Jyri Salomaa

Measuring and Creating Situational Awareness in Cybersecurity:
The Requirements Specification for Situational Awareness and Metrics Platform

Master's thesis
Master of Cybersecurity

2019

South-Eastern Finland
University of Applied Sciences

XAMK
South-Eastern Finland
University of Applied Sciences

Author (authors)

Jyri Salomaa

Degree

Master of Cybersecurity

Time

December 2019

Thesis title

Measuring and Creating Situational Awareness in Cybersecurity: The Requirements Specification for Situational Awareness and Metrics Platform

67 pages
37 pages of appendices

Commissioned by

Veikkaus Oy

Supervisor

Vesa Kankare

Abstract

Cybersecurity and risk management are an inevitable part of organisations decision-making processes. Decisions needs to be made faster and more adjusted to the context. To understand the overall cybersecurity risks in organisation, the threat actors and the relevant information shall be available.

The objective of this master's thesis was to study the essence of measuring cybersecurity, the key elements and relevance of the cybersecurity related metrics. Additionally, this thesis concentrated on what are the general requirements for cybersecurity metrics platform, how to display the metrics, what are the sources of the metrics to create a holistic cybersecurity posture and situational awareness. The goal of this research was to find and define the relevant requirements for cybersecurity metrics and situational awareness platform.

Action-based qualitative methods were used in this research study. The theoretical part included the introduction of main cybersecurity and measuring concepts. During this phase, the cybersecurity metrics were collected from the theoretical research and publication available from cybersecurity frameworks. As part of the research, a questionnaire was prepared and analysed. Key persons from the target organisation were then interviewed.

The research showed that there appears to be many different definitions related to the term of 'cybersecurity'. Cybersecurity research, attacks, threats and new technology is constantly evolving. Measuring is important part of the cybersecurity situational awareness and organisation decision making. These processes need continuous improvement. In practice, this means that the cybersecurity metrics must be reviewed and refined periodically as stakeholders has different needs and views for relevant metrics that they would like use.

Keywords

cybersecurity, metrics, measuring, situational awareness, requirements

CONTENTS

1 INTRODUCTION

Cybersecurity has become as vital part of almost every corporate strategy. The world is now more digitalized in every aspect and companies must assure that business continuity failure or security breach do not, in the worst-case scenario, lead to bankruptcy. Failure to manage the organizations cybersecurity risks is likely to damage the digital business and expose the potential impacts beyond the business opportunities. (McMillan et al., 2018.)

In August 2011 Dutch certificate authority was compromised by cyberattack and investigations revealed that valid wildcard certificates for major service like google.com were created by the unauthorized persons giving them ability to impersonate and validate website certificates to users' browsers and to see all the web traffic to those services via man-in-the-middle attack. At the end, this security incident led the certificate company into the bankrupt and had broad ramifications to other certificate authorities. It also affected the end-users who rely and trust the web certificate system based on public key infrastructure. (Fisher, 2012; Prins, 2011.)

Interestingly, also in the finance credit-rating sector has raised an interest into the organizations cyber risks. Moody's, a United States based credit-rating company announced recently (CNBC, 2018) that they will start to include in their credit-rating evaluation of organizations risk to a major impact from a cyberattack.

Furthermore, security requirements are not just getting harder to fulfil but also the sanctions have become remarkable risk element, as we have learned from the recent EU data protection regulation (GDPR). In the GDPR, "*The supervisory authorities have the power to impose administrative fines for infringements of the regulation up to € 20,000,000 or in the case of an undertaking, 4 % of the total worldwide annual turnover – whichever is higher"* (Regulation (EU) 2016/679; European Union Agency for Fundamental Rights and Council of Europe, 2018).

Because of this, cybersecurity and risk management are an inevitable part of organizations management decision-making chain so that the decisions would be better, made faster and more adjusted to the context. To understand the overall security risk from the threat actors the relevant information must be available. It would not be easy to make decisions without having accurate information and metrics available. Jaquiteh (2007) argues that only those security metrics relevant to risk management shall be the interesting ones as they are helping decision making. He also claims that we need to understand, quantify, measure, score, package and trade the security risks similar as financial sector risks. The core idea introduced by him is related to the financial concept - “value at risk” (VaR), where risk is the target, summing up the daily number of financial exposures to loss and the metric will tell how far you are from the target. In risk management there is always some uncertainty left no matter how much time and activities are used in the organization for modelling the threats, effectiveness of security safeguards or defences. (Jaquiteh, 2007.)

Measuring the security is not just complex, but also quite hard to predict in the long run (Pfleeger & Cunningham, 2010). Cheng et al. (2014) argues that the security metrics should be also adjusted and fine-tuned to fit a specific organization and business goals. Without proper metrics, it is impossible to know and build your current security posture. These metrics needs to be also collected from various sources and visualized for cybersecurity situational awareness (CSA). The phrase, “what can’t be measured can’t be effectively managed,” is applying to cybersecurity performance measuring too. (Cheng et al., 2014.)

Cybersecurity is not just having as many of the technical safeguards in place or having the security information and event management systems (SIEM) in place correlating the security events data. Using the knowledge that I personally have gained, most companies are not just lacking that technical visibility like SIEM systems for technical metrics from logs and events from the information and communication technology (ICT) systems, but they also lack many other elements to measure holistic cybersecurity. Data and metrics from the business processes combined with the knowledge of the assets that needs to be protected needs to be considered. From all these aspects, overall security posture needs to be built nearly in real-time to react on security threats in time.

This research will focus on these cybersecurity phenomena that affect many organizations not only now but also in the future, in order to better achieve their business goals. The purpose of this research is to focus on the most relevant cybersecurity measuring and metric frameworks, research and literature and to identify key cybersecurity metrics, sources, and requirements for cybersecurity situational awareness.

2 RESEARCH

2.1 Research objectives

The objective of this master's thesis is to study the essence of measuring cybersecurity, the key elements and relevance of the metrics. Additionally, this thesis concentrates on how to visualise the metrics; what are the sources of the metrics and how to use them to build up cybersecurity posture for situational awareness.

This research topic is not just important for the target organization but for all companies that want to develop and know their holistic current state of cybersecurity. Target organization has already some basic security metrics in use but maturity of the measuring, reporting and especially using the metrics is not yet fully utilized. The target organization has created cybersecurity maturity objectives, roadmap and periodical reporting of cybersecurity metrics for situational awareness. The plan is to enhance and use the cybersecurity metrics and situational awareness as part of the risk management, decision-making and to drive improvement in the overall cybersecurity development processes.

Cybersecurity as such has many different aspects and can be approached from many different angles. There are also many different security institutions and frameworks that may have slightly different angles of entry. The goal of the research is to find and define the relevant requirements for cybersecurity metrics and situational awareness. Those requirements will be used in the target organization on the next phase when selecting the cybersecurity situation awareness and reporting platform of the metrics.

2.2 Research questions

The main research focus of this thesis is related to cybersecurity metrics. The metrics are the base sources to know the maturity level of cybersecurity. There is also very general thinking that cybersecurity is considered technology related issue only. To be able to use technology efficiently there needs to be processes and also people to operate them. All these aspects shall be measured and are included in the further study.

This thesis is aiming to answer following research questions:

1. What are the key elements of the cybersecurity metrics?
2. What kind of information for the metrics is needed from the company's critical assets, business and compliance point?
3. What are the main information sources for the metrics and situational awareness?
4. What are the needed requirements for the situational awareness system?

2.3 Research methodology and methods

The approach in this research study will be action-based qualitative research study. According to Kananen (2011), qualitative methods are suitable for research studies when phenomenon needs to be understood. Qualitative method helps us to understand the research problem, the factors and interdependencies that are unknown. The qualitative research process is divided into planning, data collection, analysis and interpretation phases. (Kananen 2011, 36-37.)

The research in thesis is separated into two parts. The first part includes the theoretical research available from cybersecurity measurements frameworks and metrics. The theoretical part also includes the introduction of main concepts and basis of this research.

Situational awareness in general is not a new concept. One of the earliest theoretical models for situational awareness is described by Endsley (1995). Endsley made situational awareness concept model for aviation. The concept was factored for both systems and individuals. Endsley dived the concept of the situational awareness process in to three different levels as seen in figure 1.

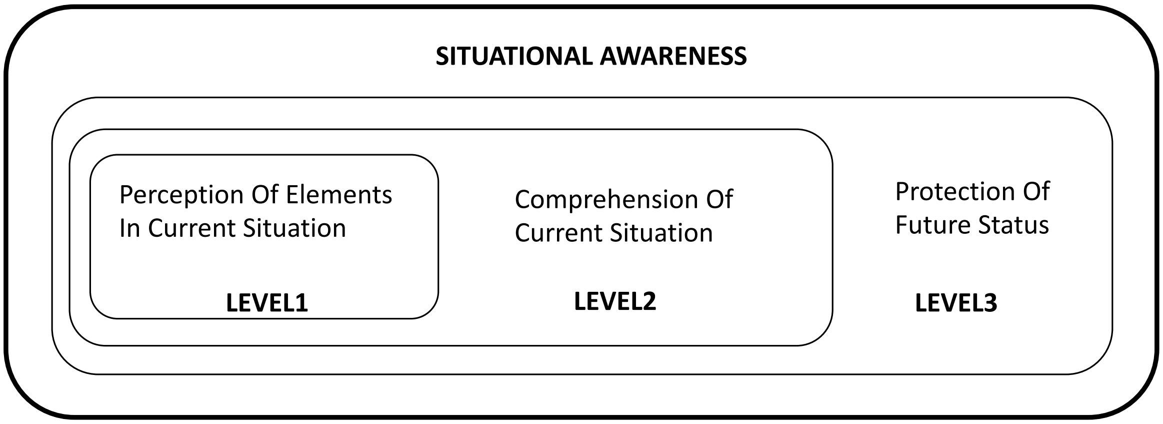

SITUATIONAL AWARENESS
Perception Of Elements In Current Situation
LEVEL1
Comprehension Of Current Situation
LEVEL2
Protection Of Future Status
LEVEL3

Figure 1. The levels of situational awareness (Endsley 1995, 35)

The process starts from level 1, where the relevant status, attributes and dynamics of the environment are perceived. On/at the next level, level 2, the elements from level 1 are disjoined for a decision maker to form a holistic picture of the significant objects and events. Based on the information and knowledge from previous levels, the decision maker would be able to proceed to the future actions in near term. (Endsley 1995, 36-37.)

Endley’s theory and concept would have similar elements that could be used for cybersecurity situational awareness. This theory will be used as a basis on this thesis.

The first part is also introducing available references from literature review, other cybersecurity metrics and situational awareness related research articles, known industry security standards and cybersecurity related websites. The reliability and validation of the literature sources and initial information about the cybersecurity metrics will be done on the second part.

The second part includes the empirical research methods based on the first part. As part of the research, a questionnaire regarding the current cybersecurity measurement practises will be prepared. Key persons from the target organization and relevant business unit people and security professionals are then interviewed. Persons will be selected in the later phase of the study. Based on the preliminary answers to questionnaire, the interviews will be held as a semi-structured to discuss about the answers. The interview questions are made after the theoretical part is done and initially cybersecurity metrics has been collected. The goal of the interviews is to get wider angle and other opinions on the selected metrics, how relevant the select metrics are for different business units and also how other organizations units are using the metrics to create situational awareness.

Interviews may also reveal if the metrics are missing some other relevant cybersecurity metrics or vital information. Questionnaire and interviews are not done anonymously but are not either published in public. Name, persons role and responsibilities will be asked in the questionnaire. This information will be used to analyses the answers. Also, the permission of recording the interview, storing of the record and the written memo from the interview for one year after the research has been published will be asked.

The results from the interviews will be analysed against the knowledge that has been gained from the first part. In the last phase the collected information and the requirements of situational awareness is compared to Endsley's key concepts. Based on the results the actual requirements for situational awareness system will be collected and documented.

2.4 Research limitations

The research is limited to the target organization current business scope, cybersecurity risks and operation model. The research only provides the metrics and suggestions relevant for the target organization but may be used for other similar companies. Validation of the metrics, effectiveness and choosing the cybersecurity awareness platform are excluded from this research.

3 CYBERSECURITY FRAMEWORKS AND TERMINOLOGY

Today, most organizations need to comply with several local, international or industry specific regulations. There are also numerous cybersecurity standards and frameworks available, which can help with the cybersecurity challenges to build and manage cybersecurity defence, establish good practises and reduce the cybersecurity risks in the organizations. However, there is no one-size-fits-all framework available and often the organizations might need to either due to regulation or other business-related requirement use multiple standards or at least customize their own security framework by using multiple cybersecurity frameworks to apply their needs. According to Dimensional Research (2016) research; Trends in Security Framework Adoption Survey, 84% of organizations in the US is using some type of security framework, and 44% use more than one framework. Based on the survey results (completed by 338 IT and security professionals in the U.S.) the most used frameworks are:

1. Payment Card Industry Data Security Standard (PCI DSS) (47%)
2. ISO/IEC 27001/27002 (ISO) (35%)
3. Center for Internet Security Critical Security Controls (CIS) (32%)
4. National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity (29%)

16% of the recipients are not using any cybersecurity framework. (Dimensional Research, 2016.)

Cybersecurity frameworks are considered to be a pre-defined and structured security control framework which can be utilized by different organisations. A framework controls are based on a set of rules and regulations or good practices. There are also other frameworks and standards that has at least similarity to previously mentioned cybersecurity frameworks. For example, The European Union Agency for Network and Information Security (ENISA) provides some cybersecurity guidance’s. In this research some other control frameworks are used also as a reference for the research topic. (Galan Manso et al., 2015.)

3.1 Definition of cybersecurity as a term

The ‘Cybersecurity’ is a rather young term as such and has many definitions and diverging understandings. According to the ENISA (Brookson et al., 2015) even the spelling of the word is differing within its context and source of the publication. However, as seen the cybersecurity terms goes by many names and no globally single or consistent cybersecurity term or definition exits. Sometimes the term is referred as digital security or IT security. (Brookson et al., 2015.) The following sub-chapters introduces a few general cybersecurity institutes and frameworks and their definition of cybersecurity terminology to open this phenomenon.

3.1.1 ENISA

ENISA does not provide a specific cybersecurity framework but has published a document for small and medium enterprises that has recommendations to improve the adoption of information security and privacy standards in general. In this document ENISA provides the guidance, recommendations steps and links them to existing information security and privacy standards (Galan Manso et al., 2015). In this document, ENISA is not using ‘Cybersecurity’ term. The document has few mentions about ‘cybersecurity’, ‘cyber threats’ and ‘cyber-attacks’ but they are not defined in the glossary nor in the document. ENISA has published a guide to determine the appropriate understanding of the term ‘Cybersecurity’ and to identify the gaps between several security standardizing organisations. Enisa’s definition in this document for the ‘Cybersecurity’ term is defined as (Brookson et al., 2015):

> “*Cybersecurity shall refer to security of cyberspace, where cyberspace itself refers to the set of links and relationships between objects that are accessible through a generalised telecommunications network, and to the set of objects themselves where they present interfaces allowing their remote control, remote access to data, or their participation in control actions within that Cyberspace.”*

Enisa also extends the above definition by stating that,

> *"SDOs are encouraged to embrace the concept of cybersecurity as the provision of security capabilities to apply to cyberspace. Existing use of the terms under the CIA paradigm when applied to single interfaces and single classes of object shall explicitly not use the term Cybersecurity."*

Enisa has also published another document; ENISA overview of cybersecurity and related terminology, where definition of cybersecurity is defined as (Tirtea, 2017):

> *"Cybersecurity comprises all activities necessary to protect cyberspace, its users, and impacted persons from cyber threats."*

Where term "Cyber space" is defined as:

> *"Cyber space is the time-dependent set of tangible and intangible assets, which store and/or transfer electronic information."*

ENISA is also extended in the same document the understanding of terminology for cybersecurity as:

> *"Cybersecurity covers all aspects of prevention, forecasting; tolerance; detection; mitigation, removal, analysis and investigation of cyber incidents. Considering the different types of components of the cyber space, cybersecurity should cover the following attributes: Availability, Reliability, Safety, Confidentiality, Integrity, Maintainability (for tangible systems, information and networks) Robustness, Survivability, Resilience (to support the dynamicity of the cyber space), Accountability, Authenticity and Non-repudiation (to support information security)."*

3.1.2 ISO/IEC 27032

ISO/IEC has a specific standard ISO/IEC 27032 for Cybersecurity which provides the guidelines for the Cybersecurity and the requirements to improve the state of the cybersecurity. This standard has defined the cybersecurity term as

> *"preservation of confidentiality, integrity and availability of information in the Cyberspace". In turn "the Cyberspace" (complete with definite article) is defined as "the complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form".*

3.1.3 NIST Cybersecurity Framework

National Institute of Standards and Technology (NIST), provides the standards and cybersecurity guidance used widely in the United States of America (USA). NIST has several glossaries in the documentation and has a quite short versions of the term 'Cybersecurity' in definitions. In the older documents, such as Glossary of Key Information Security Terms (Kissel, 2013) NIST is using following definitions for 'Cybersecurity' (Kissel, 2013):

> *"The ability to protect or defend the use of cyberspace
> from cyber attacks."*

In this document, the NIST is also referring to the 'Cyberspace' term as part of the cybersecurity definition and defines the 'Cyberspace' as

> *"A global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."*

On the newer documentation, for example in the Framework for Improving Critical Infrastructure Cybersecurity NIST is using following definitions (National Institute of Standards and Technology, 2018):

> *"The process of protecting information by preventing, detecting, and responding to attacks."*

In this newer documentation, NIST is not mentioning the "Cyberspace" term anymore and is using on prefix "cyber" and cybersecurity in all terms mentioned.

3.1.4 COBIT

Control Objectives for Information and Related Technologies (COBIT) is another commonly used enterprise governance and management of information and technology framework created by Information Systems Audit and Control Association (ISACA). COBIT provides the documentation to build and maintain the best-fit governance system with implementable set of controls for governance of information technology. Those controls include processes, organizational structures, policies and procedures, information flows, culture and behaviours, skills and infrastructure. The controls are including also the objectives that can be managed to the required capability levels. (Information Systems Audit and Control Association COBIT 2019 Framework: Introduction & Methodology COBIT, 2018). COBIT as such is not framework for cybersecurity but rather a risk-based control and governance framework. In the COBIT framework there are similarities and several references to other information security and cybersecurity frameworks. (Information Systems Audit and Control Association COBIT 2019 Framework: Governance and Management Objectives COBIT, 2018.) In the COBIT there are few mentions about 'Cybersecurity' term but those are not defined in the glossary nor in the document. ISACA is providing two public glossaries where the term 'Cybersecurity' is defined as:

> *"The protection of information assets by addressing threats to information processed, stored, and transported by internetworked information systems"*

(Information Systems Audit and Control Association Entire Glossary, 2018.), Information Systems Audit and Control Association Cybersecurity Glossary, 2018.)

3.2 Terminology in this research

According to research company Gartner (McMillan et al., 2018) each organization should pick its own terms, define and use them consistently. Gartner uses various security terms in their documentation interchangeably, throughout their research to reflect varied uses of the terms.

In the target organization term cybersecurity as such is not in use and the term is rather synonym for term ‘Security’ in general. Security in the target organization includes all the common security subcategories such as information security, risk management, physical security, personnel security, privacy, safety, operations security and business continuity. In the target organisation the meaning of cybersecurity term is mostly close to information security terminology. Information security and its assurance are considered as part of the overall risk management and it means the appropriate protection, under normal and exceptional circumstances, of information, systems, services and telecommunications by administrative, technical and other measures. In this research study the cybersecurity term is used but is also considered as synonym of security term in general. The used cybersecurity terminology may also have some variation based on the reference used, where the term is originally presented.

Also, other terms such as ‘measure’ and ‘metrics’ are used in this research in similar meaning but at the end, the point of the term is derivate from the measurement. Brotby, W. et al. 2013, is even extending the term metric to ‘metametric’ in their publication. Metametric term includes the metadata about the metric. This metadata includes descriptions of metrics such as scope, purpose, parameters, sources, and calculations. (Brotby, W. et al., 2013, 76.)

4 MEASURING CYBERSECURITY

4.1 Reasons to measure cybersecurity

In most of the industries, the companies are having economic pressure from the rising cost of the security spending to secure the ICT environment and critical assets. These environments are getting more and more complex these days. According to the Cost of Cyber Crime Study 2017, which was a joint research study of Accenture and Ponemon institute, the cost of cybercrimes has increased 23 % on a year and on average cost of cybercrime on 2017 was 11.7 million US dollars per company (where n = 254 separate companies). The trend is showing that these figures have been increasing in the last few years as seen in figure 2. (Richards K, 2017)

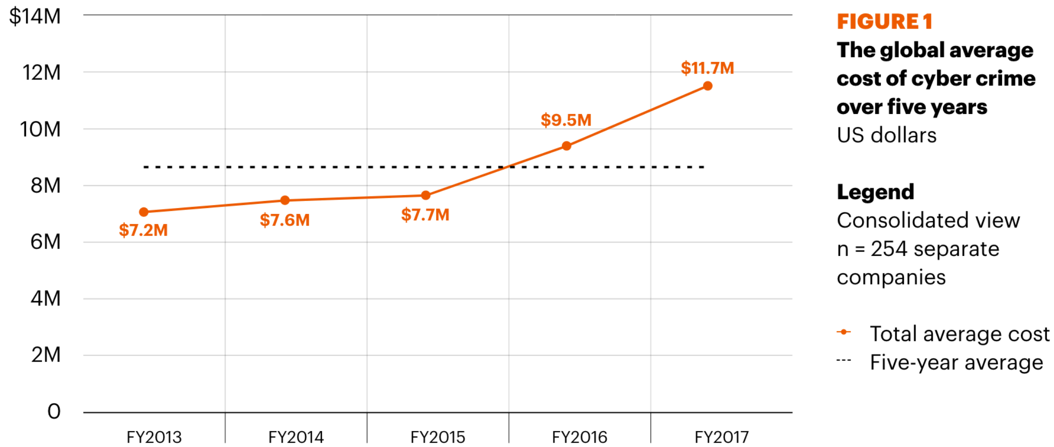


Figure 2. The global average cost of cybercrime over five years US dollars (Richards K, 2017)

In general, the study also reveals that to improve the effectiveness of cybersecurity the companies do not just need to continue to build strong foundation and harden the higher value asset safe guards but to stay ahead of the attackers, the companies needs to keep on investing into a new technology and innovation such as artificial intelligence (AI) and user behaviour analytics (UBA). According to the study this may also mean that companies needs to re-balance the security budgets on some area. (Richards K, 2017.)

International Data Corporation (IDC), who is the global provider of market intelligence and advisory services ICT and consumer technology markets has stated that global spending on security-related hardware, software and services will grow at annual growth rate (CAGR) of 9.2% between 2018 and 2022, to a total of $133.8 billion in 2022. (International Data Corporation. 2019.)

According to Andrew Jaquith (2007), who has long history of researching cybersecurity and metrics, raises that the cost pressures has driven companies to seek and to move from the uncertainty towards a formal security measuring framework to more cost-efficient information security risk management. Jaquith has listed four realizations:

> *Information asset fragility: Companies in most industries realize that efficient operation of their complex enterprises depends on information. Every known instance of critical information corruption, damage, or destruction intensifies their concern over this dependence* (Jaquith A, 2007.)
>
> *Provable security: Because no good, consistent security metrics are available, companies find themselves unable to accurately gauge the suitability or effectiveness of different security options. Consequently, the amount a company can spend on "improving" security has no natural bounds beyond the company's ability to pay* (Jaquith A, 2007.)
>
> *Cost pressures: Economic pressures and the rising cost of security solutions mean security vendors must compete with other infrastructure projects for information technology dollars. Cost-benefit analyses and return-on-investment calculations are becoming standard prerequisites for any information security sale* (Jaquith A, 2007.)
>
> *Accountability: Various industry-specific regulatory bodies, recognizing the growing exposure of their industries to information security risks, are mandating mechanisms for managing those risks* (Jaquith A, 2007.)

Another key points from Jaquith realizations are the ones related to regulatory demands on accountability. The accountability is also one the key elements in the compliance to EU GDPR requirements. From the business point of view, this is actually increasing the operational cost as some work effort is needed to prove the effectives of the security programs and investments. (Jaquith A, 2007.)

ISO/IEC 27001 requires organization to evaluate the control framework effectiveness and ISMS performance. The framework also determines that organizations shall define the following issues for measuring;

- What information security processes and controls shall to be measured?
- Methods for measuring, analysing and evaluation?
- When the measuring shall be performed?
- Who shall do the measuring?
- When and who shall analyse and evaluate the results?
- Retain the appropriate documented evidence of the measured results

ISO/IEC 27001 also states that organization should select methods that produce comparable and reproducible results to be valid. ISO/IEC 27004 monitoring, measurement, analysis and evaluation standard, which is a supplement of ISO/IEC 27001 control framework also mentions accountability as one of the major benefits for measuring of cybersecurity. Other benefits described in the ISO/IEC 27004 documentation are improved information security performance and ISMS processes of the organization to accomplish information security objectives, documented evidence of meeting the control and compliance requirements and support for risk-informed decision-making. (Jaquith A, 2007; ISO/IEC 27004, 2016.)

By following the security metrics, the organization is not just extending the visibility to its security programs effectiveness, coverage of the safeguards in risk management but also helping management to understand the size of the gap between the facts and sense of the security level of the organization. The coverage of the metrics will also help the security specialists in the organizations to pinpoint the necessary actions or development areas to mitigate or lower the security risks and to get the needed management level support and funding.

Patch management is one of the essential cybersecurity processes and risk mitigation actions to keep the system secure and to avoid the organization from unintentional security incidents e.g. from malware epidemics. Process is labour-intensive but needs to be effective, timely mannered and have high coverage. All these aspects shall be measured to find the optimal effort to the risk and cost of actions. (Jaquith A, 2007.)

Jaquith also points out that finding the direct connection between the cybersecurity risks and cost benefit analyses like monetary losses is not simple. He gives an example (1) for widely used method in cybersecurity for cost benefit analyses of risks - *'annual loss expectancy'* (ALE). ALE has simple algebraic formula Equation 1.

$$\mathrm{ALE} = \mathrm{SLO} \ast \mathrm{ARO} \tag{1}$$

where	ALE	annual loss expectancy
	SLO	single loss expectancy
	ARO	annualized rate of occurrence

The single loss expectancy (SLO) is multiplied by an annualized rate of occurrence (ARO). Jaquith criticises in general that this kind of method leaves too much variance for the risk modeller. It lacks the exact data for probabilities of occurrence in the actual loss or event and for example it's hard to characterize what is the 'typical' loss. Also, in most of the cases there is not enough events to make proper assumptions on event rates. (Jaquith A, 2007.)

The need for the cybersecurity metrics is evitable. Organizations needs to better understand the cybersecurity risks, spot the problems and weakness of the security safeguards, measure the overall cybersecurity performance, finding the process improvements, to prove accountability and at last be also cost efficient. (Jaquith A, 2007.)

According to Samuel Merrell (2013), the organization is ready for a metrics measurement program if they have a clear and formal understanding of their strategic plans and goals, has security policies, procedures and guidelines in place, has existing repeatable processes and open communication with the stakeholders. (Brotby, W. et al., 2013, 15.)

