 Questionnaire

When creating a research questionnaire, before the main questions there are usually exclusion or screening questions. Those questions will help to create

more accurate and high-quality survey data. There are also classification questions which offer background information to the interviewer for example sex, age and location. (Brace,2008,32.)

When the questionnaire is asking how the outsourced Cyber Security Operations Center has performed there are no requirements for exclusion, screening or classification questions. The reason for this is that questions are pointed to the end customer representative who is in charge of cyber security. The interviewer usually knows end customers in person so there is no need for questions that concerning respondent's background.

Exclusion, screening and classification questions are often used when respondents are unknown, and the number of respondents is high. In this research the number of respondents is limited. Several limited respondents affect that the customer survey is not quantitative. As Kananen (2011,39) mentions, when there are a couple of answers, then the research is qualitive. For example, if there would be hundreds of answers, then the customer survey would be quantitative.

Personal questions should be placed at the end of a questionnaire. When the interview proceeds, the responder is more relaxed and feels more trust in a situation (Kananen,2011,90). Although in the outsourced Cyber Security Operations Center customer survey has not personal questions to the responder, there might be questions that are business critical to the organisation that responder represent. The interviewer should consider, are questions of this kind comparable to personal information. If they are, business critical questions should be placed at the end of a questionnaire.

As Brace (2008,41) states, a flow chart of questions can help avoiding routeing issues and it gives an overview that all topics are covered. The general rule is that a questionnaire should start from general questions and then move to more detailed questions. As seen in Figure 7 the flow chart is an easy way to have an overview of questions and how the questionnaire is built. For example, the flow chart helps to identify if the questions are in the right order and how the questionnaire is routed.

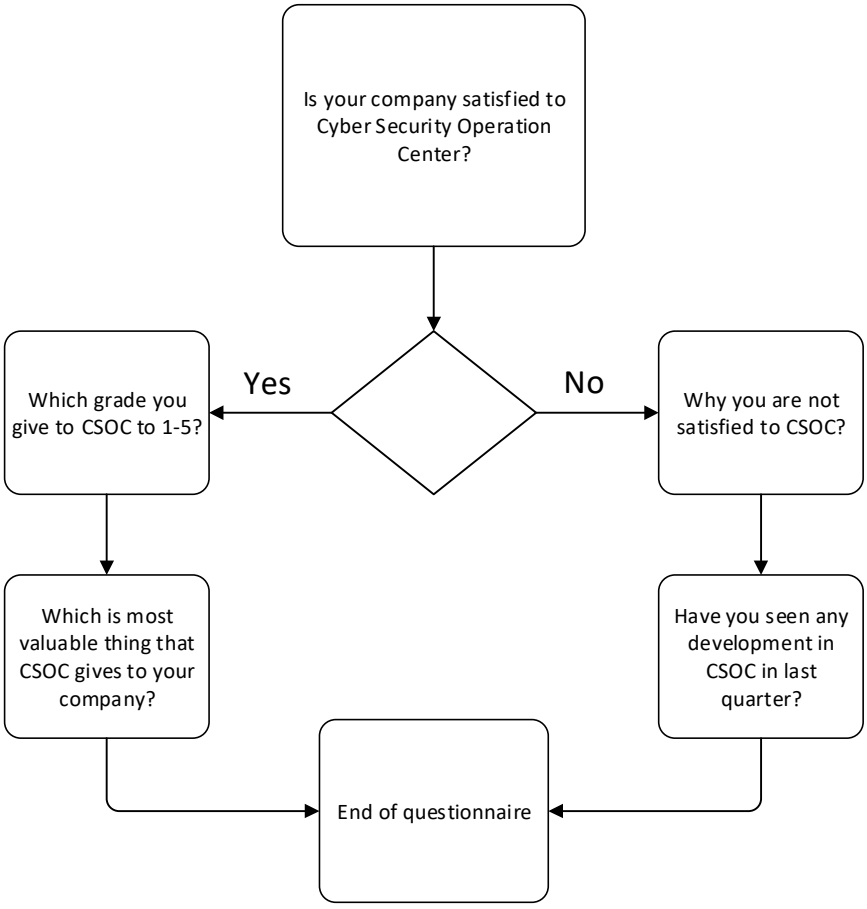

Figure 7. Example of the flow chart (Brace 2008, 42)

6.2 Types of the questions

There are different types of questions. In this research open and closed questions are used, for example See table 2. As Brace (2008,47) describes, closed pre-coded question is easy to handle an in electronic questionnaire. Data will be stored automatically to a database.

Pre-coded questions are easy to modify to KPI metrics if in the questionnaire uses ratio scale -questions. For example, if a question is like “Which grade you give to the CSOC to 1-5 (where 1 is the lowest score and 5 is the highest).”, can be moved to KPI metrics almost as is: If the answer is 5, then outsourced Cyber Security Operations Center has performed very well.

