jamk.fi

Model for national cybersecurity resilience and situation awareness improvement

An information quality –centric approach leveraging fusion of established practitioner and academic disciplines

Jani Antikainen

Master's thesis
December 2014

Master Degree Programme in Information Technology
Technology, communication and transport

JYVÄSKYLÄN AMMATTIKORKEAKOULU
JAMK UNIVERSITY OF APPLIED SCIENCES

JYVÄSKYLÄN AMMATTIKORKEAKOULU
JAMK UNIVERSITY OF APPLIED SCIENCES

Description

Author(s)	Type of publication	Date
Antikainen, Jani	Master's thesis	12.12.2014
		Language of publication: English
	Number of pages 187	Permission for web publication: Granted

Title of publication

Model for national cybersecurity resilience and situation awareness improvement

An information quality –centric approach leveraging fusion of established practitioner and academic disciplines

Degree programme

Master Degree Programme in Information Technology

Tutor(s)

Huotari, Jouni

Assigned by

Sparta Consulting Oy

Abstract

This research addresses the perceived prevailing situation, where organizations are still struggling hard to build information-as-an-asset –mindset and thus fail to recognize and control their critical information assets. These assets and operations they enable are the main interest of parties committing cyber-crimes, hence for the efficiency of cybersecurity the assets and control over them should be the focus, especially for the organizations providing critical infrastructure services, which whole national society's resilience relies on.

The research done weaves together several complex disciplines in information- and information security management and governance of those and further instantiates those in the context of cybersecurity. This is done for purposes of finding synergies and capabilities not one discipline alone could establish, but holistic value is realized. Further from the fusion of the disciplines a capability of creating situation awareness over critical information assets of national critical infrastructure service providers is provided – a capability much sought after both by Finland's Cybersecurity Strategy as well as the strategies of most G20 countries.

The outcome of the research – the model - and the target of primary research question is thus created, proof of concept is presented and later the model is introduced to leading Finnish cybersecurity experts for initial evaluation and discovery of its potential (Research Question 2) . Last (Research Question 3), from the empirical study, more evidence is highlighted on the organizations' capability for information-as-an-asset –thinking. The results show that in Finland's cybersecurity context, the information assets are identified at best on "a decent" level, there exists little if any controls over them and that the concepts of data quality and data monitoring are not established – all which is encouraging for any party interested in harming national stability, and a finding, which should be of utmost relevance for parties responsible for Finland's cyber resilience.

The created model is of high potential even on national level and at the same time it breaks classic silos of organizations' operations providing added synergy and removal of negative overlaps.

Keywords/tags

cybersecurity, master data management, information security management, data governance, information security governance, situation awareness, model development, operational resilience

Miscellaneous

JYVÄSKYLÄN AMMATTIKORKEAKOULU
JAMK UNIVERSITY OF APPLIED SCIENCES

Kuvailulehti

Tekijä(t)	Julkaisun laji	Päivämäärä
Antikainen, Jani	Opinnäytetyö	12.12.2014
	Sivumäärä 187	Julkaisun kieli Englanti
		Verkkojulkaisulupa myönnetty: kyllä

Työn nimi

Model for national cybersecurity resilience and situation awareness improvement

An information quality –centric approach leveraging fusion of established practitioner and academic disciplines

Koulutusohjelma

Master Degree Programme in Information Technology

Työn ohjaaja(t)

Huotari, Jouni

Toimeksiantaja(t)

Sparta Consulting Oy

Tiivistelmä

Vaikka organisaatiot tunnistavat teoriatasolla tiedon merkityksen toiminnalleen, ei sitä kuitenkaan käsitellä tärkeänä omaisuutena. Seuraus on kyvyttömyys tunnistaa ja hallita toiminnan jatkuvuudelle kriittistä tietoa. Juuri tämä kriittinen tieto ja sen mahdollistamat operaatioiden jatkuvuudet ovat usein kyberrikollisten kiinnostuksen pääkohde. Tarkastellen tätä kyberturvallisuuden kehitystarpeista, olisi näiden tietojen tunnistamisen ja niiden hallinnan perustamisen oltava korkean prioriteetin tehtäviä. Tämä pätee varsinkin toimijoille, jotka tuottavat kriittisen infrastruktuurin palveluita, joiden varassa on yhteiskunnan toiminnanjatkuvuus kriiseissä.

Tehty tutkimus yhdistää useita monimutkaisia ja irrallisia konsepteja tietoturvan ja tiedonhallinnan sekä näiden hallinnon osalle. Näitä tutkittiin erityisesti kyberturvallisuuden kontekstissa. Tutkimuksen tarkoituksena oli tunnistaa synergioita ja kyvykkyyksiä, joihin ko. toimintakonseptit eivät yksinään toimien pystyisi. Vain näin tekemällä voitiin luoda toiminnallisuutta, joka on holistista – yhdistettyjen osien summaa suurempaa. Yhdistelmämallista luotiin myös kyvykkyys muodostaa tilannetietoisuutta ja tilannekuvaa kansallisen kriittisen infrastruktuurin palveluiden toimittajien kriittisten tieto-omaisuuksien tilaan ja luotettavuuteen. Mallin tarkoituksena on tunnistaa ja kontrolloida tehokkaasti tietoon kohdistuvia, tietoa korruptoivia, kyberuhkia. Tällaista kyvykkyyttä ei ole ollut olemassa, vaikka sen merkitys on niin Suomen kuin useamman G20-maan kyberstrategioissa tunnistettu kriittiseksi. Strategioissa siitä puhutaan yleisesti tilannetietoisuutena.

Malli, joka oli myös tärkeimmän tutkimuskysymyksen kohde, konseptoitiin ja tutkimuksen empiirisessä osassa tutkittiin niin konseptin toimivuuden kuin mahdollisen kansallisen merkityksen osalle viiden suomen johtavan kyberturvallisuuseksperttin toimesta. Lisäksi haettiin vielä lisätodistetta mallin tarpeellisuudelle tutkimalla organisaatioiden kykyä käsitellä tietoa omaisuutena. Tulokset tästä kertovat, että kyky on korkeintaan keskinkertaista ja että kontrollit tietoon ja sen laatuun puuttuvat lähes kokonaan. Tilanne on otollinen kyberrikollisille, sietämätön kansallisen toiminnanjatkuvuuden (resilienssin) vastuutahoille. Luotu malli on hyvin potentiaalinen ja rikkoo rajoja luoden synergiaa ja poistaen päällekkäisyyksiä organisaation toiminteiden välillä.

Avainsanat (asiasanat)

kyberturvallisuus, ydintiedonhallinta, MDM, tietoturva, tiedonhallinto, tietoturvan hallinto, tilannetietoisuus, tilannekuva, mallikehitys

Muut tiedot

"So cyberspace is real. And so are the risks that come with it. It's the great irony of our Information Age - the very technologies that empower us to create and to build also empower those who would disrupt and destroy. And this paradox – seen and unseen - is something that we experience every day"

- *Barack Obama, 2009*

CONTENTS

LIST OF FIGURES

LIST OF TABLES

1 INTRODUCTION

This chapter provides background on the field that this research is targeting. It explains the motivation and relevance of the research and presents the key research questions. Research methodology as well as the key findings and the structure of the research are also presented.

1.1 Background

There are no borders, as greatest hackers know (Rice & Bucholz, 2003, p. 1289) and there are little or no rules to obey – welcome to the Era of Cyber. Actually, we have been living that era since first computers emerged, however, as the scale of practically everything related to data and information with technology enabling its processing is overwhelmingly increasing (Cukier, 2010). A phenomenon, which is creating challenges to organizations' data management practices (Das & Mishra, 2011). Both practitioners and academics are struggling to stay onboard. It might be just Titanic they are trying to hang on, not realizing the real challenge, we as one world, are facing, not seeing the sea surface steadily approaching them.

In short, what cyber – be it cyber defence, cyber resilience, cyber war, cyber risk and so forth – is ultimately about is information and data from which this information is built from. Information is power, money and even a weapon – all lucrative drivers for committing a cybercrime for hacker individuals, crime organizations, hacktivist groups, terrorists, and even nations. Especially, as risk of even getting identified yet alone caught is low (Kshetri, 2005).

Although the ship is slowly turning, many companies and public institutions still believe that cybersecurity or information security is about defence of their own perimeters, malware and virus detection and network security – about technology in short ((Crossler, Johnston, Lowry & al., 2013), (Ahmad, Hadgkiss & Ruighaver, 2012), (Tondel, Line& Jaatun, 2014)). On the positive

side, the awareness of information's role and the role of people and processes creating and using that information is on an increase (Ahmad, Bosua & Scheepers, 2014). Nevertheless, more education on the "*what are we trying to protect*" is needed. A quote from Morrow (2012) summarizes this well: "One of the biggest challenges for organizations is that corporate data is being delivered to devices that are not managed by the IT department, which has security implications for data leakage, data theft and regulatory compliance […] organizations need to focus on securing and controlling their sensitive corporate information". It both shows that the environment is getting more complex and that the focus should be on the asset itself – the information.

It seems that through the constant media visibility of cyber events something positive is also happening: companies and institutions are realizing that information is their key, if not even the most important asset, worth treating as such via starting security/cyber –programs and acknowledging the importance of information security, as a wide concept, for the resilience of their cyber operations. Some are even starting to implement wider concepts like *cyber resilience*, combining both aspects of *cyber security* and *business resilience* (IT Governance, 2014). This presents an approach which, if deployed successfully, provides the institution with the best practices of the industry (e.g. the ISO Standards family) for capabilities on both protecting them against cyber threats (ISO's security management) and managing realized risks (ISO's risk management) associated on activated threats with damage control and business recovery (business continuity management). Even though helpful, ISO-standards (and standards in general) are fit-for-all guidelines, hence one can argue like Siponen (2006) does that having standards in place and being compliant could just prove out treating those as an end of its own right – not necessarily offering the organization any real information security value.

Nevertheless the problems and high likelihood of major risks getting realized is not yet solved. As the institution struggles with general global data volume increase trend (The Department for Business, Innovation and Skills (BIS) - Gov

UK, 2013), constantly evolving threat landscape (Council on CyberSecurity, 2014 (a)) more and more of self-produced and/or outside sourced data, open data, big data, internet/industry of things data and so on, it finds itself unable to actually answer the question: "What data or information should we be protecting?". The question becomes relevant also as all data is not equal in importance, i.e. there is data critical to operations versus there is data such as 20 years old scanned meeting minutes of project ages ago gone. The institution realizes that even though how hard they tried, they cannot manage (even if they had rigorous data management practices in place) all the data with the resources they have – be it technical or people. Its data amount and diversity raises almost exponentially over time, and the complexity of the environment processing it (e.g. IT technology) is getting out of control of IT department (Silic & Back, 2014) – however the resources available to manage this chaos do not scale in the same way.

In fact many companies admit that they no longer have grasp on the situation, if they ever had (Walters, 2013). This is a very worrying trend, implicit of the fact that at some stage all organizations, no matter what the information security capabilities in place, will suffer an information security incident (attack) (Ahmad, Hadgkiss & Ruighaver, 2012) - one which can damage business operations, reputation, finance resilience from low realization to something, which can bankrupt the company (ISACA, 2012). On national perspective those can seriously hinder critical infrastructure service providers' capability to provide national critical services ((Secretariat of the Security Committee, 2013), (National Institute of Standards and Technology (NIST), 2014)). There is no longer, if there ever was, absolute defence.

Considering the afore mentioned, the few resources the institution has must be addressed to controls where they have the most effect. No institution can any longer bet on investing everything on perimeter defences (firewalls, network traffic scanners etc.). If their operations are not yet compromised by cyber-attack/security breach, it will happen rather sooner than later – no

matter what technology there is in place (The Department for Business, Innovation and Skills (BIS) - Gov UK, 2013). The author does not downplay the importance of these defences. Instead he only states that they alone, even with state of the art *intrusion detection systems (IDS)*, cannot remove the fact that the perimeters will be breached (PwC, 2014) and the core asset of the institution, the data they have, is compromised. Further, if the attacker is a real professional with clear intention and knowledge on the institution, there is high chance the institution will not even know what hit them, before they read it from the headlines.

So, the identification and management of the data and information, which matters the most for the institution, is where the high focus should be: on the subset of that information, which for each point in time (as strategies and business change over time) matters the most to the strategic, tactical and operational functions of the institution. Further considering the constantly changing nature of businesses, this core information assets' (data) management must accordingly be considered as an ongoing, not "fire and forget" function. It must constantly focus on the data and information mattering the most, however at the same time, be prepared to anticipate changes in the institution's strategy, which might provoke needs for re-focusing the data management efforts to different set of data.

The facts of not being able to protect the perimeters of the institution, that successful attack through those is inevitable and assets will get compromised presents the Chief Information Security Officers (CISO), Chief Information Officers (CIO), Chief Executive Officers (CEO) and risk management units with a another question: "What to do – to what capability should the resources be invested to provide maximum resilience for the money spent?" Added rationale is that it just is not economically feasible, not in many cases even possible to try to fully protect all the information systems and information in those (Tondel, Line & Jaatun, 2014).

The above summarizes the purpose of this research: addressing practical, but society wide, problem of "what to do" by providing high yield national-scope solutions via challenging views that single disciplines like information security management and data governance provide - fusing them together to find synergies and then providing holistic value from those for example in form of a model for controlling organizations' critical information's' integrity and thus business continuity and resilience, and sharing these e.g. integrity-quality information with other parties for common purposes and good of all.

Something, which when put to context of national cybersecurity's situational awareness of critical infrastructure providers' integrity and changes in those could prove out to be quite an interesting concept and have significant value for the society as whole. As an example it should be interesting to Finnish Cyber Security Centre, as Finland's Cyber security Strategy (Secretariat of the Security Committee, 2013) explicitly and in several parts highlights the importance of situational awareness, stating for example that "The strategic guidelines of the Cyber Security Strategy are advanced by intensifying active collaboration between actors whose aim is to achieve a shared situation awareness and effective defence against the threats", while at the same time even cyber strategists in the field see very little turning into real action or capabilities. Something, this research is directly contributing to and doing so by innovative and novel approach not yet seen presented.

While these mentioned capabilities are important for organizations, their value chains, national emergency supply –functions and so forth, they can strongly contribute also to single citizen's perception of cyber environment and the internet. Trends show that EU citizens, at least, are more and more worried about their digital identities and personal information. They have low trust in public authorities skills to protect their information (64% are concerned over this), have reported experiencing online-fraud (10%), some 7% had experienced online credit card fraud, 28% are not at all confident on their skills in internet and in general are increasingly feeling that the risk of being

crime victim in the internet has increased over the last year (76% agree so) – all this telling the message that cyber security (or lack of it) is happening on many levels at the same time – national, organizational and even single citizen's concept of information security(the European Commission, Directorate-General Home Affairs, 2013). The implications on all levels of society even more highlights the importance of the study at hand.

1.2 Short introduction of key concepts

To minimize misunderstandings, the key concepts of this research are introduced briefly with selected (as there are many presented in this thesis) definition used as generalization of the concept. The intention of this thesis is not provide extensive syntheses of different definition, hence those, most appealing to author's eye (and his experience background) are used:

Cybersecurity (or cyber security) – *The activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation*

Information Security Management – [Function which] *Ensures that within the enterprise, information is protected against disclosure to unauthorized users (confidentiality), improper modification (integrity) and non-access when required (availability)*

Information Security Governance - *system by which organization's information security activities are directed and controlled*

Master Data Management – *Processes and practices for managing Master Data - those entries, relationships, and attributes that are critical for an enterprise and foundational to key business processes and application systems*

Data Governance – *A process and quality control discipline focused on managing the quality, consistency, usability, security, and availability of information.*

Data Quality - *The totality of features and characteristics of data that bears on their ability to satisfy a given purpose; the sum of the degrees of excellence for factors related to data*

Policy –*Intentions and direction of an organization as formally expressed by its top management*

Risk - *All organizations are encountering internal or external factors and influences, that might compromise the organization's capability to reach its objectives, make things uncertain. The effect this uncertainty has on the objectives set is called risk*

Threat - *potential cause of an unwanted incident, which may result in harm to a system or organization*

Situation awareness – *the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning and projection of their status in near future*

1.3 Motivation and objective of the study

There are many motivating factors, which encouraged the author to conduct this research. Few of them are mentioned below:

- The general confusion in literature about what *cybersecurity is*, what it might include and how important it actually is, and how little literature exists on the topic. At the same time recognition that "cyber" is increasingly noted phenomenon and attracting peoples' attention worldwide (Franke & Brynielsson, 2014).
- There is a need to underline that information in many cases is the corporate's or public institution's most valuable asset ((Ahmad, Bosua

& Scheepers, 2014), (Morrow, 2012), (System Experts, 2004)), yet they seem to pay very little real interest in rigorously protecting it and thus present themselves and all dependent parties (value- or supply chain) at high risk of loss of business continuity.

- Information systems research in information security area seems to be concentrating more on technology than information itself or people, which author feels needs balancing - more research emphasis on information assets securing and people involved in organizations operations. This notion is supported by remark "[…] predominant weakness in properly securing information assets is the individual user in the organization"(Crossler, Johnston, Lowry & al., 2013).
- Just like the author has experienced and many literature entries state ((Kobielus, 2006), (Berson & Dubov, 2007, p. 286)) master data Management and data governance should not be considered IT – owned operations, business should run those. Still mainstream consider these as "IT's work to be done". The author sees similar problematics here that cybersecurity and information security management are seen as IT (Council on CyberSecurity, 2014 (a)). In their very essence they are business topics and should rank high on board's priority lists (von Solms , 2005). Similar observations are made by Henry (2003, p. 667), where he states that the security department should not report to IT director, because this could create conflicts of interest between secure processes and the push to develop new systems.
- It is noted in Franke & Brynielsson's (2014) extensive literature study that cyber situation awareness is largely centered on IT security, and that much of discussion is centered on cyber sensors rather than investigating whether ordinary sensors could contribute to the cyber situation, which is getting very little attention. The author wants to present the role of information itself (which is the target of protection) and investigate, whether ordinary data quality sensors, i.e. data quality

metrics and control system could contribute to cyber situational awareness.