4.2 Measuring methodologies for cybersecurity

Measuring concept itself is a large topic. In this research study, the measuring methodologies are based on the references used to study cybersecurity measuring and metrics.

Hubbard et al. (2016), proposes that cybersecurity measuring should be divided into three basic elements; concept, object, and method. According to them at a simplest the measuring concept and the measurement is just a rigorous theoretical constructed information. For the practical decision-making purpose, the concept of measuring and the measurement needs to be treated as observations that quantitatively reduce uncertainty. This, uncertainty reduction point of view is what is critical to business. (Hubbard et al., 2016.)

Finding the measurable cybersecurity objects is a vague until it is decomposed into actually elements that are observable objects. A simple decomposition example is “CIA” that many in cybersecurity are familiar. In this example, the observable object or actual asset is looked from confidentiality (C), integrity (I), and from availability (A) perspective. The decomposition can be leverage into more detailed level. For example, in general availability can be decomposed into system outages that may have an impact on business, how many users a system has, how critical the system is, and whether outage will affect on revenue or other operations with a financial impact that can be estimated by quantitative cost. There may be even some historical data about the duration of outages that have occurred. (Hubbard et al., 2016.)

Hubbard et al. (2016) suggests also to use a “clarification chain”, which contains short series of connections that should make the thinking of the objects, especially if something is tangible. In this chain, three steps for the object is clarified:

1. If it matters at all, it is detectable/observable.
2. If it is detectable, it can be detected as an amount (or range of possible amounts).
3. If it can be detected as a range of possible amounts, it can be measured.

In cybersecurity some measurement methods and things may seems to be immeasurable from the science and statistical point of view. For example, measuring system downtime there is no previous larger “unseen” population to assess. Often, this applies to cybersecurity there is still a need to infer something unseen from something seen, for example a small sample of data breaches and other security events may reveal something to learn. According to Hubbard et al. (2016), in context of measuring cybersecurity - “There is no single, universal sample size required to be “statistically significant.” (Hubbard et al., 2016.)

4.3 Cybersecurity metrics

For the cybersecurity professionals is not so common that the management is asking the question: “Are we secured from the cybersecurity attacks?” – there is no easy answer to that question, or the common answers is either ‘no’ or it depend as there is no 100% security. Measuring the cybersecurity risks is either non-trivial task. According Hubbard et al. (2016), setting the requirements of delivering quantitative cybersecurity measurements rather than subjective and qualitative measurements is almost beyond daunting. (Hubbard et al., 2016.)

In cybersecurity the standard process of risk management starts by modelling the cyber threats, risks and potential losses against the asset or the process that shall be protected. Modelling has similarities to measuring and elements like risk equations, loss expectancy, economic incentives are metrics by them self. Still the modelling is mostly based on scarce data and supplement by expert opinion. Although, well-informed and modelled cyber threats can help to figure out the cybersecurity metrics. There is also some correlation between these two, for example if you just follow the number of incidents you may not know what was the actual threat actor that caused the incident and what was the actual root cause why it happened. (Jaquith A, 2007.)

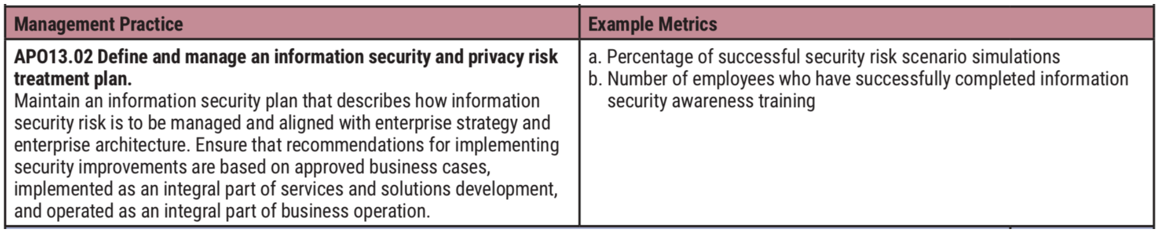
Most of the cybersecurity control frameworks like ISO/IEC 27001 and NIST Cybersecurity Framework has documentation for cybersecurity metrics. In most cases, these metrics defined in the framework documentation are more on a guidance level, build on specific area like effectiveness of information security management system (ISMS) or build on that specific compliance of the controls in that framework rather than the actual effectiveness of the cybersecurity costs, processes or safeguards in the organization. These frameworks can be considered for conceptual guidance and are broadly applicable in general but cybersecurity metrics in the organizations requires also some contextual and organization specific design. (Jaquith A, 2007; ISO/IEC 27004, 2016.)

The cybersecurity metrics can be divided in several domains. Each of the cybersecurity frameworks has a bit different and own manner of approach for measuring cybersecurity. For example, COBIT is more oriented in governance and process related approach and divides the framework into five domains. The domains are divided to governance and management objectives. The five domains correspond to the typical enterprise life cycle and development model such as Deming's Plan-Do-Check-Act (PDCA);

- ***Evaluate, Direct and Monitor (EDM)****, the governing body evaluates strategic options, directs senior management on the chosen strategic options and monitors the achievement of the strategy.*
- ***Align, Plan and Organize (APO)****, addresses the overall organization, strategy and supporting activities for I&T.*
- ***Build, Acquire and Implement (BAI),*** *treats the definition, acquisition and implementation of I&T solutions and their integration in business processes.*
- ***Deliver, Service and Support (DSS),*** *addresses the operational delivery and support of I&T services, including security.*

- ***Monitor, Evaluate and Assess (MEA)**, addresses performance monitoring and conformance of I&T with internal performance targets, internal control objectives and external requirements.*

In this example, the COBIT Management practise under the APO domain the objective is defined to maintain an information security risk plan and as a given example metric for the objective is to measure the percentage of successful security risk scenario simulations as seen in figure 3.



Management Practice	Example Metrics
APO13.02 Define and manage an information security and privacy risk treatment plan. Maintain an information security plan that describes how information security risk is to be managed and aligned with enterprise strategy and enterprise architecture. Ensure that recommendations for implementing security improvements are based on approved business cases, implemented as an integral part of services and solutions development, and operated as an integral part of business operation.	a. Percentage of successful security risk scenario simulations b. Number of employees who have successfully completed information security awareness training

Figure 3. Example metric of COBIT framework (COBIT 2019, 140)

According to Jaquith, the process metrics should measure the activities that organization sees important for promoting correct security behaviours. (Jaquith A, 2007; COBIT 2019 Framework: Governance and Management Objectives, 2018.)

Defence security metrics shall also potentially be able to measure the quality of monitoring attacks and intrusion events. Thakore (2015) has divided the defence monitoring deployment metrics into four categories:

- Coverage, as the overall fraction of the events of interest that are detectable by monitor deployment, which provides a measure of, how much of the wanted events can be detected
- Redundancy, as the estimate of the amount of evidence provided by a monitor deployment that supports to detect an event
- Confidence, as the ability to detect an event using a set of monitors given that monitors may be compromised or faulty
- Cost, as the overall value of the resources consumed by monitors that are deployed including the cost for deployment, operating, collecting, storing and maintaining monitor. (Thakore U, 2015.)

The Center for Internet Security (CIS) is a non-profit organization that has created a framework for cyber defence. Framework includes consensus of twenty most critical security controls and prioritized best practise mitigation actions that reduces the risk of most common attacks against the organization. The security controls are divided into three district categories based on the essence of the controls consider as either, “Basic”, “Foundational” or “Organizational” level as seen in figure 4. Each of the controls contains sub-controls for easier implementation. According to CIS, basic controls should be implemented in every organization for essential cyber defence readiness. The Foundational controls are more technical best practices that provides enhanced security benefits for any organization to implement. The Organizational controls are more focused on people and processes involved in cybersecurity.

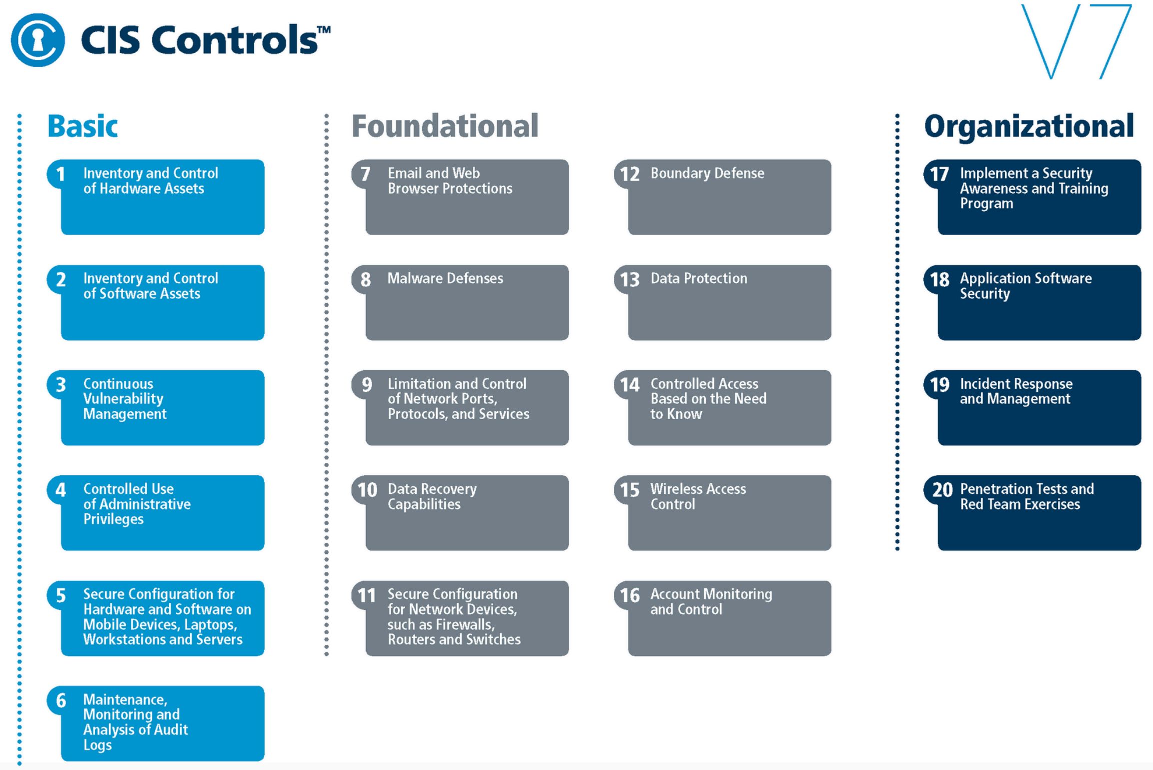

CIS Controls™
V7
Basic
1 Inventory and Control of Hardware Assets
2 Inventory and Control of Software Assets
3 Continuous Vulnerability Management
4 Controlled Use of Administrative Privileges
5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
6 Maintenance, Monitoring and Analysis of Audit Logs
Foundational
7 Email and Web Browser Protections
8 Malware Defenses
9 Limitation and Control of Network Ports, Protocols, and Services
10 Data Recovery Capabilities
11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
12 Boundary Defense
13 Data Protection
14 Controlled Access Based on the Need to Know
15 Wireless Access Control
16 Account Monitoring and Control
Organizational
17 Implement a Security Awareness and Training Program
18 Application Software Security
19 Incident Response and Management
20 Penetration Tests and Red Team Exercises

Figure 4. CIS twenty critical security controls framework (CIS Controls, 2018)

CIS has also established common metrics for the controls to measure the effectiveness of sub-controls within an organization. (CIS Controls, 2018.)

CIS security controls provides the consensus of security best practice standards and is intended to facilitate the rational framework for security controls. CIS has launched a security metrics initiative and formed a consensus team consisting of one hundred industry experts and stakeholders with a diverse set of backgrounds. The team produced a security metrics report in 2009. (CIS, 2009.)

4.3.1 Stakeholders for cybersecurity metrics

Most of the metrics in the cybersecurity frameworks are quite IT and technical centric in general. It’s good to keep in mind also the stakeholders who shall use or to whom the metrics are actually presented. Communicating and reporting industry standard cybersecurity metrics to the organizations management may see them too technical to understand and make them futile. According to Andrew Storms (2016), the cybersecurity metrics shall show the contextual value to the organization rather than presenting industry standard metrics without any further explanation. Although cybersecurity metrics mostly asses the risks that organization is facing, they shall also show the enablement of the business goals on day-to-day basis. Storm highlights that each cybersecurity metrics shall have a clear explanation that includes contextual reason why the metric has been chosen, how the metrics relates to risk, and how the numbers will lead to enablement. (Storms A, 2016.)

For management, the measuring is essentially a governance issue. Brotby, W. et al. (2013) claims that finding data for cybersecurity metrics is not an issue but selecting useful and meaningful metrics that are relevant for decision making for management and particular helping them to make strategic investment decisions is difficult. (Brotby, W. et al., 2013.)

Most of the metrics seems to be control based and leaves the organization to adapt the suitable metrics for their own. By collecting cybersecurity metrics, the organization can fine tune the design of security architecture, measure the cybersecurity objectives, requirements and controls effectiveness and measure the efficiency of security operational processes.

4.3.2 Essential attributes of cybersecurity metrics

As stated before, the measuring and the cybersecurity metrics shall help organization on decision-making. The metrics shall be defined clearly. The metric shall inform what it is and how it was contextually defined. According to Jaquith (2007) the good metrics are having following attributes:

- It can be consistently measured,
- It is cheap to gather,
- It is expressed by cardinal number or percentage,
- Expressed using at least one unit of measure.

By constantly measuring the metric shall also pass so called *litmus* test (Jaquith A, 2007). In the litmus test, the same measuring question is asked from two or multiple different person and they would produce the same answer to the metric. Metrics can be collected manually but this may produce human errors on them. The goal of the collecting and displaying the metrics shall be automation. By automating the collection process, it would be cheaper and gain some cost savings on measuring. (Jaquith A, 2007.)

Jaquith (2017) also argues that metrics which are not quantifiable or cardinal numbers do not qualify as good metrics. He is also expressing that traffic light (Green-Yellow-Red) kind of metrics are not metrics at all, as they do not contain any unit of measure nor a numeric scale. According to him those can be still used sparingly to draw attention on the presentation layer and supplement the numeric metric. The evaluated number should also contain at least one or two associated units that characterizes what is being measured. Jaquith gives an example for, “number of application security defects per application” that contains only one unit, but to be able to benchmark and compare with other applications defects, the metric could be extend to “number of application security defects per 1000 lines of code”. (Jaquith A, 2007.)

In another example Jaquith raises up that some metrics cannot be used for thoroughly monitoring effectiveness as they might have some software capability level accuracy involved in them. One example of this kind of metric is a number of spam detected in email gateways. The metric is heavily relying on technical capabilities in software level to detect all the spam messages and there might be some false positives involved in them too. In this case, Jaquith suggests that also the spam emails reported by the end users shall be monitored as one of metrics for email security effectiveness. Combination of these metrics shall be used to measure the spam detection miss rate metric. These kind of combined security metrics, are also good examples that shall be used to monitor the labour costs and manual actions in security events. (Jaquith A, 2007.)

For technical security analyst pure metrics such as amount of malware are probably good metrics to follow but for management this doesn't tell much. Brotby, W. et al. (2013) argues that this kind of metrics are not relevant and interesting information or trend to follow to senior management and are concerned about the bigger picture and future direction. (Brotby, W. et al., 2013.)

All in all, there are plenty of cybersecurity related processes, controls and functions in typical organization that would be a potential measurable object.

- ISMS implementation
- physical security
- security awareness
- endpoint and malware defence
- vulnerability management
- penetration testing
- application security
- network security
- security architecture
- identity and access management
- security compliance and audits
- configuration management
- risk management
- business continuity management
- incident management, -response and forensics and many more

(Hubbard et al., 2016, ISO/IEC 27004, 2016)

The cybersecurity metrics does not need to be perfect in the beginning. Defining a set of basic metrics that are defensible and quantifiable, and then using them is a good start to ensure that things are improving. (Hubbard et al., 2016.)

4.4 Implementing cybersecurity metrics

4.4.1 Process of implementing cybersecurity metrics

One of the most famous security professional, Bruce Schneier has written already in year 2000 that – “Security is a process, not a product” (Schneier B., 2000). This mantra fits also into cybersecurity metrics implementation process. Metrics are created through iterative process and needs to be revised continuously. Measurement process needs constant analysis and interpretation of results from the security analysts.

ISO/IEC organization standards use typically the four-phase structured - Plan-Do-Check-Act (PDCA) process model, which is based on the Deming cycle. ISO/IEC 27004 measuring standard follows that also as seen in figure 5:

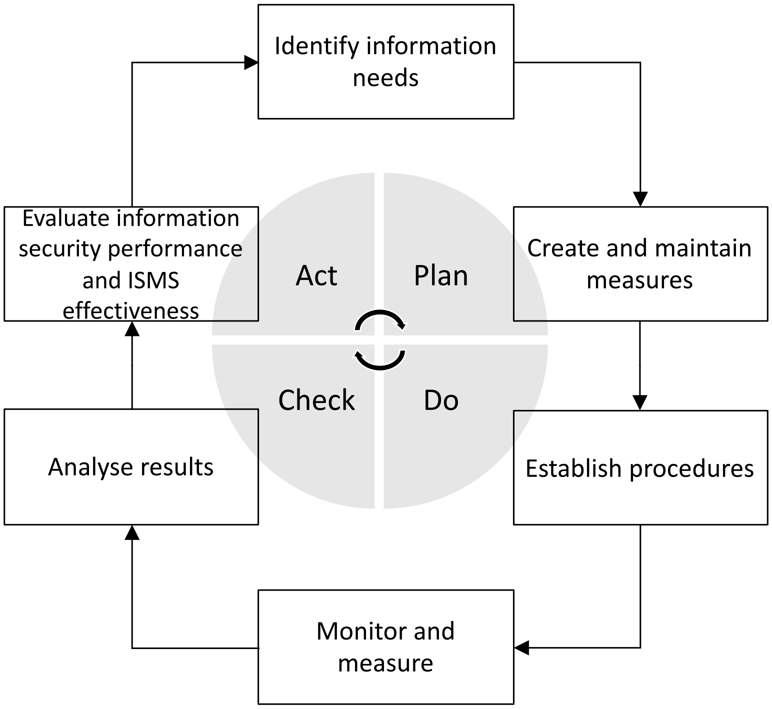

Identify information needs
Create and maintain measures
Establish procedures
Monitor and measure
Analyse results
Evaluate information security performance and ISMS effectiveness
Act
Plan
Check
Do

Figure 5. ISO27004 Monitoring, measurement, analyses and evaluation process (ISO/IEC 27004, 2016)

The ISO/IEC 27004 standard consist of six phases as shown in figure 5 for implementing measuring process:

1.) **Identify information needs** – this phase includes typically gathering the initial needs, organizations strategic direction, policy and control objectives, other legal, regulatory or contractual requirements for measurement
2.) **Create and maintain measures** – in the second phase the identified needs are inventoried and associated to the existing security measurements.
3.) **Establish processes** – In this phase the measurements are implemented or updated to the security processes.
4.) **Monitor and measure –** In fourth phase the measuring data is collected and verified.
5.) **Analyse results** – in this phase the verified metrics are analysed. The analyses identify the potential caps or points of improvements.
6.) **Evaluate information security performance and ISMS effectiveness** – in the last phase the information of improvements is interpreting to the organization's security performance and ISMS effectiveness.

The ISO/IEC 27004 standard highlights that it is important to define and collect the metrics data so that it can be re-used for multiple purposes and for different interested stakeholders and their information needs. (ISO/IEC 27004, 2016.)

In the NIST performance measurement guide for information security, Chew et al. (2008) also mentions that implementing cybersecurity measuring is iterative process. According to Chew et al. (2008), the organization should invest more time into early phase of the process as it is more effective than retrofitting the metric requirements afterwards. NIST guidance is dividing the measurement development process into two major activities as shown in figure 6.:

1. **Identification and definition** – the phase include the current information security program

2. **Development and selection** – the phase include specific measures to gauge the implementation, effectiveness, efficiency, and impact of the security controls.

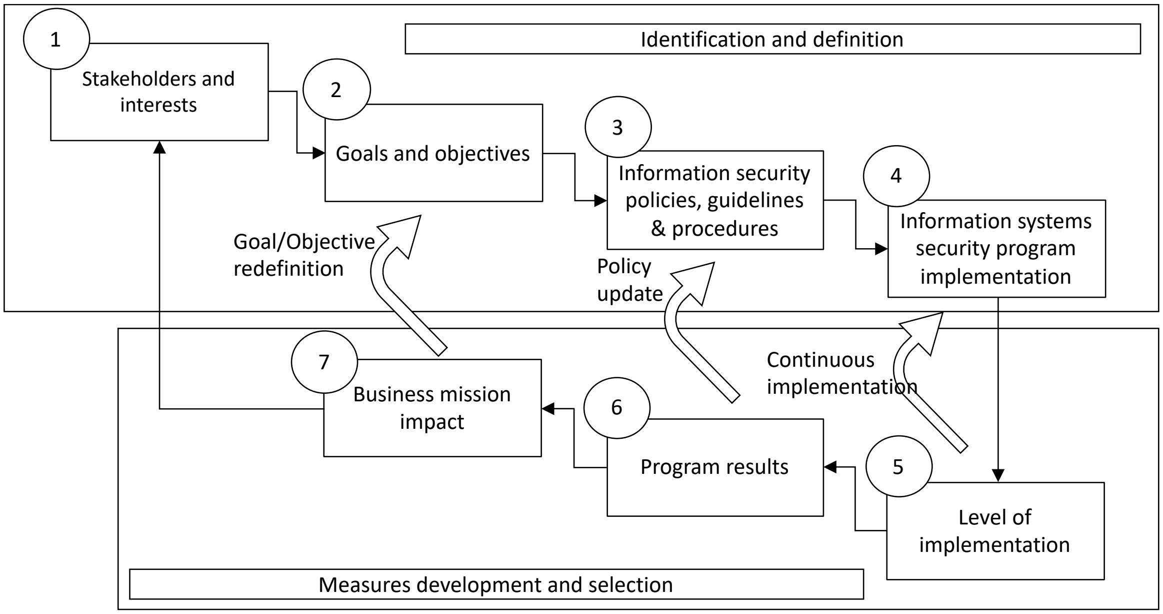

Identification and definition
1
Stakeholders and interests
2
Goals and objectives
3
Information security policies, guidelines & procedures
4
Information systems security program implementation
Goal/Objective redefinition
Policy update
Continuous implementation
7
Business mission impact
6
Program results
5
Level of implementation
Measures development and selection

Figure 6. The NIST information security metrics process (Chew et al., 2008)

In the NIST development model there is also iterative relationship between the major level activities and its steps in the process. So, in theory NIST model supports more agile iterations for the process and for example the Information security goals and objectives could be updated after the measurement process has recognized business mission impact as shown in steps 7 and step 2 in figure 6. (Chew et al., 2008.)

For cybersecurity measurement process to be effective it needs a stakeholder and nominated sponsor or program owner from the organization. According Chew et al. (2008) anyone in the organization could be a stakeholder for metrics but primary stakeholders are:

- The head of organization unit
- C-level managers such as Chief Information Officer (CIO) or Chief Information Security Offices (CISO)
- Program managers / information system owners and
- System administrators, -engineers and support personnel

There could be also secondary interest groups for example the organization business departments, Chief Financial Officer (CFO), human resources, Internal inspectors and Privacy Officer. (Chew et al., 2008.)

Each organization has different strategic goals and objectives. These enterprise level goals and objectives derivates normally into information security plans and policies. These documents are good starting point to validate candidates for the cybersecurity measurements for the organization. The documented security controls, requirements and processes needs to be reviewed for potential security metrics. Chew et al. (2008), highlights that these documents should not only be reviewed in the initial development phase but regularly in the future to identify exhausted metrics. (Chew et al., 2008.)

In the initial implementation phase, based on the organizations existing security policies and procedure maturity level, the potential security metrics in the organization could be quite large. At this phase the metrics should be prioritized. According to Chew et al. (2008) it would be important to select two to three high-priority measures per stakeholder and use a risk-based approach in the metric selection. The selected metrics should

- Facilitate improvement of high priority security control, sourcing e.g. from internal auditor report, security risk-assessment, through continuous security monitoring or based on goals set by the organization
- Using data from existing sources and data repositories
- Measures consisted processes that already exist and are established

Although some of the security metrics are operational and measures the effectiveness for example the amount security events handled, setting the longer period performance targets might also need to be adjusted for implementation type of metrics. The organization could set the implementation milestones based on the current metric baseline as shown in figure 7.:

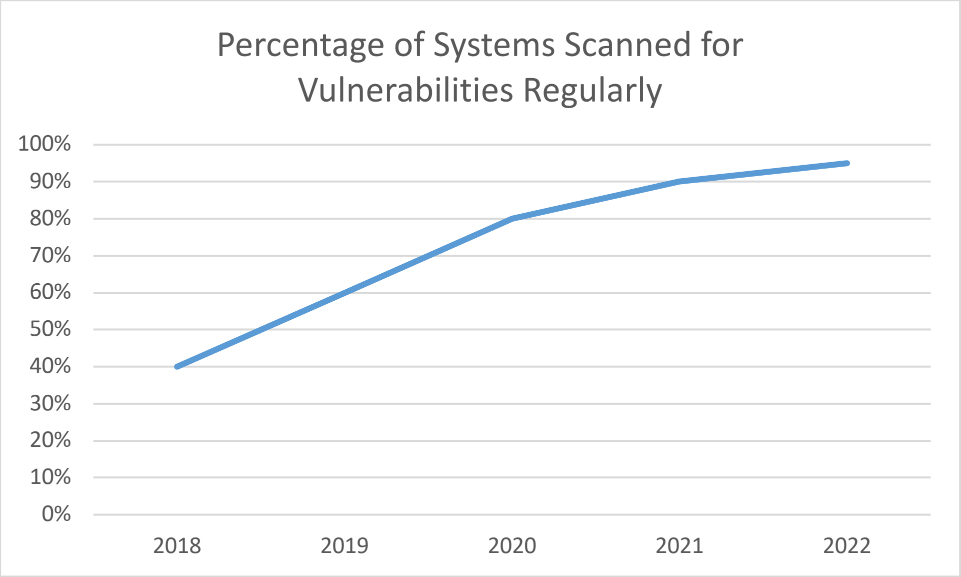


Figure 7. Example of milestone implementation for the metric based on current baseline

NIST extends the security metrics implementation phase into more detailed level process. This detailed process includes 6 phases, which ensures that metrics are continuously monitored for performance improvements as shown in figure 8.:

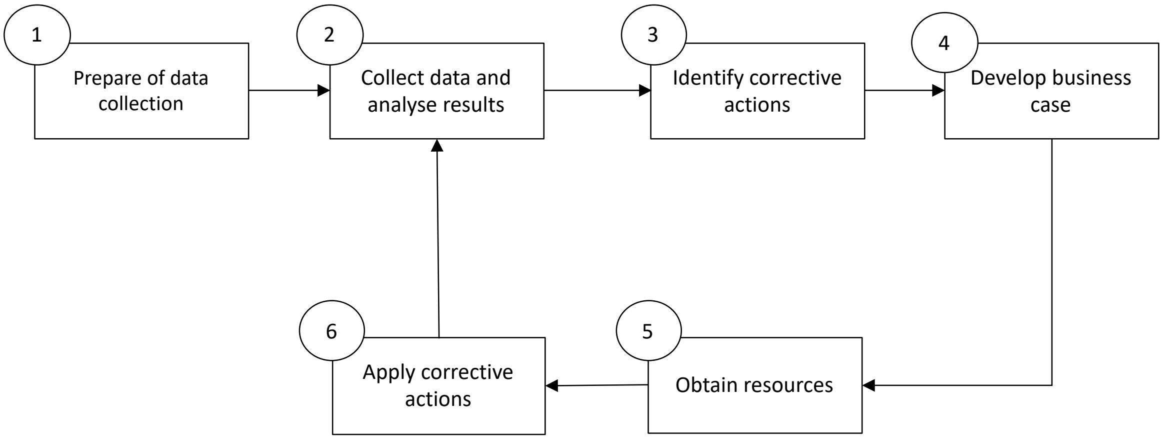

1
Prepare of data collection
2
Collect data and analyse results
3
Identify corrective actions
4
Develop business case
5
Obtain resources
6
Apply corrective actions

Figure 8. NIST measurement program implementation process (Chew et al., 2008)

For each step the stakeholders should be involved to guarantee the measurement program overall success, the actual business case and goal for the metric. Chew et al. (2008), states that there are three types of measurable aspects for cybersecurity metrics: business impact, efficiency and implementation from the stakeholder’s point of view. For example, the executive level is more interested about the business impact and operational level about the efficiency of processes and the implementation level that may affect on current risk level. (Chew et al., 2008.)