In the questionnaire there is also a possibility to use open questions with pre-codes. Open questions with pre-codes are open questions where presupposed answers are pre-coded. In the questionnaire should also be space for answers which are not pre-coded. (Brace, 2008,47.)

Question type		Question example
Open question	Open-ended	Why you are not satisfied to CSOC? Please answer in your own words.
Closed question	Pre-coded	Is your company satisfied to Cyber Security Operation Center? Please answer Yes or No.

Table 2. Example of question types (Brace 2008, 47)

6.3 Types of the customer survey

There are several ways to produce a customer survey. As Brace (2008,22) describes, there are three main methods: Interviewer-administered, self-completion and interviewer-supervised self-completion.

This research will focus on the web-based self-completion of the customer survey. Because of low numbers of end-customers, can be presumes that a response rate is 100%. There is some criticism about web-based self-completion (Brace, 2008,33), such as misunderstood with questions. This can be avoided with interviewer-supervised self-completion.

When using an interviewer-supervised self-completion, a responder can ask advice from an interviewer if there are some unclear questions. Otherwise the interviewer does not interfere the answering process. (Brace, 2008,23) There is chance that the response rate is higher, when the interviewer and the responder meet face-to-face. For example, if a link to a web-based survey is sent by an email, there is chance that the responder does not open the survey. A personal request to fill the customer survey is stronger than email.

A data collection to a database is easier when using a web-based survey versus a paper survey. If the customer survey team is using paper surveys, there is a manual phase where all results are transferred to the electronic database.

When using a web-based customer survey the manual phase of the data collection is easier. Also, the data is available as soon as the responder has responded to the survey.

6.4 Summarizing customer survey

A customer survey is not the easiest data source for metrics. A problem is not technical, for example, transforming results from the customer survey to metrics. Rather the problem is more how to create the customer survey in the first place. As described in the preciously chapters, creating a customer survey requires some dedication and background information.

In an optimal situation, there is a possibility to get help from people who make customer surveys as their full-time job. This will help creating a credible customer survey. Also, when someone outside a project team reviews the questions, there is a possibility to find problems, such as questions that are designed badly.

When answering the customer survey, an end-customer feeling may affect to result. For example, if the end-customer has a bad day, the answers may not reflect how the outsourced Cyber Security Operations Center has actually performed. The end-customer may vent bad feelings on the customer survey. Naturally, this will lead to wrong results in terms of metrics.

The customer survey is also a very ruthless metric. There might be a situation, where the outsourced Cyber Security Operations Center has generally performed very well, but just before the customer survey the outsourced Cyber Security Operations Center has failed with one incident. The end-customer will remember this one failed incident over all other incidents that were handled successfully. This problem can be reduced by using a face-to-face survey, where the interviewer underlines that answers should reflect a longer time period.

The project manager should also remember that in the organisation there might already be a customer survey for end customers. Before sending the

customer survey to the end customer, there should be a review is there any other surveys to the end customers. As Glazer (2015) states, it is irritating as the perspective of the end customer if receiving too often customer surveys.

7 COMPARSION OF DIFFERENT METRICS

When creating metrics from different sources, there should be a careful review of how metrics from different sources are emphasized. For example, if the organisation uses metrics such as the incident handling time and the uptime of a service there should be careful review if those sources are equally good.

As Flater (2018, 66) states, there are some matters that should be taken care of when comparing metrics and results; For example, a misleading scale in different alerts. The outsourced Security Operations Center might get alerts from an Intrusion Detect System and from a firewall. The Intrusion Detection System alert severity might be at a scale 1 to 3, but on the firewall alert severity scale is at 1 to 10. When measuring alerts, it should be carefully considered how malicious alerts are from different sources.

There might also a be situation that the organisation's upper management gives more recognition to the incident handling time than uptime of the service. If the accentuation of those two metrics is equal the metric is not good.

To mitigate the problem of not equally good metrics, the different weight for metrics can be used. As Breier and Hudec (2011) describes, the different weight of metrics helps the organisation to fulfil the defined objects.

Table 2 represents the difference between two measurements. As shown in table 2, there is a difference when a weight of the used metrics is changed.

The mathematic formula used in table 3 is defined through equation 1. Weight tells how important the metric is. Grade is formed from raw data after it is analysed.

$$TotalGrade = (GradeOfX * WeightOfX) + (GradeOfY * WeightOfY \quad (1)$$

Option A			
Metric	Grade (1-10)	Weight	KPI-grade
Incident handling time	4	50,00 %	2
Service uptime	10	50,00 %	5
		100,00 %	7

	Option B		
Metric	Grade (1-10)	Weight	KPI-grade
Incident handling time	4	80,00 %	3,2
Service uptime	10	20,00 %	2
		100,00 %	5,2

Table 3. Difference between measurements

Under the column “Metric” there are incident handling time and service up-time. These are the metrics that are measured in this example. Grade scale is 1-10, where 1 is the worst grade and 10 is the best grade.