- From the discussions the author has had with cybersecurity professionals, he has become more and more convinced that the much mentioned "situation awareness" greatly emphasized in e.g. Finland Cyber Security Strategy (Secretariat of the Security Committee, 2013) is somewhat elusive and not yet well concretized or materialized in the operative capabilities of Finland's cybersecurity.
- Previous, summed up with notions of information security management not perhaps really concentrating on the assets themselves (i.e. the information and how to identify the critical part of whole asset with capability to tell the objective quality of the asset) hints that there might be room for combining several disciplines and concepts for holistic gains.

The author recognizes that entwining so many different complex constructs and concepts and their possible dependencies is usually out of the scope of Master's thesis researches. Yet, the author does want to face the challenge and is confident that his years of experience in the industry allow him to handle and process the complex big picture. At the same time the author sees that only through analyzing these constructs and concepts together, can the possible synergies, new models and systems be created. Most of the themes, apart from situation awareness, presented in this research are familiar and well known to the author and thus constructing the big picture view has become possible.

The scope of this research is to investigate two "root" phenomenon (with their materialized disciplines and models included, where needed) which the author recognizes from personal experience: data quality and information security. Further, the concept of situation awareness is included to present the novel new construct made possible by the two phenomena. It should be mentioned that to limit the scope of the research, the concepts and constructs

presented are researched only to the level where sufficient general knowledge of the themes is achieved and can be used for the empirical part of the study. Intention is not to discover all facets of concepts presented. Following explicit limitations must be mentioned:

1) Data governance and information security governance are observed only for the parts, which present possible synergy or overlaps between these two
2) Analogously, master data management and information security management are restricted in scope
3) Data quality, being likewise a concept worth hundreds of studies, is limited to be investigated only for the author's own conceptual model of it supported by literature, with intention to build a bridge between data governance and information security governance as well as master data management and information security management
4) Cybersecurity is considered for purposes of building the study context that the other concepts are operating in. Physical infrastructure like hardware and first line defences (firewalls, antivirus, network traffic analysis etc.) as well as information systems security are outscoped – the focus is on data /information and management of those.
5) Classifications, hierarchies and taxonomies -building are out of scope of this thesis. This limitation is worth highlighting as e.g. *data governance* and *data quality* can be seen as sub-parts of *master data management* (Antikainen & Käkölä, 2011) and the other way round *data governance* can be inclusive of *data management* and *data quality* (Berson & Dubov, 2007, s. 114). To raise the complexity, *data quality* can be seen as ultimate wrapper of all concepts mentioned, as it can for example include the Consistency, Integrity and Accuracy – ultimate targets of *information security management* (DAMA (UK), 2013) as mere few quality dimensions of overall data quality. Hence, it depends on the context in which these are observed - there exists no rigorous definition on how these concepts relate and organize.

6) Although few theories like Situation Awareness (SA) are presented as frameworks to study the concepts, the intention is not to present results via rigorous exercise of those. Target is merely to present initial, high level model and concepts, from which rigorous research follows later.

The context of this research is cybersecurity and the focus is on "information as an asset needing appropriate security and quality monitoring added with capability of sharing the quality metrics to outside party". Time span of the focus is continuous operations of an organization, so the findings can be applied to any lifecycle phase of an organization, where they are deemed practically applicable. When presenting the concept of the model this thesis is aiming to create (Chapter 7), the time focus spans over boundaries of single critical infrastructure operators (like a company). The latter concept hence considers different life cycles of nations and infrastructure operators of it – be they public or private.

The main objective of this research can be summarized as follows: Investigate, whether a novel and innovative model can be made for enabling situation awareness via monitoring critical infrastructure service providers critical information assets' data quality, especially data integrity. This is studied via combining established disciplines of information management, information security management, data governance, information security governance and situation awareness. The model is to be constructed and empirical evidence on the model's applicability and possible relevance via interviews of recognized Finnish cybersecurity strategists and tacticians is to be obtained as well.

1.4 Research questions

There are three main research questions (Qs) which the author intends to answer. These questions have emerged from the author's extensive experience in information management and business development; especially from the notions of the author, where he has felt that his personal empiric experience is

in contradiction with scientific and common practitioners' views and practices or that those views are limited in forming synergies or evolving new concepts that author sees beneficial. Hence the intuitional "There is a need for novel models"-feelings have been formalized to research questions, studied via literature and formation of a theoretical prototype and further investigated and enriched with data from an empirical study of five cybersecurity experts from both strategic as well as tactical and operational mindset. The key questions forming the standing stone of this research are:

> **Q1: Can a novel model be built leveraging from established disciplines of master data management (and data governance), information security management (and information security governance)combined with situation awareness for purposes of:**
>
> 1. **providing organizations capability to identify their critical information, build controls over it and identify any attempts to tamper the critical information assets**
> 2. **presenting command and control -type operator (like Cyber Security Command Center) with a situation awareness and early warning capability over threats compromising information assets of identified critical service providers?**
>
> **Q2: If such a novel model (as per Q1) could be built, what would be its potential value for national cybersecurity capability of Finland?**
>
> **Q3: In Finland's cybersecurity context, is information understood as an asset by critical infrastructure service providers:**
>
> 1. **Are these assets identified and protected accordingly?**
> 2. **Are there decent controls over information assets?**
> 3. **Is the concept of data quality and its monitoring present?**

A wide range of research questions could be derived from the potent of this research and the findings presented, however to prevent the research from exploding in scope the focus is on the three main questions. Some of these possibilities are discussed further in section 10.8.

1.5 Research methodology

The present research consists of three parts. Firstly, a conceptual research based on literature review is conducted to understand the main concepts and constructs of the research to form conceptual models needed later as well as to make initial observations from the secondary data. The second part is a construction phase, where the formed conceptual models are fused into a prototype novel model – the focus of the RQ1. The last is the third part - an empirical qualitative research based on a semi-structured interview: theme interview. The research approach and plan is visualized in FIGURE 1. The research approach

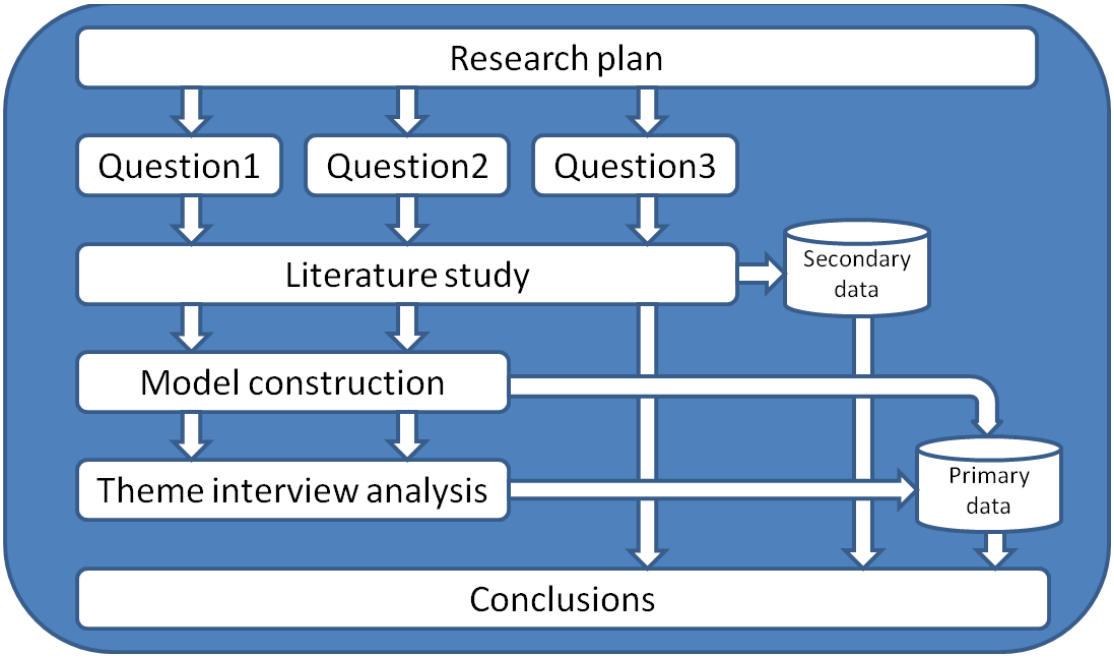


FIGURE 1. The research approach

FIGURE 1. The research approach explains that the research has started with a research plan (including initial literature study). The research questions have then arisen from the research plan. The conceptual models and constructions needed for the research questions are produced from the literature study part. Questions 1 is concluded partly already (by demonstrating the model) in Model construction phase (Chapter 7) and concluding is finished in Chapter 10.1: Concluding research question 1. Question 2 is concluded almost as such

from the interviewee answers in the Theme interview analysis part (Chapter 9), whereas Question 3 is answered in Chapter 10.3: Concluding research question 3.

The figure also shows the data collection approach in the research: the secondary data (the data already available as known/published and easily available) is gathered from literature reviews and it works as input to the model building as well as theme interviews; the primary data is the data gathered and analyzed from the interviews. Both the primary and the secondary data contribute to the conclusions.

Qualitative research conducted and the methodology used is further elaborated in Section 8.1. Possible limitations and reliability of the research are covered in Sections 8.3 and 10.6.

1.6 Key findings

Only the findings central to the presented research questions are briefly introduced here. All other, significant, findings are available in Chapter 9: Interview study analysis and Chapter 10: Conclusions, limitations and future research. The following findings should be seriously considered, especially in the context of cybersecurity, for the purposes of developing situation awareness in an organization or on national scope or when either researching or practicing information management and information security management:

- Very promising models for needs of situation awareness and critical information asset integrity assurance, control and monitoring can be built and combined from established disciplines and models of master data management, information security management, data quality and governance of these.
- The model proposed in this research was deemed as extremely important and promising by leading Finnish cybersecurity strategists,

tacticians and operative persons. There is great potential for early warning system of threats targeting to compromise critical infrastructure service providers' critical information assets and thus cause great nation-wide damage. Similar models might prove out to be very useful in preventing battle damage escalations and controlling the threat or attack vectors targeting to degrade information assets.

- There is evidence in both literature and from the interviews conducted that "information as an asset" -thinking is still not established in but few organizations. Security measures are more concerned about technology than the information the technology should be processing and thus efforts are somewhat inefficiently directed. To enhance the situation, organizations should treat information as any other key asset, identify where it resides, name the most critical part of it and establish decent controls over these assets. Also, streamlining could be realized between information management functions and those of information security functions for better efficiency and shared goals.

1.7 Significance of the research

This research has been initiated from the author's keen interest on the topics covered and the author's perceived importance of these topic. The author has been led by his intuition that the findings of the study are also very relevant to the scientific community, to the practitioner community of enterprise as well as cyber strategists and tacticians working on national level thriving to improve nation's cyber security. On the last listed, author sees this work contributing directly and at the same time with high possible gain to society's resilience and general feeling of positive control and safety.

Classic roles of Chief Information Security Officers, Chief Information Officers, Risk Managers, Information Security managers and even top management e.g. Chief Executive Officers responsible especially for the governance of information and its security are target group of this study.

As this research is limited in its data scope, namely the number of interviews, some care must be practiced when utilizing the findings of the research. Generalization should only be applied with caution and generally only to similar contexts as the research is presenting. Although a limited number of cyber-professionals was interviewed, it is worth noting that the persons interviewed have been very central for example to formulation of Finland's Cyber Strategy and deriving operational plan for executing it. Hence, the findings should be considered very significant through their views on them - at least when inspecting the findings in Finland's national scope.

This research contributes to rethinking the dominant classical silo -models in information management, information security management, data quality and governance of these by introducing a fusion of concepts -view on a very little researched area (although there is extensive literature on all of the separate topics). The perspective presented is challenging, as it weaves together many concepts and constructs and thus challenges academics and practitioners to further integrate the studied areas.

Yet, the research presents a fresh and innovative view and a new way of thinking, not yet seen in any previous studies and offers many open windows for further research as elaborated in Section 10.8: Further research possibilities

1.8 Structure of the research

For being able to draw the "big picture" of the researched topic, the author is presenting the key concepts and constructs in literature study from Chapter 2 to Chapter 6. All the concepts and models referred later in this research, especially the themes investigated in the empirical part, can be grounded back to the entities in the literature part. Although synthesis is always important in scientific results delivery, the literature part's main function is to present concepts to be fused together, not rethink the established concepts or provide innovative syntheses of those.

Drawing from the literature study, a novel and innovative new model proposed in RQ1 is formulated and presented in Chapter 7. The model is later tested in empirical study.

As the knowledge background is established, the approach and justification for the empirical study is explained in Chapter 8. Once the approach is elaborated and the interviewees are presented, Chapter 9 shows the analysis of the interviews separated into themes that investigate related phenomenon or questions and it also reflects the author's personal opinions and findings in comparison with those in the expert interviews.

Chapter 10 draws the conclusions as answers to the presented research questions and provides other conclusions that are related to the research questions and can help further to understand the answers to the research questions. It also closes this research with suggestions for future research.

2 CYBERSECURITY

For the empirical part of this thesis it is relevant for both the readers and the interviewees to investigate the elusive term and definitions of *cybersecurity* as it is the context, in which other concepts of this study are investigated in. This chapter will start with inspecting different definitions for cyber security and providing conceptual synthesis of it for the purposes of this thesis. Furthermore, cyber security threats are introduced for the reader to understand why cybersecurity either is or is not an important theme. Lastly, notions made through the chapter are summarized.

2.1 Cybersecurity definition

It is identified that there is no universally accepted definition for cyber security. Hence, for the purposes of this thesis, some synthesis must be derived from found information on the subject to put other phenomenon identified into context.

Even organizations like Council on Cyber Security seem to avoid and only offer results of compromised cyber security like (Council on CyberSecurity, 2014 (a)): "Massive data losses, theft of intellectual property, credit card breaches, identity theft, threats to our privacy, denial of service – these have become a way of life for all of us in cyberspace". The closest they come to any definition is (Council of Cybersecurity, 2014 (b)): "We are at a fascinating point in the evolution of what we now call cyber defence". As such, this definition, even if not even trying to address cybersecurity is ambiguous and evasive. For them "cyber" seems to be a yet undefined period in time, where frightening ICT-technology assisted crimes happen in "cyberspace". They still see that this "cyber" is something, which is blurring traditional infrastructure borders like company's networks by stating that the data that used to be there, is now distributed across multiple locations, not part of that "old times" classis technology nor physical infrastructure (Council of Cybersecurity, 2014

(b)). All this leaves a notion that the "cyber" and the time dimension of it is something, that is somewhat changing the rules and control over things (like data) is getting harder to maintain. This notion is worth noting as it describes the "spirit" of the "cyber" to an extent.

Further definitions follow as "The state of being protected against criminal or unauthorized use of electronic data, or the measures taken to achieve this" (Oxford University Press, 2014). Although a university press, this definition lacks the recognition of other assets than information (e.g. people, technology). The interesting viewpoint of an desired state of "being protected" is good and practically aligns with Finland's Cyber security Strategy's(Secretariat of the Security Committee, 2013) (note, written forms do also differ between definitions, e.g. cybersecurity vs. cyber security) definition: "Cyber security means the desired end state in which the cyber domain is reliable and in which its functioning is ensured". The Strategy's definition further elaborates the desired end state, there is no disturbance to operations or functions dependent on electronic information (data) processing and relies on actors in cyber domain (companies and institutions) implementing appropriate and sufficient information security procedures (Secretariat of the Security Committee, 2013).

Some definitions are quite narrow in view (naturally common people need definitions, which they can understand) and are sure to create disparity on discussions and literature, should someone adopt them. Such an example is Merriam- Webster's(Merriam-Webster, Incorporated, 2014) definition of: "measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack". Now, as quite obvious, focus is solely on technology, the information -part is neglected.

An online tech dictionary for IT professionals and educators, Webopedia (QuinStreet Inc., 2014), offers the following definition: "Cybersecurity refers to the technologies and processes designed to protect computers, networks and

data from unauthorized access, vulnerabilities and attacks delivered via the Internet by cyber criminals". This definition identifying the core components possibly affected by lack of cybersecurity, although it puts cybersecurity into context of Internet, which might not be the case, e.g. SCADA-vulnerabilities (Teixeira, Dán, Sandberg & Johansson, 2011) on isolated and not internet-connected automation networks. Also, the term "cyber-criminal" is interesting and could lead to long philosophical discussion whether a state is a cyber criminal, if it actively renders useless a technology of an attacker compromising its cybersecurity status.

National Initiative for Cybersecurity Careers and Studies definition (2014) is very activity centric with: "The activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation". According to this definition, it is not anymore about mere protection and security, but also about defence, which can be in military terms "active" (Denning, 2014). Definition lacks the part of critical infrastructure per se, but considers the ICT-side of it solely.

Gartner, although quite recognized professional company falls dramatically short in its own definition, totally lacking the information (i.e. asset to be secured) –part of the definition. Gartner(2013) defines cybersecurity as: "Cybersecurity encompasses a broad range of practices, tools and concepts related closely to those of information and operational technology security. Cybersecurity is distinctive in its inclusion of the offensive use of information technology to attack adversaries". Additionally to neglecting the information asset, Gartner distinct itself with explicit inclusion of IT in cybersecurity.