Additionally, the implementation phase of the measurement program should be documented into a plan. The plan should define what and how the metrics will be collected, analysed and reported. The documented metrics ensures that organizations can understand how metrics were derived, what is purpose and allows organizations to derive confidence from the transparency, which is increasing trust in the metrics program. (Jaquith A, 2007.) Once the collected metrics are analysed those can be used to identify corrective actions or development activities. Those actions can be either technical, management, and operational areas of security controls. Typically, security controls need investments and budget that turns into a formal business case and resources. (Chew et al., 2008.)

Naturally, the implementation phase should include the visualization design, reporting and holistic view of the measurement. These things are look into more detailed level in chapter 6. Situational Awareness.

4.4.2 Selecting and modelling cybersecurity metrics

To be able to implement effective cybersecurity metrics program, the environment that we protect should be known and threat modelled first. The modelling should include the quantitative values of the assets, threats, exposure, controls and the current counter-measures the environment has. The modelled frame should include also the logical ICT environment and necessary processes. Jaquith (2007) introduces a simple way to logically model of ICT security controls.

In this very simple model the three elements: threats, exposures and countermeasures interact as part of the ICT security control processes as seen in figure 9. Jaquith describes the elements as following:

- ***Threats*** *are things that can happen or are the result of proactive acts against one or more target assets. Vulnerabilities are characteristics of target assets that make them more prone to attack by a threat or make an* *attack more likely to succeed or have impact. Threats exploit vulnerabilities, the results of which are **exposures** to the assets.*

- ***Countermeasures** are designed to prevent threats from happening or to mitigate their impact when they do. Underlying each of the three preceding concepts (threats, exposures, and countermeasures) are **assets** - namely, the targets of threats, the possessors of exposures, or the beneficiaries of countermeasures. Assets are the things we were supposed to be protecting in the first place.*

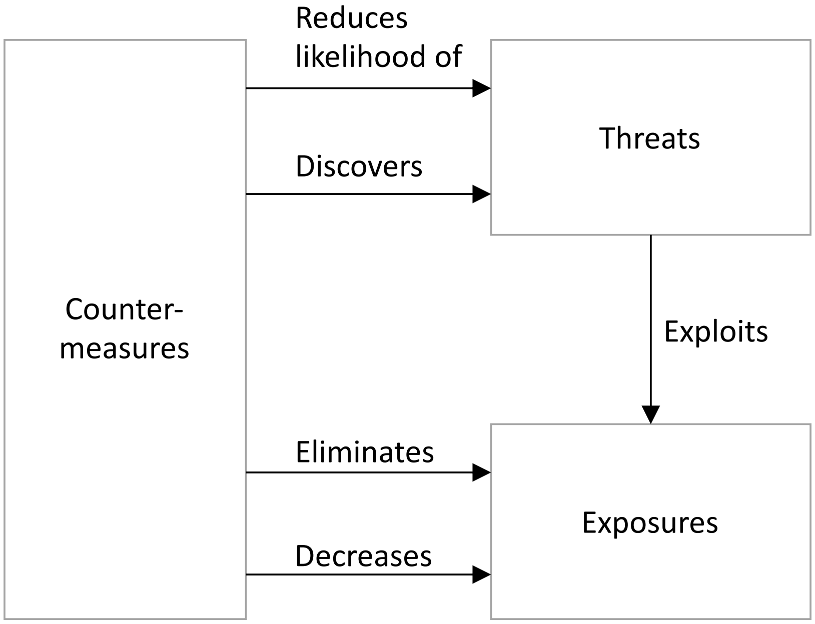


Figure 9. Logical model of ICT security controls (Jaquith A, 2007)

In the more complete data modelling, all three areas of the security controls can be decomposed into more detailed level as seen in figure 10, including the assets that the organization is trying to protect. At this level the measuring of the threat modelling becomes more concrete. The attacks patterns have frequencies, which are measured for the detected events per unit of time. Those events can have several sub-attributes such as severity, event type or criticality of asset. Further, this information can be correlated for example with the responsible business unit, owner of the asset or the business process itself. From the risk management point of view these inputs the information about the exposure of the assets and its current state of vulnerabilities. After knowing this, the risks need to be analysed and decisions made for further risk mitigation steps or acceptance of the residual risk. The risk may have also different type of countermeasures in place from detective to preventive controls. Those countermeasures can in most case be also measured by the effectiveness and quantified. One typical example of detective control is Intrusion detection system (IDS), it will not block the attacks but informs about them. As a corrective control, the security operation could then block the attack on the firewall, which would act as a preventative control for the risk. From the metrics point of view this could be measured as e.g. amount of attacks prevented.

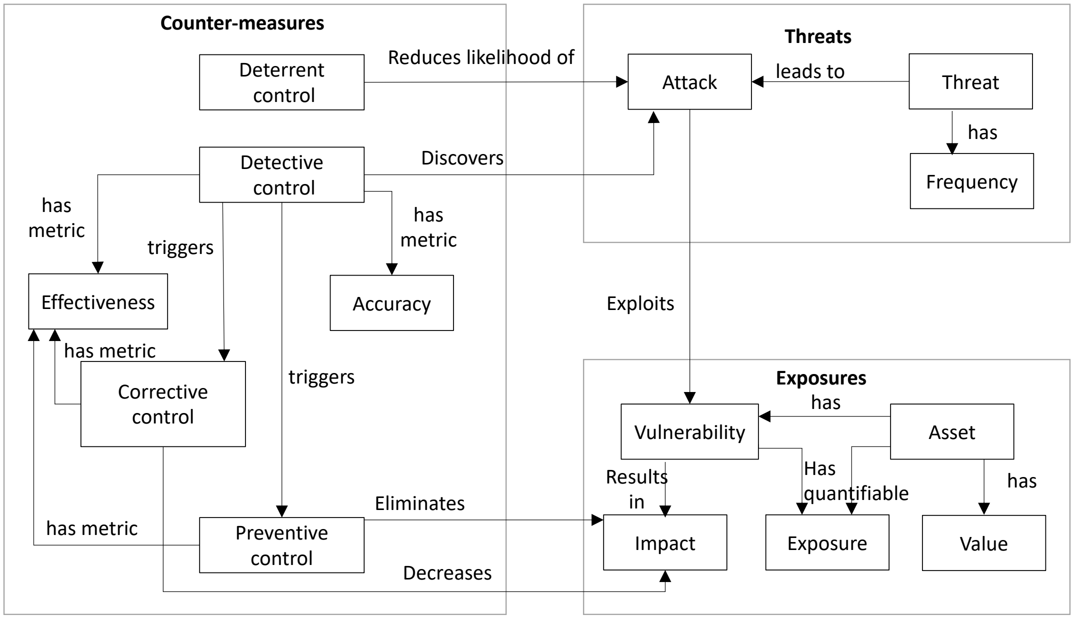


Figure 10. Decomposed logical model of ICT security controls (Jaquith A, 2007)

According to Jaquith (2007), these and various other models gives the basic understanding of the containment and relationships between the areas, but a lot of customization is always needed to map the individual components of the metrics to the system they comprise.

A high percentage of external cyberattacks are initiated via end-users by phishing and installing the malware on the end-user’s endpoint. This is just an example that could be used to model the potential measurable object based on actual threat and attack modelling. (Hubbard et al., 2016.)

A well-known issue with metrics accuracy is false-alarms or false-positives. These terms refer to case, where the actual alarms not a real event or attack. From the measuring point of view, it means that some tuning and testing needs to be done before counting on metric and using the metrics in risk management process or making further decisions based on them. (Jaquith A, 2007.)

Brotby W. et al. (2013), takes more practical way to model cybersecurity metrics by introducing their own 'PRAGMATIC' method. This method uses nine different criteria for assessing and selecting metrics as seen in figure 11.

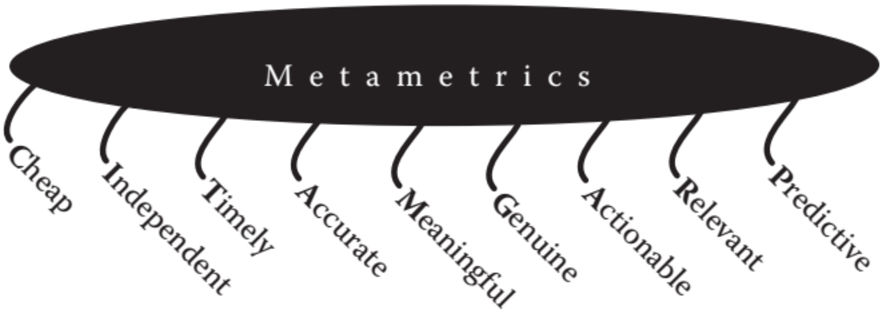


Figure 11. Nine PRAGMATIC criteria's for selecting metrics (Brotby W. et all., 2013, 81)

According to Brotby W. et al. (2013), most of the other sources (books, articles, and standards) for security metrics tries to cover too theoretical way of designing the metrics and miss or lack guidance on how to determine, which security aspects to measure. In more practical method for selecting cybersecurity metrics needs to be workable, useful, and, above all, valuable. (Brotby W. et al., 2013, 78.)

4.5 Data sources for the cybersecurity metrics

Cybersecurity metrics needs data from multiple external sources. The data can be almost anything related to the business environment, process, security controls or the protected assets. The data may be in pre-formatted, correlated or even raw data. According to Jaquith (2007) the typical organization environments are so complex that there are more than enough data sources for cybersecurity metrics. In typical data center environment already the business applications, systems and services provide a lot of data that generate hundreds of metrics and security analyst can become overwhelmed. Data sources may also be permutation and combination of other data sources. In some of the environments there may be more than one authoritative data sources such multiple identity and access management systems. (Jaquith A, 2007.)

Although most of the cybersecurity metrics are collected from the technical systems that creates the actual controls or safeguards there are data sources which are non-technical. Budgeting system is an example of non-technical data source that can be used as an input to cybersecurity metrics to measure the effort of value spend on some cybersecurity control and calculate the return on investments. (Jaquith A, 2007.)

4.6 The automation of cybersecurity metrics data collection and handling

Automation has many benefits when collecting cybersecurity metrics but the associated processes and systems must be well defined. Good automation will not only save cost and time but they make the security metrics collection accurate, repeatable and reliable and brings a higher level of assurance. Automation also makes the collecting process transparent and auditable for reviewing. Once the automation has been proven to be working also the frequency of measurement can be increased or optimized to monitor the other security processes. One example of this type of optimization is the correlation between security vulnerability metrics and installed security patched. Vulnerability metrics shall be collected after the regular security patch management process has been executed, otherwise the vulnerability metrics is not accurate. (Jaquith A, 2007.)

In today’s world automation is the ultimate goal of many things. We are trying to make processes faster with minimal human interaction. There is already a lot of automation in ICT software development and operations process. New software builds are made to the production environment via continuous integration (CI) pipelines. According to Gartner, Inc (DeBeasi P. 2019) one of the biggest challenges in modern organizations today is to create effective hybrid ICT environments for organizations on-premise and cloud environments. These complex technology ecosystems will require more self-service provisioning, configuration and automations to be productive. The trend that Gartner, Inc (DeBeasi P, 2019) highlights to gain more effectiveness is that in the future the infrastructure and operations will be driven by machine learning (ML) and artificial intelligence (AI). These techniques are still quite premature but according to Gartner, Inc a greater focus on these techniques in operational data will influence monitoring strategies, resulting in more proactive and automated operations. (DeBeasi P, 201.9)

Similar trend can be seen in cybersecurity operations. Effective cybersecurity monitoring and incident response will require automation in analytics, data and metrics collection. Effective analytics and decision making needs the data and metrics to be available almost in real time. According to Gartner analyst Anton Chuvakin (2018), security teams are suffering from staff shortages, have to deal with an ever-increasing security tools and has productive challenges. He also highlights that the volume of threats and events are increasing from existing and traditional security products such as firewalls, endpoint protection platforms (EPPs), security information and event management (SIEM), secure web gateways (SWGs) and identity proofing services (IDPSs). (Chuvakin A, 2018.)

Traditionally the spreadsheets have been used in most cases to create security metric calculations and data processing for different kind of visualization on security reports. They still are useful for many use cases to manual create elements to the security reports. Spreadsheets have even some methods to integrate to the metrics sources, but capabilities are still quite limited in external connectivity APIs, data querying, data storing and handling. According to Jaquith (2007) the spreadsheets are good for prototyping and piloting security metrics but not suitable for real automation tasks for security metrics collections (Jaquith A, 2007).

Business intelligence (BI) and other business data-mining tools are designed to analyse business related data. This does not mean they would be suitable for automating security related data and especially the metrics collection part.

Jaquith points out that the key challenges in BI tools is that they are oriented to perform ad-hoc exploration of large data set not to automate and manage security metrics collections over the time. These tools are also not necessarily suitable to integrate and fetch data from security products. (Jaquith A, 2007)

SIEM solutions has been traditionally the central storage of operational security event log data. SIEM solutions has also capabilities to fetch data from application programming interfaces (API), which could collect the security metrics data from various sources especially from security products. SIEM solutions are operational events oriented and tends to focus on anomaly detection instead of process measurement. SIEM solutions may also lack the ability to connect to semi-structured external data sources and non-security sources such as ERP and HR information systems. SIEM solutions has some build in reporting tools such as dashboards but generally they are limited to the feature set of SIEM system. (Jaquith A, 2007)

Another security tool that is raising maturity to help security teams to operate in faster and more standardize working methods is security orchestration, automation and response (SOAR) tools. Gartner, Inc (Chuvakin A, 2018) defines SOAR as security technology that enable organizations to collect security data and alerts from different sources in to one orchestration platform for security operations. Gartner analyst Anton Chuvakin (2018) highlights multiple reasons to invest in SOAR tools. According to him, the SOAR tools make operational security analyst work more effective to respond, contain, and to remediate the security event or incident by automating the tasks to incident playbooks. Playbooks are built on security process flow that has tasks. Tasks will collect the necessary data in context and execute some the steps automatically for the security analyst. SOAR tools can also enrich the data from multiple sources, for example add the owner of the asset and contact information. SOAR tools could also at least in theory be used to collect and process the security metrics data. These tools have the key elements to provide necessary data collection, workflow engine, API integrations, data handling and scripting capabilities. (DeBeasi P, 2019; Chuvakin A, 2018.)

4.7 Technical requirements for cybersecurity metrics environment and platform

According to Jaquith (2007) the key functionality requirements for automating cybersecurity metrics from raw data into insight metrics starts from the design environment. The graphical interface shall not require programming skills as the main user group to operate in the security metrics design environment are mostly security analysts rather than software developers. To be able to use some programming capabilities like basic scripting and using for example regular expression would still be needed for advanced data handling. (Jaquith A, 2007)

The technical environment shall also have enough computing power for the raw data handling and data calculation functionality. The platform should also provide scalability to provide robustness into automation. One of the key requirements according to Jaquith (2007) is also auditability. The metrics shall be collected from the authoritative sources to provide traceability and integrity to data over the time in all phase from raw metrics data fetching, storing to the environment and data handling. As the cybersecurity metrics collected from the various sources are combine to business context, they must be reliable and provide value to business processes and business decision during to metrics life cycle. Some of the data collection tools may also require adapters or connectors to fetch the data from the external data source. (Jaquith A, 2007)

Jaquith (2007) also mentions the flexible results publication as one of the key requirements. According to him the environment should provide adaptive mechanism to communicate the metrics to the reports. The distribution of the results shall be entitled based on who and what results can be seen. The results shall be also possible to deliver automatically in various forms like PDF report to email or to existing corporate intranet platform. (Jaquith A, 2007)

5 SITUATIONAL AWARENESS

5.1 Cybersecurity situational awareness

In this chapter, methodologies used to build the cybersecurity situation awareness (CSA) and the visualisation of the cybersecurity metrics are discussed in more detail.

In the research, the Endsley's theoretical model for situational awareness (SA) starts by dividing it into several level. According to Endsley (1995), the SA involves far more than being aware of numerous pieces of data. The pieces of data in this research is considered as the actual information from the cybersecurity metrics that were introduced in the previous chapter. In the advanced level on the Endsley's theory, which requires the projection of future system state and knowledge of operator pertinent goals (Endsley 1995, 32), the security analysts need to understand the level (or criticality) of situation and relevance to the business.

To ensure business continuity (or business initiatives) and to prevent organization from the damage of cyber-attacks, the potential impact of cyber incidents needs to be prevented or minimised. To achieve this goal, sufficient CSA needs to be created and the business environment monitored continuously. Traditionally, security monitoring has been focused on network and system monitoring. In organisation network environment, the security analyst monitors the network and user activities, recognise abnormal activities and needs to response into anomalies in a timely manner. This work is not only work intensive but is also error prone to make the holistic view of the CSA. Security metrics are natural requirement and important part of the coordinated defence activities and CSA management. (Cheng et al., 2014.)

Although, security monitoring is vital part of the organisation environment and CSA, it lacks meaningful metrics and actual risk assessment work from preventative and mission assurance point of view. For example, analysts cannot quantitatively evaluate or determine the exact impact of security incident on business or mission objectives. Cheng et al. (2014) argues that security metrics should be adjusted and fitted to organization or situation and ideally be meaningful to organizational goals and key performance indicators. Creating security metrics for CSA requires advanced mission-to-asset mapping, modelling and evaluation technologies. According to Cheng et (2014), measurement for CSA needs to consider two distinct possible issues:

1. How to define and use metrics as quantitative characteristics to represent the security state of a system or network, and
2. How to define and use metrics to measure CSA from a defender's point of view.

(Cheng et al., 2014.)

5.1.1 Knowledge of organisation environment and assets as part of the cybersecurity situational awareness

Attackers are constantly finding out potential weakness and exploitable new vulnerabilities. According to Distil Networks (2017), "Bad Bots" made up to 20% of all web traffic. Not only the attackers have shown the ability, patience, and willingness to "inventory" organisations Internet assets at very large scale in order to support their opportunities but there are services in Internet like Shodan (https://www.shodan.io/), which are creating huge database of Internet connected devices including very detailed information about the versions.

External devices or even the devices which are connected to the Internet from internal network e.g. endpoints can be used by the attackers who have already gained access to organisation network to find for other internal pivot points or lateral movement. To be able to protect organisations environment the assets need to be known and inventories keep-up-to date as part of the CSA. The first two basic level security controls from CIS Twenty Critical Controls framework are:

- CIS Control 1: Inventory and Control of Hardware Assets
- CIS Control 2: Inventory and Control of Software Assets

According to CIS organisations that has large, complex and fast-changing environments may struggle with the challenge of keeping the inventories up-to-date and managed. (CIS Controls, 2018.)

The critical assets should be prioritised by criticality, based on the impact, relevance, and asset value for the business (Cheng et al., 2014.)

5.1.2 Risk and threat management as part of the cybersecurity situational awareness

Risk management is an inevitable part of the CSA. Risk analysis approach is the most common way to help in decision making of CSA and security metrics. In general, the security risks are commonly expressed and calculated with formula of Equation 2.

$$Risk = Threat\ x\ Vulnerability\ x\ Impact \tag{2}$$

where

Risk	The probability of something bad happening
Threat	Event with the potential to adversely impact an asset
Vulnerability	The existence of a weakness that can lead to an unexpected, undesirable event compromising the security of the computer system, network, application, or protocol involved
Impact	The result of an unwanted incident

Quantifying the risk and each variable to meaningful values is not simple. In order to quantify e.g. the cost of the risk and translate it to actionable item security analyst should know the information asset value from several points:

- Productivity value of using the asset e.g. user’s time (salary)
- How much revenue the asset is making e.g. transactions
- Liquid financial value e.g. assets under management

- Intellectual property value e.g. trade secrets
- Potential loss e.g. confidentiality of personal data

According to Lindström P. (2005) to define a risk for an entire enterprise is next to impossible but manageable approach is to break it down to small units and types. This will help organisations to assigning values to security formula and defining what risk means to your enterprise. (Lindström P. 2005.) By, continuously seeking improvements in our methods is important to assess cybersecurity risks (Hubbard et al., 2016).

5.2 Scorecards as an input for cybersecurity situational awareness

As stated earlier, the purpose of the cybersecurity is to protect the digital business initiatives, assets and data. The business initiatives are traditionally applied and measured by method called “Balanced scorecard” (BSC). Balanced scorecards are adopted by thousands of organisations around the world. The balanced scorecard is a tool to make and score the performance measurement and strategy implementation in the organisations to align with organisation’s mission, values, vision, and strategy. (Kaplan R. 2010.) Other similar business or process level scorecards exists, few to mention are Total Quality Management (TQM), Six Sigma, and Kaizen.

Balanced scorecard has four primary perspectives: financial, customer, internal business process, and learning and growth. Although, the balanced scorecard is not directly suitable for cybersecurity there are frameworks that utilize the principles and methods from the balanced scorecard techniques and are structured along the balanced scorecard dimensions such as COBIT (Governance and Management Objectives COBIT, 2018). According to Jaquith (2017), the scorecard perspectives could be used and transferred to create a “security centric” scorecard. He gives an example that balanced security scorecard could have four dimensions like; threats, vulnerabilities, identity and access management and policies and compliance. Jaquith (2007), critics taxonomy used in the operational security scorecards, which according to him are not logical and does not speak of the same language for the executives (money, people, time) (Jaquith A, 2007.)

One of the key perspectives in balanced scorecards is the financial perspective. From security point of view, implementing security controls will in general generate costs for the organisation. Measuring security cost only on organisations ability to make money and growth or reduce risks would be a false assumption. According to Jaquith (2007), the link between security to revenue is still strong and shown in many of the precedents. The financial perspective should at least measure organisation abilities to:

- Increase usage of systems that generate revenue
- Increase the integrity of systems that generate revenue
- Increase revenue generated using systems Increase the integrity of the process of accounting for revenue
- Decrease the risk of using systems to generate revenue
- Decrease the risk of using systems to account for revenue
- Decrease the cost of securing systems
- Decrease the direct cost of downtime and security incidents

whereas the systems cover all the technology, infrastructure including the servers and applications and other resources such as people as well. (Jaquith A, 2007)

From financial perspective the security measurements could include for example:

- System uptime or downtime costs
- Cost of security incidents (including investigation)
- Cost of work time used to keep the system up to date (vulnerability management, system patching)
- Cost of work time used to monitor, investigate and fix the security issues

The list of the example measures is quite high level and could be extended to suite the organisation needs, environment and the service model. Also, the other non-financial balanced scorecard perspectives could be used into the current state or situational awareness with adjustments. Scorecards can help organisations to measure their performance and security programs. (Jaquith A, 2007.)

One of the well-known, cybersecurity scorecard is NIST cybersecurity framework (CSF) released in 2013. Although, it is mainly used to asses critical infrastructure, it has a list of combined security controls from several sources, which could be used as a security scorecard to design the security metrics and as part of the situational awareness of the security controls. CSF is divided into several core functions that provide a high-level strategic view of the lifecycle of an organisation's management of cybersecurity risks:

1. Identify
2. Protect
3. Detect
4. Respond and
5. Recover

These functions have categories (Asset Management etc.) and subcategories for each function that matches them with other references such as existing standards, guidelines, and practices for each subcategory (ISO/IEC 27001, COBIT etc.) (National Institute of Standards and Technology, 2018.)

5.3 Reporting situational awareness

Obviously, the security metrics are vital part of the situational awareness and needs to be communicated and reported. Jaquith, (2007) highlights that not only selecting and collecting the cybersecurity metrics is complex but also showing it to the management either literally or figurately is quite difficult too. Jaquith continues that visual representation can dramatically enhance this and to make of cybersecurity issues and current status better understandable. He also generally criticizes that information security data visualization and especially product vendors provide inflexible graphical reporting tools. (Jaquith A, 2007.)

Although, the security metrics will be help on reporting of situational awareness, it’s not always straightforward. Reporting of ongoing security incidents for example has a lot of uncertainty. Investigating a computer virus incident in the system and answering to question – "how long does the downtime last"? may depend on several things like, if a forensic evidence work is necessary to be done before the system is brought up again. Sometimes, the answers in the report is only a best guess based on the previous incidents. (Hubbard et al., 2016.)

Reporting everything in one report may not be meaningful. Some of the security metrics and information in report is more important for other stakeholder than the others. To be able to drill into more detailed reporting may help on triggering natural remedial actions. For example, vulnerability metrics that disclose also the responsible department may spawn a healthy competition in organisation to remediate the vulnerabilities on their systems. (Payne, 2007, 6.)

5.4 Visualisations principles for cybersecurity metrics

It is said in general that, "a picture is worth a thousand words". In cybersecurity, this can be turned into sentence "A picture is worth a thousand log records". Human brains are devoted to visual processing more than any other sense. This ability to process rapidly visual input turns data into information visualisation and knowledge. According to Marty R. (2009), visualisation shall be as simple and clear as possible, as otherwise the brains starts to apply the scepticism filter and viewer starts to ask questions and may not anymore trust it. Still, visualisation is one of the key elements in situational awareness that helps to analyse large amount of data very quick and turn it into something meaningful to make decisions (Marty R. 2009.)

Jaquith (2007) gives six design principles and recommendations for effective visualisation. According to him, the first priority should be in the data. The design of the metrics shall not be decorated with any 3D elements, specific fonts or photo like graphs but rather be simple and clean to the audience to understand the actual metric data behind them. He also recommends avoiding all unnecessary ornaments like profusion of superfluous ticks, grid lines, plot frames, and chart frames. For using colours in visualisation he recommends to not use overwhelming saturated colours. To emphasize the key points with colours, the visualisation shall have a small focused swatch of saturated colour or monochromatic colour palette. (Jaquith A, 2007.)

One thing to remember when using colours is that approximately 8% of all men and 0.5% of all women are colour blinded and for example, they cannot see the traditional traffic light colours because of red-green colour blindness (Flück D, 2012). The metric elements of visualisation shall also be clearly titled and labelled for meaningfully to the audience.