Column “Weight” demonstrates what is a weight between two metrics. In table 2 option A has the equal weight between metrics. When metrics are trans-formed in to KPI-grade and are the summation of KPI-grade is 7.

In a case that the organisation is using option A and the upper management is focusing on reducing Incident handling time it can be said that the metric is in-appropriate. Total grade is 7 which is above average. However, the more meaningful metric grade to the upper management is below average. This leads incorrect information to the upper management. In the worst-case sce-nario, incorrect metrics lead to incorrect conclusions and actions. For exam-ple, if the upper management has made a statement that the grade should be more than 7 and the Incident handling time is our main priority it can be said that in the option A grade 7 gives a wrong result.

If the organisation uses option B from table 2, the weight of the Incident han-dling time is 80% and the Service uptime is 20%. With these ratios grades represent better the way upper management has thought if the Incident han-dling time is the organisation priority.

Overall grade is more truthful in option B than in option A. In option B overall grade is 5,2 and the grade of the Incident handling time is 4. The difference

ratio between overall grade versus the grade of the Incident handling time is 1,2 when in option A difference ratio is 3. In this example, the low difference ratio gives more truthful information to the upper management.

The method of weighted metrics will give an overall grade on how the outsourced Security Operations Center has performed, if metrics are carefully chosen and taken from the whole technical range of the outsourced Security Operations Center. For example, the upper management chooses metrics for overall incident handling time, first response time and service uptime. Those metrics will measure how fast the outsourced Security Operations Center will handle customer incidents. Service uptime is measured because if a service is down, it can lead data to a breach, when the service does not produce any alerts.

8 CHOOSING THE RIGHT METRICS

One of the hardest things is choosing the right metrics. As Brotby and Hinson (2013,75) describe, there are several metrics that can be measured. The problem is to choose the right metrics.

Brotby and Hinson (2013,77) have developed a PRAGMATIC method into choosing the right metrics. In the PRAGMATIC method there are nine Metametrics (Predictability, Relevance, Actionability, Genuineness, Meaning, Accuracy, Timeliness, Independence and Cost) which each have an individual rating ratio. Score of the metric is the average from nine Metametrics, as demonstrated in table 4.

It can be said that the Brotby's and Hinson's (2013) PRAGMATIC method is useful when developing metrics into the outsourced Cyber Security Operations Center. PRAGMATIC method gives good view how meaningful the metrics are for the stakeholders. For example, if stakeholders want to use metrics measuring how many SSH-attacks have been done the PRAGMATIC method helps to perceive if the number of SSH-attacks is the best source for metrics.

Brotby's and Hinson's (2013,81) PRAGMATIC method Metametrics are:

Predictive: How good a metric is to predict trends. An outcome of the metric is correlating with metric.

Relevant: How relevant metrics is in organisation goals.

Actionable: Is there a chance to do anything for getting the better outcome of the metric.

Genuine: How credible the metric is.

Meaningful: How meaningful the metric is. The metric should give value to the stakeholders.

Accurate: How accurate the metric is. Value of the metric should be consistent over several measures.

Timely: How long it takes from collecting metric to correcting actions.

Independent: How objective the metric is.

Cost: What is cost of the metric, when it is collected, analysed and used.

Metametric/Metric	SSH-attacks to DMZ	Incident Handling Time	Service Uptime
Predictive	30 %	80 %	80 %
Relevant	60 %	80 %	80 %
Actionable	20 %	70 %	50 %
Genuine	50 %	90 %	95 %
Meaningful	20 %	100 %	100 %
Accurate	60 %	80 %	100 %
Timely	20 %	70 %	50 %
Independent	100 %	80 %	90 %
Cost	50 %	90 %	70 %
Score	**46 %**	**80 %**	**74 %**

Table 4. Example of Metametrics

In Table 4 three different metrics on the PRAGMATIC method have been compared. A stakeholder may want to, for example, use SSH-attacks to DMZ as key metric. Still when using the PRAGMATIC method, the stakeholder sees that the score of the SSH-attacks is much lower than the Incident Handling Time or the Service uptime.

In the best scenario, the stakeholder understands that the SSH-attacks is not the best metric and does not want to use it. There is probably some conversation about how the score has been formed. When presenting metrics there should be good arguments of how different metrics are rated.

When thinking about the ratio between different metrics a score from the PRAGMATIC method is useful. As it can be seen from table 3, there are three metrics and dispersion of the score is quite clear. The Incident Handling Time score is 80%, Service Uptime 74% and SSH-attacks to DMZ 46%.