Last definition investigated is provided by International Telecommunication Union (2014) and states as follows:

> *Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise the following:*
>
> - *Availability*
> - *Integrity, which may include authenticity and non-repudiation*
> - *Confidentiality*

ITU's definition is rather extensive, nevertheless at the same it includes everything and thus nothing. For example "cyber" can be single person or "cyber environment". Although nation can be understood as "organization" of a sort, ITU's proposal lacks the many times mentioned intention to affect infrastructure of a nation, which to author seems of importance to be included in a synthesis of cybersecurity. On the positive side, ITU recognizes the classic CIA-dimensions of information security as integral part of cybersecurity and thus building glue between these two concepts.

That being said, the author feels that in general the definitions offered (via not rigorous scientific search on the topic) all base more on classis information security (management) responsibilities, targets and controls. What is distinctive is that scope of definitions varies a lot from almost single computer to very large systems of systems, of which nobody really even can understand the causalities and relationships they form. Terms are somewhat confusing and even mixed, there is a clear need for standardization bodies to take strong initiative on setting the same meanings for key concepts.

2.2 Snapshot on cybersecurity threat landscape

Naturally as "cyber" is getting more and more media attention there is a human nature's trait to think along the line that cybersecurity threats are dramatically increasing. This could be called "bias of availability" as per (Kahneman, 2012, p. 129). It is thus feasible to research few studies done on the volumes of cyber threats and present statistics to build a general view on the trend and the phenomenon.

First, it is worth noting what these threats are about. Where financial sector is very good at (in theory) is that they are capable of identifying and processing risks and manage as well as govern the organization through risks. With this mindset, it possible to form a simple classification of cyber threats through seeing them via risks. An example of such view is provided by The Atlantic Council in co-operation with Zürich Insurance Company (2014) shown in TABLE 1, in which risks are aggregated to seven main categories. It shows that the risks (and thus threats) are very multifaceted in nature and come both in technology and people.

TABLE 1. Seven aggregations of cyber risk (The Atlantic Council and Zurich Insurance Group, 2014)

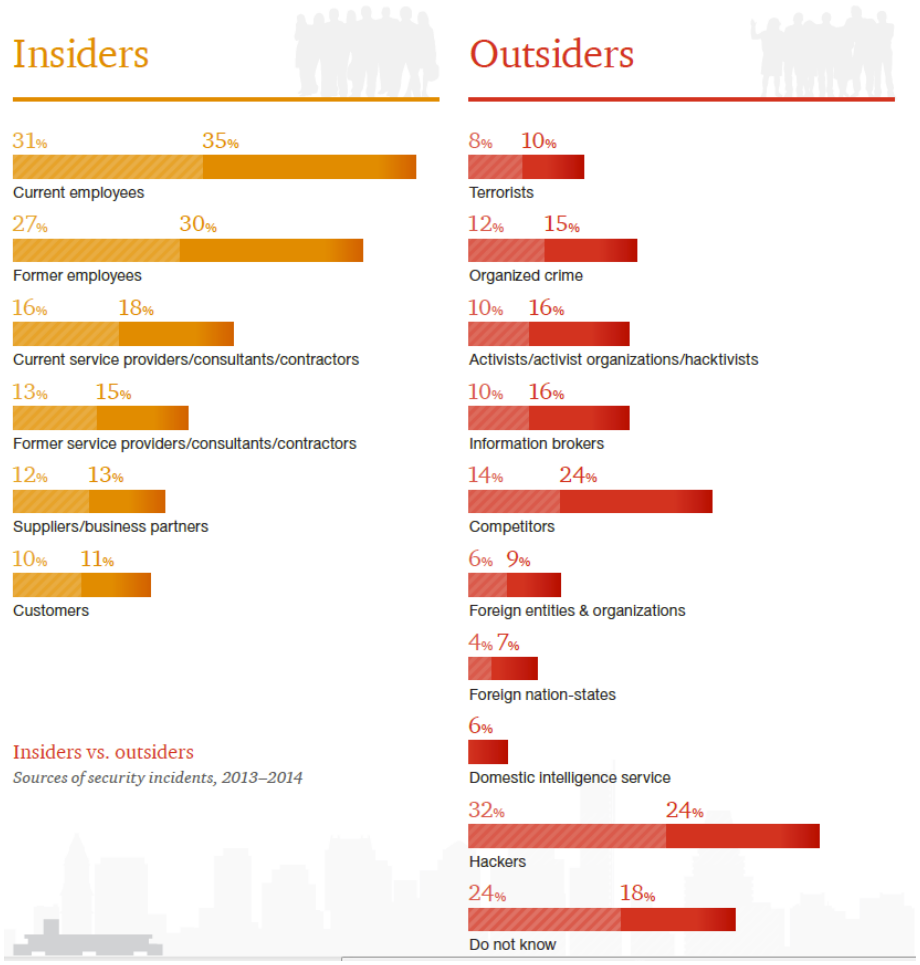
	Description	Examples
Internal IT enterprise:	Risk associated with the cumulative set of an organization's (mostly internal) IT	Hardware; software; servers; and related people and processes
Counterparties and partners:	Risk from dependence on, or direct interconnection (usually non-contractual) with an outside organization	University research partnerships; relationship between competing/cooperating banks; corporate joint ventures; industry associations
Outsourced and contract:	Risk usually from a contractual relationship with external suppliers of services, HR, legal or IT and cloud provider	IT and cloud providers; HR, legal, accounting, and consultancy; contract manufacturing
Supply chain:	Both risks to supply chains for the IT sector and cyber risks to traditional supply chains and logistics	Exposure to a single country; counterfeit or tampered products; risks of disrupted supply chain
Disruptive technologies:	Risks from unseen effects of or disruptions either to or from new technologies, either those already existing but poorly understood, or those due soon	Internet of things; smart grid; embedded medical devices; driverless cars; the largely automatic digital economy
Upstream infrastructure:	Risks from disruptions to infrastructure relied on by economies and societies, especially electricity, financial systems, and telecommunications	Internet infrastructure like internet exchange points and submarine cables; some key companies and protocols used to run the internet (BGP and Domain Name System); internet governance
External shocks:	Risks from incidents outside the system, outside of the control of most organizations and likely to cascade	Major international conflicts; malware pandemic

The technology vs. people threats is discussed next, but a note should be made to highlight two risk categories (TABLE 1):

- Internal It enterprise – what is very worrying is that according to the study only 1/3 of London Stock Exchange 350 companies management had clear understanding of their information assets, 60% reported "basic understanding" and further – 25% reported that the board –in 25% of the studied companies – had very poor understanding of where their information assets resided and were they shared e.g. with third parties
- Supply Chain – is not commented by Atlantic Council, but author would like to pay attention to this risk category as organizations are increasingly outsourcing and building value and supply chains, over which they perhaps ultimately have only contractual control, which provides, in authors thinking, major risk escalations. The organization might even quite well manage its own information asset, but if the other parts in the chain do not and the organization

has no visibility to this, its own functions are very much in jeopardy. This is investigated further in the empirical part.

Without drilling into details, as cyber risks and threats are studies of several dissertations, author wishes to underline one aspect of cyber threats, which is relevant for this study too, as the problem statement in Chapter 7 is assuming that there is no absolute defence. It further assumes that organizations do not generally have clear understanding, ownership and control over their information assets (as noted e.g. in "Internal It enterprise" –risk elaboration earlier). Fundamentally increasing the later presented threat –description's danger is that technology cannot prevent the perimeters from being breached. This is shown well in The Global State of Information Security Survey 2015 (PwC, 2014) with indication of the sources from which cyber threats (and information security threats in general) hail from.



Insiders vs. outsiders
Sources of security incidents, 2013–2014

FIGURE 2. Insider vs. outsiders –threats (PwC, 2014)

Survey well identifies the sources of threats and shows trend changes (year 2014 is represented by solid color, while 2013 by striped fill of the graph) all this good for purposes of introducing the scene. Author stresses a fact, which elaborates the importance of understanding the role of *insider threat*: "In the 2014 US State of Cybercrime Survey, we found that almost one-third (32%) of respondents said insider crimes are more costly or damaging than incidents perpetrated by outsiders". (PwC, 2014)

On the numbers of how the amount of threats/risks has been developing it is also worth to investigate few studies presenting figures from before 2010 as well as the development from 2009 and onwards. A steady trend on malicious cyber activity targeting US Department of Defence can be observed in TABLE 2 and although the increase is high on annual perspective, the growth is more linear than e.g. exponentially increasing.

TABLE 2. Cyber activity targeting US Department of Defence (adapted from (Choo, 2011))

Calendar year	Number of reported incidents of malicious cyber	Percent increase from previous year
2000	1415	N/A
2001	3651	158,02
2002	4352	19,2
2003	9919	127,92
2004	16110	62,42
2005	23031	42,96
2006	30215	31,19
2007	43880	45,23
2008	54640	24,52
2009	71661	31,15

The increasing trend, seems to continue from that of 2009 (TABLE 2) in 2013 as similar observations are made in a security breaches study in UK by The Department for Business Innovation and Skills (2013) reporting that 93% of

UKs large companies had breaches 2012 with median of 113 breaches suffered annually for large companies and that the general trend is increasing in security breaches.

A global survey(PwC, 2014) of some 9700 (2014) security, IT and business executives conducted annually since 2009, reports (FIGURE 3) steady increase with a rather dramatic jump from 2013 to 2014 (48%) as well as the number of reported security incidents in the study summing up to 42,8 million annual or 117 339 per day – compound annual growth rate from 2009 to 2014 has been 66%

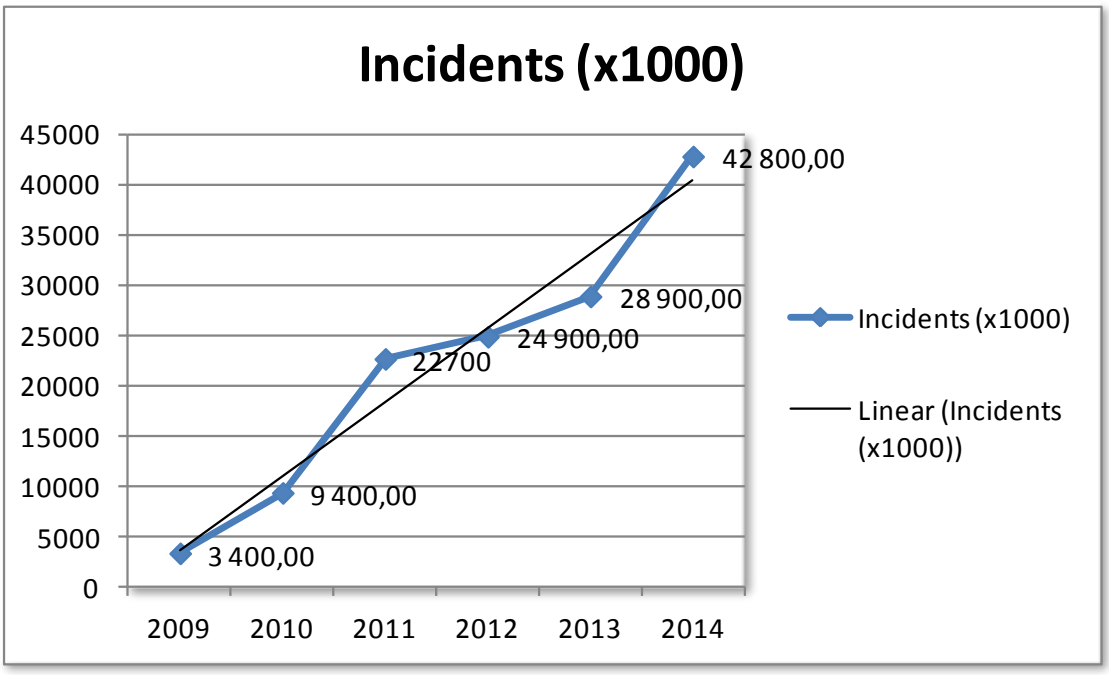


FIGURE 3. Incidents growth rate from global survey 2009-2014 (adapted from (PwC, 2014))

These few views combined, yes, there is a clear increase, but due to what the increase mostly is, remains a question, which is not even intended to be answered here. It could be plain increase of ICT -technology, which would

correlate with the threat number; better technological capability to detect the attacks and so forth.

To just show trends (like most of these surveys do) on something without trying to explain, what the reason is for it, is in author's mind even misleading. Should we be more worried about cyber threats increase, or put it into context of ICT-technology trends all being on the raise (e.g. number of devices, computing capacity)?

Whatever the reason is, it seems to be impacting on how EU citizens are feeling more insecure in the internet-connected technology domain. According to one of the surveys, "Special Euro barometer 404 ´Cyber security´"(the European Commission, Directorate-General Home Affairs, 2013), users are worried about their personal identities getting stolen (52%) and are generally worried that their personal information is not kept safe in website (70%). What is very worrying is that citizens have rather low trust on public authorities, where only 36% have no concern on these authorities not compromising their personal information and in general 76% agree that the change of finding oneself as cybercrime target has increased over last year(the European Commission, Directorate-General Home Affairs, 2013). With even only these figures presented by somewhat trustworthy authority, it seems that the general opinion is on increase of cyber crimes and thus feeling less secure in the digital world.

2.3 The author's elaboration and a summary on cybersecurity

First the term cybersecurity was researched to provide enough material for being able to build a conceptual model on the phenomenon, which seems so much to be in the headlines and which is the context of this study. Few remarks are to be done. First, it is quite clear that the terminology is not established yet and thus cybersecurity is seen both as miniature as protecting single IT-system to something of universal entropy taking over. This naturally

is not desirable as it is more oil for tabloids to build headlines, which build availability of bias for the community at large – although nothing dramatic would not being happening at all. At the same time, "cyber" is nothing new, it has been known with names like information warfare or electronic warfare, when put to military context.

Second, it a short study was introduced for sake of understanding what the cyber (and information security) threats are about through risk management thinking and further it was shown that insider threats are very important, if not even more important than outsider threats, for cybersecurity for realization of damages from the threats. Later, through few reports the trends of cybersecurity breaches and attacks were investigated to build some understanding through numbers. Looking through the numbers, increase is more like linear (although significantly increasing), not anything exponential by nature. How the growth then can be explained are several answers, which are not studied here, which one is closest to reality. First, it can be that as information security breaches have been and are still, very delicate matters especially to listed and high brand-value corporate, the interest of sharing security compromises has not been high, but culture could be changing and sharing information is seen as good of everyone. Second, as technologies to prevent and detect threats have advanced late few years, so are the number of threats increasing with perhaps even 1:1 causality. Third, one should not forget that information, computing capacity, sheer number of mobile devices is increasing quite dramatically also – could the trend be explained much due to this correlation?

The author recognizes the fact that producing malware and "cyber threats" have become more and more available to even persons of almost entry levels in utilizing ICT-technologies – it is no longer geeks with soda and pizza in the cellar, it could be the neighbor next door. This naturally has impact on the trend. Again, there are also trends like digitalization having more and more

attention, which means there more to attack, more to gain, which could also have impact on the trend.

In short, terms and definitions are a mess, which fosters confusion, misunderstanding and tabloid scandal reporting, trends are increasing, be the reason whatever – so, the "cyber" sure is here, has been here and will be here more in increasingly amount. It is better to be safe than sorry.

Now that the context is much set, next chapter starts investigating the disciplines of which the Research Question 1's model is to be into fusion.

3 INFORMATION SECURITY GOVERNANCE AND INFORMATION SECURITY MANAGEMENT

The author has put much significant elaboration effort on describing what *information security governance (ISG)* and *information security management* (*ISM*) are about. The purpose of this is to create a deep enough conceptual model for the reader, so she can process *ISG* and *ISM* in the closely linked concept of *cybersecurity* presented earlier (Chapter 2). Concepts are also needed to be studied to a level that alignment with empirical part's interviews can be assured.

This chapter starts by introducing information security governance, followed by inspecting few conceptual definitions of ISM. Next, the threats against which ISG and ISM are offering protection against are studied. Followed by the threats, cybersecurity as an operation function in scope of single organization is perceived. Reason for including the previous viewpoint is to compare, if ISM and cybersecurity do differ significantly in context of single organization (which is especially not part of e.g. emergency supply network). Closing the chapter a summary is provided on the extensive list of concepts studied.

3.1 Information security governance

To better understand the following concepts of information security governance and later data governance, first a look is taken at the concept of governance in general. Doing that, the concepts of data governance and information security governance as sub-classes of governance can be reclected. Governance comes in tens of definitions and hundreds, if put to context. For relevant purpose, *corporate governance* was selected to set the boundaries in which both data governance and information security governance operate. A neutral synthesizing source was used. Wikipedia defines (with 66 references) it as (Wikipedia, 2014):

> *"Corporate governance broadly refers to the mechanisms, processes and relations by which corporations are controlled and directed. Governance structures identify the distribution of rights and responsibilities among different participants in the corporation (such as the board of directors, managers, shareholders, creditors, auditors, regulators, and other stakeholders) and includes the rules and procedures for making decisions in corporate affairs. Corporate governance includes the processes through which corporations' objectives are set and pursued in the context of the social, regulatory and market environment."*

As the concept of governance set, information security governance is to be explored starting with ISO27000 –standard's(ISO/IEC, 2014) definition as: "system by which organization's information security activities are directed and controlled" and the governing body as "person or group of people who are accountable for the performance and conformance of the organization".

As ISO is talking about accountability, which naturally is important factor, a view can be also taken via commitment as leadership, like Von Solms (2005) does: "Information Security Governance consists of the management commitment and leadership, organizational structures, user awareness and commitment, policies, procedures, processes, technologies and compliance enforcement mechanisms, all working together to ensure that the confidentiality, integrity and availability (C-I-A) of the company's electronic assets (data, information, software, hardware, people, etc.) are maintained at all times".