A trend is a common way to visualise security metrics. It has a relative start and current point. Depending on the timescale it can also be used to predict the course. Trends may also have random fluctuations. The key point is not to predict too far to be conscious. According Brotby W. et al. (2013), even with the best of information available, events may conspire from the current situation into severe incidents (Brotby W. et al., 2013, 84).

5.5 Graphical design

Simple and easy to read graphs are most important elements of effective design guidelines of graphs. Marty R. (2009, 13), emphases a list of graph design principles that should be considered and understood when designing graphs;

- Reduce nondata ink, e.g. use simple bar charts
- Distinct attributes, e.g. do not use multiple shapes
- Gestalt principles, e.g. highlight patterns and important information
- Emphasize exceptions, e.g. use color to highlight exceptions
- Show comparisons, e.g. show baseline in graph
- Annotate data, e.g. add information to the graph about the potential reason for exception
- Show causality, e.g. use another graph to identify the root cause of exception

According to Marty R. (2009, 20), by applying the previous principles into graphical design, it will generate simple, visually pleasing graphs and data visualizations.

5.5.1 Bar charts

Bar charts are one of the most common used type to visualise cybersecurity metrics. They can be either simple column, stacked columns or waterfall charts. According to Jaquith (2007) the stacked columns are more suitable for analysing more than two time periods of categorised data for example vulnerability distribution by vendors. The primary advantage is that audience can compare the time periods against to each other. Waterfall type of charts are similar to stacked charts but provide an alternative view for the data. Waterfall charts can illustrate the relative contributions of different factors to the total. They can be also more readable than stacked columns if there is text included in the categories. (Jaquith A, 2007.)

5.5.2 Time charts

Time series charts are probably the most common and easiest way to visualise and understand the cybersecurity metrics. Especially when the cybersecurity metrics would need to compare two or more attributes over the time. Time interval can be in typically any of the normal time variables from hours to years. Time series charts can accommodate line, area or bar charts depending on the preference of the cybersecurity metric or the audience. This type of visualisation is normally used to display the cybersecurity improvement or trend of the cybersecurity metrics over the time against a baseline. It can also show to the audience whether the actions or process improvements has been more effective than in the previous measured time slot or over the time. In most use cases the normal linear trend line is more than enough but there might be some specific use case for other types of graphs such as logarithmic trend lines or bivariate charts, where two metrics needs to be shown in the same graph. In some use cases, the time charts need to show each data point as a multiple of its normalized starting value to analyse rather relative than absolute value. This is called indexed time series charts and suitable for a group of comparable series. (Jaquith A, 2007.)

5.5.3 Matrices charts

One of the most used matrices charts is called two-by-two. This is a special form of bivariate chart. Gartner's Magic Quadrant is one example and well known in ICT and cybersecurity industry. It's also commonly used in management reports and executive summaries. According to Jaquith (2007) this form of 2x2 grid has proven to be tremendously resilient because it speeds up comparison by grouping the data into simple quadrant buckets that are more understandable for the audience. It also gives the small and logical set of options. Jaquith also gives a good example how this kind of matrices could visualise the business impact on vulnerabilities. In this example the vulnerabilities have three attributes: degree of exploitability, cost to fix the vulnerability and the actual business impact.

5.5.4 Tables

Tables are typically used to show data that has few data points and spanning a single series of data, which any of them dominates. Normally the data in the table is also more relative than precise and the data cannot be explained by numbers alone. The actual data shown in the table can be relatively anything. It can show text, colors, graphics or figures. (Jaquith A, 2007.)

5.5.5 Treemaps

One alternative way to visualise the data set is treemap views. In the treemap view the data structure aggregates hierarchically. Rectangular nodes appear as a patchwork of the other rectangles. The size of each node represents the weight of the attribute. Nodes can also be colored to display the relative importance, criticality or membership in arbitrary category. According to Jaquith (2007) the treemaps are useful for large scale data visualisation that needs simple and compact visual paradigm which fit into small space and are naturally suited for aggregation. (Jaquith A, 2007.)

5.5.6 Other visualisation elements

There also other visualization elements and charts to use for specific needs. Some examples are sankey, stacked donuts and pareto charts which are used when the audience needs to understand each category’s contribution to the total and determine whether the data was disproportionately contributed. (Jaquith A, 2007.)

6 ANALYSES OF QUESTIONAIRE AND INTERVIEWS

As part of the research, a questionnaire was prepared to conduct a qualitative research to obtain information about the research questions and to also further enhance the current cybersecurity measurement practises in the target organisation. The questionnaire was built with Microsoft Office forms and included 5 sections and 20 questions. Draft version of the cybersecurity metrics was given as a reference link and a background material. The open answers of the persons participating in the questionnaire were analysed to find the new or other relevant aspects from the answers. The questionnaire and questions are presented in Appendix 1, questionnaire.

The questionnaire was sent to 67 persons in target organisation and 31 persons answer to it. 19 of those persons were having management role and rest of them were having more operational or technical role. The persons answering to the questionnaire were working in different ICT, business and data analytics, services and operations, internal audit, corporate security and premises organisation units. (Question 3)

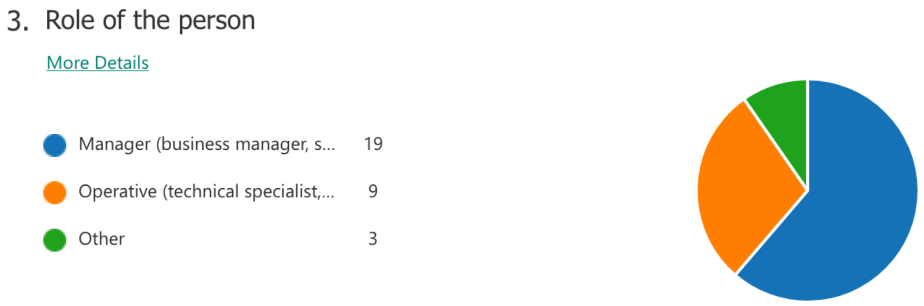
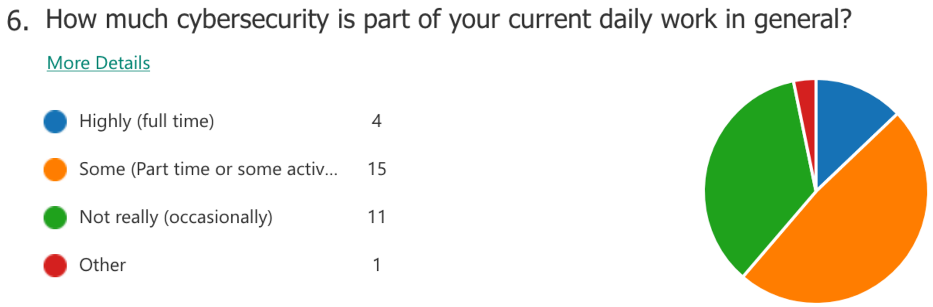


Figure 12. Question 3. of the questionnaire

Nine persons from the target organisation and relevant business unit management persons were selected for the interview. The selection of the interviewed persons was based on their role and to whom the cybersecurity metrics and situational awareness is regularly reported. Interviews were based on the preliminary answers to questionnaire and the interviews were held as a semi-structured to discuss about persons own answer and the particular question. Interviews were held in Finnish language and they took around 45 minutes per each. The actual notes from the interviews are classified as company confidential and cannot be published in this research but some sentences are cited. The information from the interviews were then analysed against earlier part of the theoretical research and the draft version of the metrics. The cybersecurity metrics and requirements for the situational awareness platform were updated based on the ideas from the interviews and the answers from the questionnaire. Both of these are attached in appendixes.

More than half of the persons who answered to the questionnaire has been involved in the cybersecurity work at the target organisation at least part time and 4 persons answered to be working in full time. During the interview, it was found out that one person who responded “Some” felt that he was working part-time on cybersecurity tasks, even though he is actually working full time as Information security specialist. This substantiate the point made earlier that cybersecurity term is not used in target organisation and that the definition of cybersecurity is unambiguous in general. (Question 6)



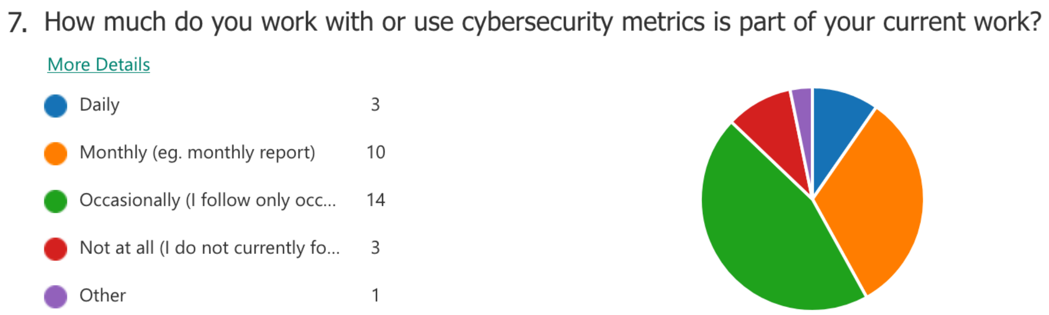
6. How much cybersecurity is part of your current daily work in general?

More Details

●	Highly (full time)	4
●	Some (Part time or some activ...	15
●	Not really (occasionally)	11
●	Other	1

Figure 13. Question 6 of the questionnaire

Most of the persons are also involved regularly in cybersecurity metrics either producing the metrics or following the metrics which is clearly the majority of how the persons are utilising the information from the metrics. There is also clear association that more persons were having manager role and are naturally utilizing the reported metrics rather than producing them. (Questions 7, 8 and 9)

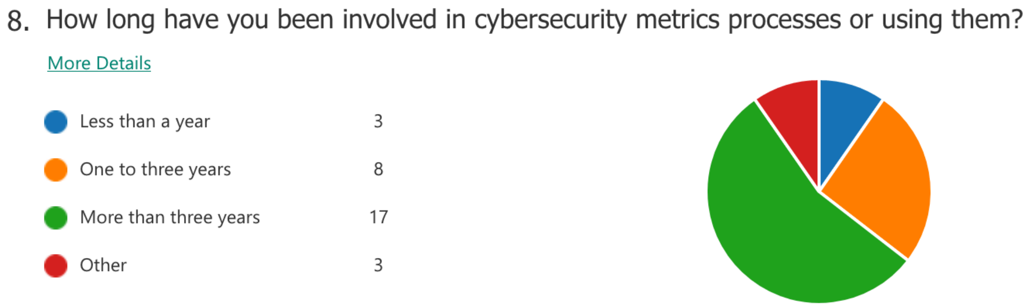


7. How much do you work with or use cybersecurity metrics is part of your current work?

More Details

🔵	Daily	3
🟠	Monthly (eg. monthly report)	10
🟢	Occasionally (I follow only occ...	14
🔴	Not at all (I do not currently fo...	3
🟣	Other	1

Figure 14. Question 7 of the questionnaire

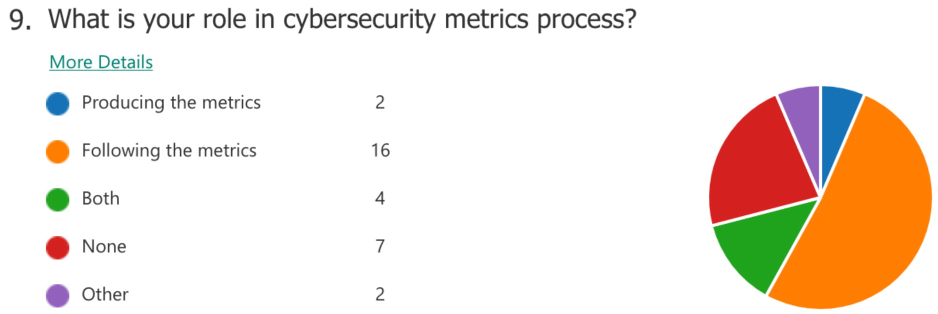


8. How long have you been involved in cybersecurity metrics processes or using them?

More Details

🔵	Less than a year	3
🟠	One to three years	8
🟢	More than three years	17
🔴	Other	3

Figure 15. Question 8 of the questionnaire



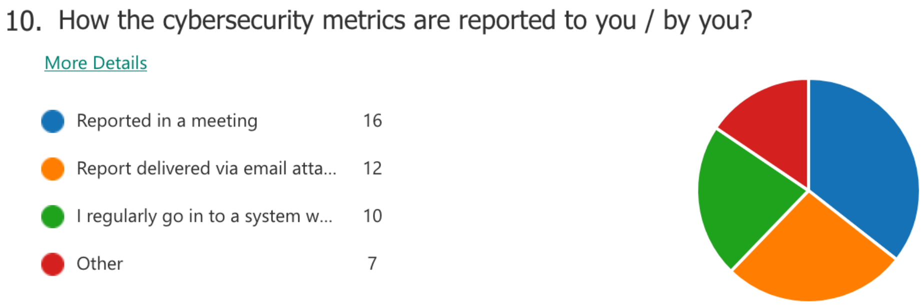
9. What is your role in cybersecurity metrics process?

More Details

🔵	Producing the metrics	2
🟠	Following the metrics	16
🟢	Both	4
🔴	None	7
🟣	Other	2

Figure 16. Question 9 of the questionnaire

In the target organisation the cybersecurity metrics are mostly reported monthly and quarterly by creating standard report in PowerPoint format. These reports are then either send via email or stored in central document repository and then introduced in regular meetings. Some persons who are more involved in operational security are also following the metrics daily and there is also some ad hoc reporting e.g. findings from the security audits. (Questions 10 and 11)

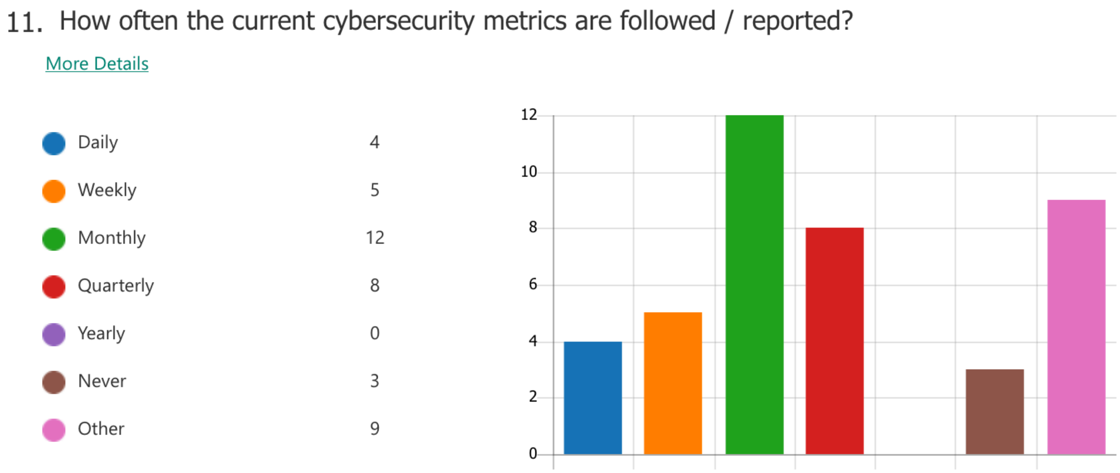


10. How the cybersecurity metrics are reported to you / by you?

More Details

● Reported in a meeting	16
● Report delivered via email atta...	12
● I regularly go in to a system w...	10
● Other	7

Figure 17. Question 10 of the questionnaire



11. How often the current cybersecurity metrics are followed / reported?

More Details

● Daily	4
● Weekly	5
● Monthly	12
● Quarterly	8
● Yearly	0
● Never	3
● Other	9

Figure 18. Question 11 of the questionnaire

12. What cybersecurity metrics are you currently measuring/reporting/following (daily/monthly/periodly)?

In this open type of question persons answers variated quite heavily. This was kind of expected results and didn’t reveal any new metrics or measures from the target organisation. The answers contained the expected areas of cybersecurity metrics such as availability of services, vulnerabilities and patches, infected endpoints, pen-test findings and risk management related measures. (Question 12)

13. What are the current challenges on those cybersecurity metrics or reporting them?

This question revealed that there some challenges in current processes, in metrics general and in reports. Some people mentioned that they have not been involved in the metrics collection and reporting processes, so they were not aware of the metrics used or the challenges involved. This issue can be tackled in the future by raising the awareness of the cybersecurity, creating more organisation unit specific metrics and expanding the delivery of reports and details of the metrics to wider target audience such as all ICT system owners.

Other challenges mentioned in this question were that metrics are cumbersome to gather, takes time and metrics are reported in several places or documents, which makes it hard to follow and challenging to make overall picture of the current status of the cybersecurity. Some persons also answered that target organisation is lacking some relevant information to use with the metrics and to gather the information to a centralized asset and configuration database for cybersecurity needs is challenging task. The information about the assets are on different databases and are more designed to be used by the service providers. Getting the information in one place for cybersecurity needs would probably help within metrics collection too.

Some metrics and their reporting also require fine-tuning for collection frequency and automation. More frequently collected data can be utilized in an almost real-time, automated overview (dashboard) on key metrics. One responder answered that, *“Generating reports requires manual work from specialists so I do not want to ask them these stats too often.”*

Few persons also mentioned that cybersecurity and metrics should be more connected to business and business risks. According to one person,

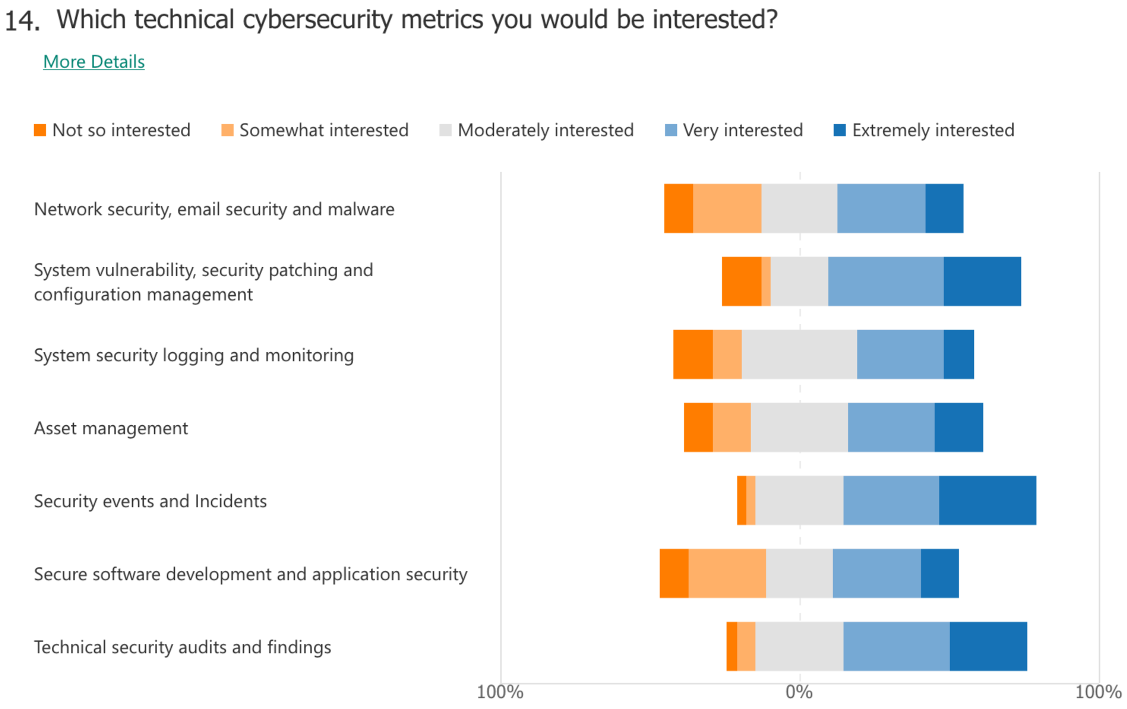
“Metrics should be more relevant for business and top management. Also metrics should have more holistic approach to the potential risks. At the moment some more known issues get more importance in report than they should get if issues would be evaluated on risk basis.”. Also, based on two persons answers it is not clear if the reports lead to any action.

“there is no visibility how the reported data drives the management decisions (impact of the month report?), holistically it's not visible if security efforts and investments are rightly balanced (are we working in silos or towards common up-to-date goals)?”, where as another person answered as,

"What kind of actions are expected to be done based on the report?"

One of the persons in interview also raised that the reporting of current status of cybersecurity in target organisation should also include the global phenomenon's such as latest risks of phishing or ransomware activities.

These answers and the information from the interviews clearly state that the current cybersecurity reports are actually lacking some of the suggested actions based on the reported metrics and numbers. The reported metrics should also be relevant to business- and business-related risks in overall situational awareness. From the interviews, it's also clear that the top management is not actively demanding the reports by them self and those needs to be rather pushed to them to the meeting agenda to make them regular. This could also raise the general knowledge and discussion of today's importance of cybersecurity for business in top management. (Question 13)



14. Which technical cybersecurity metrics you would be interested?

More Details

Figure 19. Question 14 of the questionnaire

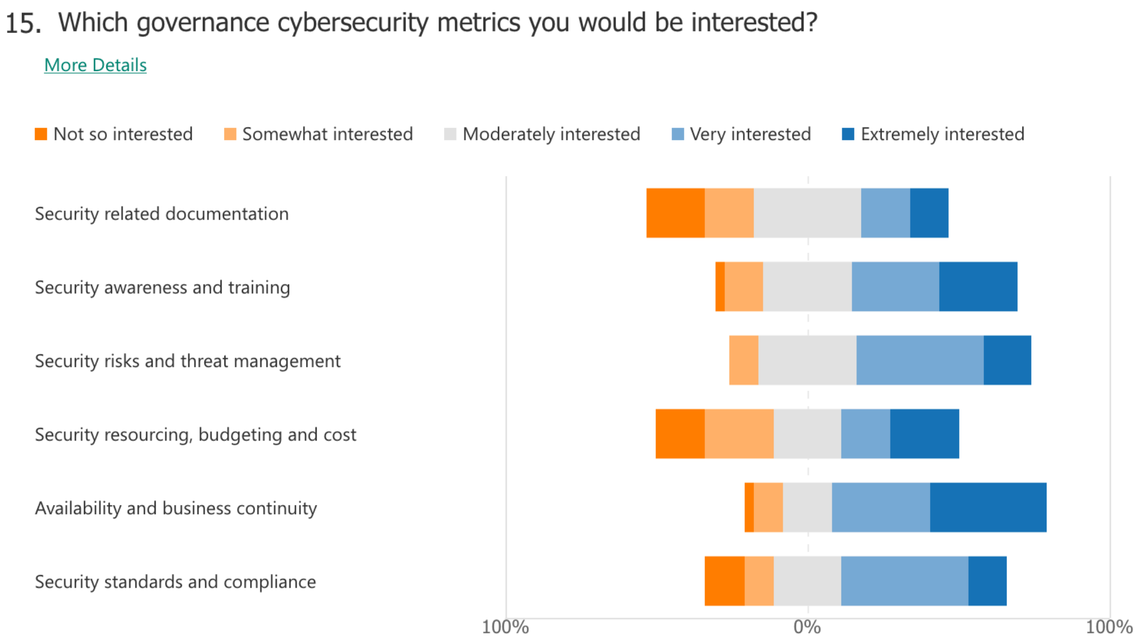


Figure 20. Question 15 of the questionnaire

In general both of the technical and governance type of cybersecurity metrics is interesting to persons answering to this questionnaire. In more technical metrics the most interesting ones are related to security incidents, security audits and findings from them and also ICT system related technical cybersecurity metrics. On the other hand, the system related metrics, which included the malware were also having the most answers combined in “Not so Interested” and “Somewhat interested options”. By analysing the actual answers, it was revealed that all persons who choose this option are not working so closely with ICT in system level, but there were also opposite answers from even one of the person in board level who thinks that systems level metrics are “Extremely interested”. Software and application security related metrics were having little less in interest than the average of other metrics. In this questionnaire, this could be explained that in the target organisation current cybersecurity metrics and the maturity of this cybersecurity area is under active development. In the interviews this area was raised as one of the key metrics areas to be further developed in the future.

In this questionnaire, the availability and business continuity related metrics are seen as the most interesting cybersecurity metric in governance area. This is not surprise in general and also substantiate the earlier point that cybersecurity metrics shall be linked into the business. Metrics in security related documentation are not seen so important among persons, although is important from the compliance point of view in the target organisation. What makes some sort of interesting result is that cost and resourcing is seen almost as equal in interested and not so interested options from the persons answers. There was no clear link between the answer and the background of the person role. In the interviews, the transparency of cybersecurity cost was seen as one of the metric areas that would help to understand organisation to optimise the cybersecurity investments on relevant assets to be protected.