If the organisation and a metrics developer trust the PRAGMATIC method, the ratio of the Incident Handling Time is the most important metric. It is followed by the Service Uptime and the SSH-attacks to DMZ. Low score from the SSH-attacks to DMZ can lead to a conclusion that the metric has to be excluded because the stakeholder or the metrics developer notice that the metric is not useful.

8.1 Summarizing choosing metrics

Choosing the right metrics is the most essential phase of the project. As described in the previous chapters, there should be conversation between stakeholders and employees on what metrics are good and accurate. After the conversation, there should be an idea of what are the parts of an organisation or a process that are measured.

If there are several metrics that could be useful, this research recommends using the PRAGMATIC method by Brotby and Hinson (2013). The PRAGMATIC method is useful when comparing different metrics. The PRAGMATIC method will also help to sort different metrics.

The Brotby's and Hinson's (2013) PRAGMATIC method is also beneficial when metrics have been chosen and the organisation begins to think about a ratio of the different metrics. For example, inside the organisation there might

be different views if the metric A is better than metric B. After using the PRAGMATIC method, it is clear that the metric B is better, and it should give the better ratio than metric A.

It should also be remembered that there can be several metrics that can be used. When management is choosing the metrics, it should be considered if all metrics are equally good. If the management or a project group notice that some metrics are more important, then there is a possibility to use weighted metrics.

9 DESIGNING PROJECT

9.1 Creating a Project Plan

As Hayden (2010,160) describes, a project plan is the first phase when creating a project about metrics. Because it is written in one document, it is a guide to how to complete the project. Minimum requirements of the project plan are the goals of the project, the project deliverables and the milestones of the project. Those requirements help to review if the project follows the timetable.

Meetings between a project manager and stakeholders should include a review status of the project. Goals and timetables should be checked. Also, there should be a chance to add or remove goals or other requirements from the project plan. There might be a situation that stakeholders have changed their goals or for some other reason the goals must be changed. Therefore there should be regular meetings. It is recommended that those meetings are documented in the project plan. (Hayden, 2010,161)

It should also be remembered that the project does not end when the results have been obtained. There be should also be a review of the results and a Plan of Action of how to correct problems. The project should not end even after the problems are corrected. Measuring metrics should be a continuous job. Only a cycled, monitored process can ensure that the problems do not re-occur after some time. (Chew et al. 2008,40.)

Hayden (2010,161) also pinpoints that documenting during the project is important. After the project It helps to memorize what has been done. Recommendation is that all members of the project add their documents to the project plan. For example, when auditing the project conclusion it is useful that all documents are available: For instance, were there problems and how those problems were solved.

9.2 Gathering and protecting metrics

The first step in data collection is to find out if some of the metrics are available from already existing sources. If there are no existing sources for metrics then those sources or databases should be created. The best practice is that all the data is in the same database. In a situation where the centralized database is not possible a project analyst should gain access to all the databases that are needed in creating metrics. (Hayden, 2010,163.)

When the necessary data has been gathered the data is stored and protected. This is important because the used data should remain the same. If the data changes between collecting and a presenting the results the results are not valid. (Hayden, 2010,164.)

As Chew et al. (2008, 16) state, standardized data reporting is important. It will ensure the data validity. For example, if a financial department of the organisation takes an incident report from a different database than other departments, it will give misleading results.

There are also legal and ethical perspectives about gathering the data, especially when the collected data involves personal information. There are General Data Protection Regulation (GDPR) which gives strong regulation to organizations on how to use personal data.

There should be careful review of what information an organisation collects. For example, is there a need to collecting a personal data, such as respond-

ents age, sex, location, or other personal information. This is especially important when collecting data with a customer survey. There might be a temptation to ask more information than is needed, because it is easy.

Because of the GDPR, respondents have the right to review and delete personal material from the data. This is an important legal point, which should be taken into account in project planning. If planning related to the GDPR fails it might lead to legal consequences.

9.3 Analysing data

According to Hayden (2010,165), there are two main concerns when analysing data. The first is that one the analyst might choose results that are biased because the analyst has they own theory or opinion concerning the results. Another is representing results without proper data analysing.

The project plan is for great help when creating objective analyses of the results. When the project plan is updated regularly the analyst can check and follow the goals anytime when needed. Those regular checks will support maintaining an objective approach to analysing the results. If the analyst has some preconception about the results, review from the project plan will help to follow the pre-defined goals. (Hayden 2010,165.)

The analyst should also see “through the numbers” and ask themself, “Why numbers are like these?”. As Jaquith (2007) states, knowing different statistical techniques will help the analyst to tell the audience what something is not just a measure of something.