One viewpoint to information security governance is to see it consisting of two parts – the operational information security management and information security compliancy management (von Solms, 2005). This line of thinking is based on good company government principles that no function should be auditing itself (like IT department should not do IT audit, nor financial compliancy audit done by finance department). Thus as von Solms (von Solms , 2005) puts it, the separation of operational management and the compliancy

management must be separated and "[…] the Information Security Compliancy Management function must be housed either as a totally separate department or section, or hosted by some other department or section, for e.g. Audit or Risk Management". This governance separation from operative function is supported by Henry (2003, p. 667) when he underlines that separation is needed as conflicts are otherwise risen between interests of secure processes and IT-systems development. Such compliancy function should have quite direct lines or even be part of C-level operations to be able to 1) monitor and report data security related IT risks in a model where IT is a service function to compliancy function (von Solms , 2005) and to 2) capture the policies made by the top management and force the policies made by top management with needed authority.

Now that the concept of information security governance has been explored in short, it is worth investigating, what operational capability the governance then should be governing, i.e. management of information security, which is following next.

3.2 Information security management

Hardy (2006) expresses it well, why information security management is important by saying that just one – just one – successful security breach, theft, error, hack or virus attack on a company may result in serious reputational or financial damage.

There are numerous definitions for *information security management (ISM)* . Some are studied to form a needed level of consensus between studied definitions for purpose of being able to provide a synthesis of ISM for both creating information so that reader can form a conceptual model of ISM and also to check the definitions with definitions gained from empirical part.

One way to define ISM is through purpose, as von Solms & von Solms (2004) do by stating that the purpose of information security management is presenting measures, which mitigate risks addressing information resources. Per that information security management can be seen as form of risk management for certain functionalities of the company. Capability to mitigate the risks comes back to notion in Background –section (1.1) to need to understand, what the company is protecting, i.e. what are the assets needing protection.

A view through objectives setting is presented as a short synthesis from Bernand, Gerber and von Solms and Mellado et al by Mas & Mesquida (2014) as "The main objective of information security (management) is to properly protect information from unauthorized access, use disclosure, disruption, modification and destruction". Again the definition is lacking the target other than "information". Something, as the volumes of data → information → knowledge → wisdom assets are getting out of hands as per problem stated in Introduction Chapter 1, is getting more and more important.

The author sees that the synthesis to be provided should consider the priorization of data-derived information assets to be resource-wise and protect that, which is most vital to operations or compliancy –needs. The sheer volumes and complexity of the information is presenting a situation, where not all the information can and should not (invest vs. gain) be protected and quality assured the same way.

A Classical view (from the 90s already) is to view information management through CIA-concept. A definition from ISACA (2012), provider of COBIT 5 IT management frameworks, is short for the purpose of presenting CIA via their definition of information security: "Ensures that within the enterprise, information is protected against disclosure to unauthorized users (confidentiality), improper modification (integrity) and non-access when required (availability)".

Now that the relation of ISG and what it covers, i.e. IMS is introduced it is worth adding into formula the factor of what is ISM presenting protection against – this is studied as follows.

3.3 Information Security threats and risks

Measures to prevent information security incidents, unwanted or unexpected security event with high probability of affecting negatively business operations and information security (ISO/IEC, 2011) are numerous. Four notions, which are relevant for the scope of the thesis should be noted, which will be tested later in the empirical part. The author summarizes the situation we have reached in 2014 as "partly the battle is lost". Organizations have to accept that they will be attacked successfully and that they cannot protect all their assets":

1) Sheer volume of data and the number systems processing it are steadily growing(Cukier, 2010) – it has become obvious that protecting all systems (and the data in those) fully just is not economically sound(Tondel, Line & Jaatun, 2014).
2) As Ahmad, Hadgkiss & Rughaver (2012) put it: "It is inevitable at some stage that organizations will suffer an information security incident. Such an incident may result in multiple negative impacts, such as loss of company reputation and customer confidence, legal issues, a loss of productivity and direct financial loss."
3) Common and flawed thinking has been that threats to assets come from outside (PwC, 2014), be it the main gate or firewall and defences needed are perimeter defences. "Inside" and "outside" has greatly diminished in meaning or there is no more such things, it's all blurred (Trope, Power, Polley & Morley, 2007). This is greatly due to s people are *bringing their own devices (BYOD)* and *-applications (BYOA)* to environments (e.g. workplace) which are not prepared to manage, i.e. IT has no control over those and thus present major information

security threat and a way through which cyber threats can realize their potential ((PwC, 2014), (Silic & Back, 2014), (Morrow, 2012) & (Walters, 2013)

4) Many organizations' management do not know what their information assets are or where they reside (The Atlantic Council and Zurich Insurance Group, 2014). With the misalignment between business and IT, this leads to situation that neither does the IT department has control over them. And via increasing use of cloud services, outsourcing etc. this is getting more and more vague ((Webb, Atif, Maynard & Shanks, 2014) & (PwC, 2014))

All organizations encounter internal or external factors and influences that might compromise the organization's capability to reach its objectives, make things uncertain. The effect this uncertainty has on the objectives set is called *risk*. (ISO/IEC, 2009)

Threat can be defined as(ISO/IEC, 2014) "potential cause of an unwanted incident, which may result in harm to a system or organization". Information security risk associates with a threat or threats and the potential of those causing damage to information assets and via that to the organization. Information security threats exploit vulnerabilities, i.e. weaknesses of assets or controls modifying the risk associated with the threat.

Threats and information security concerns are everyone's business. The trends show (Tondel, Line & Jaatun, 2014) that it is the people, like employees, that the attacks are directly targeting, not so much the technical systems. The soft side of information security is more emphasized with notion of: "Although a predominant weakness in properly securing information assets is the individual user within an organization, much of the focus of extant security research is on technical issues"(Crossler, Johnston, Lowry & al., 2013). Hence it is really a question to consider – "how should an organization balance its limited security resources – on the technical domain or people and

information"? A possible answer is provided Kevin Mitnick (2004, p. 4), a reformed computer criminal and later a security advisor: "It is much easier to trick someone into giving a password for a system than to spend the effort to crack into the system".

That being said, still researchers report via many studies that information security is still viewed as technical issue – report like this are identified in Tondel et al's (2014) study e.g. made by Jaatun et al. (2012) and Ahmad et al (2012). Question should be relevant as even scientific researchers indicate (and they have a natural lag on their findings due to review-cycles) that nearly half of intrusions and violations of security are actually caused within the organization by insider to the organization (Crossler, Johnston, Lowry & al., 2013). Similarly studies show that information security is not about technical security performance, but that some of the most serious security incidents are in fact due to people threats (Henry, 2003).

Threats in context of information security management can be roughly categorized as being technical or people threats. This classification is the same as presented in Chapter 2.2. Further the same chapter it was identified that threats can be classified of being either internal (insider) or external threats (outsider). Like it was in context of cyber, it is worth even though through repetition to underline the importance of people in the formula. In short - by Henry (2003, p. 663) - people are thought to be the weakest link in information security management.

As detail taxonomies building of threats is out of this study's scope, it is sufficient to proceed with the notions made already and threats introduced in Chapter 2.2. It is to be noted that the threats (classic information security vs. cyber threats) are actually much the same thing, when looked in the scope of a single organization. A remark, which hints of possible near 1:1 –relation of cybersecurity and information security management in the scope mentioned. This is to be investigated further in the empirical part.

In the following chapter author is presenting cybersecurity as it can be understood as tactical and operational capability. The intention with this presentation is to form a picture of "what cybersecurity on practical level" could mean. Forming a conceptual model, it can be further compared to model presented earlier for ISM.

3.4 Cybersecurity tactical operations in an organization – same as ISM?

To better understand, what cybersecurity does mean in form of action and capabilities a few elaborations are made a short introduction to a framework, which entitles itself as being cybersecurity –framework is given. All this done with intention to understand practical cybersecurity operations and further compare that with operations of ISM presented earlier in Chapter 3.2.

The author wishes to make some distinction, if there is any, between controls suggested by "classical" information security and management of it, like ISO 27000-family and COBIT5 and frameworks, models, and literature in general, which is describing controls or processes for management of information security. To further simplify, there is no line drawn between controls and processes, although the author recognizes that controls (which modify risk) can consist of process, policy, device, practice or other actions have impact on the risk control is addressing(ISO/IEC, 2014).

Looking at "The Critical Security Controls for Effective Cyber Defence" by Council of Cybersecurity one makes two notions. First the critical controls presented are "nothing new" as such – they are just a subset of controls presented in NIST –framework or ISO 270002:2013 and can actually be mapped to those. Hence, they can be considered as one unofficial (not aiming to regulatory compliance or internationally acknowledged standard) best practice model for information security management via approach of "quick wins", i.e. identifying the controls, which have the most effect. The second, and very unfortunate observation is that none of the "First Five Quick Wins"

has any contact surface on information itself, merely technology (Council of Cybersecurity, 2014 (b)):

> *For those wanting a highly focused and direct starting point, we have emphasized the "First Five Quick Wins": sub-controls that have the most immediate impact on preventing attacks. These actions are specially noted in the Controls listings, and consist of:*
>
> - *1. application whitelisting (found in CSC 2); 2. use of standard, secure system configurations (found in CSC 3);*
> - *3. patch application software within 48 hours (found in CSC 4);*
> - *4. patch system software within 48 hours (found in CSC 4); and*
> - *5. reduced number of users with administrative privileges (found in CSC 3 and CSC 12).*

Actually, of the 20 controls (FIGURE 4) only four have any direct relevance to managing the information as an asset. There is no practical advice (which is supposed to be the core of the whole framework) on how to really identify information assets, classify them, understand their system and business lifecycle or how to ensure their integrity and confidentiality. Advice is much limited to encrypting data and proving classification of "public data" and "private data". Control concepts like data quality management or master data management to define and manage the assets are everything but mentioned.

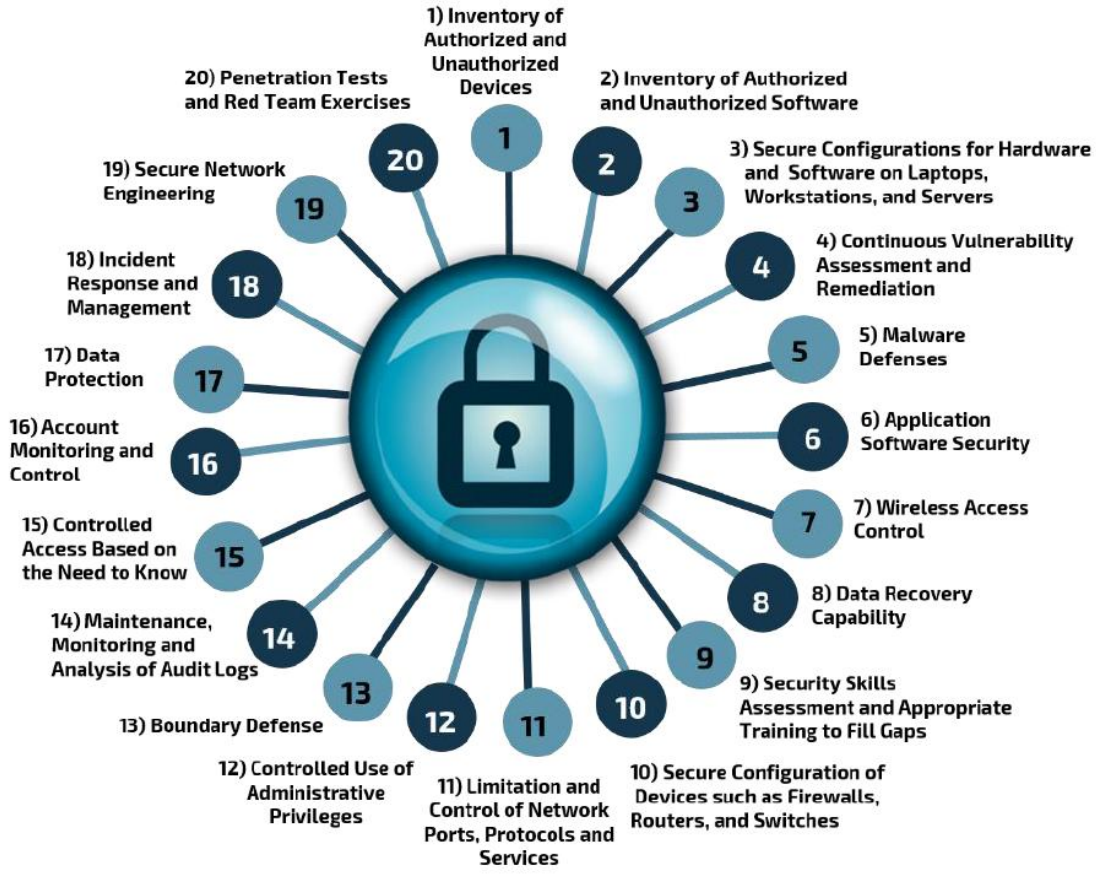


FIGURE 4. 20 Controls per (Council of Cybersecurity, 2014 (b), p. 8)

Of the presented 20 critical controls only controls 8, 15 and 17 try to address the asset itself, information, in any reasonable way. This shows that Council of CyberSecurity's approach is very technology centric and cannot provide much help for organizations viewing security through information management glasses. Of the attack vectors or attack types, which were basis for the prioritization of critical controls presented only four (out of 23) address information integrity and confidentiality directly. Even though the attack vectors are relevant, the remedies and protections presented produce very little real value. The four attack types are listed in TABLE 3. Shortlisted attack types from (Council of Cybersecurity, 2014 (b), pp. 106-107), which address information assets. The number on the right hand side column refers to presented 20 Critical Controls (FIGURE 4), which are addressing the attack type risk. One note to be made is also that the Control #8, which author associates remotely with "information as an asset" is not mentioned in any of

the Attack Types (total of 23) as a Control to block, detect or manage the problem. This presents a question on why the Control #8 was even selected as "Critical", if it does not address any of the Attack Types, which were basis for selecting the Controls?

TABLE 3. Shortlisted attack types from (Council of Cybersecurity, 2014 (b), pp. 106-107), which address information assets

Attack type	Critical Control
Attackers use malicious code to gain and maintain control of target machines, capture sensitive data, and then spread it to other systems, sometimes wielding code that disables or dodges signature-based anti-virus tools.	5, 15, 17
Attackers gain access to sensitive documents in an organization that does not properly identify and protect sensitive information or separate it from non-sensitive information.	15, 17
Attackers gain access to internal enterprise systems and gather and exfiltrate sensitive information without detection by the victim organization.	17
Attackers compromise systems and alter important data, potentially jeopardizing organizational effectiveness via polluted information.	15, 17

Regarding from the scope of the study -point of view, the four Controls identified here are the ones, which can be mapped as the Controls that contribute (even remotely) to author's later in Chapter 7 presented model for establishing and maintaining critical information's integrity and sharing its quality metrics to command and control functions in national cybersecurity context.

Next a summary of rough comparison between ISM and cybersecurity operative capabilities is given.

3.5 Operative Cybersecurity and information security are much the same

When limiting the scope to a single organization and its operations in security and comparing the concepts of ISM in Chapter 3.2 and concept, which describes cybersecurity on operational level in Chapter 3.4, observation is

raised that they are very much akin. Why this notion can prove important is that it could reduce the "noise" and misunderstanding, which seems to prevail in the industry on how single companies – especially those not part of any emergency critical supply network – should comprehend cybersecurity in their operations.

With much fraction done, author does perceive that they can be understood as the same for sake of simplicity. A Remark, which is backed up by e.g. Finland's Cyber Strategy. It states that an individual organization normally implements cyber preparedness through the traditional means, methods and structures of information security (Secretariat of the Security Committee, 2013). Never the less, companies (and organizations in general) should be better prepared to evaluate the risks and consequences of cyber attacks as well as the required action.

Closing the chapter, a summary of the extensive themes covered is provided.

3.6 Summary on information security governance and information security management

Although the chapter was mainly about ISG and ISM which were introduced, and covered in form of few definition and conceptualization with related threats described, it was also intending to build a capability to compare ISM with operational cybersecurity in scope of a single organization.

The author wished to do this to how that the best single organization – especially when not part of critical infrastructure services supply network (which has complex dependencies and little room for error in times of crisis), can start considering cybersecurity in operations as investing more on their current ISM capabilities by enhancing those practices and frameworks familiar. This is not to downplay cybersecurity as mere ISM, which is not, but to provide some practical guidance for organizations struggling with trying to understand cybersecurity and at worth getting paralyzed by the situation.

Although organization's need to accept the hard facts that absolute defence is impossible (via threats presented), surrender is not required. Identifying critical information assets, protecting those with priority one via well established data- and information management practices, as defined throughout this thesis, remains the key. It is essential that the most valuable data and information is well managed and protected – as this should be the primary mission of any information security operation.

Following chapter presents *information governance (IG)* and *master data management (MDM)* – already mentioned disciplines, which are (with *ISM* and *ISG* and later *data quality (DQ) and situation awareness (SA)*) the key components, which are to form the model as per Research Question1 (RQ1).

4 DATA GOVERNANCE, DATA QUALITY AND MASTER DATA MANAGEMENT

National Association of State Chief Information Officers (NASCIO) arguments in short, but with a clear message the importance of good quality data – NASCIO (2014): "Government performance depends on accurate and timely information" – *accurate* and *timely* being few dimensions of data quality. It might prove out to be endless debate among academics whether for example, data quality is a part of master data management or is master data management merely a materialization of a tool to achieve better data quality.

The author is not wishing to start a philosophical discussion. In this chapter he presents *data governance*, *data quality* and *master data management* only on the very surface, however with enough information to be able to form the "Novel, innovative model" presented later in Chapter 7 which combines the wide concepts presented.

4.1 Data governance

"Data governance refers to the operating discipline for managing data and information as a key enterprise asset. This operating discipline includes organization, processes and tools for establishing and exercising decision rights regarding valuation and management of data" (NASCIO), 2008), a well put definition for data governance. A specially worth noting is that NASCIO includes data quality, data security and –access as well as data risk management data valuation as part of this whole framework.