In the interviews it was also raised that broad area of different kind of cybersecurity metrics is seen as a good way to keep transparency on daily cybersecurity work in general and to keep a situational awareness of it. This would then help the organisation to understand the long-term development of different cybersecurity areas and the evolution of potential cybersecurity risks. (Questions 14 and 15)

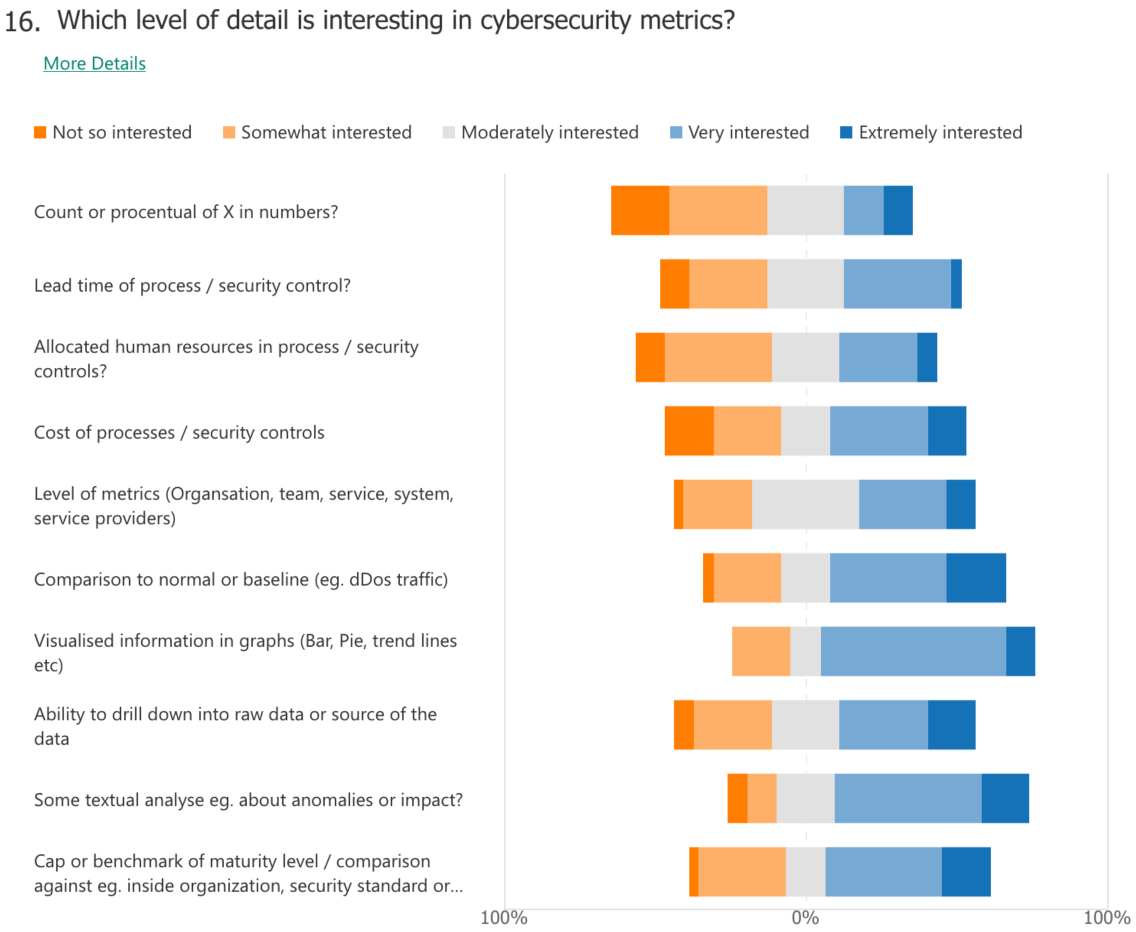


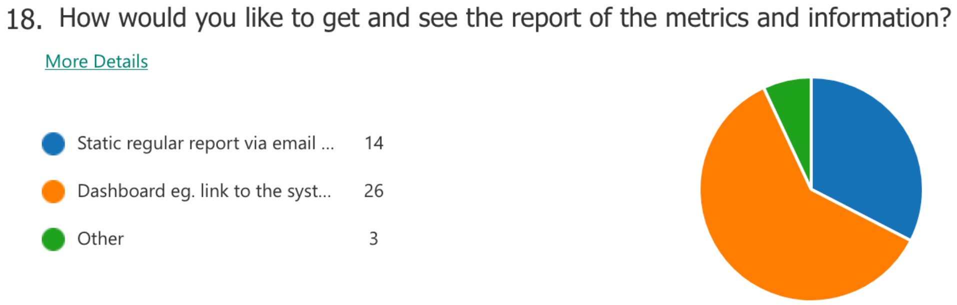
Figure 21. Question 16 of the questionnaire

Although Question 16 reveals that a specific count or number of some measure as a metric as such is not seen an important level of detail, it makes the bases for the more visualisation of the metrics. It is also clear that metrics needs to have some textual analyses of it. By visualising the trend or similar comparison to the baseline is more interesting information than just pure figure or percentual value. Also, as in governance area of cybersecurity metrics the resources and cost are not seen in general so interesting to follow as they seemed to be also in technical area of cybersecurity metrics. Nevertheless, in open answers (Question 17) there was a mention about the relevance of “*threat compared to value (€) of protected asset*”, which would make again the direct link from metric to the risk assessment as a valid argument.

Another person also raised an important point that “*I need to be able to track larger phenomena, but at times, need to drill down to smaller details too.*”. This would mean that the level of details shall be dynamically available for the persons, from the big picture to raw details of the metrics and its source.

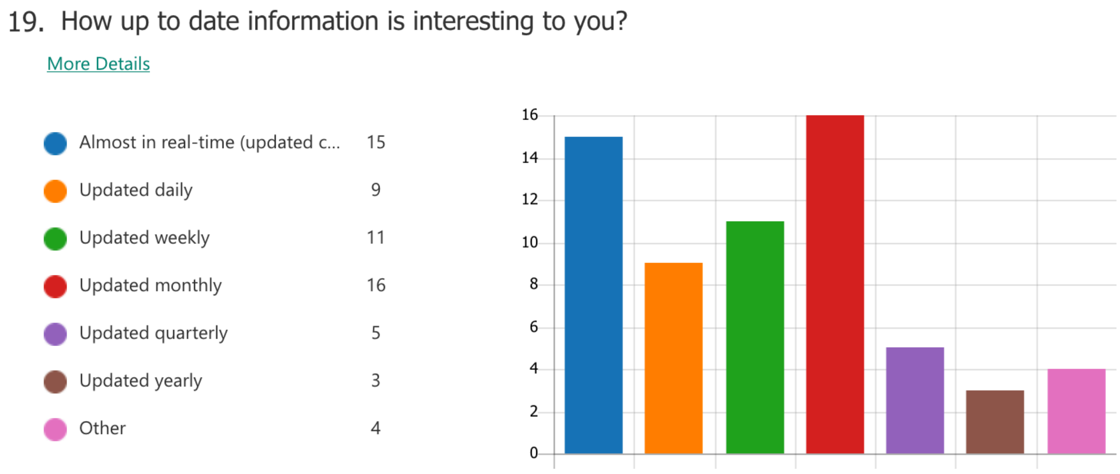
In the interviews it was raised that the level of metrics shall be possible to go at least into team level. This would probably make the actual corrective actions more effective if the metric is more personal or directly affecting the team and giving some public pressure. One person gave an example of such a metric as amount of cybersecurity audit findings per each team. This kind of top teams list would probably work so that the fixes on e.g. vulnerabilities would be introduced in more timely manner. In the interviews it was also raised that potential anomalies are easier to pin-point from the graphs.

Visualisation and especially the colouring were raised as one off the important details. One person in interview said that *“If I have to go through quickly the report, I mostly check if there are any issues highlighted or colored in red in the report”*. This is also substantiating the theory part in this research and the general importance of visualisation also in cybersecurity metrics and situational awareness. (Questions 16 and 17)



18. How would you like to get and see the report of the metrics and information?

Figure 22. Question 18 of the questionnaire



19. How up to date information is interesting to you?

More Details

●	Almost in real-time (updated c...	15
●	Updated daily	9
●	Updated weekly	11
●	Updated monthly	16
●	Updated quarterly	5
●	Updated yearly	3
●	Other	4

Figure 23. Question 19 of the questionnaire

A report that is regularly and statically created is not ideal based on the answers. There is a clear need to be able to create a dashboard type of reports of the metrics that can fulfil all the needs from almost in real-time information to yearly comparison of the cybersecurity metrics in timeline wise. Ideally, this kind of dynamic dashboard could be exported as a static report to be send separately via email.

In the interviews few persons raised that the almost in real-time information and situational awareness is necessary to be able to act on time in operational level in the current world of cybersecurity. The monthly or quarterly based reporting cycle works more like as a diary and is still a valid information for development and to make a baseline comparison. (Questions 18 and 19)

7 RESULTS AND DISCUSSION

It is clear that there appears to be many different definitions related to the term of ‘cybersecurity’. The understanding of the term is diverging in many publications, security institutes and frameworks. Although, this was not the primary research target in this study, the same phenomenon was also seen during the interviews and by analysing the answers from questionnaire. It was stated few times during the interview that the term was not so familiar to them and that it may have affected some of their answers. It also appears that there is no single cybersecurity framework that extensively covers cybersecurity metrics. Also, the parameters or variables used to present the cybersecurity metrics in the various frameworks are incomplete and appear to be inconsistent, and in some have not even been defined. This can lead to their inability to use or at least make harder to implement in some organisations. Cybersecurity is a broad topic and covers multiple sub areas. Without a proper definition of the scope, it is difficult to include appropriate cybersecurity measurements.

The main result and outcome of this thesis was the examples of collected cybersecurity metrics and the requirements for cybersecurity situational awareness platform. They are presented in Appendix 2. and Appendix 3. The cybersecurity metrics were collected from several cybersecurity control frameworks and publications and later modified to meet the needs of target organisation after the interviews.

These appendices contain the key elements of the cybersecurity metrics, information sources and the data that is needed to build cybersecurity measuring and situational awareness. These collected metrics would at least work as a starting point for the whole for other organisations. The information sources may vary on other organisations and would for example, heavily depend on the available information technology, processes and the assets that needs to be protected in that particular organisation.

Although some of the metrics are already in used and are regularly measured in target organisation there is not yet holistic cybersecurity situational awareness created on them. So, in this research it cannot be proven whether these collected metrics work in practise or are they still relevant for the purpose or how much they still need some fine tuning.

In general by analysing the answers in this questionnaire and from the interviews, it is clear that there are different views and interests focus in person and even in same or similar roles working in this target organisation. The answers and the interest of the persons in target organisation is reinforcing the commonly raised point of views in the theory part of this research e.g. the importance of visualization of cybersecurity metrics. Also, by having the situational awareness and proper metrics in place, the maturity of cybersecurity in the organisation would be easier to measure.

It is also clear from the research that risk management processes, and in particular the cost of risk factors to the organisation, need to be somehow included in the measurement and overall picture. In this research, cost factors were only briefly addressed as part of the metrics and would definitely require much more research to make them useful for situational awareness.

In this research Endsley theoretical model (Endsley, 1995) was used as a background theoretical model. This model has similarities in cybersecurity situational awareness. Without the information from cybersecurity metrics and their possible contexts, it is not only ineffective, but also extremely difficult to understand the current state of the organisation's cybersecurity posture. This would also make the predictability impossible and at the end could lead into the exposure of unwanted cyber risk.

As described in earlier chapters, an important part of the cybersecurity metrics design process is continuous improvement. In practice, this means that the cybersecurity metrics must be reviewed and refined periodically. Based on the experiences in this research, organisations should use more time on the design phase. Potential stakeholders should be involved as soon as possible in cybersecurity metrics design processes as they have different needs and views. The cybersecurity metrics design should start with small steps. By using sources that are already available, the organisation would certainly go a long way in measuring metrics and processes. Also the use of modern agile working methods, characterized by the dividing of tasks into smaller entities and their repeated reassessment, would probably be effective in designing and reviewing cyber security metrics. When properly designed, then implemented and keep up to date the cybersecurity metrics can be very useful for the organisation to create a cybersecurity situational awareness.

It was also recognized that it is important to visualize the metrics. Visualisations are inevitable for humans to pinpoint abnormal behaviour or exceptions. Also, the mere numbers for the current state of cybersecurity may not always be sufficient. The number alone does not reveal, for example, if the situation is getting worse or better. Nor do the numbers alone indicate the historical information needed to predict and create situational awareness.

The requirements for cybersecurity situational awareness platform (Appendix 2.) has evolved during the research. The cybersecurity metrics and especially the sources has been the driver to write the requirements. As an outcome the platform shall be as dynamic as possible. The key features of proper cybersecurity metric platform are versatile integration capabilities and ability to create versatile views for the audience. The data processing is also important. The ability to process raw data and combine it with another source will produce the best results for different kind of needs.

In cybersecurity there is always some uncertainty. The research of cybersecurity and cybersecurity metrics area poses still open problems for researchers – there is not clearly defined cybersecurity framework for metrics to taken into use. Obtaining and building cybersecurity situational awareness based on metrics is clearly not enough. It is still a pretty good starting point for evaluating organisation and protecting the information assets and business. Although this research was conducted in only one organisation, the results and the requirements of cybersecurity situational awareness platform can be applied to any organisation as a starting point for creating cybersecurity measurement and situational awareness.

7.1 Suggestions for further research

Cybersecurity is constantly evolving field of research for the attacks, threats and new technologies. There are multiple cybersecurity frameworks available and most of them has taken risk-based approach to define and implement the controls. These frameworks could be enhanced to include a more standard and to provide essential metrics for the actual controls. These frameworks also kind of lack the physical part of the cybersecurity area and those metrics could be defined and included. Although most organisations do work in different business areas and has also different approaches to cybersecurity, the frameworks could be more standardised in the metrics and especially their parametrisations. This would make comparison and benchmarking possible between the different frameworks.

Another proposal for further research is to research how the metrics collection could be automated and orchestrated. Most of the technology used to implement security controls are capable of providing events e.g. SIEM system but not necessary to collect and prepare the information needed for the actual cybersecurity metrics and situational awareness. There would probably be a lot of manual work that could be automated and pre-processed before being analysed by humans.

Cybersecurity incident response capability is important for every organisation. Incident response needs fast reaction and decision to be made during the attack. Almost real time situational awareness during the cyber incident would be beneficial to mitigate the attacker actions. A closer look at what information and metrics would help during the attack and make the incident more effective could be researched in that field.

There are also new areas of research and capabilities that could assist in the analysis of cybersecurity metrics. Artificial intelligence and machine learning, for example, are both areas that can be used not only to help monitor and detect abnormal behaviours or abnormalities, but also to raise potential problems for the future and help with decision making.

REFERENCES

Black P.E., Scarfone K.A, Souppaya M.P. 2009. Cyber Security Metrics and Measures. National Institute of Standards and Technology, Gaithersburg, Maryland, United States.

Brookson C, Cadzow S, Eckmaier R, Eschweiler J, Gerber B, Guarino A, Rannenberg K, Shamah J, Górniak S. 2015. European Network and Information Security Agency. Definition of Cybersecurity: Gaps and Overlaps in Standardisation. Heraklion.

Brotby W. K., Hinson G. 2013. PRAGMATIC Security Metrics: Applying Metametrics to Information Security. Taylor & Francis Group, LLC. CRC Press. Florida, United States

Center for Internet Security. 2018. CIS Controls. WWW document. Available at: https://www.cisecurity.org/controls/

Cheng Y., Deng J., Li J., DeLoach S.A., Singhal A., Ou X. 2014. Metrics of Security. In: Kott A., Wang C., Erbacher R. (eds) Cyber Defense and Situational Awareness. Advances in Information Security, vol 62. Springer, Cham, pp 263-295.

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

Chuvakin A. 2018. Preparing Your Security Operations for Orchestration and Automation Tools, ID G00325580. Gartner, Inc. WWW document. Available at: https://www.gartner.com/document/3860563 [Accessed 14 February 2019]

CNBC. 2018. Moody’s is going to start building the risk of a business-ending hack into its credit ratings. WWW document. Available at: https://www.cnbc.com/amp/2018/11/12/moodys-to-build-business-hacking-risk-into-credit-ratings.html [Accessed 10 January 2019].

Cunningham R. Pfleeger S.L. 2010. Why Measuring Security Is Hard, IEEE Security and Privacy Magazine 8(4), 46–54. https://www.researchgate.net/publication/220496799_Why_Measuring_Security_Is_Hard [Accessed 22 July 2018].

DeBeasi P. 2019. 2019 Planning Guide Overview: Architecting Your Digital Ecosystem. WWW document. Available at: https://www.gartner.com/document/3891192 [Accessed 14 February 2019]

Dimensional Research. 2016. Trends in Security Framework Adoption: A Survey of IT And Security Professionals. WWW document.

http://static.tenable.com/marketing/tenable-csf-report.pdf [Accessed 13 November 2018]

Distilnetworks. Bad Bot Report 2017. WWW document. Available at: https://resources.distilnetworks.com/white-paper-reports/2017-bad-bot-report [Accessed 22 March 2019]

Flück D. 2012. Color Blind Essentials. Colblindor. WWW document. Available at: http://www.color-blindness.com/wp-content/documents/Color-Blind-Essentials.pdf. [Accessed 10 February 2019].

European Union Agency for Fundamental Rights and Council of Europe. 2018. Handbook on European data protection law, 2018 Edition. Publications Office of the European Union, Luxemburg. WWW document. Available at: https://publications.europa.eu/en/publication-detail/-/publication/5b0cfa83-63f3-11e8-ab9c-01aa75ed71a1/language-en [Accessed 22 October 2018].

Fisher D, 2012. Final Report on DigiNotar Hack Shows Total Compromise of CA Servers. WWW document. Available at: https://threatpost.com/final-report-diginotar-hack-shows-total-compromise-ca-servers-103112/77170/ [Accessed 22 July 2018].

Endsley M.R. 1995. Toward a Theory of Situation Awareness in Dynamic Systems. Human Factors Journal 37(1).

Galan Manso C., Rekleitis E., Papazafeiropoulos F., Maritsas V. 2015. European Network and Information Security Agency. Information security and privacy standards for SMEs: recommendations to improve the adoption of information security and privacy standards in small and medium enterprises. ENISA, Heraklion.

Hayden L. 2010. IT Security Metrics: A Practical Framework for Measuring Security & Protecting Data. McGraw-Hill Companies, United States.

Hubbard D.W., Seiersen R. 2016. Howto Measure Anything in Cybersecurity Risk. John Wiley & Sons, Inc., Hoboken, New Jersey, United States.

International Data Corporation. 2019. Worldwide Spending on Security Solutions Forecast to Reach $103.1 Billion in 2019, According to a New IDC Spending Guide. WWW document. Available at: https://www.idc.com/getdoc.jsp?containerId=IDC_P33461 [Accessed 29.11.2019]

Information Systems Audit and Control Association, 2018. COBIT 2019 Framework: Introduction & Methodology. Information Systems Audit and Control Association, Schaumburg, Illinois, United States.

Information Systems Audit and Control Association, 2018. COBIT 2019 Framework: Governance and Management Objectives. Information Systems Audit and Control Association, Schaumburg, Illinois, United States.

Information Systems Audit and Control Association 2018. Entire Glossary. Information Systems Audit and Control Association. WWW document. Available at: https://www.isaca.org/Knowledge-Center/Documents/Glossary/glossary.pdf [Accessed 16 November 2018]

Information Systems Audit and Control Association 2018. Cybersecurity Glossary. Information Systems Audit and Control Association. WWW document. Available at: https://www.isaca.org/Knowledge-Center/Documents/Glossary/Cybersecurity_Fundamentals_glossary.pdf [Accessed 16 November 2018]

ISO/IEC 27001:2017. Information technology. Security techniques. Information security management systems requirements. International Organization for Standardization, Geneva, Switzerland.

ISO/IEC 27002:2017. Information technology. Security techniques. Code of practice for information security. International Organization for Standardization, Geneva, Switzerland.

ISO/IEC 27004:2016. Information technology – Security techniques – Information security management – Monitoring, measurement, analysis and evaluation. International Organization for Standardization, Geneva, Switzerland.

ISO/IEC 27032:2016. Information technology – Security techniques – Guidelines for cybersecurity. International Organization for Standardization, Geneva, Switzerland.

Jansen W. 2009. Directions in Security Metrics Research, NISTIR 7564. National Institute of Standards and Technology, Gaithersburg, Maryland, United States.

Jaquiteh A. 2007. Security Metrics: Replacing Fear, Uncertantity and Doubt. Pearson Education, Inc. Addison-Wesley Professional, United States.

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

Kaplan R. 2010 Conceptual Foundations of the Balanced Scorecard. WWW document. Available at: https://www.hbs.edu/faculty/Publication%20Files/10-074_0bf3c151-f82b-4592-b885-cdde7f5d97a6.pdf [Accessed 21 March 2019]

Kissel R.L. 2013, Glossary of Key Information Security Terms, NISTIR 7298 Revision 2. National Institute of Standards and Technology, Gaithersburg, Maryland, United States.

McMillan R., Proctor P. 2018. Cybersecurity and Digital Risk Management: CIOs Must Engage and Prepare. WWW document. Available at: https://www.gartner.com/document/3846477 [Accessed 13 January 2018]

Lindström P. 2005. Security: Measuring Up. WWW document. Available at: https://searchsecurity.techtarget.com/tip/Security-Measuring-Up [Accessed 22 March 2018]

Marty R. 2009. Applied Security Visualization. Pearson Education, Inc. Boston, United States.

National Institute of Standards and Technology, 2018. Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. National Institute of Standards and Technology, Gaithersburg, Maryland, United States.

Payne S. 2007. A Guide to Security Metrics. SANS Institute. WWW document. Available at: https://www.sans.org/reading-room/whitepapers/auditing/guide-security-metrics-55 [Accessed 2 April 2019]

Prins J.R. 2011. Interim Report DigiNotar Certificate Authority breach. WWW document. Available at: http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/rapporten/2011/09/05/diginotar-public-report-version-1/rapport-fox-it-operation-black-tulip-v1-0.pdf [Accessed 22 July 2018].

Regulation (EU) 2016/679. European Parliament And Council. 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). WWW document. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN [Accessed 5 August 2018].

Richards K., Lasalle R., Devost M., Kennedy-White J. 2017. Cost of Cyber Crime Study. WWW document. Available at: https://www.accenture.com/us-en/insight-cost-of-cybercrime-2017 [Accessed 24 November 2018]

Schneier B. 2000. The Process of Security. WWW document. Available at: https://www.schneier.com/essays/archives/2000/04/the_process_of_secur.html [Accessed 15 March 2019]

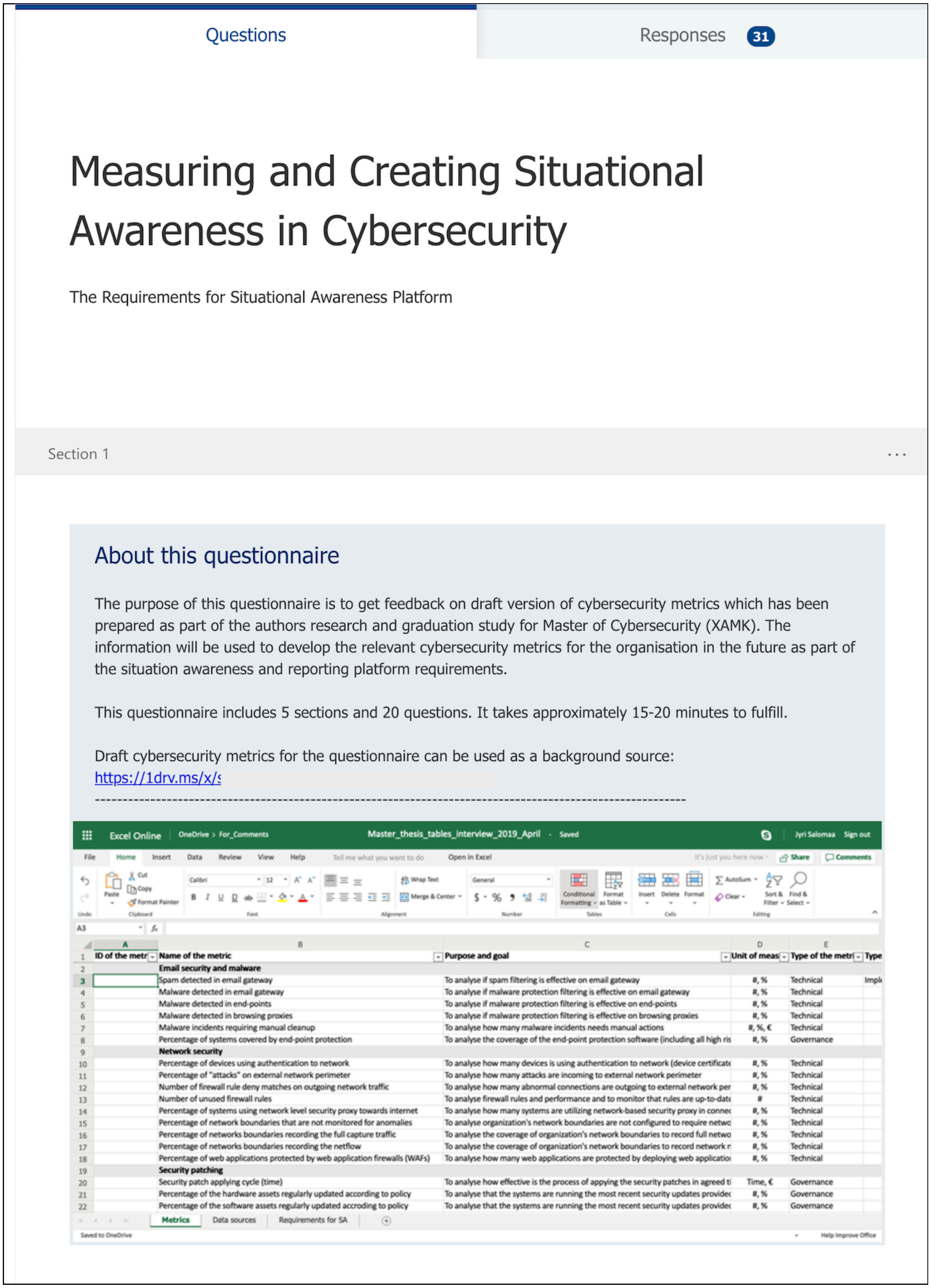
Storms A. 2016. How To Talk About Security With Every C-Suite Member. WWW document. Available at: https://www.darkreading.com/vulnerabilities---threats/how-to-talk-about-security-with-every-c-suite-member/a/d-id/1326784 [Accessed 24 February 2019]

Thakore U. 2015. A Quantitative Methodology For Evaluating And Deploying Security Monitors. WWW document. Available at: https://www.ideals.illinois.edu/bitstream/handle/2142/88103/THAKORE-THESIS-2015.pdf?sequence=1&isAllowed=y [Accessed 2 April 2019]

LIST OF FIGURES

Appendix 1.

Questionnaire about cybersecurity metrics and situational awareness



Measuring and Creating Situational Awareness in Cybersecurity

The Requirements for Situational Awareness Platform

Section 1

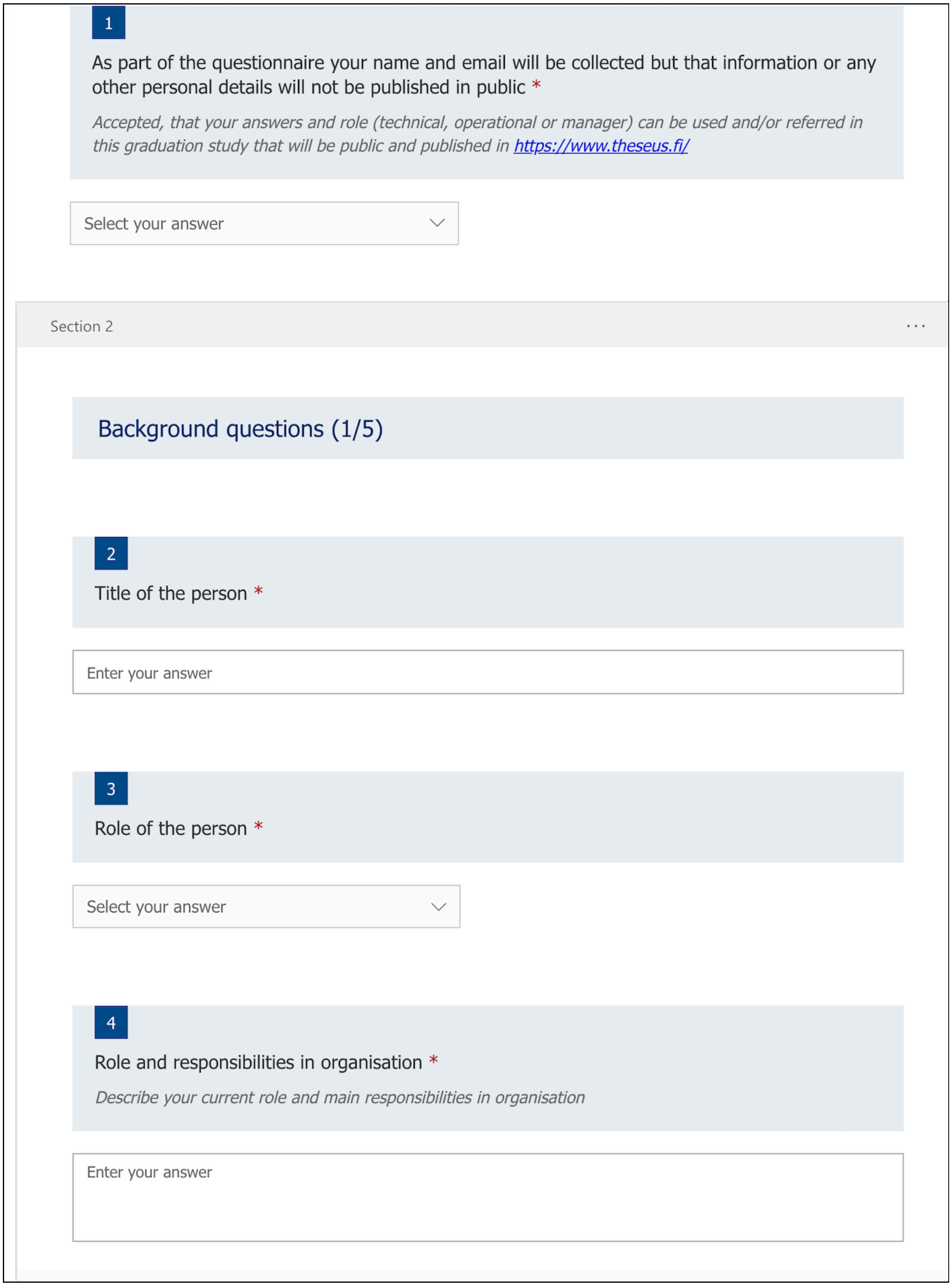
About this questionnaire

The purpose of this questionnaire is to get feedback on draft version of cybersecurity metrics which has been prepared as part of the authors research and graduation study for Master of Cybersecurity (XAMK). The information will be used to develop the relevant cybersecurity metrics for the organisation in the future as part of the situation awareness and reporting platform requirements.