Sometimes when the results are collected, stakeholders want to know them as soon as possible. This might put pressure on the analyst to do the analyses in a hurry. This can be avoided if the timetable of presenting results is in the project plan. This will give some time to work in peace and produce better analyses. (Hayden,165.)

Hayden (2010,165) also states that an unexpected finding from the results puts pressure on the analyst. For example, there might be a situation where the stakeholder is not satisfied with the results. When the project plan is well organized and updated it is much easier for the analyst to justify the conclusion.

The gap analysis helps identifying problems when predefined target values do not match the results. Gap analysis hopefully support recognizing what is the problem. When the problem is defined it is time to make corrective actions. Those actions can be for example, providing education to employees or making configuration changes to hardware. (Chew et al. 2008,37.)

Data analysing methods depend on if the data is quantitative or qualitative. Quantitative data is usually contain of numbers that can be analysed in different ways; fort example, by standard deviation or mean, depending on what is the goal of the data analysis. (Hayden,2010,122,128) Qualitative data can also be mixed with quantitative data. It gives more perspective to the analyst how analysed data correlated. (Hayden,2010,141)

Furthermore, qualitative data can be used as quantitative data after transforming it into numerical form. As Hayden (2010,143) highlights, professionals in cyber security usually do not use customer surveys as a data source. Customer surveys are not daily tasks of cyber security professionals. Generally, the professionals do not use them, because they do not have any experience of surveys or creating customer surveys. (Hayden, 2010,140.)

9.4 Presenting results

When presenting the results, it should always be considered who is the target audience. For example, if the target audience is the upper management without any technical knowledge a presentation should focus on things that the audience understands. In this case, it could be things such as finances or productivity. (Brotby & Hinson 2013,302-303.)

It is a good practice to represent results to personnel especially if there will be some action which involves personnel (Hayden 2010,166). Good result presentation with walkthrough is additional important, if metrics is also a KPI-metrics or metrics affect to the merit pay. Usually, personnel are interest how much merit pay they earn. Presentation to the personnel also adds transparency and trust to the metrics.

As Jaquith (2007) states, visualization is important when presenting the results. When visualization is done in an appropriate way it will help the upper management to understand what security is. When planning visualization too simple and too complicated charts should be avoided. When a chart is too simple it is not efficient. The chart might take too much space from the presentation compared to the information that the chart offers. The same kind of problem occurs if the chart is too complicated and essential information might vanish. (Jaquith,2007.)

Flatter (2018,76) states very well that in the documentation should be clear when presenting the results. There might be a chance that the stakeholders misunderstand what has been measured. Flatter is recommended when presenting results there would be no mention about future actions. As said, it might give a misleading view for audience.

Before starting to write the document about results it should be considered in which format the results are documented. Although the project plan is usually made as a slideshow-presentation a textual summary would be useful if after some time someone else need to review the results. (Hayden,2010,167) For example, if someone leaves an organisation a new employee perhaps would like to know what have been done in terms of metrics. If there are just project plans and some slideshow-presentation it might be time consuming to read all notes of the project. The textual summary would help a new employee to understand all essential data from a project plan.

9.5 Implementing repairing actions

It is not enough that the organisation has good metrics and those metrics produce valid results. There might be a situation, where metrics show that organisation has a problem: for example, a customer survey grade is too low.

As Chew et al. (2008,38) describes, the root cause should be solved first and examined how it could be repaired. For example, if the customer survey grade is too low there should be a review of the survey and research on what is the reason behind the low grade. Then corrective actions should be prioritized. The organisational guidelines should help prioritizing those corrective actions. (Chew et al. 2008,38). If there are no organisational guidelines, at least there should conversation with stakeholders on how to prioritize repairing actions.

When repairing actions have been prioritized work should start for correcting those actions. It is important to monitor by different sources if the implemented corrective actions are those actions working or not. (Chew et al. 2008, 40.)

9.6 Summarizing the Project design

As presented in this research, creating cyber security metrics is not a simple project. There are many details that must be taken into account. If a project group has an attitude “Let’s just measure something” it can lead to poor results in terms of the metrics. The results might look good on theory but in practice metrics may not measure employees core working.

A project plan with a timetable will help a project group to ease the pressure from the upper management. If there is no timetable, the upper management might put some pressure on finishing the project. Too strict timetable or pressure from upper management might lead to too fast analyses. If the analyses are done in a hurry results might be false.

As Valkama (2018) states, employee’s work is related to how the measuring is done. For example, if Key Performance Indicator -metric is incident handling

time, it can be said that the employees concentrate on fast incident handling. This may lead to a situation where incidents are just closed fast and the root cause of incidents is not found. In some cases, the same incidents occur regularly. If there would be a little bit more time for analyses the employees could find the root cause of the incident so that it could be fixed.