The few special notes to be made from the presented NASCIO-definition is that it is inclusive of governing the following (but not limited to) (NASCIO, 2008):

1) Data valuation

2) Data risk management
3) Data quality
4) Data security
5) Data access

These make it an extensive (heavy), however at the same time holistic governance framework.

What was worth noting in the presented definition, and thus within the scope of *data governance (DG*) is, that it is explicitly inclusive of information security aspects, as well as inclusive of identifying the information assets – something, which is mentioned also in the top challenges of information security incident management capabilities for establishing the operative capability (Webb, Atif, Maynard & Shanks, 2014).

Data governance can be seen as the unifying program for bringing together people, processes and IT in order to identify the needed roles and responsibilities for naming the organization's critical data and simultaneously ensuring its quality (de Freitas, Michel, de Macedo Rodrigues, dos Reis & Gronovicz, 2013). This again highlighting that DG is holistic and covers (among other things) data quality and control over critical information assets, e.g. master data.

Partly, it still remains the situation as it was back in the 2000 (Hinde, 2000) that corporate executives, although nowadays most understand that they can be held liable for neglecting their responsibilities over information and its quality, still consider in risk plans for example the destruction of a computing center as "an IT problem". So, they recognize their governance responsibility over information security, but fail to see the assets to be protected – the data and information derived from it.

Last, it is to be noted that only through integrating heavily in organization's strategy can DG be established. A cite from Cochrane (2009) illustrates this fact by: "Data policies. Data standardization, compliance regulations and quality controls will be major areas of focus for driving overall data quality […] Remember that data governance should be seen as a core competency and not as a project with predefined start and end dates".

4.2 Data quality

Most CIOs have had the courage to admit that their data is of poor quality. A study run by IBM (Cukier, 2010) tells that half of the managers who need to make a decision based on information received do not trust the information. It seems that data is besting us. Saha & Srivastava (2014) reveal that poor quality data is estimated to cost some 600 billion dollars annually to US businesses alone. The effect for building new warehousing systems that the low quality data is causing is a wide estimate from 30% to 80% of the whole development time and budget (Saha & Srivastava, 2014) – they are calling for data quality management to remedy the situation. Even though the estimate is +/-25% (in average 55%) it is still a remarkable effect that bad data quality can have.

As the other concepts, *data quality (DQ)* is huge in scope. It has been discussed in several sections of the thesis already and for example, ultimately the next topic, master data management, is about data quality. So is data governance. So is much of information security (management) as they all can be translated to quality dimensions at the end of the day. For example information security management has been classically concerned about C-I-A (confidentiality, integrity and availability) (ISACA, 2012) of the information assets the organization has (if ever identified through classic information security management). C-I-A can be translated to quality dimensions (feature of the data that can be measured), thus they are actually about DQ – and the other way around. For the purposes of this thesis a definition to author's own liking describing DQ is used: "The totality of features and characteristics of data that

bears on their ability to satisfy a given purpose; the sum of the degrees of excellence for factors related to data" (Roebuck, 2011).

Not to complicate the concept more, it is only necessary to understand that DQ is implicitly a part of the presented other key concept apart from perhaps situational awareness. Although there are no standards for DQ dimensions, Data Management non-profit organization DAMA (UK chapter especially) has presented in author's opinion the best description of key DQ dimensions. They are presented in FIGURE 5 where the six dimensions together can build a complete view on the quality of the data, although they are not always (and in many cases with good justification) used in combination of all six. DAMA (2013) itself defines data quality dimension as: "[…] feature (characteristic, attribute or facet) of data that can be measured or assessed against defined standards in order to determine the quality of data".

FIGURE 5. –Six Core Data Quality Dimensions (DAMA (UK), 2013, p. 8)

The dimensions of data quality as per DAMA are introduced in short, as they build the capability to form trustable *master data* (introduced in Chapter 4.3), critical information for operations to run. Once trustable and good quality master data is formed, it can be change controlled to ensure only valid changes to master data are taking place. Further via *data quality monitoring* we can capture possible changes violating business data definitions and data quality rules and manage their incident handling.

The six data quality dimensions are defined as (DAMA (UK), 2013):

> *1. Completeness is "The proportion of stored data against the potential of "100% complete""*
> *2. Uniqueness is "No thing will be recorded more than once based upon how that thing is identified."*
> *3. Timeliness is "The degree to which data represent reality from the required point in time."*
> *4. Validity is "Data are valid if it conforms to the syntax (format, type, range) of its definition."*
> *5. Accuracy is "The degree to which data correctly describes the "real world" object or event being described."*
> *6. Consistency is "The absence of difference, when comparing two or more representations of a thing against a definition."*

The last mentioned DAMA DQ dimension, consistency, needs to be further elaborated, which is following next.

4.2.1 Consistency –data quality dimension

For the purposes of providing the "Novel innovative model" in Chapter 7, which encompasses all the studied main concepts, DAMA's data quality dimension of "Consistency" is most relevant to note (described in TABLE 4). It is later used for monitoring purposes of established and quality assured (other DAMA dimensions are verified) baseline critical operational data and controlling changes in that.

TABLE 4. Consistency – one of the DAMA UK's (2013) DQ -dimensions

CONSISTENCY

Title	Consistency
Definition	The absence of difference, when comparing two or more representations of a thing against a definition.
Reference	Data item measured against itself or its counterpart in another data set or database.
Measure	Analysis of pattern and/or value frequency.
Scope	Assessment of things across multiple data sets and/or assessment of values or formats across data items, records, data sets and databases. Processes including: people based, automated, electronic or paper.
Unit of Measure	Percentage.
Type of Measure: • **Assessment** • **Continuous** • **Discrete**	Assessment and Discrete.
Related Dimension(s)	Validity, Accuracy and Uniqueness
Optionality	It is possible to have consistency without validity or accuracy.
Example(s)	School admin: a student's date of birth has the same value and format in the school register as that stored within the Student database.
Pseudo code	Select count distinct on 'Date of Birth'

Consistency as per DAMA is not enough for the model construction purposes (Chapter 7) purposes, but it will be encompassed with *integrity* as described in the following chapter.

4.2.2 Integrity of information (data)

Integrity of information is seen playing a major part today in managing information in general (Cukier, 2010). There are readily available meters for many dimensions of data quality as mentioned in the previous chapter. For the purposes of this thesis integrity is focused on, as it is the key data quality dimension to be monitored and subject of inter-organizational data quality status information exchange presented in Chapter 7. Integrity of information can be seen as (ISACA, 2012) "[…] means guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity". Integrity for ICASA (2012) purposes is broken down into dimensions of completeness and accuracy, but for this study, the ICASAs definition (without accuracy & completeness breakdown) is better suited.

Next, Master Data Management – a framework, which instantiates data governance, as well as data quality and parts of information security management also, is presented to provide the needed pieces for building the big picture later in Chapter 7.

4.3 Master data management

Information (which is data put into a context) should be handled just like other important assets of the organization. In information intensive organizations information actually is their most important asset (Mesquida & Mas, 2014), (Cukier, 2010), (NASCIO, 2008) & (ISACA, 2012)). It should be addressed with same control and supervision as other major assets (Hardy, 2006). This requirement is becoming increasingly difficult to fulfill, as sheer volumes of digital information (data) are were increasing tenfold every five years (Cukier, 2010). Yet, many organizations treat their information assets as a by-product, not as product – a problem already highlighted before the turn of millennia (Wang, Lee, Strong & Strong, 1998).

Master Data Management (MDM) is conceptually very elusive, and no generally agreed upon definition for it exists to this date(Antikainen & Käkölä, 2011). One definition, which is according to author's extensive experience on the topic of MDM, quite comprehensive and to the point is provided by Berson and Dubov: (2007, p. 11) MDM is a "framework of processes and technologies aimed at creating and maintaining an authoritative, reliable, sustainable, accurate, and secure data environment that represents a ´single version of truth´, an accepted system of record used both intra- and inter-enterprise across a diverse set of application systems, lines of business and user communities".

Again, as with data governance, it is worth underlining the words from the previous: "reliable, "sustainable" "accurate" and "secure". These adjectives can be linked directly to *data quality* and *information security management* as

well as *information security governance*. It is becoming obvious that the main concepts of the thesis do indeed link closely together.

Master Data (MD) can be observed as being the critical information related to the transactional and analytical operations of the organization. Alarmingly high, 75%, of leading companies were reported not being able to form a "single view" of their customer across operational silos and islands of data. What MDM can do, is bring common definitions for main organizations entities (like customer, product, supplier, chart of accounts, person and so on), provide business consistency and importantly – data integrity (Das & Mishra, 2011). In this context, consistency and data integrity are the glue between the larger studied concepts.

Master data, as defined earlier, is shared critical information across the organization as a whole. The relation of master data to rest of the organization's data is shown in FIGURE 6. Master data is at the very core of the data set and the other data and functions very much rely on it. In its nature, master data is slowly changing or even almost constant, unlike transactional data, which relies on master data to provide the key elements of a transaction – an example: *customer to whom product was sold and to who's warehouse location it was delivered and to which accounts receivable the transaction should be recorded*. In the example, the verbs present the transactions and the nouns the master data.

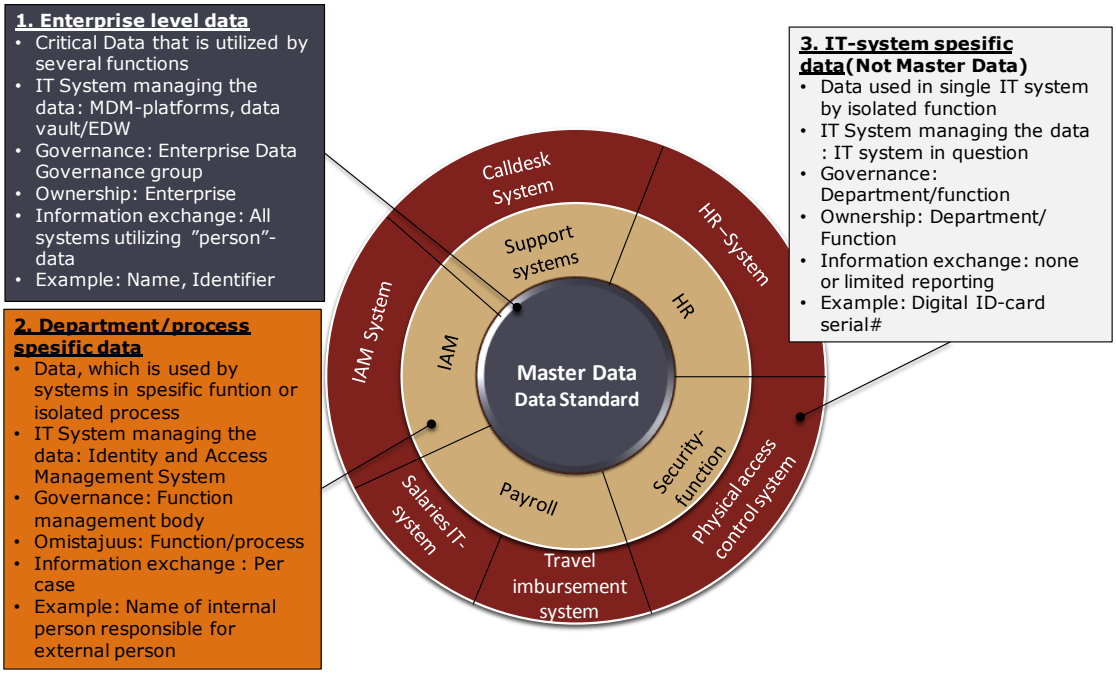


FIGURE 6. Relation of Master Data and its governance between different levels of organizational functions as well as IT-systems – an example of "person master data"

The *data standard* in the FIGURE 6 represents the *technical data quality rules* (the form and fit of the data are in order (the data looks right) and the *business quality rules* (the function of the data is right, i.e. it presents the right business concept in the context) combined into a presentation, which both drives consistent creation of master data, but as well as any changes to it – all which need to comply to the requirements of the data standard. In short, data standard is a set of rules for the data in a set context, which define whether the data (information) is of good quality or not when metered against set data quality metrics (dimensions) set (see 4.2).

MDM as a framework (or a body of knowledge as there are no standards for it yet) is not new. Along the lines already presented one finds a elaboration from 2006 by Kobelius (2006) describing MDM as key to corporate compliance, and the term referring to infrastructure, tools and best practices for governance of official corporate records and that MDM is also about data quality, integrity and security, which are everything, when compliance is concerned. By this definition and the one's before that, one can consider MDM as "*instantiation of*

data governance, which is targeting the very critical core information of the enterprise, ensuring its good quality, providing controls to maintain & enhance that quality, providing capability to efficiently share the information across function in a secure way and taking care of information's integrity across systems and departments of the organization – all this while maintaining rigorous control over master data's changes".

A characteristic, which is common for master data management and its data management processes is important to be mentioned as it is later used in the Chapter 7: The model of inter-organisation information assets' integrity monitoring for situational awareness. *Segregation of duties* is a operational principle of breaking an operation into tasks, which no single person can complete all on her own from process initiation to its end (Henry, 2003, p. 675). This principle, that it take more than one person to execute a process is crucial for ensuring that the controls for creation and change (master data very seldom is deleted) of master data, called *data management process*(*es*), cannot be executed by a single person. Only via change approval process of n+1 (where n=>1) persons, can created or changed master data be released into system landscape and be used in any business operations. Rationale is extensive, but this principle realized via data management processes is there in MDM to:

- minimize the number of human errors made to critical data (two eyeball checks minimum) and also to
- provide a model, where persons or systems without deep business knowledge can create or change "draft" (not published yet) data objects with the form & fit of the data as per defined in e.g. data standard.
- Later in the approval flow a business context-aware person can validate for functional correctness.
- Via this person's approval is the data promoted to be used in operations.

There are numerous various conceptual models for MDM. These models are ignored as being irrelevant for the scope of the thesis. MDM is presented as "instantiation" of both data governance and data quality. Although it is partly already in many comments show, these concepts are heavily entwined, and overlapping but for good shared purposes. As said, in the context of this study MDM –capability is a concrete operational "way of working", which realizes the targets of both *data governance* (introduced in Chapter 4.1) and *data quality* (Chapter 4.2), where both mentioned are apart of most MDM models.

The following chapter is to summarize this theme focused on information asset –concepts.

4.4 Summary on Data Governance Data Quality and Master Data Management

This chapter introduced the concepts and disciplines of data governance, data quality and master data management. They are a crucial part for building the model envisioned in the topic of this thesis.

Data governance is a governance function, which should reside as part of organization's other governance functions. Only via such approach can a organization state that it treats information (or data) as a real asset and it is governed and managed (via e.g. MDM) as other key assets are. Master data management was presented as a framework for managing *master data* - entities, relationships and attributes that are critical for an organization and foundational to key business processes and application systems. As such, the management function consists of roughly of the processes and technologies aimed at creating and maintaining the mentioned master data.

Data quality was studied and although controversial definitions and dependencies exist between DG-MDM-DQ (classic chicken-egg –problem) and there was no intention to dig into those, DQ was introduced via metrics (or dimensions), which are meaningful for e.g. estimating data's (or

information's) usability and trust one should put into it, they are at the very core of the model to be build in Chapter 7, as they are the measure, through which the model observes, if information is compromised by a threat or is it worth the trust needed to make decisions and operate processes based on it.

Although it was earlier mentioned through Chapter 2 to Chapter 3 that people were seen as possibly the weakest link in information security management, the author argues that through systems (process, people, technology) like Master Data Management (MDM, which is presented in next chapter), people can actually be the key enablers of information security. This is through their capability to process tacit business understanding and logic implicit in the data that cannot be easily modeled for automation and data validity estimation.

Where automated data quality rules can analyze the form and fit of the data, the function of the data, i.e. does it describe valid business logic, is something, which is very hard or impossible to teach to the machine. And the people in this form-fit-function -link need to be those executing the core business functions, not IT-people. This is best supported by a notion of a very common practice in any business data migration or quality improvement related IT-activity that the data is "checked and corrected" by business. This means that although IT-department people can screen the data for the form and fit, they do not understand the business context of it (the function) and the rules on which the data is deemed either "ok" or "not ok" - only business operations' persons can define that.

5 OVERLAPS BETWEEN STUDIED CONCEPTS

Through introduction of key concepts relevant for this study from Chapter 2 to Chapter 4, there has been clear signs observed by the author that the concepts are somewhat overlapped, although they are well separated in literature and in practice. In this chapter, some of the obvious overlaps are listed. This serves as part of the grounding on which the model presented in Chapter 7 is based on. It serves also as further study's possibility to rethink these silo-models and gain possible synergy by unison of them.

5.1 Information security policy and data policy

First to understand what both information security policy and data policy should both present is framed by ISO's(ISO/IEC, 2014) definition of policy as "intentions and direction of an organization as formally expressed by its top management". One can understand this as part of realization of organizations overall strategy. Hence, both information security and data policies should be directly manifestations of operative guidelines, i.e. realizations of the overall strategy in contexts of ISM and DM.

For a strategy to be realized it is common that policies are needed to drive the change needed to reach the target of the strategy, these policies been considered as guidelines according to which actions should be considered, so vision could be realized one day. In information security management programs the lack of vision and thus policies is seen as one main reason these programs provide little if any results (Henry, 2003, p. 664).

Von Solms & von Solms (2004) argue very strongly that according to their knowledge all international best practices, i.e. standards (like ISO or COBIT) are stressing the fact that an information security policy is the very starting point of proper ISG of and standing point for all sub-policies, standards and

procedures. They state that policy should be a short one and signed by CEO to show executive management's commitment.