This questionnaire includes 5 sections and 20 questions. It takes approximately 15-20 minutes to fulfill.

Draft cybersecurity metrics for the questionnaire can be used as a background source:
https://1drv.ms/x/s

	A	B	C	D	E	
1	ID of the metr	Name of the metric	Purpose and goal	Unit of meas	Type of the metr	Type
2		**Email security and malware**				
3		Spam detected in email gateway	To analyse if spam filtering is effective on email gateway	#, %	Technical	Impl
4		Malware detected in email gateway	To analyse if malware protection filtering is effective on email gateway	#, %	Technical	
5		Malware detected in end-points	To analyse if malware protection filtering is effective on end-points	#, %	Technical	
6		Malware detected in browsing proxies	To analyse if malware protection filtering is effective on browsing proxies	#, %	Technical	
7		Malware incidents requiring manual cleanup	To analyse how many malware incidents needs manual actions	#, %, €	Technical	
8		Percentage of systems covered by end-point protection	To analyse the coverage of the end-point protection software (including all high ris	#, %	Governance	
9		**Network security**				
10		Percentage of devices using authentication to network	To analyse how many devices is using authentication to network (device certificate	#, %	Technical	
11		Percentage of "attacks" on external network perimeter	To analyse how many attacks are incoming to external network perimeter	#, %	Technical	
12		Number of firewall rule deny matches on outgoing network traffic	To analyse how many abnormal connections are outgoing to external network per	#, %	Technical	
13		Number of unused firewall rules	To analyse firewall rules and performance and to monitor that rules are up-to-date	#	Technical	
14		Percentage of systems using network level security proxy towards internet	To analyse how many systems are utilizing network-based security proxy in connec	#, %	Technical	
15		Percentage of network boundaries that are not monitored for anomalies	To analyse organization's network boundaries are not configured to require netwo	#, %	Technical	
16		Percentage of networks boundaries recording the full capture traffic	To analyse the coverage of organization's network boundaries to record full netwo	#, %	Technical	
17		Percentage of networks boundaries recording the netflow	To analyse the coverage of organization's network boundaries to record network r	#, %	Technical	
18		Percentage of web applications protected by web application firewalls (WAFs)	To analyse how many web applications are protected by deploying web applicatio	#, %	Technical	
19		**Security patching**				
20		Security patch applying cycle (time)	To analyse how effective is the process of appying the security patches in agreed ti	Time, €	Governance	
21		Percentage of the hardware assets regularly updated according to policy	To analyse that the systems are running the most recent security updates providec	#, %	Governance	
22		Percentage of the software assets regularly updated accroding to policy	To analyse that the systems are running the most recent security updates providec	#, %	Governance	



1

As part of the questionnaire your name and email will be collected but that information or any other personal details will not be published in public *

Accepted, that your answers and role (technical, operational or manager) can be used and/or referred in this graduation study that will be public and published in https://www.theseus.fi/

Select your answer

Section 2

Background questions (1/5)

2

Title of the person *

Enter your answer

3

Role of the person *

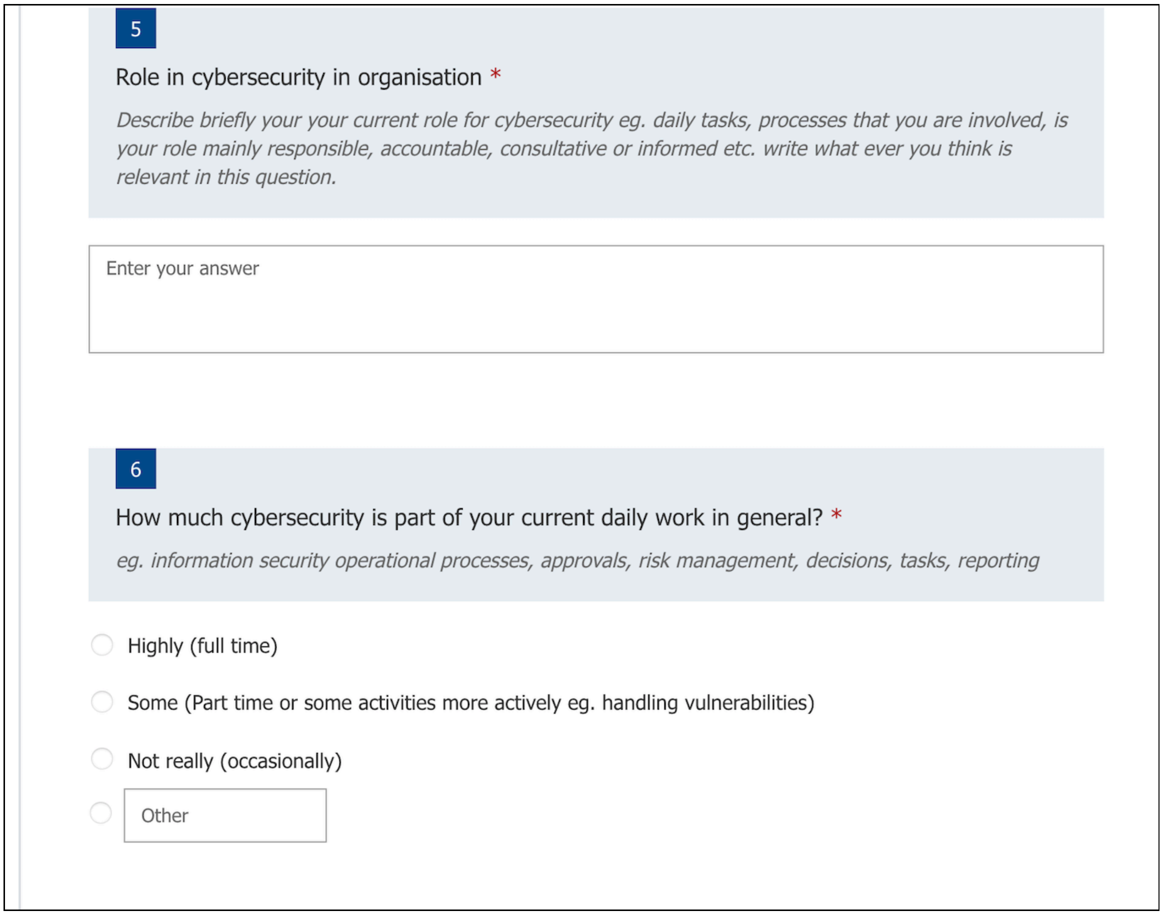
Select your answer

4

Role and responsibilities in organisation *

Describe your current role and main responsibilities in organisation

Enter your answer



5

Role in cybersecurity in organisation *

Describe briefly your your current role for cybersecurity eg. daily tasks, processes that you are involved, is your role mainly responsible, accountable, consultative or informed etc. write what ever you think is relevant in this question.

Enter your answer

6

How much cybersecurity is part of your current daily work in general? *

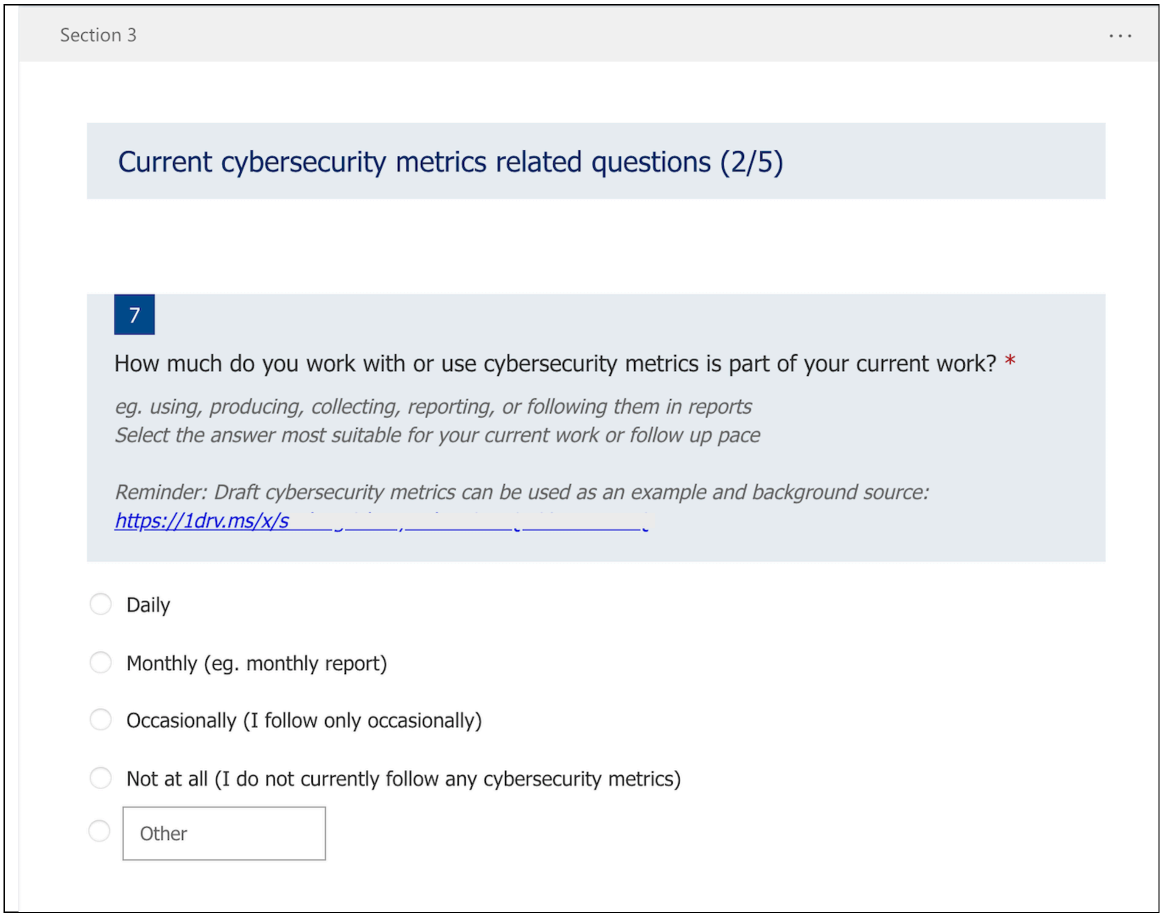
eg. information security operational processes, approvals, risk management, decisions, tasks, reporting

○ Highly (full time)

○ Some (Part time or some activities more actively eg. handling vulnerabilities)

○ Not really (occasionally)

○ Other



Section 3

Current cybersecurity metrics related questions (2/5)

7

How much do you work with or use cybersecurity metrics is part of your current work? *

eg. using, producing, collecting, reporting, or following them in reports
Select the answer most suitable for your current work or follow up pace

Reminder: Draft cybersecurity metrics can be used as an example and background source:
https://1drv.ms/x/s[redacted]

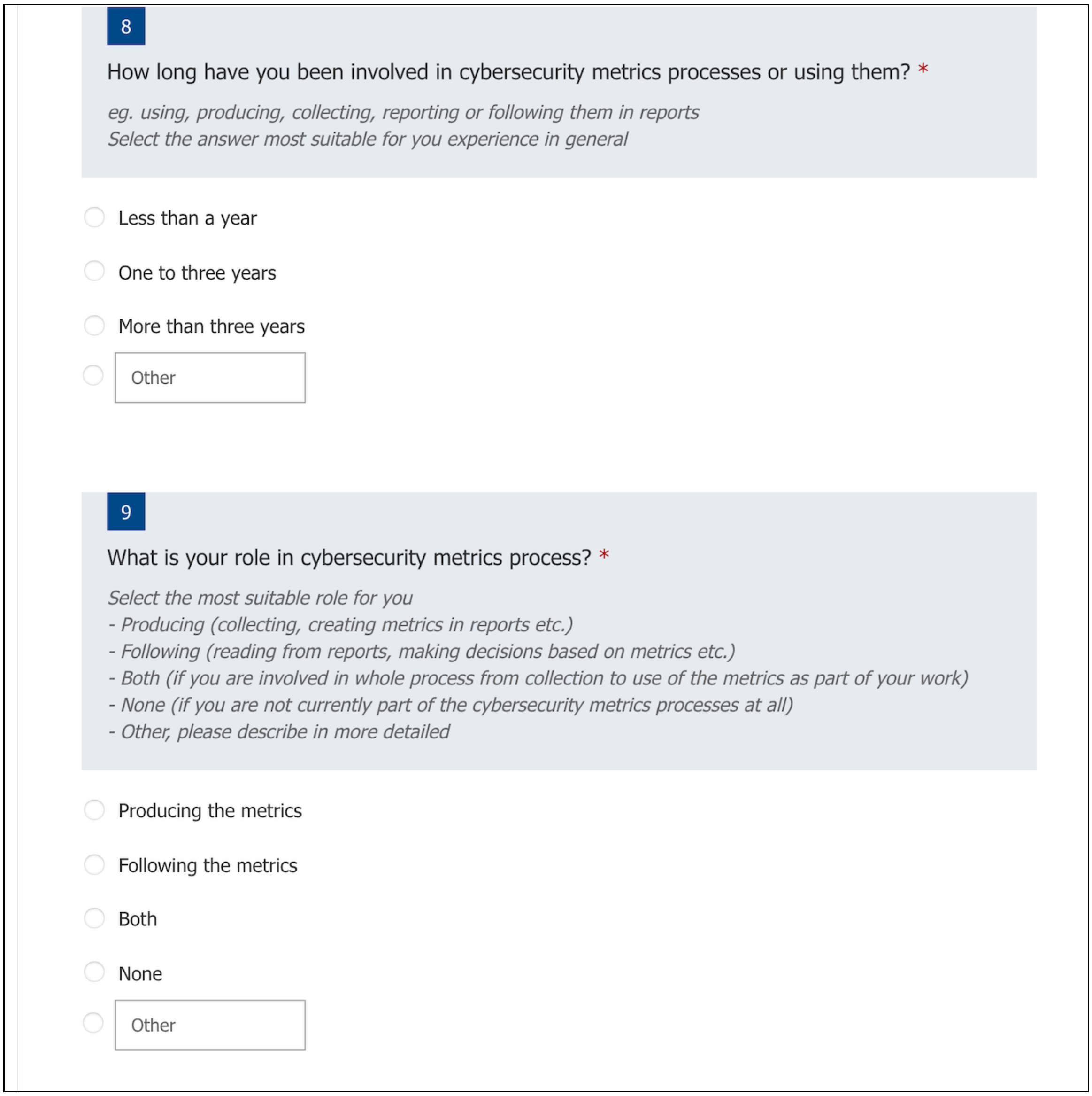
○ Daily

○ Monthly (eg. monthly report)

○ Occasionally (I follow only occasionally)

○ Not at all (I do not currently follow any cybersecurity metrics)

○ Other



8

How long have you been involved in cybersecurity metrics processes or using them? *

eg. using, producing, collecting, reporting or following them in reports
Select the answer most suitable for you experience in general

○ Less than a year

○ One to three years

○ More than three years

○ Other

9

What is your role in cybersecurity metrics process? *

Select the most suitable role for you
- Producing (collecting, creating metrics in reports etc.)
- Following (reading from reports, making decisions based on metrics etc.)
- Both (if you are involved in whole process from collection to use of the metrics as part of your work)
- None (if you are not currently part of the cybersecurity metrics processes at all)
- Other, please describe in more detailed

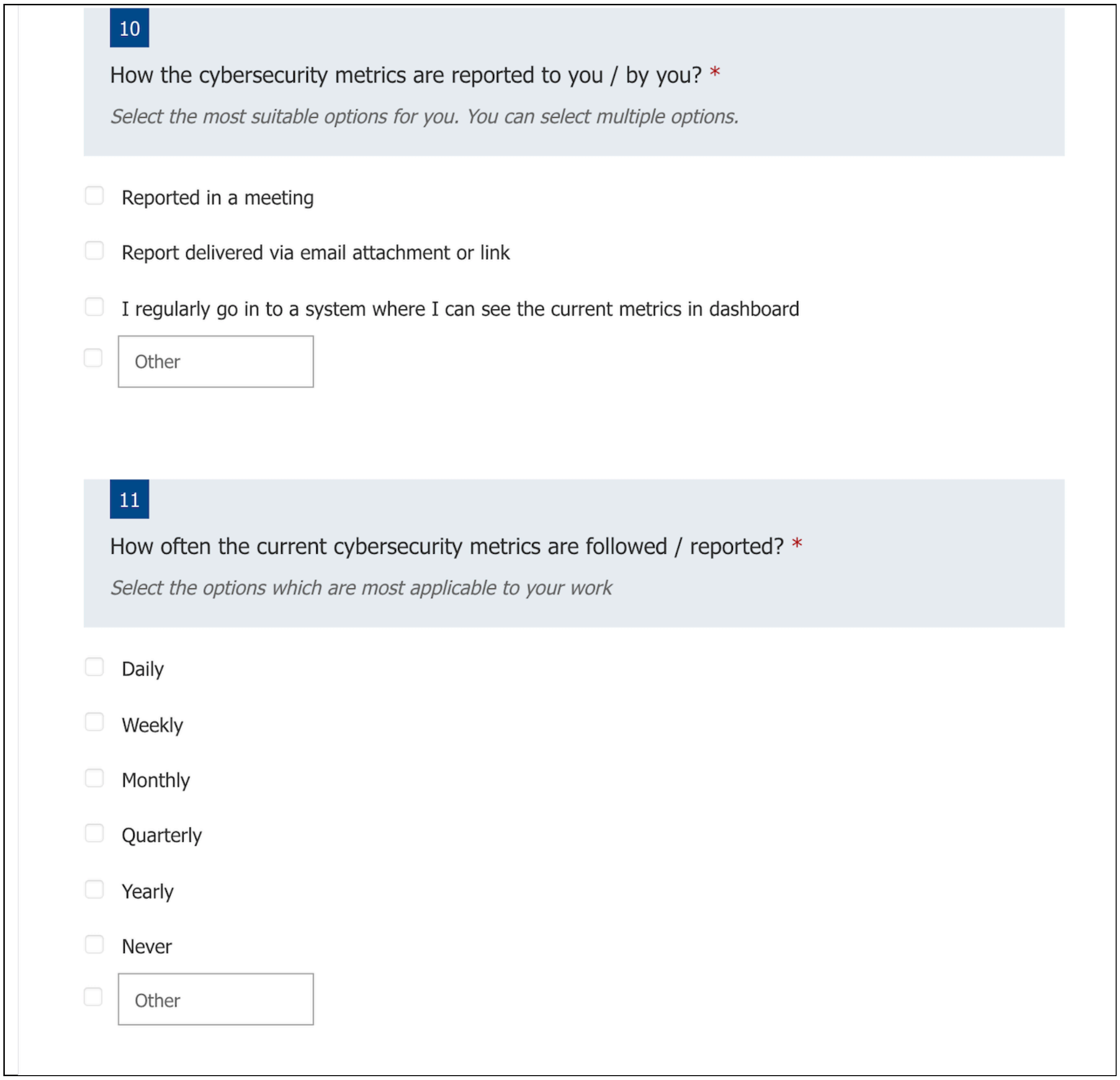
○ Producing the metrics

○ Following the metrics

○ Both

○ None

○ Other



10

How the cybersecurity metrics are reported to you / by you? *

Select the most suitable options for you. You can select multiple options.

□ Reported in a meeting

□ Report delivered via email attachment or link

□ I regularly go in to a system where I can see the current metrics in dashboard

□ Other

11

How often the current cybersecurity metrics are followed / reported? *

Select the options which are most applicable to your work

□ Daily

□ Weekly

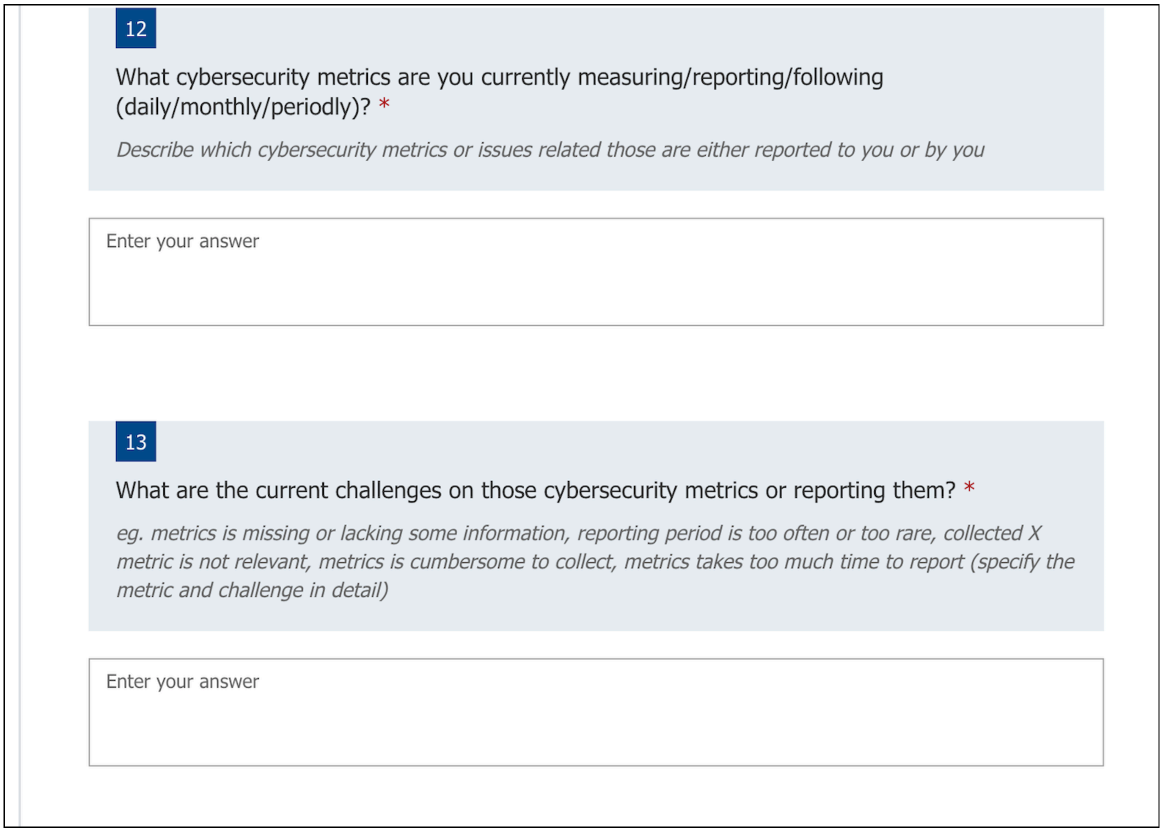
□ Monthly

□ Quarterly

□ Yearly

□ Never

□ Other



12

What cybersecurity metrics are you currently measuring/reporting/following (daily/monthly/periodly)? *

Describe which cybersecurity metrics or issues related those are either reported to you or by you

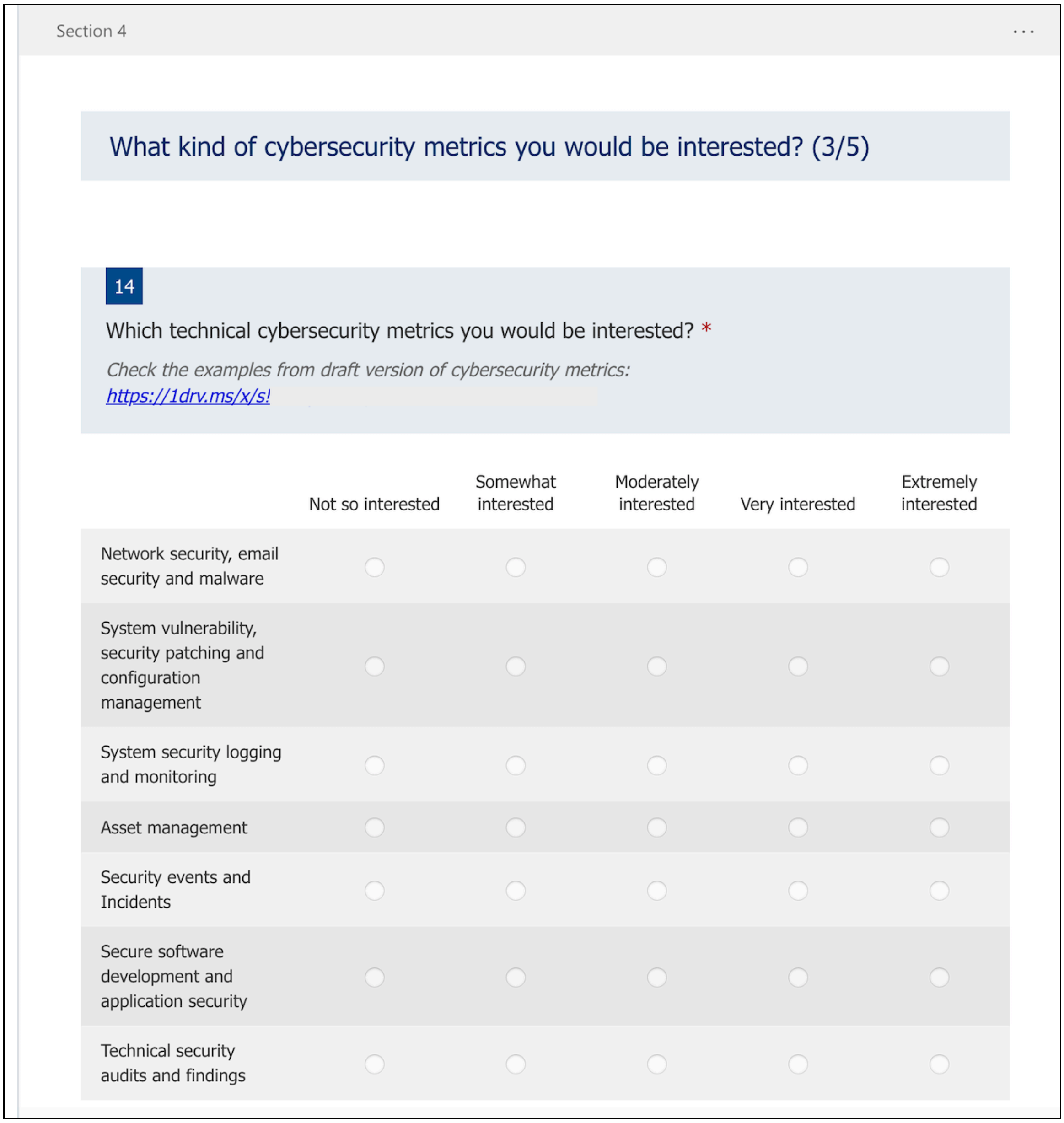
Enter your answer

13

What are the current challenges on those cybersecurity metrics or reporting them? *

eg. metrics is missing or lacking some information, reporting period is too often or too rare, collected X metric is not relevant, metrics is cumbersome to collect, metrics takes too much time to report (specify the metric and challenge in detail)