When the right metrics are chosen, an automated measuring of the metrics should be thought. The automated collection would release the workload from the employee who is responsible of the metrics. Should also be remembered that automated measuring is probably more reliable than manually created metrics. When metrics are created manually there is always a risk of human error. When the automated report of the metrics is created the risk of human error is not so significant. (Chew et al. 2008,12.)

In a project design it is possible to use different kind of flow charts and figures to maintain the focus of the project. For example, using Ramos et al. (2017) Classification of Security Metrics (Figure 4) would help the Project Manager to notice all issues related to security metrics. In Figure 8. is ideal situation is presented: There is a project plan that includes all phases of the project. When there is proper planning and enough time to analyse results the project has better chances to succeed.

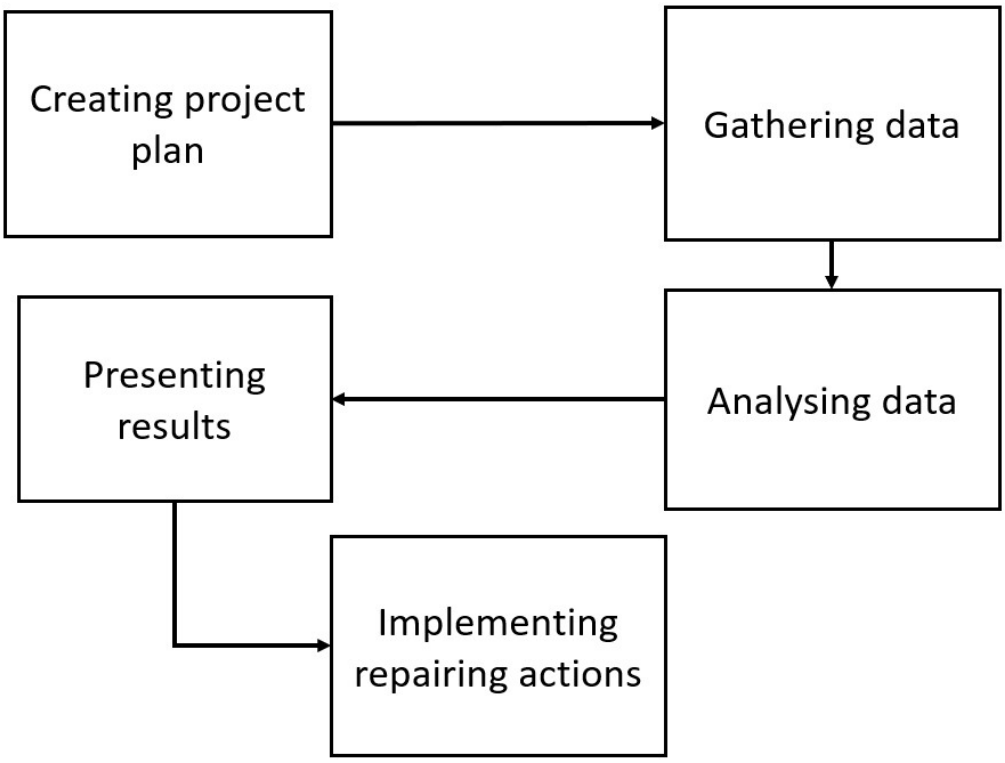

Figure 8. Phases of the project

Unfortunately, there can be a situation where the metrics are just ordered from the upper management. It can lead to a situation where the employees are not satisfied with metrics or the metrics do not represent the actual situation. If the upper management has strong opinions concerning metrics it is important to focus on how to present results. When a presentation is good there is a better chance that the upper management will accept the proposed metrics.

10 PEER REVIEW

As a part of this research interviews were conducted. The reason for the interviews was a lack of field study. In terms of the interview, responder's anonymity was secured. Before the interview a responder got an email where the idea of weighted metrics and forming them was explained. The main question was "Do you think that the method presented in this research could be a good way to measure the outsourced Security Operations Center?".

10.1 Responder A

Responder A has a strong background in leading a team and skills on cyber security. Currently responder A is not in a managerial position.

Responder A points out that “you get what you measure”. For example, the outsourced Security Operations Center measures how fast incidents are handled, the quality of analysing incidents might be lost. The analysts will focus more on speed than the root cause of the incident. Responder A also mentions that the background of stakeholders will affect what to measure. For example, the upper management is interested in different metrics than team leaders. Although metrics as such are out of the scope of this research, responder A has good arguments. The background of stakeholders and nature of metrics are important to understand.

When the question, “Do you think the method presented in this research could be a right approach to measure the Outsourced Security Operations Center?” is asked, responder A has a positive attitude towards this research. Responder A’s main consider is a lack of field study. He also wonders what would be used as metrics in practice. With the responder A, there was also a good conversation on how to use the gathered metrics. In terms of the customer survey, responder A suggests that especially if results are poor, there should be a meeting with a customer to find out, what are the reasons for poor results. After that, a process of improving a customer experience should be started.