This fact that policy, which should align with organizations' strategy, is an important success factor, is further underlined. It is even noted that in many cases policy is understood and interpreted as strategy (Knapp, Morris, Marshall & Byrd, 2009), which is rather understandable from operational level point of view. The non-existence of information security policy leaves the company and its information security enabler programs with little if any anchoring points and thus render them weak and not able to provide real results (von Solms & von Solms, 2004).

5.2 Synergies of Data Governance and Information Security Governance

Through literature study made, it seems there is already obvious overlap also between *data governance* and *information security governance*. Some were already mentioned, nevertheless this chapter lists few more secondary data findings from literature, which concretize the mentioned relation.

One possible glue between mentioned governance concepts can be found by taking a look on what Organization for Economic Cooperation and Development, OECD (2004) has stated in its "Principles of Corporate Governance":

> *[Responsibilities of the Board include] ensuring the integrity of the corporation's accounting and financial reporting systems, including the independent audit, and that appropriate systems of control are in place, in particular, systems for risk management, financial and operational control, and compliance with the law and relevant standards.'*
>
> *[...]*
>
> *'In order to fulfil their responsibilities, board members should have access to accurate, relevant and timely information.'*

Here we can observe explicitly observe that the board has direct responsibility over controls, which requires effort of governance from them. Also integrity is called after, which means (with the controls added into equitation) that ISG – capabilities are needed as well as DG-capabilities (DQ explicitly addressed) in the latter snippet "[...]should have access to[...]" need to be in place.

Demanding more push for the need of information security governance Hardy (2006) says that board of directors and senior management should ensure their information assets' protection and that governance of those should be on top of agenda with being regularly addressed. This promotes again union between ISG and DG as it implicitly means that the assets must be identified (DG) to be protected (ISG) and that this should happen as a continuous governance capability rather than one time effort.

Sarbanes- Oxley Act of 2002 (107th Congress of the United States of America, 2002) both requires that CEO/CFO ensuring that the company has proper controls in place and at the same time also requires that any deficiencies in the data used must be identified. This means that the signing officer must have a concept of the quality of the data used and also acknowledges the risks that might be addressing the reporting data, which can be translated to information security (as integrity being one security requirement as well as data quality indicator). Also, one should not be able to say that internal controls are good if the information management systems are not secure. These requirement put together show more synergy between ISG-DG as well as on operational level uniting MDM and ISM.

Overlaps are clearly presented in regulations and compliances which have been introduced in the previous few years. Many of those are driving towards realizing of information's relevance to whole corporate operational capability, e.g. ones like SOX, BASEL II/III and Solvency II. These, like Solvency II does (European Insurance and Occupational Pensions Authority (EIOPA), 2009) directly and quite explicitly demand capabilities to manage the

data in a formalized and demonstrable way (data management processes, data standards, data integrity, etc.), something, which requires a governance structure to really be compliant. Hence, board of directors has a direct corporate governance responsibility over data assets as well as their security ((von Solms , 2005) & (Hardy, 2006)).

Last, although it is out of the scope of this study, how the governance should be organized or executed, the following needs to be taken into consideration on the matter. It highlights the disparity between IT and business (it has been there and not vanished yet), especially in light of what was earlier noted about compliancy governance requirements (e.g. controls in place to systems, security and reliable data). Why ISG and DG should not reside as part of IT, already back in 2006 (Hardy, 2006) states that according to a non-profit organization, ITGI's, survey of 335 CEOs, CIOs and other executives more than 2/3 of the CEOs were not comfortable answering questions about governance and control over their IT processes. A finding that with good probability indicates that even with their current responsibilities (if they are even defined) IT is somewhat detached from the business, i.e. they are not governed and controlled as should. Similar evidence on the linkage between business strategy and IT projects being weak is summarized for example by Steward (2008, p. 206) summarizes as follows: "[…] IT investments are often accompanied by poor vision and implementation approaches, insufficient planning and coordination and are rarely linked to business strategies".

Next, some clear overlaps between master data management and information security management are observed.

5.3 Overlaps of Master data management and information security management

As done for data governance and information security governance, now some observed connections and possible synergies between master data

management and information security management (as well as thus implicitly data quality) are presented as secondary data findings from literature.

Through literature study made, it seems there is already obvious overlap also between *master data management* and *information security management*. Some were already mentioned, nevertheless this chapter lists few secondary data findings from literature, which concretize the mentioned relation.

ISO/IEC 27000:2014's definition for information security is one anchor between information security management and master data management. ISO (2014) states that information security can be seen as: "preservation of confidentiality, integrity and availability of information". These are the classic C-I-A –properties of *information security* (Chapter 3.2), nevertheless these are at the same time also at the very core dimensions in *data quality* (Chapter 4.2), which is a key driver of MDM (Chapter 4.3). A clear overlap can be seen here between these three concepts.

Accountability of information is another anchor point. For example, if there are no clear responsibilities and a named individual to be responsible for a piece of information as an owner for that information, serious security risks will arise (von Solms & von Solms, 2004). Ownership is a shared target of both MDM and ISM, although most ISM -models only mention it, not providing concrete means to establish data ownership, whereas MDM does.

Last notion, however of significant relevance is that it is seen that neither ISM nor MDM for either compliancy monitoring and enforcement capabilities(von Solms & von Solms, 2004) nor data standards and processes definition should reside in IT operations. This promotes the need to find a home for these business operations, which both need clear identification of information assets to be managed and both need being governed as ongoing operations. It makes sense to consider, whether these two concepts of ISM and MDM should be

combined for synergy benefits and for removal of overlap to same operative and governing bodies?

Although some conclusions based on literature data findings were already made on presented concepts overlaps, the next sub-chapters summarize the topic.

5.4 Other possible synergies between the concepts – per author

Few additional remarks need to be made, which author deems significant for the topic. Remarks, which could enhance the connection between the concepts, remove redundancy and build efficiency as well as capability to execute successful organizational change management, something, which is of essence in any change.

First, all discussed governance establishments, MDM, ISM and data quality exercises are very difficult, due to their nature to address almost whole of the organization and presenting significant need for change. It is noted by Talburt & Williams (2014) that there is strong resistance from e.g. data owners for information quality programs and the "who" (i.e. people) need to be addressed, while they also state that skills in project and change management are seen essential for these exercises. The author cannot but agree, as he sees the mentioned themes of MDM, DQ, ISM, etc. are cross-organization scope exercises requiring a real paradigm shift. In similar "classic" exercises like ERP -deployments, which cross organizational boundaries it has been discovered that organizational change management is the single utmost theme project and program managers should focus on to obtaining success (Antikainen & Käkölä, 2010).

Second, within the topic of *information security risk management (ISRM)* Webb, Ahmad, Maybard & Shanks (2014) make a remark that efficient *ISRM* is extremely difficult to establish as a function as it requires thorough

identification of information asset (complete and accurate list of discrete information assets, vulnerabilities etc.), which is an expensive task in many organizations. As this task is similarly involved in any MDM/DQ establishment to certain degree and should be addressed in any ISM-exercise, the common goal could provide reasoning for joining resources.

Considering the mentioned difficulty of both getting the top management's commitment and establishing the capabilities of e.g. MDM and ISM, it should be considered – especially the in light of shown evidence between presented concepts, that should they be governed and even operatively executed as joint efforts as many of the targets of the concepts are the same? Could the shown overlap and even synergy out win more easily also the organizational change resistance, if run as joint-program. To the author it sounds resource wise. This question will be further investigated in empirical study.

5.5 Summary of overlaps of the concepts

Both the governance –dimension of information and security of it (*DG* and *ISG*) as well operational level frameworks and capabilities (*ISM* and *MDM*) were further investigated for both negative (e.g. double organization, lack of efficiency, conflict of interests) and positive overlaps (e.g. same goals). Through the details provided and already partly observed in previous chapters, it seems that the concepts are not that tightly separated as one could think. The overlaps, if used positively, could results in synergies, which can execute even very demanding change projects, even paradigm changes in an organization with shared goals and resources efficiently used. Some of these possibilities are extendable for example to information *security risk management (ISRM)* – a risk management centric view on information security, where identifying the information assets is deemed the utmost success factor and at the same time the most difficult tasks, where things usually fail (Webb, Atif, Maynard & Shanks, 2014).

In short, there is clear overlap between the concepts, it would make sense to harvest the overlaps in positive way and fusion them for capabilities not achievable, when the concepts operate on their separated silos. All this being foundation for Chapter 7. Before introducing the model this thesis is thriving to create, it is necessary to pay attention to last critical component of the model, *situation awareness* (SA), which is covered next.

6 SITUATION AWARENESS

The last concept to be presented prior to combining the seemingly (somewhat) detached earlier concepts is Situation awareness. In this chapter, situation awareness is presented through one well established model; there is no need to investigate multiple conceptual models and definitions. Next, some remarks of situation awareness are made in context of cybersecurity and mainly through raising remarks from Finland's Cyber Strategy concerning situation awareness as well as few general information security –related situation awareness findings. Last, an existing example of (limited) nation critical infrastructure SA capability, HAVARO, is presented.

6.1 Concept of situation awareness

Situation awareness (SA) is defined by the mother of the theory, Endsley (1995) as: "the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning and projection of their status in near future". The main reasoning for selecting SA for this study is that it is widely recognized scientific construct, as well as recognized at least as high level construct in for example Finland's Cyber Strategy (Secretariat of the Security Committee, 2013), which is in focus in next sub-chapter. It can be also understood via process thinking, as a chain of actions(Webb et al., 2014) – an approach which is highly compatible with the other parts of the study's fusion of concepts.

Endsley's model (FIGURE 7) is presented as whole SA –"process" with factors of systems and individuals affecting the ability to utilize the SA. For the scope of the study the progressive stages (perception-comprehension-projection) in Endsley's model as well as the mentioned factors are not investigated. Scoping is limited to offering "State of the environment" (highlighted in red in FIGURE 7) for both organization's roles responsible over data quality and data management processes as well as for operators in national cyber

command & control –function. How they perceive the state with all connected factors is a matter of a whole completely new study. Nevertheless, explanation of key elements and "process" of the Endsley's model needs to be done.

The model depicts the whole of the process, how SA is achieved in steps (Endsley, 1995):

1) Level 1 is, where actor builds a *perception* of the environments different elements and e.g. their status and dynamics (as model concerns time and space), from which the actor moves to
2) Level 2, where the actor does comparison of actor's own "mental models" which have been built over time (e.g. knowledge on similar situations with some recognizable features, which unite them with the one compared) – i.e. actors own understanding of the perceived state. The actor has achieve *comprehension*, from which the actor moves to
3) Level 3, where the actor becomes aware of the perceived information's meaning and significance to the goals and objectives. At this last SA-"stage" the actor can predict (*projection*), what will probably happen next through actor's understanding of causality.

If the actor does not fail at any of the levels, the actor has achieved the SA and has the basis available for informed *decision making* and execute *action* and thus provide *feedback* (e.g. possibly change the environment) to the state of the environment. The task/systems factors as well as individual factors influence the SA building, nevertheless they are always context-tied and thus become meaningful on a specific situation. Examples of system/task factors could be complexity of the system used for SA building, UI design of it, level of visualization, the task load presented by the system. On the Individual factors examples could be a person's experience, the expectations the person has, how well the person is trained for the SA buildup and systems enabling it as well as his own concepts of set goals and objectives.

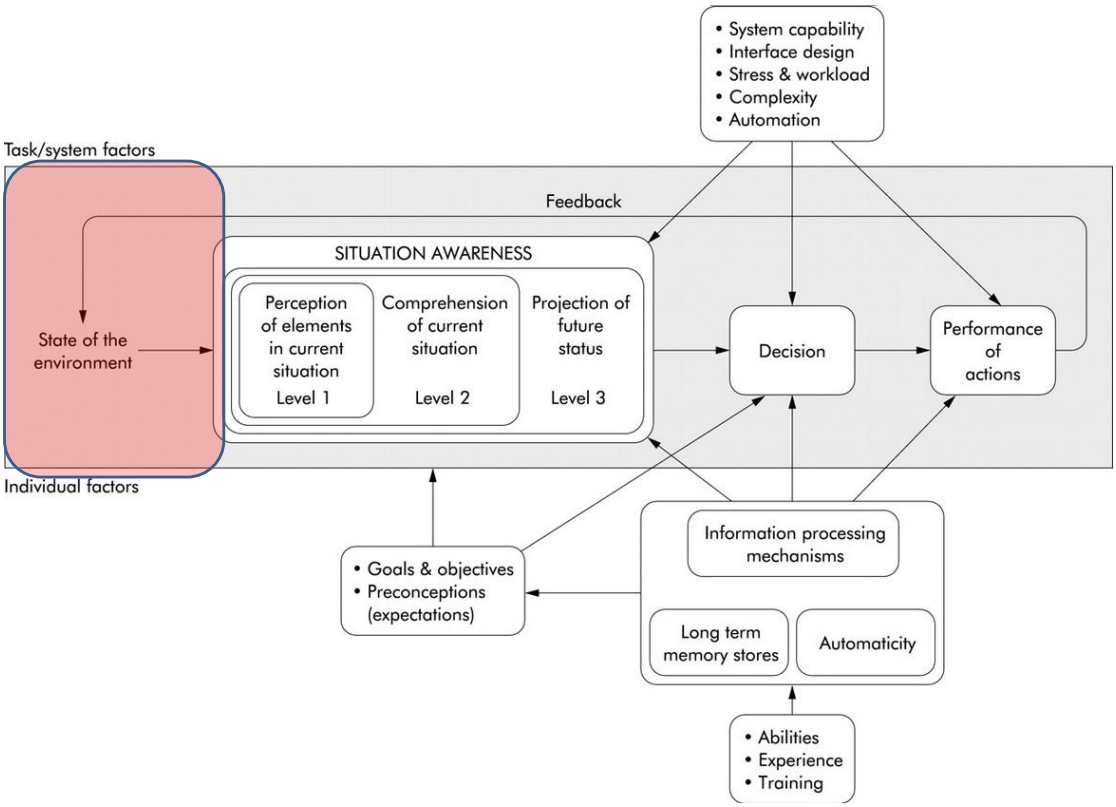


FIGURE 7. Endsley's (1995, p. 35) SA model

As the fundamentals and purpose of SA (build understanding of the existing situation and be able to predict its continuums in various scenarios so that informed decision can be made and acted upon) is presented, it is worth examining, how SA relates to Finland's Cyber strategy. SA is mentioned in several countries' cyber strategies e.g. Australia, USA, France, Estonia, Germany, Canada and the UK (Franke & Brynielsson, 2014). Considering its visibility in national strategies, it is logical to be used as an anchoring point.

6.2 Situation awareness as part of Finland's Cyber strategy

For building more context and relevance for the study made, the author is situating the research question 1's (Q1) model (Chapter 7) into Finland's current cybersecurity situation and its future development activities. Primary data is gathered through the interviews, however to limit the scope of the theme interview, it is relevant to highlight some findings from Finland's Cyber security Strategy as secondary data, which builds justification for the theme interview questions asked and also connects the construct of situation awareness into national cyber security context.

Finland published its Cyber Security Strategy early 2013 and the execution of targets set by strategy are ongoing during writing of this thesis. The status is elaborated via the interviews results presentation in Chapter 9.5. Finland sees that cyber threats are on a dramatically increasing trend and nation's cyber resiliency is in need of enhancement, especially for scope of *critical infrastructure*, which is defined as "[…]structures and functions indispensable for the vital functions of society. They comprise physical facilities and structures as well as electronic functions and services". Further *critical information infrastructure*, which can be seen as a "tool" for enabling critical infrastructure services is: "[…] the structures and functions behind the information systems of the vital functions of society which electronically transmit, transfer, receive, store or otherwise process information (data)". The empirical part relies on these definitions, when validating that interviewer and interviewee are discussing the conceptually same topic. (Secretariat of the Security Committee, 2013).

USA's presidential Executive Order 13636 (via (National Institute of Standards and Technology (NIST), 2014)) from February 2013 somewhat more integrates the physical word and the digital one by referring to cybersecurity as: "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a

debilitating impact on security, national economic security, national public health or safety, or any combination of those matters". The scope, meaning and "spirit" of the definitions are very close to each other .