Enter your answer



Section 4

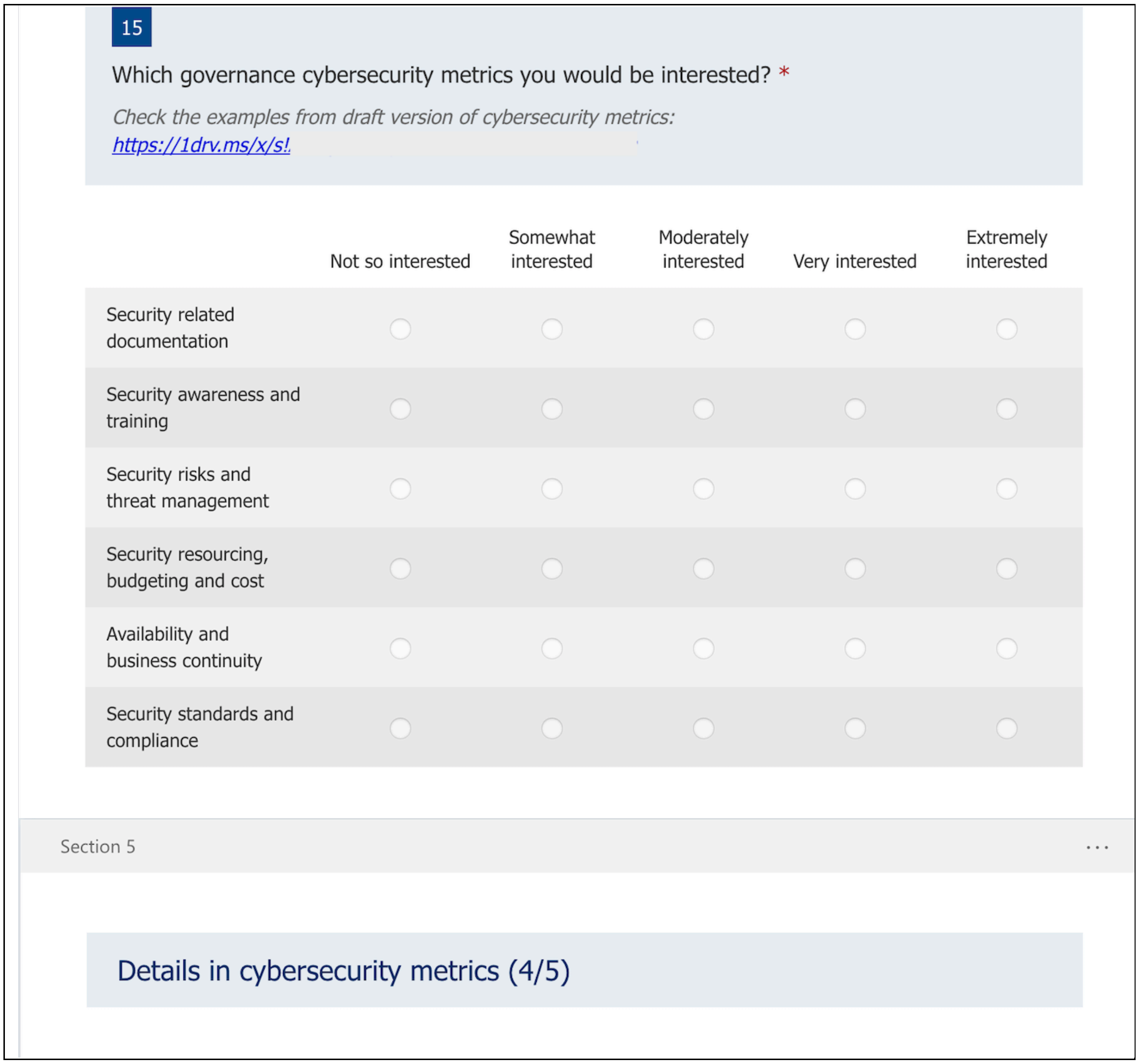
What kind of cybersecurity metrics you would be interested? (3/5)

14

Which technical cybersecurity metrics you would be interested? *

Check the examples from draft version of cybersecurity metrics:
https://1drv.ms/x/s!

	Not so interested	Somewhat interested	Moderately interested	Very interested	Extremely interested
Network security, email security and malware	○	○	○	○	○
System vulnerability, security patching and configuration management	○	○	○	○	○
System security logging and monitoring	○	○	○	○	○
Asset management	○	○	○	○	○
Security events and Incidents	○	○	○	○	○
Secure software development and application security	○	○	○	○	○
Technical security audits and findings	○	○	○	○	○



15

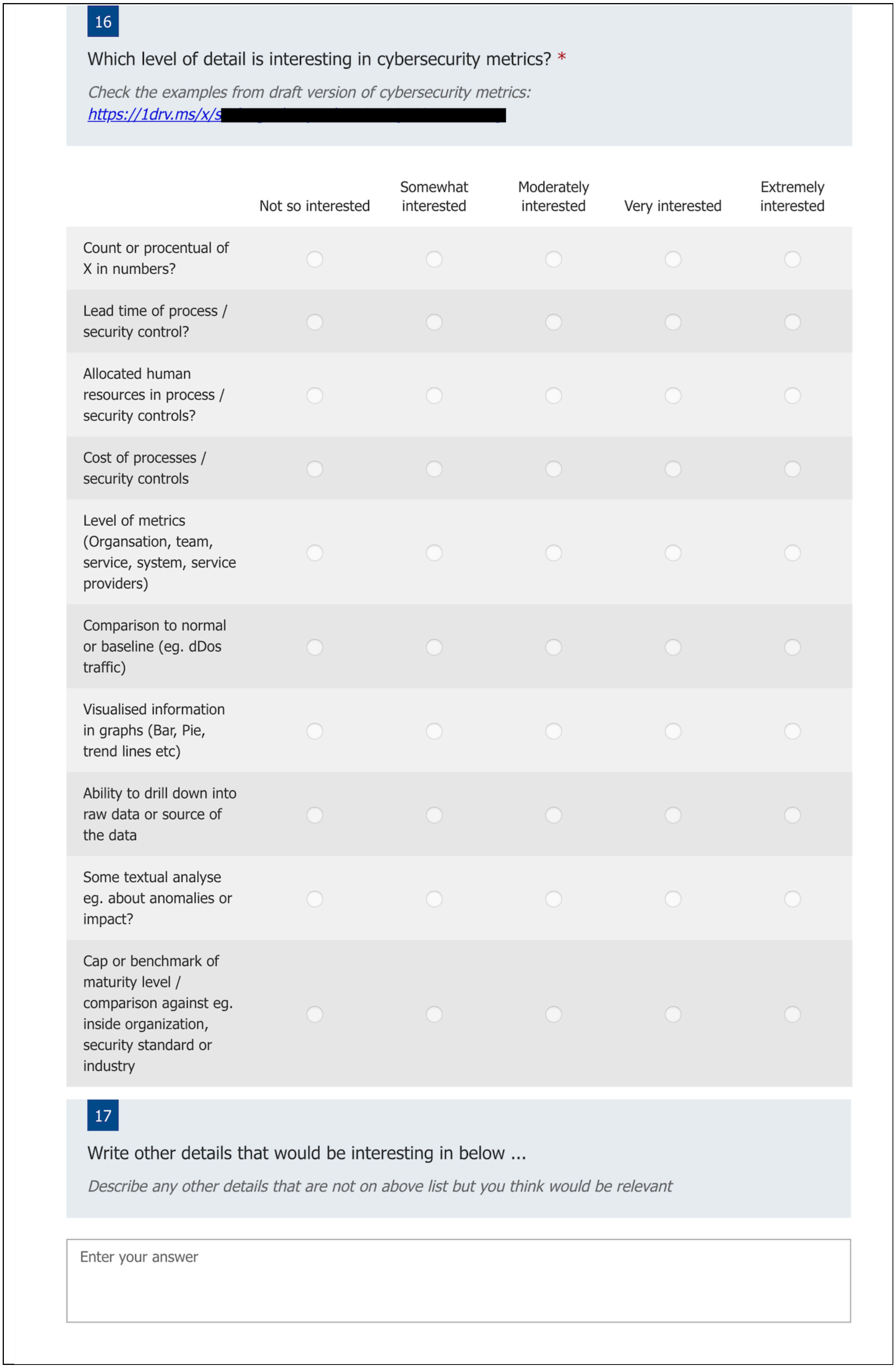
Which governance cybersecurity metrics you would be interested? *

Check the examples from draft version of cybersecurity metrics:
https://1drv.ms/x/s!

	Not so interested	Somewhat interested	Moderately interested	Very interested	Extremely interested
Security related documentation	○	○	○	○	○
Security awareness and training	○	○	○	○	○
Security risks and threat management	○	○	○	○	○
Security resourcing, budgeting and cost	○	○	○	○	○
Availability and business continuity	○	○	○	○	○
Security standards and compliance	○	○	○	○	○

Section 5

Details in cybersecurity metrics (4/5)



16

Which level of detail is interesting in cybersecurity metrics? *

Check the examples from draft version of cybersecurity metrics:
https://1drv.ms/x/s[redacted]

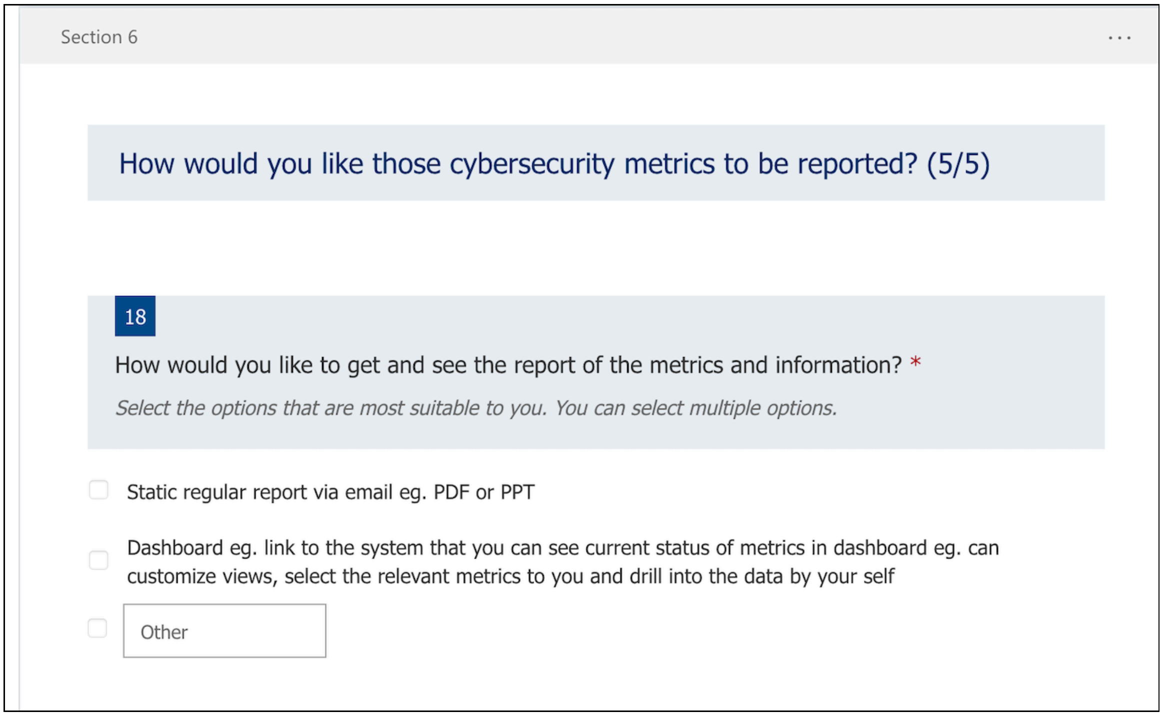
	Not so interested	Somewhat interested	Moderately interested	Very interested	Extremely interested
Count or procentual of X in numbers?	○	○	○	○	○
Lead time of process / security control?	○	○	○	○	○
Allocated human resources in process / security controls?	○	○	○	○	○
Cost of processes / security controls	○	○	○	○	○
Level of metrics (Organsation, team, service, system, service providers)	○	○	○	○	○
Comparison to normal or baseline (eg. dDos traffic)	○	○	○	○	○
Visualised information in graphs (Bar, Pie, trend lines etc)	○	○	○	○	○
Ability to drill down into raw data or source of the data	○	○	○	○	○
Some textual analyse eg. about anomalies or impact?	○	○	○	○	○
Cap or benchmark of maturity level / comparison against eg. inside organization, security standard or industry	○	○	○	○	○

17

Write other details that would be interesting in below ...

Describe any other details that are not on above list but you think would be relevant

Enter your answer



Section 6

How would you like those cybersecurity metrics to be reported? (5/5)

18

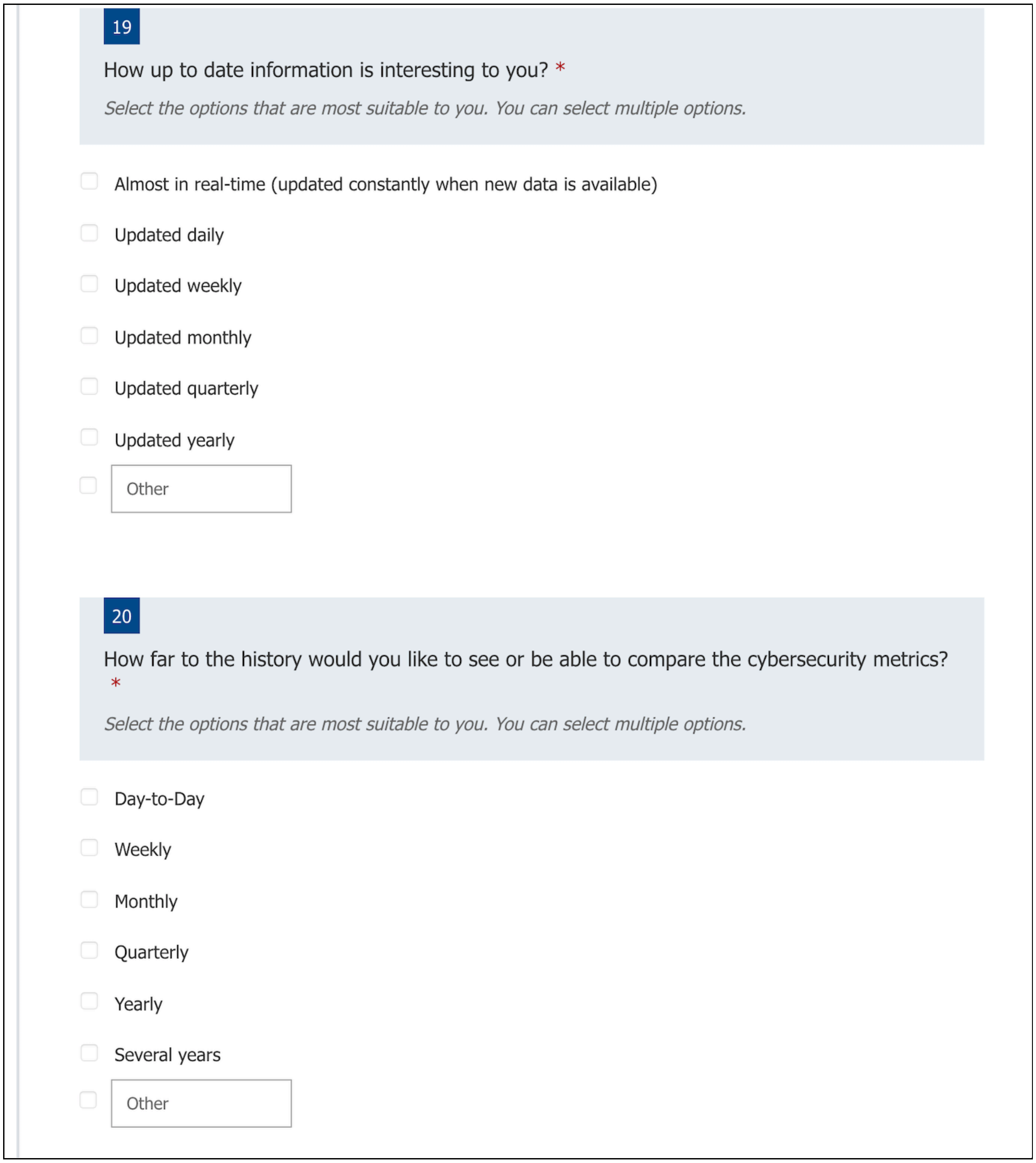
How would you like to get and see the report of the metrics and information? *

Select the options that are most suitable to you. You can select multiple options.

□ Static regular report via email eg. PDF or PPT

□ Dashboard eg. link to the system that you can see current status of metrics in dashboard eg. can customize views, select the relevant metrics to you and drill into the data by your self

□ Other



19

How up to date information is interesting to you? *

Select the options that are most suitable to you. You can select multiple options.

□ Almost in real-time (updated constantly when new data is available)

□ Updated daily

□ Updated weekly

□ Updated monthly

□ Updated quarterly

□ Updated yearly

□ Other

20

How far to the history would you like to see or be able to compare the cybersecurity metrics? *

Select the options that are most suitable to you. You can select multiple options.

□ Day-to-Day

□ Weekly

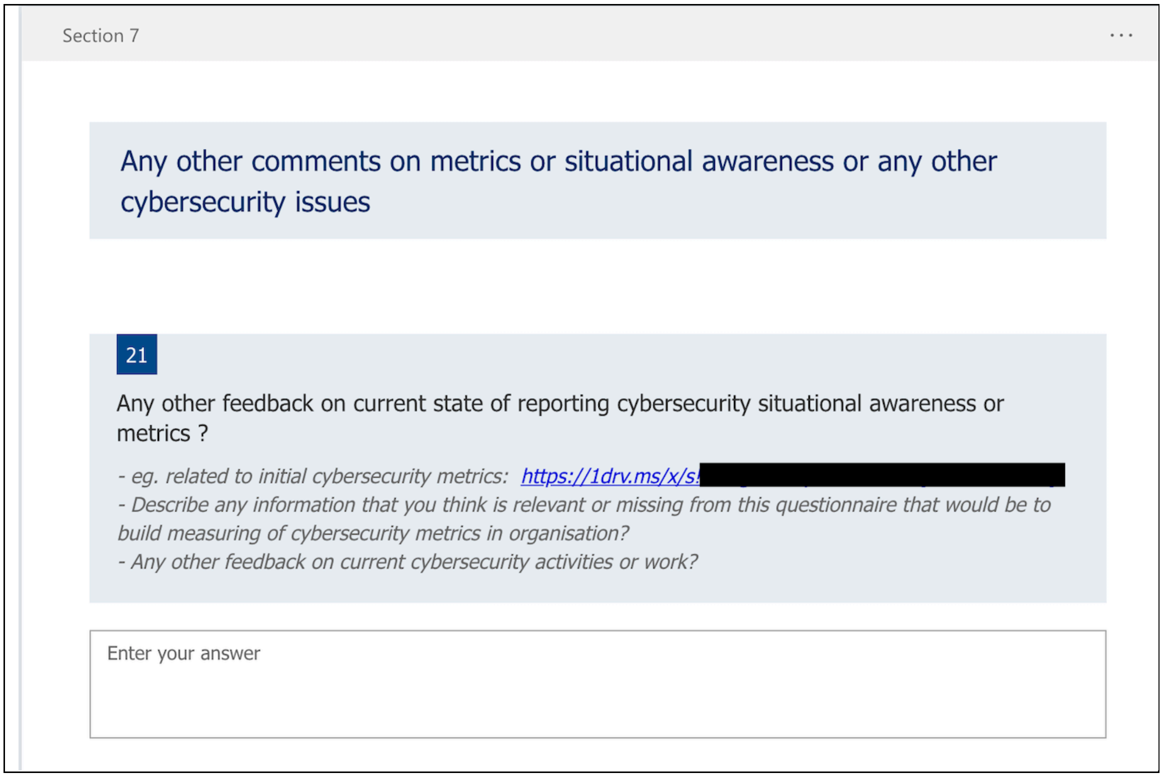
□ Monthly

□ Quarterly

□ Yearly

□ Several years

□ Other



Section 7

Any other comments on metrics or situational awareness or any other cybersecurity issues

21

Any other feedback on current state of reporting cybersecurity situational awareness or metrics ?

- eg. related to initial cybersecurity metrics: https://1drv.ms/x/s![redacted]
- Describe any information that you think is relevant or missing from this questionnaire that would be to build measuring of cybersecurity metrics in organisation?
- Any other feedback on current cybersecurity activities or work?

Enter your answer

Appendix 2

Table of example requirements for cybersecurity situational awareness and metrics platform

Basic platform functionality
The platform shall be able to scale to multiple sources
The platform shall be able to scale CPU and memory for the peak raw data handling tasks
The platform shall be able to scale storage of the raw data
The platform shall support different data storage retention times
The platform shall support automatic notification e.g. alerts for anomalities or when the new reports has been created
The platform shall be able to create reports automatically in set intervals
The platform shall be able to deliver the reports as email
The platform shall be able to deliver the metrics and reports to another platform e.g. SharePoint
The platform shall be possible to integrate to corporate IAM system
The platform shall be ability to show raw data for different role, e.g. manager, technical analyst
The platform shall support different user level access to data and visualizations e.g. dashboards
The platform shall support version controls or be able to integrate into corporate version control system
Data collection
Basic automation of metrics collection shall be possible without programming skills e.g. have supported integrations to security products
The platform shall support API integrations e.g. REST APIs
The platform shall support secure connections to integrated data sources
The platform shall support authentication to integrated data sources
Data shall be possible to collect with different time scheduler functionality
Data collection functionality shall be auditable from the log files
Data collection shall be possible to filter e.g. regular expression
Raw data shall possible to normalize into common information model e.g. raw data from various vulnerability scanners to same data format
Data handling
Basic metrics data handling shall be possible without programming skills
End-user shall be ability to roll up or zoom in/out and drill down into a raw data set
Advanced metrics data handling shall be possible with scripting language

Collected raw data shall be possible to handle e.g. make basic calculations (sum etc.)
Data handling shall be possible to filter e.g. using regular expression
Shall be possible to work with real time data
UI shall support filtering and selecting data with mouse e.g. select certain time range from the visual timeline
Visualisations
Shall support different kind of visualisations e.g. Bar, pie and time charts
Shall be possible to compare different time scale e.g. Hour, day, month, quarterly, year
Shall support customisable dashboards per user need
Visualised information shall be visible without the need to hover the mouse
Visualisations shall be interactive
Visualisations shall be searchable
Visualisations shall be zoomable
Visualisations shall be scalable
Visualisations shall be able to possible to export as image
Other
Shall supports different measurement criteria levels ex. Sigma 1-6 CIS, CMM etc.
Shall support ON/OFF metrics
Shall support benchmarking e.g. against other metric frameworks
Shall support machine learning and AI capabilities for data e.g. pinpoint exceptions
Shall support data export functionalities e.g. to csv format
UI shall support automated refresh in selected time interval
Shall support capability to add text inside to metric e.g. hover the mouse on metric

Appendix 3

Table of example cybersecurity metrics for situational awareness

ID of the metric	Name of the metric	Purpose and goal	Unit of measure	Type of the metric	Category of metric	Example sources	Stakeholders of the metric	Notes / sub metrics	Frequency	Reporting format	Agreed target or expected range
	Email security and malware										
ESM-01	Spam detected in email gateway	To analyse if spam filtering is effective on email gateway	#, %	Technical	Email security	Email gateways	Operational	Incoming / Outgoing, vs endpoint via email	month		
ESM-02	Malware detected in email gateway	To analyse if malware protection filtering is effective on email gateway	#, %	Technical	Email security	Email gateways	Operational	Incoming / Outgoing, vs endpoint via email	month		
ESM-03	Malware detected in endpoints	To analyse if malware protection filtering is effective on endpoints	#, %	Technical	Malware protection	Endpoint protection software	Operational	On Desktops, Mobile, Servers	month		
ESM-04	Malware detected in browsing proxies	To analyse if malware protection filtering is effective on browsing proxies	#, %	Technical	Malware protection	Internet proxies	Operational	On Desktops, Mobile, Servers, vs. endpoint via proxy	month		
ESM-05	Malware incidents requiring manual cleanup	To analyse how many malware incidents needs manual actions	#, %, €	Technical	Malware protection	ServiceDesk tickets and EPP	Operational	On Desktops, Mobile, Servers, Costs of the actions	month		
ESM-06	Percentage of systems covered by endpoint protection	To analyse the coverage of the endpoint protection software (including all high risk systems for malware)	#, %	Governance	Malware protection	Endpoint management software	Operation and Management	On Desktops, Mobile, Servers, up to date signatures or software level	month		
	Network security										

ID of the metric	Name of the metric	Purpose and goal	Unit of measure	Type of the metric	Category of metric	Example sources	Stakeholders of the metric	Notes / sub metrics	Frequency	Reporting format	Agreed target or expected range
NS-01	Percentage of devices using authentication to network	To analyse how many devices is using authentication to network (device certificate, 802.1x port control etc)	#, %	Technical	Network security	Network management, device management	Operational	On Desktops, Mobile and other endpoint devices	quarter		
NS-02	Percentage of "attacks" on external network perimeter	To analyse how many attacks are incoming to external network perimeter	#, %	Technical	Network security	Firewall / Network IDS	Operational	All external networks	month		
NS-03	Number of firewall rule deny matches on outgoing network traffic	To analyse how many abnormal connections are outgoing to external network perimeter. Find out potentially infected hosts.	#, %	Technical	Network security	Firewall / Network IDS	Operational	All external gateways	month		
NS-04	Number of unused firewall rules	To analyse firewall rules and performance and to monitor that rules are up-to-date	#	Technical	Network security	Firewall	Operational	All firewalls in networks	quarter		
NS-05	Percentage of systems using network level security proxy towards internet	To analyse how many systems are utilizing network-based security proxy in connections towards Internet (url filter etc.)	#, %	Technical	Network security	Network management, device management	Operational	External network facing firewalls	quarter		
NS-06	Percentage of network boundaries that are not monitored for anomalies	To analyse organisation's network boundaries are not configured to require network-based Intrusion Detection Systems (IDS) sensors to look for unusual attack mechanisms and	#, %	Technical	Network security	Firewall / Network IDS	Operational	All networks that has boundaries	quarter		