10.2 Responder B

Responder B has a strong background of team leading. Responder B has also some experience of leading the outsourced Security Operations Center.

Responder B points out that the weighted method presented in this research is not related to any standards. Because the weighted method is not standard some stakeholders might be sceptic to use it.

Criticism towards non-standard metrics is valid especially when stakeholders are end-customers. To avoid a problem with the non-standard measuring method responder B suggests different metrics for customers and to internal users. For example, in terms of the customers only Service Level Agreement metrics could be implemented and when measuring the outsourced Cyber Security Operations Center to upper management, weighted metrics could be used.

Responder B also raises question of what the weighted metric score is. It is a number but does it include some correlation to something else. For example, the value of weighted KPI metrics may be 4, but is it a good or a bad value? Responder B asks a good question. It is important to evaluate if values are good or bad. Generally, stakeholders should have an opinion concerning good values. For example, if the metric is measured at a scale 1-10 the stakeholder could say that they think value above 8 is good.

Naturally, there was some conversation on what should be measured. Responder B points out effectiveness and service availability. For example, if the analyst does not receive IDS-alert because the IDS is down it might compromise end-customer security. That is the reason why it is important to measure service availability. It should also be remembered that the weighted metric measures how the overall performance of the outsourced Cyber Security Operations Center if the metrics are carefully chosen. For example, a combination of service uptime, Service Level Agreement and overall incident handling time would give an overall view on how the Outsourced Cyber Security Center has performed.

11 DISCUSSION

The main results showed that previous studies mainly focused just one or two metrics. Often previous studies focused on metrics like cost which is not useful for outsourced Cyber Security Operations Center. Some of the suggested metrics of previous studies can be used by outsourced Cyber Security Operations Center but there should be carefully review what metrics to use. According this study, when measuring outsourced Cyber Security Center should take

consideration needs of different stakeholders, like an end customer and an upper management. Recommended practice would be combining different metrics.

Because the previous studies had problems to match the criteria of the outsourced Cyber Security Operations Center in this research were studied the weighted method, which will help outsourced Cyber Security Operations Center to combine the different metrics. This thesis also described how to create a customer survey and how to combine a customer survey as a part of the metrics. A good practice to choose metrics is the PRAGMATIC method. When there is a need to compare different metrics, there is a possibility to use the weighted method. This research will give a framework for the future studies.

Furthermore, in this research has studied best practice for the project to create and implement the KPI-metrics into the organisation. It is important to remember that good project take care transparency of how the metrics are created. Transparency of the metrics give confidence through the organisation that the metrics is meaningful.

Unfortunately, this research has a shortcoming of a field study. Future research on weighted metrics should focus on implementing a project that utilizes weighted KPI-metrics. As can see results of the peer review, field study is needed to deeper analyses of the weighted method. Both responders were cautious about the weighted method, because it is not in general use.

Interesting a research topic would be comparing an organisation’s current KPI-metrics and the metrics created by the weighted method. The main idea would be using the same data. Then an analyst would have a good opportunity to compare metrics that are created in different ways. Comparing the organisation’s current metrics and metrics that are created by a weighted method would also give some results concerning it the weighted method is useful. As responder B points out, there are no standards or comparable KPI-metrics in the industry when using the weighted method.

When comparing the organisational data by which the metrics are created, there is also a possibility to focus on comparing different metrics. For example, the organisations current metrics could be evaluated with PRAGMATIC-method. This would offer some insight into the current metrics.

It is also possible to study best practices of a customer survey: Especially, when a customer survey is designed for end-customers. Also, there should be research on how to design questions and how questions should be arranged. This research could be multidisciplinary. In a workgroup there could be specialists who know technical aspects and people from the marketing department. It can be said that technical specialists are not experts in creating a customer survey. That is the reason why people from marketing department are needed, because they have more experience of customer surveys.

12 CONCLUSIONS

The objects of this thesis were achieved. The main object was to study how the outsourced Cyber Security Operations Center can measure how it is performing. During the research also additional questions about the best practices for a customer survey were brought to the fore. This object was also achieved. Another additional question was “what is the best way to compare and choose the right metrics?”. This object was also contributed to.

This thesis is more pragmatic than some other studies or literature on cyber security metrics. It can be said that this thesis offers an easy approach to those who want study or create cyber security metrics. This thesis considers several aspects that are needed when designing the project and measuring the outsourced Cyber Security Operations Center. Future research should consider how to implement the customer survey as the KPI-metrics.

REFERENCES

Bodeau D.& Graubat R.& LaPadula L.& Kertzner P.& Rosenthal A.& Brennan J. Cyber Resiliency Metrics, Version 1.0, Rev. 1, 2012. Mitre Corporation.