Finland's vision for cyber security ("*desired end state in which the cyber domain is reliable and in which its functioning is ensured*"). Finland's Cyber Strategy process is part of the holistic Security Strategy for Society, where vital functions (seven in number) of society are identified as per illustrated in FIGURE 8. This figure also states Finland's vision for cyber security, on which Finland sees itself as possessing excellent changes to be in the vanguard of cyber security. (Secretariat of the Security Committee, 2013)

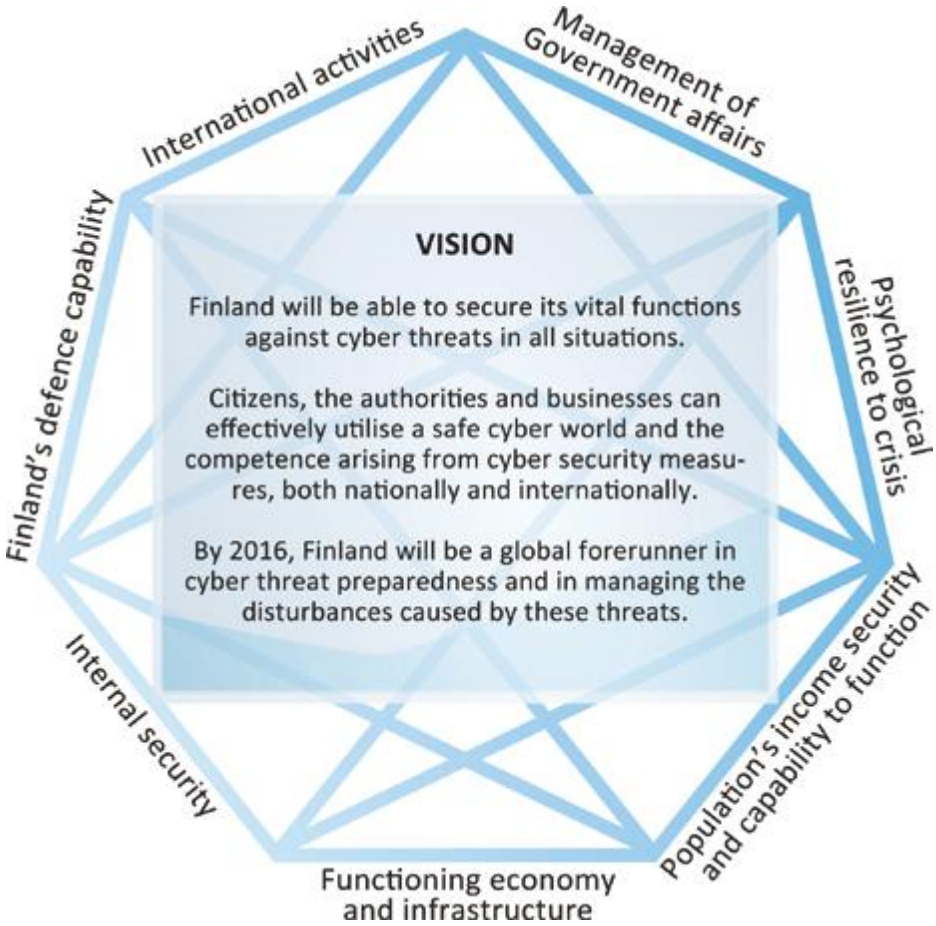


FIGURE 8. Finland's(Secretariat of the Security Committee, 2013, p. 3) Vision for cyber security

Finland does see few key themes (SA and *information sharing*, later also relevant for scope of the study), in which situation awareness seems to play a major role for realizing the vision set in the strategy. The strategy's management part (Secretariat of the Security Committee, 2013) states: "Cyber security management and disturbance management require that the Government and different actors have a reliable, real-time cyber security situation picture of the condition of society's vital functions as well as disturbances which affect their functioning". The principles of the strategy further highlight the importance of shared situation awareness, which is partly enabled by efficient information collection, analysis and gathering system, something that both require establishment of *Cyber Security Center*.

Noteworthy quotes from the strategic guidelines are(Secretariat of the Security Committee, 2013):

- *The strategic guidelines of the Cyber Security Strategy are advanced by intensifying active collaboration between actors whose aim is to achieve a shared situation awareness and effective defence against the threats.*
- *Cyber defence will be advanced by promoting the exchange of information and regulations as well as through cooperation between the authorities and the business community.*
- *[…] improve the situation awareness of different actors by furnishing them with real-time, shared and analysed information regarding vulnerabilities, disturbances and their effects.*
- *The Government situation centre must have a reliable, comprehensive and real-time total assessment of the cyber security situation at its disposal. The assessment encompasses the combined situation picture compiled by the Cyber Security Centre[…]*

The quotes were picked from the very first two principles (out of ten), in which situation awareness (and information sharing to establish SA).

In the background dossier of the strategy, several picks are worth underlining to set the importance of SA for Finland's Cyber security strategy (Secretariat of the Security Committee, 2013):

- *Strategic sensitivity entails the capability to rapidly compile a situation picture and establish situation awareness. The commitment of the leadership requires integrated situation awareness, coordinated and networked management and the optimisation of collective benefits.*
- *As the vulnerability of society increases it is necessary to be able to rapidly start managing sudden disturbances in the cyber domain, aka cyber incidents* (implicitly requiring slow latency situation awareness over critical services).
- On the responsibilities of the (now established) Cyber Security Centre*: The most important service of the Cyber Security Centre is to compile, maintain and distribute the cyber security situation picture to those who need it. The compilation of the situation picture requires the ability to collect and analyse relevant information and to meet the information requirements of different actors. The integrated situation picture, compiled by the Cyber Security Centre and its support network, comprises a technical situation picture and an evaluation of the total consequences of the cyber security violations to the vital functions of society.*

In the light of the presented direct quotes from the cyber strategy, it is noted that situation awareness seems as key enabler for the strategy to reach its vision and it is also the main responsibility of the operative cyber security – the Cyber Security Centre. Also to be noted is that efficient and across actors' borders realized real time information sharing further enables capability to provide the timely and valuable situation picture (awareness). The latter is supported e.g. by Choo on the topic of cyber threat landscape and its future challenges and research directions. Choo (2011) makes a strong remark that information-sharing mechanisms for secure, timely and actionable cyber-threat information between actors both on private and public sector must exist. Although the author but agrees, it is worth noting that idealism hardly ever meets reality and one major challenge to overcome is the "trust question". This is well noted by Webb et al. (2014) on context of SA for security risk management by stating that one of the key challenges will be intelligence acquisition from other necessary stakeholders (beyond own institution's borders) as it would require profound trust relationship between the actors.

How could SA then manifest itself in the context of a single organization or its supply and value chain – that is briefly described next.

6.3 Information security's situation awareness in context of single critical infrastructure services provider

As summarized in sub-chapter 3.6, cyber security is for individual organization's preparedness means and actions mostly classical ISM. Nevertheless, individual organizations should note their role in e.g. supply chains, especially, as production practices like *just in time (JIT)* have become very popular and e.g. material stocks are low and replenished only, when production planning is so instructing to be done. Hence, the organization should identify the possible risks to them on breakage of supply chain and the impact from them downstream the supply chain, should information breaches impact either critical services providing or even normal business operations essential to the organization. They should be aware of their business environment and possible threats to them or from them to other parties on prioritized basis – NIST Cybersecurity Framework recognizes this function as "Business Environment (ID.BE)" (2014), otherwise *single points of failures* are easily starting to exist in the chain.

Limited by the scope of the study, and the model to be created (Chapter 7), individual (especially critical infrastructure services provider) organization should have control over their information assets on prioritized basis. This means that information, which is critical to operations and continuity of the critical processes producing critical infrastructure services, should have special focus, data quality metering and information governance instantiated by business capability like MDM. Via DQ -monitoring and MDM data quality assurance, inclusive of anomaly detection (critical data does not comply to defined data standards and business rules or breaks data lifecycle rules), organization should be able to build a situation awareness and control over their critical information. Last, they should be able to share that information over organization borders ((Choo, 2011) & (NIST, 2014)) to function like Cyber Security Centre on real-time basis (Secretariat of the Security Committee, 2013).

Before closing the chapter, an existing instantiation of a system providing some SA visibility over (limited number of) Finnish critical infrastructure service providers cyber threat situation is presented.

6.4 HAVARO – and existing SA implementation

As it was many times highlighted in Finland's Cyber Security Strategy and noted as Cyber Security Center's primary responsibility, building SA over Finnish critical infrastructure services providers' cyber-status is essential (Chapter 6.2). Steps towards those target capabilities have been taken. There exists a service provided in joint operation with Cyber Security Center and The National Emergency Supply Agency (NESA). It needs introduction, as the model created (Chapter 7) and HAVARO present possibilities where they could complement each other for extended SA over cybersecurity status at critical infrastructure organizations. Named after "detect"(HAVaitse) and "alarm"(vAROita), HAVARO is an *intrusion detection system (IDS)* operating at the network perimeter of observed organization, analyzing (selected subset) of inbound and outbound traffic and detecting patterns and anomalies in traffic further informing Cyber Security Center's operations on detections ((Lagus, 2013) & (NESA, 2014)).

There is very little public information available about HAVARO, however according to National Emergency Security Center's Manager Christian Fjäder (NESA, 2014) there is no corresponding system available on the open markets and that HAVARO does have constantly added new threat profiles, some public, some exchanged as international cooperation between governmental functions. Fjäder (NESA, 2014) reveals that some 20 organizations (private sector) involved in national emergency supply –network have HAVARO coverage and intention is to double that during 2014; also, there is representation from all seven sectors of the emergency supply network in the mentioned 20 organizations.

One of those organizations is Fingrid Oyj, the enterprise responsible for functioning of the nation-wide high-voltage grid, the backbone of electricity transmission. Fingrid's CIO Kari Suominen states in an interview of Yle – news, a national news agency, that they have had few "red alerts" via HAVARO -system; the worst case being a malware penetrating perimeters and starting sending user IDs/rights outbound from the company. Compromising of the system was detected by HAVARO and the infected computer was identified during resolution. In those cases the separated networks, in which automation systems controlling the power grid reside, were not compromised. Still, Suominen states that it is not a question, if an advanced threat especially targeted at Fingrid will emerge, it is more a question of when it will happen - preparations need to be made.(Yle News, 2014)

Closing the theme of situation awareness, a summary is presented next.

6.5 Summary on situation awareness

A widely adopted theory for situation awareness was presented, which is will prove out to be a crucial component of the model created in Chapter 7. It was noted that many G20 countries in the world have raised situation awareness as one of the key themes they see their cybersecurity capabilities developing through. Finland is not an exception in that sense. SA is strongly promoted in Finland's Cyber Security Strategy and highlighted as no1. capability to focus on.

But SA is not just for national orchestrators to get benefit from. SA is very relevant for single companies also, especially, as trends are suggesting that information security breaches are on a rise and the threats are getting more and more advanced. Hence, for the purposes of leveraging SA also in scope of single companies it was shortly studied with MDM and DQ to prototype

capability, which could establish controls over organization's key information assets and integrity of those.

Last, HAVARO, an intrusion detection system (IDS), which is offered for Finnish critical infrastructure private sector service providers by National Emergency Supply Agency, was introduced to the level that its public information exists on. HAVARO is a good step towards national SA build up, however it is limited in that sense as it cannot provide any visibility to the integrity and quality of the critical information of the organization providing critical services. Hence, the model created in next Chapter is in author's thinking deemed as something, which combined with e.g. HAVARO, could provide significant improvement to national SA over critical infrastructure service providers' operational status. As it is regulated for example in aviation, that incidents compromising security must be reported to authorities, thus does the author believe that will be the case for reporting information security threats of organizations to e.g. Cyber Security Command Center - perhaps in the near future already.

With the closure of SA, the author transports the attention to what this thesis is mostly about – the novel model challenged to be created by Research Question 1.

7 THE MODEL OF INTER-ORGANISATION INFORMATION ASSETS' INTEGRITY MONITORING FOR SITUATIONAL AWARENESS

This chapter combines the concepts presented to form a model of a *system of systems*, which enables separated organizational actors to establish control and monitoring over their critical information's quality (especially dimension of integrity), capability to process anomalies in critical information (master data) and report them real-time to any outside party, which needs situation awareness over multiple actors' critical information quality. The chapter introduces the general basic model and instantiates it later by placing it into context of cybersecurity and adding components' synergy benefits. Last, the model is presented in more formalized mode.

7.1 Purpose of the model

The sole purpose of the model is to present a solution to a perceived practical problem that although national critical infrastructure situation awareness is promoted as most important responsibility of Cyber Command Center and the Finland's Cyber Strategy promotes is important strategic objective, there seems to be shortage of solutions for building SA to (national) critical information assets state and attributes. At the same time, information is recognized as the important asset to be protected, be it information for critical infrastructure operators' capability to provide their core services. Situation might not be any better from single organization's point of view on their information assets (if even recognized as assets) quality.

This considered, a general model consisting from both practitioner as well as academia recognized concepts was put together to provide a solution via "standard components" to achieve something more than the sum of the parts.

The significance and potential of the model and the hypothetic capabilities it brings along, once operational, are tested on the empirical part. Although the basic model is context-agnostic, in the interviews of cyber strategists and tactical professionals, the model is presented as one instantiated into context of cybersecurity. In that presented context critical infrastructure service providers operate with a requirement of a situational awareness over their critical information's quality being needed by Cyber Command Center. Cyber C&C needs to build a national status of critical service providers' information integrity for purposes of detecting anomalies, which might be due to attacker compromising service providers' capability to deliver services via using stealth persistent threat targeting to degrade targets critical information – a attack type hard to detect via traditional security measures and even advanced IDS-tools like presented HAVARO.

7.2 Approach taken for the model development

For ease of implementation, author has selected (from his own knowledge base and literature study) well established concepts, which are combined to create a system, that on its own does not exist and which could prove out to be difficult to be built from the scratch.

Selected concepts and the synergies detected between them are integrated parts of the model and are used for realizing the proposed internal models for the organizations as well as for the capability to build SA for needing party(parties) outside monitored organizations.

As start of many design science research, this effort has also began with simplified conceptualization and representation of a problem to be solved for serving human purposes (Hevner, March, Park & Ram, 2004). The presented model does not comply with Design-Science Research guidelines, neither is it intending to, as thesis in Higher Polytechnic degree is targeted more to address very practical, even "hands on" results delivery, not needing to

comply with e.g. requirement of scientific rigor or use of established models and theories.

Concerning the mentioned, the approach taken in this thesis is far beyond scope of higher polytechnic thesis (with detectable scientific approach), however at the same time fulfilling the requirements of thesis with providing practical problem solving in form of a very relevant solution (e.g. the model built). On the other hand, the provided model, i.e. the solution is wider in scope than classic design science as in the model exists both implicit and explicit concepts (like joining ISM and MDM –efforts) for organizational deployment of the model, which usually are out of scope of information systems design science research as per Hevner et al. (2004). Possibilities of further developing the prototype model (and concept it represents) are discussed in Chapter 10.8.

7.3 The created generic basic model

As mentioned, the model is constructed based on concepts investigated (mostly detached from each other) in the literature part and findings from it. As the scope of the thesis is already immersive, the model is not examined into e.g. process level of each main component (like *data governance*) - only the fundamental conceptual basics are highlighted.

With the introduction of the very basic model FIGURE 9, it is seen that although the model has the elements and key responsibilities in place and as a conceptualization should fulfill the problem solution expectations, it shows much of the overlap on responsibilities of different "components (e.g. both information security governance and data governance are to identify (and later "prioritize") organization's information assets). In the following subchapter (7.4) an instantiated version of the model is presented, which realizes the positive overlaps of key components.

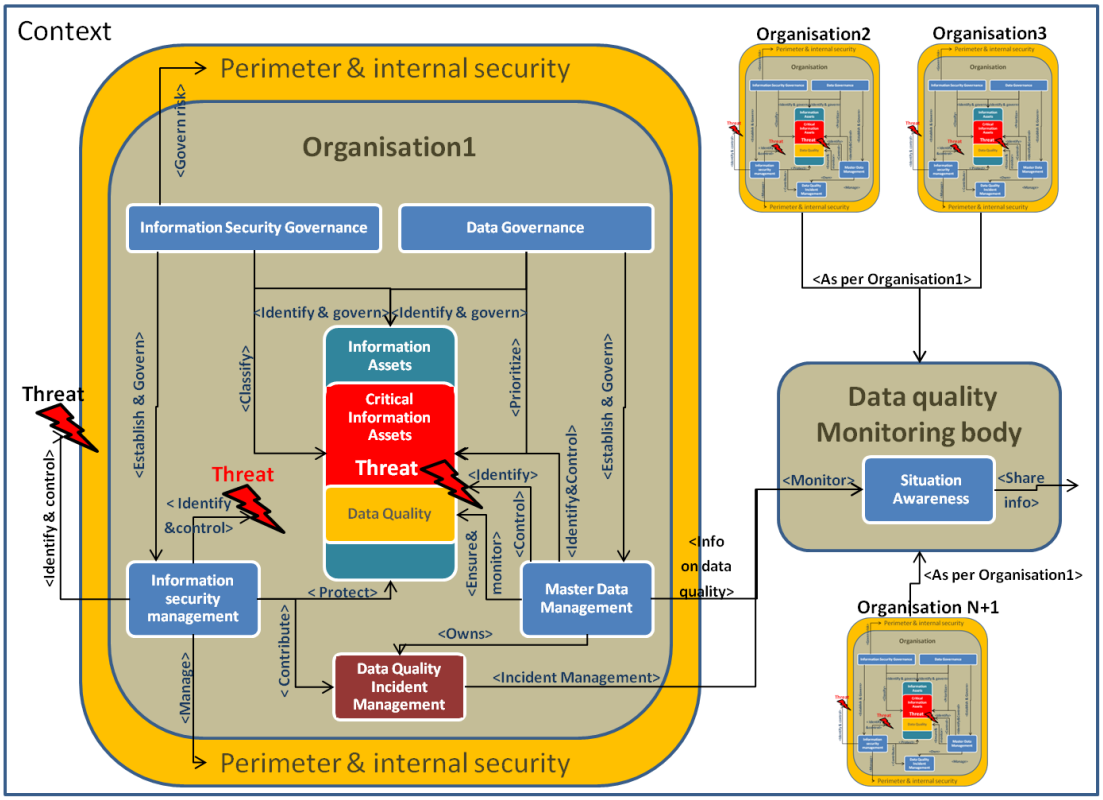


FIGURE 9. The very basic model with components, their dependencies and key responsibilities of the components in this study's scope

A short explanatory legend for the model (FIGURE 9):

- **Blue frame around elements is the context** for which the basic model is agnostic and hence the context should always be established
- **Orange rounded rectangle can be perceived as the same as the organization**. More, it represents the perimeters of the organization, e.g. the fiber optic connection to which organizations first router connects to. It is also inclusive of internal information security, e.g. classic malware, network traffic analysis, and also security of any technology or media
- **Grey/brown rounded rectangle is a "zoom in"** into one of the organizations in context's scope
- **Zoomed out organizations** are 1:1 with inspected Organization1
- **The main components** (concepts) investigated in earlier chapters **are the blue boxes**

- **Sea-blue "Information Assets"** represents all the information the organization has (non tacit / tacit)
- Red "Critical information assets" are in the model's case master data of the organization and other identified critical services production continuity data/information – the model highlights that critical information assets are only part of the inventory of information assets. At the same time they are the part, which needs most attention, control and quality metering
- **Yellow Data Quality** is the capability to define, meter and monitor the objective quality of the inspected data/information asset. In this model Data Quality is implemented by MDM-capability and deferred to it
- **Data Quality Incident Management** can be seen as capability or process owned by MDM-component, however due to its central role in the model's operation it is shown as a separate component
- **Arrows are representing responsibilities** of the components
- **Data quality monitoring body is the abstraction, which is interested to monitor inspected organizations' internal operations data quality** and possibly data quality incidents (e.g. DQ thresholds are broken or critical information asset has been compromised)
- **Red lightning are the outside or inside threats** addressing the Organization, be it directly targeting the critical information asset (which is the special scope of interest for DQ monitoring body), classic malware threat or stolen computer etc.