ID of the metric	Name of the metric	Purpose and goal	Unit of measure	Type of the metric	Category of metric	Example sources	Stakeholders of the metric	Notes / sub metrics	Frequency	Reporting format	Agreed target or expected range
		detect compromise of these systems the boundary?									
NS-07	Percentage of networks boundaries recording the full capture traffic	To analyse the coverage of organisation's network boundaries to record full network packets passing through the boundary into incident response purposes	#, %	Technical	Network security	Network management, traffic recording systems	Operational	All networks that has boundaries	quarter		
NS-08	Percentage of networks boundaries recording the netflow	To analyse the coverage of organisation's network boundaries to record network netflow passing through the boundary into incident response purposes	#, %	Technical	Network security	Network management, traffic recording systems	Operational	All networks that has boundaries	quarter		

ID of the metric	Name of the metric	Purpose and goal	Unit of measure	Type of the metric	Category of metric	Example sources	Stakeholders of the metric	Notes / sub metrics	Frequency	Reporting format	Agreed target or expected range
NS-09	Percentage of web applications protected by web application firewalls (WAFs)	To analyse how many web applications are protected by deploying web application firewalls (WAFs) that inspect all traffic flowing to the web application for common web application attacks. For applications that are not web-based, specific application firewalls should be deployed if such tools are available for the given application type. If the traffic is encrypted, the device should either sit behind the encryption or be capable of decrypting the traffic prior to analysis.	#, %	Technical	Application security	Network application security appliances	Operational	All external web applications	quarter		
	Security patching										
SP-01	Security patch applying cycle (time)	To analyse how effective is the process of applying the security patches in agreed time for patch cycle	Time, €	Governance	Patch management	Patch management software, Change management software	Management	On Desktops, Mobile, Servers, other systems, OS and Application level, Cost of actions	month		

ID of the metric	Name of the metric	Purpose and goal	Unit of measure	Type of the metric	Category of metric	Example sources	Stakeholders of the metric	Notes / sub metrics	Frequency	Reporting format	Agreed target or expected range
SP-02	Percentage of the hardware assets regularly updated according to policy	To analyse that the systems are running the most recent security updates provided by the hardware vendor, including BIOS and firmware	#, %	Governance	Patch management	Automated System Patch Management Tools	Management	On Desktops, Mobile, Servers, other systems, OS and Application level, Cost of actions	month		
SP-03	Percentage of the software assets regularly updated according to policy	To analyse that the systems are running the most recent security updates provided by the system vendor, including OS and 3rd party applications	#, %	Governance	Patch management	Automated System Patch Management Tools	Management	On Desktops, Mobile, Servers, other systems, OS and Application level, Cost of actions	month		
SP-04	Percentage of systems having unsupported OS	To analyse that the systems are running the most recent OS security updates provided by the system vendor	#, %	Governance	Patch management	Automated System Patch Management Tools, CMDB systems or software catalogs	Management	On Desktops, Mobile, Servers, other systems, OS and Application level, Cost of actions	month		
SP-05	Percentage of systems having unsupported applications	To analyse that the systems are running the most recent security updates provided by the system vendor including 3rd party applications	#, %	Governance	Patch management	Automated System Patch Management Tools, CMDB systems or software catalogs	Management	On Desktops, Mobile, Servers, other systems, OS and Application level, Cost of actions	month		

ID of the metric	Name of the metric	Purpose and goal	Unit of measure	Type of the metric	Category of metric	Example sources	Stakeholders of the metric	Notes / sub metrics	Frequency	Reporting format	Agreed target or expected range
SP-06	Percentage of endpoints covered by latest security patches (after patch cycle)	To analyse the coverage of the security patches installed	#, %	Governance	Patch management	Patch management software, Vulnerability management software	Operation and Management	On Desktops, Mobile, Servers, other systems, OS and Application level	month		
SP-07	Percentage of endpoints coverage that are unpatched for more than 3 months	To analyse the coverage of uninstalled security patches	#, %	Governance	Patch management	Patch management software, Vulnerability management software	Operation and Management	On Desktops, Mobile, Servers, other systems, OS and Application level	month		
	Secure application configuration										
SAC-01	Percentage of systems in compliance with approved configuration	To analyse the compliance of system configuration standard (eg. CIS hardenings)	#, %	Governance	Host security	Configuration management software, Vulnerability management software	Operation and Management	On Desktops, Mobile, Servers, other systems, OS and Application level, network and other devices	month		
SAC-02	Percentage of systems regularly utilizing automated configuration check	To analyse how many systems has been recently scanned configuration monitoring system to verify all security configuration elements, and alert	#, %	Governance	Host security	Configuration management software, Vulnerability management software	Operation and Management	On Desktops, Mobile, Servers, other systems, OS and Application level, network and other devices	month		

ID of the metric	Name of the metric	Purpose and goal	Unit of measure	Type of the metric	Category of metric	Example sources	Stakeholders of the metric	Notes / sub metrics	Frequency	Reporting format	Agreed target or expected range
		when unauthorized changes occur									
SAC-03	Percentage of systems utilizing application whitelisting	To analyse how many systems has application whitelisting technology in place to block unauthorized applications from executing on the system?	#, %	Governance	Host security	Configuration management software, Vulnerability management software	Operation and Management	On Desktops, Mobile, Servers, other systems, OS and Application level, network and other devices	month		
SAC-04	Percentage of systems having unauthorized applications	To analyse how many systems has unauthorized applications installed (e.g. User installed)	#, %	Governance	Host security	Configuration management software, Vulnerability management software	Operation and Management		month		

ID of the metric	Name of the metric	Purpose and goal	Unit of measure	Type of the metric	Category of metric	Example sources	Stakeholders of the metric	Notes / sub metrics	Frequency	Reporting format	Agreed target or expected range
SAC-05	Percentage of systems having host-based firewalls or port filtering tools on end point systems	To analyse how many systems has host-based firewalls or port filtering tools	#, %	Technical	Host security	Configuration management software, Vulnerability management software	Operation and Management		month		
SAC-06	Percentage of portable systems having full-disk encryption	To analyse how many portable endpoint devices are utilizing approved whole disk encryption software	#, %	Technical	Host security	Configuration management software, CMDB	Operation and Management	On Desktops, Mobile, Servers, other systems, OS and Application level, network and other devices	month		
	Security logging and monitoring										
SLM-01	Percentage of systems logging remotely (basic level of OS events)	To analyse how many systems are logging remotely (avoiding local tampering of logs)	#, %	Technical	Monitoring	Endpoint management software, SIEM	Operation and Management	On Desktops, Mobile, Servers and other equipment in scope	month		
SLM-02	Percentage of systems in active security monitoring (logging to SIEM)	To analyse the coverage of active security monitoring of systems to SIEM and SOC	#, %	Technical	Monitoring	Endpoint management software, SIEM	Operation and Management	On Desktops, Mobile, Servers	month		
SLM-03	Percentage of critical systems in active security monitoring (logging to SIEM)	To analyse the coverage of security monitoring of critical systems to SIEM	#, %	Governance	Monitoring	Endpoint management software, SIEM	Operation and Management	Critical assets	month		

ID of the metric	Name of the metric	Purpose and goal	Unit of measure	Type of the metric	Category of metric	Example sources	Stakeholders of the metric	Notes / sub metrics	Frequency	Reporting format	Agreed target or expected range
SLM-04	Percentage of systems with customer data (PII) in active monitoring (logging to SIEM)	To analyse the coverage of security monitoring of critical systems that has PII data to SIEM	#, %	Governance	Monitoring	SIEM, CMDB systems	Operation and Management	Critical PII customer assets, secondary HR related PII	month		
SLM-05	Percentage of systems logging command-line activities (logging to SIEM)	To analyse how many systems have not enabled command-line audit logging for command shells, such as Python or Windows PowerShell	#, %	Governance	Monitoring	SIEM	Operation and Management	On Desktops, Servers and other equipment in scope	month		
	Asset Management										
AM-01	Percentage of the known hardware assets recently inventoried	To analyse the coverage of hardware asset inventories and information are up to date	#, %	Governance	Asset management	CMDB systems or software catalogues	Operation and Management	All critical ICT assets	month		
AM-02	Percentage of the known software assets recently inventoried	To analyse the coverage of software asset inventories and information are up to date	#, %	Governance	Asset management	CMDB systems or software catalogues	Operation and Management	All critical ICT assets	month		
AM-03	Percentage of the networks recently been scanned by an active asset discovery tool	To analyse the coverage of asset monitoring tools to identify unknown hardware assets in the network	#, %	Governance	Asset management	Asset scanning systems	Operation and Management	All critical ICT assets	month		
AM-04	Percentage of unknown hardware assets in the network	To analyse the coverage of unknown assets in the network	#, %	Governance	Asset management	Asset scanning systems	Operation and Management	All critical ICT assets	month		

ID of the metric	Name of the metric	Purpose and goal	Unit of measure	Type of the metric	Category of metric	Example sources	Stakeholders of the metric	Notes / sub metrics	Frequency	Reporting format	Agreed target or expected range
AM-05	Percentage of the software (applications or operating systems) currently un-supported by the software's vendor	To analyse the coverage of applications currently under active support e.g. security patches are available	#, %	Governance	Asset management	CMDB systems or software catalogues	Operation and Management	All critical ICT assets	month		
AM-06	Percentage of the unapproved software installed into endpoints	To analyse the amount of unsupported software installed by end-users	#, %	Governance	Asset management	CMDB systems or software catalogues	Management	All critical ICT assets	month		
AM-07	Percentage of systems not having up-to-date RACI details	To analyse that RACI details are kept up to date	#, %	Governance	Asset management	CMDB systems or software catalogues	Management	All critical ICT assets	Quarter		
	Vulnerability Management										
VM-01	Percentage of systems scanned actively for vulnerabilities	To analyse the coverage of systems under active vulnerability scanning	#, %	Governance	Monitoring	Vulnerability management software	Operation and Management	On Desktops, Servers, External networks, internal networks, cloud, authenticated scans. Network vulnerabilities, application vulnerabilities, host level (log in)	month		

ID of the metric	Name of the metric	Purpose and goal	Unit of measure	Type of the metric	Category of metric	Example sources	Stakeholders of the metric	Notes / sub metrics	Frequency	Reporting format	Agreed target or expected range
VM-02	Number of vulnerabilities	To analyse the risk based on the amount of vulnerabilities in general	#	Governance	Vulnerability management	Vulnerability management software	Operation and Management	On Desktops, Mobile, Servers, from scanners and manually handled public vulnerability announcements. Network vulnerabilities, application vulnerabilities, host level (log in)	month		
VM-03	Number of critical vulnerabilities	To analyse the risk based on the amount of critical vulnerabilities	#	Governance	Vulnerability management	Vulnerability management software	Operation and Management	On Desktops, Mobile, Servers, from scanners and manually handled public vulnerability announcements. Network vulnerabilities, application vulnerabilities, host level (log in)	month		

ID of the metric	Name of the metric	Purpose and goal	Unit of measure	Type of the metric	Category of metric	Example sources	Stakeholders of the metric	Notes / sub metrics	Frequency	Reporting format	Agreed target or expected range
VM-04	Number of new vulnerabilities per month	To analyse how much effort (workload) is needed to triage security vulnerabilities	#	Governance	Vulnerability management	Vulnerability management software, Ticketing system	Operation and Management	On Desktops, Mobile, Servers, status NEW	month		
VM-05	Number of closed vulnerabilities per month	To analyse how many corrective actions and how much effort (workload) is needed to triage security vulnerabilities	#	Governance	Vulnerability management	Vulnerability management software, Ticketing system	Operation and Management	On Desktops, Mobile, Servers, status CLOSED	month		
VM-06	Time to triage the vulnerabilities (from scanners)	To analyse how effective is the process to triage the vulnerabilities (analyse, mitigation actions, patch management)	Time, €	Governance	Vulnerability management	Vulnerability management software, Ticketing system	Management	On Desktops, Mobile, Servers, status from NEW to CLOSED, Critical assets or general?	month		
VM-07	Time to triage the vulnerabilities (from public announcement)	To analyse how effective is the process to triage the vulnerabilities (analyse, mitigation actions, patch management)	Time, €	Governance	Vulnerability management	Vulnerability management software, Ticketing system	Management	On Desktops, Mobile, Servers, status from NEW to CLOSED, Critical assets or general?	month		

ID of the metric	Name of the metric	Purpose and goal	Unit of measure	Type of the metric	Category of metric	Example sources	Stakeholders of the metric	Notes / sub metrics	Frequency	Reporting format	Agreed target or expected range
VM-08	Business adjusted high vulnerability risk (BAR)	To analyse the vulnerabilities to risks on the business context	RiskScore	Governance	Vulnerability management	Vulnerability management software, Ticketing system	Management	BAR (BAR (1 to 25) = business impact (1 to 5) × risk of exploit (1 to 5, depending on business context))	month		
	Security events and Incidents										
SEI-01	Number of information security events	To analyse the trend of information security events that are raised	#, Time, €	Governance	Incident management	SIEM	Management	Number, used time allocations, costs	month, year		
SEI-02	Number of information security investigated security events	To analyse the trend of information security events that are investigated	#, Time, €	Governance	Incident management	Ticketing system	Management	Number, used time allocations, costs	month, year		
SEI-03	Number of information security incidents	To analyse the trend of information security incidents	#, Time, €	Governance	Incident management	Ticketing system	Management	Number, used time allocations, costs	month, year		
SEI-04	Number of information security incidents (PII/privacy impacted)	To analyse the trend of information security incidents that involves personal data (privacy)	#, Time, €	Governance	Incident management	Ticketing system	Management	Number, used time allocations, costs	month, year		
SEI-05	Number of information security incidents that triggered improvement actions	To analyse the trend of information security incidents effect on security improvements	#, Time, €	Governance	Continues improvement	Ticketing system	Management	including privacy	month, year		

ID of the metric	Name of the metric	Purpose and goal	Unit of measure	Type of the metric	Category of metric	Example sources	Stakeholders of the metric	Notes / sub metrics	Frequency	Reporting format	Agreed target or expected range
SEI-06	Number of information security contacts to service desk	To analyse the trend of contacts to service desk related to information security problems	#	Governance	Continues improvement	Ticketing system	Management	Number, used time allocations, costs	month, year		
SEI-07	Number security findings reported by users	To analyse the trend of reported security findings and suggestions via reporting channels (NOT events or incidents)	#	Governance	Continues improvement	secure development plans	Management	Number, used time allocations, costs	month, year		
SEI-08	Number of partners or external reported security findings	To analyse the trend of reported security findings and suggestions via reporting channels (NOT events or incidents)	#	Governance	Continues improvement	secure development plans	Management	Number, used time allocations, costs	month, year		
SEI-09	Estimate damage (€) from all security incidents	To analyse the trend of security incident costs	€	Governance	Security budgeting	Ticketing system, post-mortem meetings	Management	Number, used time allocations, costs	month, year		
SEI-10	Percentage of incident response playbooks are up to date	To analyse the incident response playbooks are kept up to date (reviewed regularly)	%	Governance	Incident management	Information security documentation and review plans	Management	formal table top review	year		
	Security resourcing and budget										
SRB-01	Total budgetary resources allocation for information security	To analyse the trend for budgetary costs and invests on information security	€	Governance	Resource allocations	Information security budget	Management		month, year		
SRB-02	Budgetary resource allocation per information security area	To analyse the trend for budgetary costs and invests on different	€	Governance	Resource allocations	Information security budget	Management	e.g. based on metric categories	month, year		

ID of the metric	Name of the metric	Purpose and goal	Unit of measure	Type of the metric	Category of metric	Example sources	Stakeholders of the metric	Notes / sub metrics	Frequency	Reporting format	Agreed target or expected range
		information security areas									
SRB-03	Number of full-time human resource allocation for information security	To analyse the trend for human resources to work with information security	#, Time, €	Governance	Resource allocations	Information security resource allocation	Management		month, year		
SRB-04	Number of full-time human resource allocation for different information security area	To analyse the trend for planned human resources to work with specific information security area	#, Time, €	Governance	Resource allocations	Information security resource allocation	Management		month, year		
SRB-05	Percentage of security budget on ICT overall budget	To analyse the trend of information security budgeted for ICT and in technical controls	%, €	Governance	Security budgeting	Information security resource allocation	Management	current vs. previous year, overall ICT budget	month, year		
SRB-06	Percentage of security budget on operational, new programs, external eg. external audits, managed services	To analyse the trend of information security budget in operational threats, new threats and adhoc costs	%, €	Governance	Security budgeting	Information security resource allocation	Management		month, year		
	Security documentation										
SD-01	Percentage of information security documents reviewed	To analyse if security documention is reviewed at planned intervals and is up to date	%	Governance	Information security management, Compliance	Information security documentation and review plans	Management		year		

ID of the metric	Name of the metric	Purpose and goal	Unit of measure	Type of the metric	Category of metric	Example sources	Stakeholders of the metric	Notes / sub metrics	Frequency	Reporting format	Agreed target or expected range
SD-02	Count of management reviews of information security monthly reports	To asses management commitment for information security review	#	Governance	Information security management, Compliance	Information security documentation and review plans	Management		year		
	Security risk and treat management										
SRTM-01	Number of high (above medium) exposed information security risks	To assess the trend of high risks (above medium) exposed information security risks	#	Governance	Risk management	Information security risk register	Management		month, year		
SRTM-02	Percentage of information security risks reviewed in agreed interval	To analyse if information security risk management process and risks are reviewed at planned intervals and is up to date	#, %	Governance	Risk management	Information security risk register	Management		month, year		
SRTM-03	Percentage of critical assets reviewed for security risks	To analyse trend of critical assets risk management process	%	Governance	Risk management	Risk and critical asset registers	Management		quarter, year		
	Security audits and findings										
SA-01	Number of internal security audits performed compared with planned security audits	To analyse trend if internal security audit plan is effective against the security audit plan	#, %	Governance	Security audits	Audit plans	Management		quarter, year		
SA-02	Number of external security audits performed compared with planned security audits	To analyse trend if internal security audit plan is effective against the security audit plan	#, %, €	Governance	Security audits	Audit plans	Management		quarter, year		

ID of the metric	Name of the metric	Purpose and goal	Unit of measure	Type of the metric	Category of metric	Example sources	Stakeholders of the metric	Notes / sub metrics	Frequency	Reporting format	Agreed target or expected range
SA-03	Number of audit findings	To analyse the trend of audit findings	#	Governance	Security audits	Audit findings	Management		quarter, year		
SA-04	Percentage of high-risk audit findings	To analyse the trend of audit findings criticality	%, #	Governance	Security audits	Audit findings	Management		quarter, year		
	Security awareness and training										
SAT-01	Number of computer-based security awareness trainings	To analyse the trend of computer analysed awareness trainings	#, %	Governance	Training and awareness	Online awareness training system	Management	per online course	year		
SAT-02	Number of human held security awareness trainings	To analyse the trend of awareness trainings held	#, %	Governance	Training and awareness	Awareness training plan, trainers	Management	per online course	year		
SAT-03	Number of security awareness campaigns	To analyse the trend of awareness campaigns	#	Governance	Training and awareness	Intranet, emails, specific awareness systems eg. Hoxhunt	Management		year		
SAT-04	Number of succesfully reported social engineering attacks	To analyse the trend of awareness of social engineering attacks eg. Phishing emails, % simulated attacks	#, %	Governance	Training and awareness	Specific awareness systems eg. Hoxhunt	Management		month, year		
	Indentity and access control management										
IAM-01	Percentage of user access rights reviews on critical systems	To analyse the trend of user access review process	#, %	Governance	Access management	User access management system	Management		year		

ID of the metric	Name of the metric	Purpose and goal	Unit of measure	Type of the metric	Category of metric	Example sources	Stakeholders of the metric	Notes / sub metrics	Frequency	Reporting format	Agreed target or expected range
IAM-02	Percentage of critical systems in centralized IAM system	To analyse the trend of how many systems are under central IAM privisioning system	%	Governance	Access management	User access management system	Management		year		
IAM-03	Number of unauthorized access tries into facilities that contain information systems	To analyse systematically that physical access control is working from access logs	#	Governance	Physical security	Physical access control systems	Operational		year		
IAM-04	Number of privilege accounts on non-admin users	To analyse how many privilege user accounts are on non-admin users (not part of the job role)	#, %	Governance	Access management	User access management system	Management		month, year		
IAM-05	Number of privilege accounts without multifactor authentication	To analyse how many privilege systems and accounts are used without multi-factor authentication (such as administrator, root, or other high-risk accounts)	#, %	Governance	Access management	User access management system	Management		month, year		
IAM-06	Percentage of administrators that are not utilizing a dedicated machine, located on a dedicated management network, for all administrative tasks or tasks requiring elevated access to the organisation's systems?	To analyse how many administrators are not utilizing a dedicated machine, located on a dedicated management network, for all administrative tasks or tasks requiring elevated access to the organisation's devices?	#, %	Governance	Access management	User access management system	Management		month, year		

ID of the metric	Name of the metric	Purpose and goal	Unit of measure	Type of the metric	Category of metric	Example sources	Stakeholders of the metric	Notes / sub metrics	Frequency	Reporting format	Agreed target or expected range
IAM-07	Number of accounts in system not in centralized inventory	To analyse that all accounts in the systems are known, inventoried to centralized IAM and under active life cycle management	#, %	Governance	Access management	User access management system, System secure configurations systems	Management		month, year		
IAM-08	Time to deactivate former employee credentials	To analyse the effeectiveness of access revocation process	Time	Governance	Access management	User access management system	Management		month, year		
IAM-09	Time to deactivate access to the critical system	To analyse the effeectiveness of access revocation process to critical assets	Time	Governance	Access management	User access management system	Management		month, year		
IAM-10	Percentage of access rights review to critical systems done in agreed interval	To analyse how effectively the access rights to critical systems are reviewed	%	Governance	Access management	User access management system	Management		month, year		
	Availability and business continuity										
BC-01	Availability of critical systems	To analyse availability of services and information systems	%	Governance	Availability	Monitoring systems, ticketing systems	Management	MTRR, RTO in incidents	month, year		
BC-02	Unplanned downtime of critical systems	To analyse if change management is working	#, Time, €	Governance	Availability	Monitoring systems, ticketing systems	Management		month, year		

ID of the metric	Name of the metric	Purpose and goal	Unit of measure	Type of the metric	Category of metric	Example sources	Stakeholders of the metric	Notes / sub metrics	Frequency	Reporting format	Agreed target or expected range
BC-03	Unplanned downtime due to the security incidents in critical systems	To analyse if down time root cause is security incidents	%, #, Time, €	Governance	Availability	Monitoring systems, ticketing systems	Management		month, year		
BC-04	Percentage of up-to-date business continuity plans for critical process	To analyse how many business continuity plans are up to date on critical processes	%	Governance	Business continuity	Information security documentation and review plans	Management		year		
BC-05	Percentage of up-to-date system recovery plans for critical systems	To analyse how many system recovery plans are up to date on critical systems	%	Governance	Business continuity	Information security documentation and review plans	Management		year		
BC-06	Percentage of business continuity plans tested	To analyse how many business continuity plans on critical processes has been tested	%	Governance	Business continuity	Information security documentation and review plans	Management		year		
BC-07	Percentage of system recovery plans tested	To analyse how many system recovery plans on critical systems has been tested	%	Governance	Business continuity	Information security documentation and review plans	Management		year		
BC-08	Percentage of systems configured to back up system data automatically on a regular basis	To analyse how many systems are configured to back up system data automatically on a regular basis	%	Governance	Business continuity	Backup systems	Management		year		
BC-09	Percentage of systems backups not been tested recently (in last year) to ensure that the backup is working properly?	To analyse how many systems back up is tested on a regular basis	%	Governance	Business continuity	Information security documentation and review plans	Management		year		

ID of the metric	Name of the metric	Purpose and goal	Unit of measure	Type of the metric	Category of metric	Example sources	Stakeholders of the metric	Notes / sub metrics	Frequency	Reporting format	Agreed target or expected range
	Contracts and third-party management										
CA-01	Percentage of relevant third-party agreements including security requirements	To analyse that all relevant third-party agreements includes security requirements	%	Governance	3rd party agreements	Agreements	Management		year		
CA-02	Percentage of relevant third-party agreements including privacy requirements	To analyse that all relevant third-party agreements includes privacy requirements	%	Governance	3rd party agreements	Agreements	Management		year		
CA-03	Percentage of relevant third-party agreements audited for security requirements	To analyse that all relevant third-party agreements are audited on regular bases	%	Governance	4th party agreements	Agreements	Management		year		
	Secure software development										
SDL-01	Number of secure development actions and tasks	To analyse the trend of information security improvements against the plan	#, %	Governance	Continues improvement, Compliance	secure developmentplans	Management		month, year		
SDL-02	Number of corrective actions	To analyse the trend of total corrective actions to mitigate security findings (vulnerabilities, internal and external audit findings)	#, Time, €	Governance	Continues improvement	secure developmentplans	Management		month, year		
SDL-03	Percentage of systems scanned for static code analyses tools	To analyse that coding practises are monitored with automated software	%	Governance	Secure development	Application security tools, static source code anayser	Management		month, year		

ID of the metric	Name of the metric	Purpose and goal	Unit of measure	Type of the metric	Category of metric	Example sources	Stakeholders of the metric	Notes / sub metrics	Frequency	Reporting format	Agreed target or expected range
SDL-04	Percentage of systems scanned for dynamic code analyses tools	To analyse that software and 3rd party libraries are monitored with automated software	%	Governance	Secure development	Application security tools, static source code anayser	Management		month, year		
SDL-05	Number of security code defects per 1000 lines of code by automatic tools	To analyse the effectiness of secure development code practises	#	Governance	Secure development	Application security tools, static source code anayser	Management		month, year		
SDL-06	Percentage of false possitive security code defects of reported per 1000 lines	To analyse the effectiness of secure development code practises	%	Governance	Secure development	Application security tools, static source code anayser	Management		month, year		
SDL-07	Percentage of design reviews for the released	To analyse the effectiness of secure development practises	%	Governance	Secure development	Software sprint documentation	Management		month, year		
SDL-08	Percentage of security code reviews done for the release	To analyse the effectiness of secure development code practises	%	Governance	Secure development	Software sprint documentation	Management		month, year		
SDL-09	Percentage of go live penetration test before release	To analyse the effectiness of secure development practises	%	Governance	Secure development	Software sprint documentation	Management		month, year		
SDL-10	Number of vulnerabilities in 3rd party libraries	To analyse the effectiness of secure development software vulnerability remediation	#	Governance	Secure development	Application security tools	Management		month, year		
SDL-11	Number of different kind of application vulnerabilities	To analyse the effectiness of secure development software vulnerability remediation	#, %	Governance	Secure development	Application security tools	Management		month, year		

ID of the metric	Name of the metric	Purpose and goal	Unit of measure	Type of the metric	Category of metric	Example sources	Stakeholders of the metric	Notes / sub metrics	Frequency	Reporting format	Agreed target or expected range
SDL-12	Percentage of critical systems code analysed by security tools	To analyse the effectiness of secure development software vulnerability remediation	%	Governance	Secure development	Application security tools	Management		month, year		
	Security standards and compliance										
STC-01	Number of findings in compliance audits	To analyse the trend of findings in compliance audits	#	Governance	Security audits	Audit findings	Management	for each applicable standard or audit such as PCI, ISO etc.	year		