Brace I. 2008. Questionnare Design, how to plan, structure and write survey material for effective market research. Kogan Page Ltd.

Breier, J. & Hudec, L. 2011. Risk analysis supported by information security metrics. Proceedings of the 12th International Conference on Computer Systems and Technologies - CompSysTech ’11.

Brotby, W. & Hinson, G. 2013. Pragmatic Security Metrics. Applying Metametrics to Information Security. Taylor and Francis Group.

Cambridge University. 2019. Cambridge Dictionary. WWW document. Cambridge University Press. Available at: https://dictionary.cambridge.org/ [Accessed 21 April 2019].

Chew E.&Swanson M.&Stine K.&Bartol N.&Brown A.&Robinson W. NIST Special Publication 800-55 Revision 1. Performance Measurement Guide for Information Security, 2008. National Institute of Standards and Technology.

Coughlin T. 2017. WannaCry Ransomware Demonstrates The Value Of Better Security and Backups. WWW document. Forbes. Available at: https://www.forbes.com/sites/tomcoughlin/2017/05/14/wannacry-ransomware-demonstrations-the-value-of-better-security-and-backups/#7842861f70b8 [Accessed 14 April 2018].

Flatter D. 2018. Bad Security Metrics Part 1: Problems. IT Professional (Volume: 20, Issue: 1, January/February 2018).

Flatter D. 2018. Bad Security Metrics Part 2: Solutions. IT Professional (Volume: 20, Issue: 2, Mar./Apr. 2018).

Flyktman J. 2016. Implementing Information Security Management System as a part of business processes Where to gain competitive advantage for ISMS?. Master thesis JAMK University of Applied Sciences.

Glazer R. 2015. Feedback Fatigue: Stop Over-Surveying Your Customers. WWW document. Forbes. Available at: https://www.forbes.com/sites/theyec/2015/06/15/feedback-fatigue-stop-over-surveying-your-customers/ [Accessed 9 April 2019].

Haaranen M. 2017. Security Analyst. Conversation November 2017. Elisa Oyj.

Hayden L. 2010. IT Security Metrics: a practical framework for measuring security & protecting data. McGraw-Hill Company.

Jaquith A. 2007. Security Metrics: replacing fear, uncertainty, and doubt. Ebook. Pearson Education, Inc. Available at: https://www.amazon.com/Security-Metrics-Replacing-Uncertainty-Doubt/dp/0321349989 [Accessed 03 December 2019].

Kananen J. 2011. Rafting Through the Thesis Process. Step by Step Guide to Thesis Research. JAMK University of Applied Science.

Kowtha, S. & Nolan, L. A. & Daley, R. A. 2012. Cyber security operations center characterization model and analysis. 2012 IEEE Conference on Technologies for Homeland Security (HST). IEEE.

The MITRE Corporation. 2019. WWW document. Available at: https://www.mitre.org/about/corporate-overview [Accessed 16 March 2019].

Official Journal of the European Union. 2016. PDF document. REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL. Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN [Accessed 14 April 2018].

Oltsik J. 2019. The Cybersecurity Skills Shortage Is Getting Worse. WWW document. ESG Blogs. Available at: https://www.esg-global.com/blog/the-cybersecurity-skills-shortage-is-getting-worse [Accessed 21 April 2019].

Pendleton M.& Garcia-Lebron R.& Cho J. & Xu S. 2016. A survey on systems security metrics. ACM Comput. Surv. 49, 4, Article 62.

Ramos A.& Lazar M.& Holanda Filho R.& Rodrigues J. 2017. Model-Based Quantitative Network Security Metrics: A Survey. IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 19, NO. 4, FOURTH QUARTER 2017.

Ranne S. 2017. Security Analyst. Conversation December 2017. Elisa Oyj.

Ropponen S. 2017. Manager, Professional Services. Conversation November 2017. Elisa Oyj.

SFS-ISO/IEC 27004:2016, 2016. Information technology. Security techniques. Information security management. Monitoring, measurement, analysis and evaluation.

Shah A.& Ganesan R.& Jajodia S.& Cam H. A methodology to measure and monitor level of operational effectiveness of a CSOC, 2017. Springer Berlin Heidelberg.

Sritapan V.& Stewart W.& Zhu J.& Rohm Jr. 2011. Developing a Metrics Framework for the Federal Government in Computer Security Incident Response. PDF document. Communications of the IIMA: Vol. 11: Iss. 3, Article 5. Available at: https://scholarworks.lib.csusb.edu/cgi/viewcontent.cgi?article=1170&context=ciima [Accessed 03 December 2019].

Valkama H. 2018. Security Analyst. Conversation September 2018. Elisa Oyj.