As the graphical presentation does not show time dimension and dependencies between components' operational capability, it needs to be elaborated further. The elaboration is explained only for the parts, which require the operational maturity to distribute critical information assets' *integrity data quality* (and optionally other data quality metrics status) to an outside party, which must be capable of receiving and processing the information.

The capability as scoped in previous paragraph is materialized through time-linear expectations (or build-process steps), which are:

For the organization:

1. Some form of ISG and DG must exist, if not they are to be established and policies formed
2. ISM and MDM are establishing (if not existing) by ISG and DG
3. ISM builds incident management process execution capability, which can operate for purposes of taking inputs of possible data quality deviations
4. MDM –function builds the following capabilities:
    a. Through identification of organization's information assets, the sub-set of it is scoped, which is designated as critical information asset through e.g. inspecting critical business processes, and the information those processes needs
    b. The critical information is defined organization wide for:
        i. technical data quality rules (form-fit (e.g. allowed values like, taxonomies etc.) and
        ii. business quality rules (logic how separated information elements relate to each other and should interact (e.g. if product must have a internal product owner role-person as owner of it (dependency between "person" and "product") and the person assigned resigns from the organization, a signal to designate new internal person with sufficient role qualifications is raised)
    c. Baseline Critical information data set is formed and set as "reference point" for trustable critical information to which other systems critical information is compared, ownership of parts of critical information is defined and responsible roles formed
    d. Quality metrics (e.g. completeness, accuracy, timeliness) are established and their thresholds and targets set

e. Change control (create, edit, delete) with segregation of duties – philosophy data management processes is forced to change manage critical information assets
    i. This includes both human parts of change control as well as..
    ii. …the technical system part, which must comply to critical information lifecycle management, e.g. rules on which systems can create/change/delete which critical information and…
    iii. …to which systems is the critical information supposed to be published to and with what logic (e.g. scope of data, timing rules)
    iv. Critical information lifecycle control must be able to detect breaches of earlier defined rules and take control of the critical information, which breach targets and further:
        1. Halt the distribution of the breached critical information further in the system landscape (stop the possible damage from escalating further)
        2. Raise an exception to DQ to handle the breach
f. Monitoring capability over system landscape of critical systems' information (those producing critical services and needing critical information) and its lifecycle is established – this monitors the rules set in "d."
    i. For internal purposes (e.g. ensuring good quality business, decision making and analytics data)
    ii. For external purposes of releasing data quality status to monitoring body (optional)
g. Exception handling process for "d."&"e." to raise the DQ-issue to further investigation process (Data quality incident management)

5. Combination of MDM and ISM –components form Data quality incident management process –capability (handling DQ-exceptions) to:
    a. Interpret, if the critical information create/change/delete-events or set other breach of set rules subject to exception handling is root caused to:
        i. Normal user or system error, i.e. "not intentional", in which case the critical information inspected is put to change management –process to correct it (business approval needed) – critical information assets' integrity is not compromised
        ii. "Intentional", which means security breach (someone or something is trying to degrade the critical information asset – critical information assets' integrity is compromised). The incident needs attention of risk management and it needs publishing to Data quality monitoring body
6. Capability to publish the critical information asset integrity compromise –event to Data quality monitoring body. For method and form the general basic model is agnostic – only requirement being the near "real time"/online information exchange.

<u>For the Data quality monitoring body</u> (capabilities can be built parallel to previous mentioned:

1. Establish capability to receive:
    a. Critical information assets' *integrity compromised* –event information from monitored organizations
    b. Continuous *data quality metrics* status information from monitored organizations (optional)
2. Situational awareness –continuous production process over monitored landscape, i.e. the organizations in scope of monitoring

3. Capability to share information further from SA to designated parties (e.g. warn other monitored organizations of escalating data integrity – compromising attack vectors)

With these capabilities established in designated components of the model, the continuous operation (cyclic process) of the model is enabled.

Few limitations to be mentioned:

- Presentation techniques available do have some shortcomings:
    - e.g. MDM and DG cannot be presented for their overlapping part, i.e. DG can establish (as it does in the model) operational capability MDM, which establishes data definitions, data controls and monitoring of DQ and on the other hand if there is no existing DG in place, MDM can be established on its own and it will implicitly be inclusive of DG for master data / critical information assets, though not having control over the rest of the assets (which holistic DG should consider)
- What is left of simplicity, for its sake:
    - the model is not e.g. making differentiation between information assets "inside" and "outside" of the organization. All information assets are considered to be subject to same capabilities of control.
    - In "later-to-be-developed" -version of the model there should be distinction between assets controllable and assets, which Organization has little or practically no control over (e.g. critical customer data in CRM cloud service provided by PartyX, hosted in country Y by party Z in premises <unknown> with implemented security measures of <not verifiable> or total lack of them).
- Basic model does not either consider e.g. supply chain of the organization and its data assets' DQ-status for organization of being

able to build SA over its whole supply chain. Neither does the advanced model next – this is left for future development also.

7.4 An advanced model instantiated in cybersecurity context

The basic model presented in previous sub-chapter is refined to highlight the synergies of the concepts/components from the literature study. At the same time, the model is instantiated into context of cybersecurity – the context, which is relevant for the scope of the empirical research part (Chapter 9).

Furthermore, the cybersecurity-context is scoped to "Cybersecurity of Finland" for the sake of being able to introduce "HAVARO" and naming the organizational components. A sample threat is presented to which the model presented is offering significant security.

Setting the context of cybersecurity affects the model by:

- Context is set to Cybersecurity in Finland
- Data quality monitoring body is Finland's "Cyber Security Command Center
- Organizations are named as existing examples of Finland's critical infrastructure organizations
    - NOTE: the instantiated model does not represent in any way the named organizations' execution capability of the model!
- "HAVARO" IDS is introduced into model, describing its different posture and capabilities to those of the capability presented by suggested critical information integrity SA.
    - At the same time, instantiation shows, how these two concepts (HAVARO IDS and Critical infrastructure service providers' critical information integrity SA complement each other for more holistic national SA for the Cyber Security Command

Center) – this is more described in summary of the theme, Chapter 7.6.

- Not a known feature of current Cyber Security Command Center's SA-capability, still for purposes of providing an example, the SA data for monitored organizations is visualized by simple traffic lights to give the reader an idea, what a simple SA -process could base on (perception of the environment) for critical information monitoring purposes.
    - *Green* – current critical information asset is not under incident management
    - *Yellow* - incident management is ongoing for critical information asset integrity breach or a breach is verified without assets being compromised
    - *Red* – verified critical information asset integrity compromised-event in effect

The components changes over basic model – providing more synergy - are:

- Governance of critical information assets (**Pink rounded rectangle**):
    - ISG and DG are united for overlapping parts (e.g. need to identify and govern Information assets
    - Governance synergy is also presented by shared Policy of Secure Data (combines the overlaps between Data policy and Information security policy)
- Management of critical information asset(**Light green rounded rectangle**):
    - MDM and ISM are combined to form Management of Secure Information to emphasize that ultimately both have responsibility over critical data (information) from different viewpoints, which are more efficiently, should the efforts be combined e.g.

- MDM includes security of data, roles and responsibilities – focus is more on people, process & data -lifecycle management, where security is often not understood thoroughly
- ISM is inclusive of data security, though often the assets to be protected are more systems, not the information. ISM often fails to target "what to protect" also and is not capable of providing decent data management processes.
- *Cyber Security Control Center* has responsibility over sharing SA on critical infrastructure service providers' information integrity status as per "traffic lights" (to prevent competition –sensitive legal issues, abstraction level is made high enough).

Example APT (Advanced Persistent Threat) -threat description materialized as an attack, which the instantiated model is subject to:

- Threat's attack capability is advanced and targeting specific organization (and its information assets)
- It is a persistent stealthy deception threat, where organization's (and its supply and value chain's) data - critical operational and tactical assets - is silently degraded over longer period of time
- It has a passive profile, i.e.
  - Threat does not present e.g. significant network traffic, which could be detected as a anomaly, it operates during business hours
  - It does not need to communicate to "outside" of the organization (thus e.g. HAVARO does not recognize it)
  - It masquerades itself as "normal user activity" possibly using valid credentials of an existing user
- Detection of the threat is difficult due to its silent nature and non-aggressive attack philosophy

- It degenerates the data via trying to maintain form-fit of the data, e.g. replacing delivery addresses with other "valid" addresses
- Possibly detected only via user reporting or slow general understanding that something is "wrong" as deliveries for example end up in many cases to wrong places
- Why especially dangerous: attacked organization (or organizations in a orchestrated large scale attack on critical infrastructure) involved possibly could not, with required certainty, reference the point in time, in which the attack started, making back up recovery and business continuity challenging tasks
    - This is due to they have no understanding of their (critical) information assets' "normal state", e.g. business validated master data
    - Even though the degraded data could be identified and fixed, the impact to victim organization could still prove out to be enormous as the operations done during effect of the attack (which could be weeks/months) need to be backtracked and effects risk managed

With the modifications and instantiating factors presented, the model is presented in FIGURE 10. The synergy-added model instantiated in cybersecurity-context in Finland.

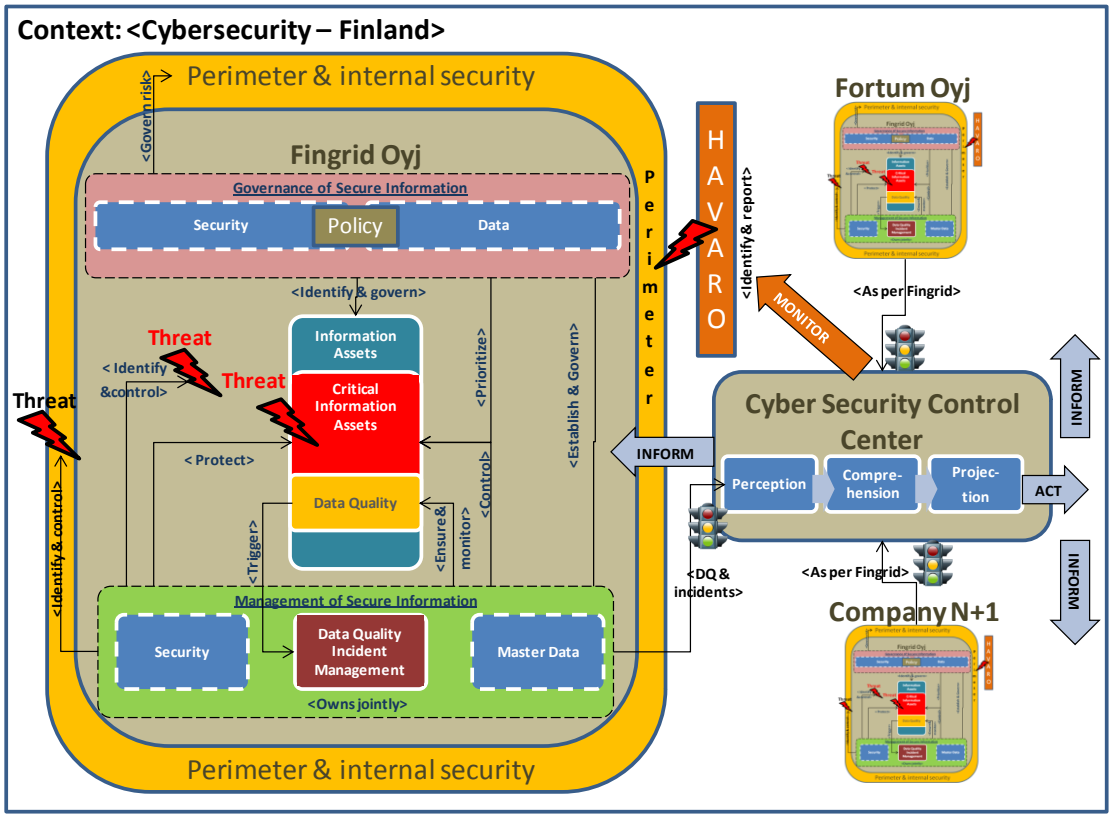


FIGURE 10. The synergy-added model instantiated in cybersecurity-context in Finland

Notions, why author deems the model efficient to handle the example threat:

- It provides early detection of attack (through rigorous critical information asset controls (change control, segregation of duties, lifecycle management)
- It prevents attack escalation in organization
- It understands business context and rules, which few, if any solutions do, thus detecting attack, which is degrading critical information by trying to maintain form-fit rules (data seems right, however it is actually misinformation)
- Online data quality monitoring with previous mentioned capabilities provides (if wished) instant "heads up" to Cyber Security Command Center)
- Via previous Cyber Security Command Center can update their SA fast and form holistic picture through the monitored organizations and

    - follow and analyze trends (like number of incidents, frequency of incidents, heat map of incidents in the environment etc) inform relevant parties, monitor threat in inspected landscape) based on which (SA) it can
    - decide on taking/not taking action (form of action not discussed)
- Classic IDSs struggle hard to detect threats like this due to its nature of not presenting "clear" anomalies. This is especially the case, if the organization has not defined its standard (form-fit-function) for data entities (like product, customer, location) and has no quality controlled baseline data – in such a case, detecting threat like this is of pure luck or through user reporting, in which case some damage has already taken place.

7.5 Putting it all together – a formalized presentation of the model

The model for enabling organizations' objective visibility over their critical information assets' state as quality indicators, at the same time building controls over critical information, leveraging the key participating components synergies and last being able to share the status information to an outside party, which can receive status information from multiple organizations and build situation awareness over them all has been presented.

The visualizations emphasizing the interactions and key responsibilities (in this study's scope) of the main components of the model was done in Chapter 7.3 and Chapter 7.4. The principles behind the model (e.g. utilizing existing resources and targets) and the key process involved, i.e. the capability to react on detected anomalies in data quality and assess those, are now put together. FIGURE 11. The formalized advanced model, represents this effort as a more formalized presentation layer.

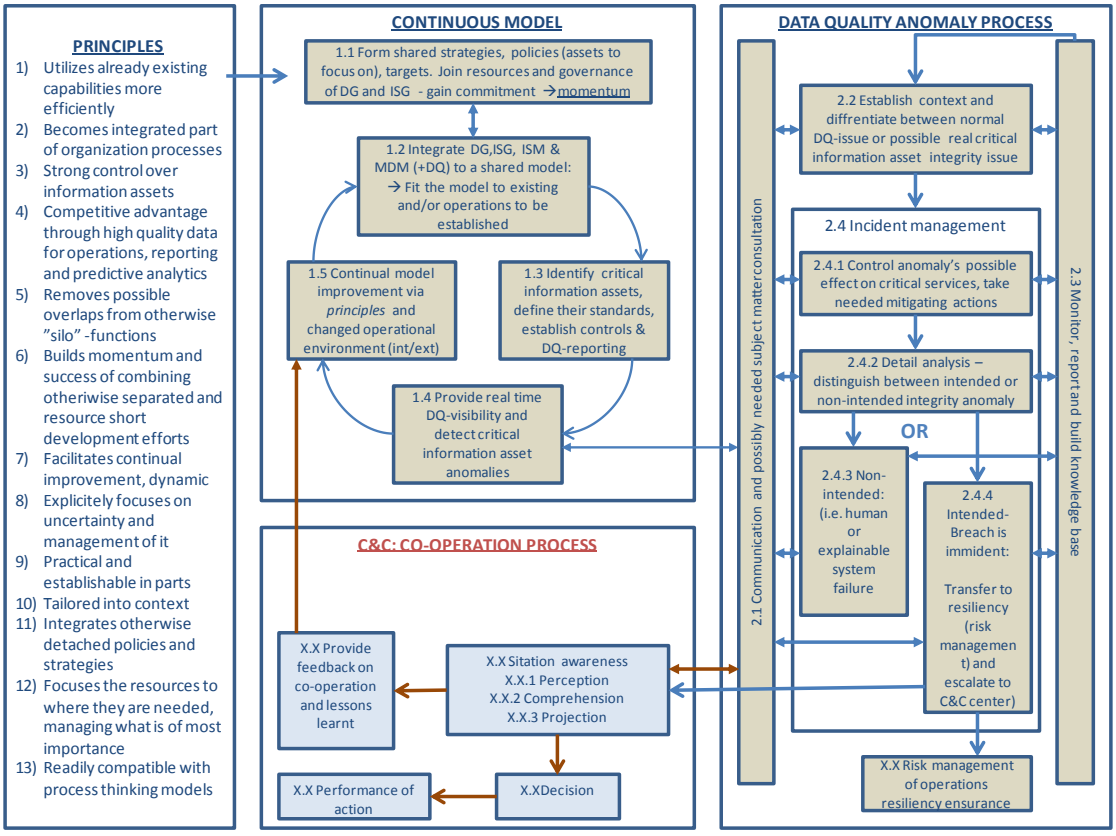


FIGURE 11. The formalized advanced model

A time-dimensioned conceptual model for it can be built by:

- Start from the *Principles* – these are the drivers behind the model, which are to build basis for gaining upper management (and board) attention and commitment (e.g. build the business case) for the model's implementation and use
- *Continuous model* describes the key processes to be executed to build the capability for continuous and ever-developing operative way of working.
- *Data quality anomaly process* is the key process in operative ways of working to handle any anomalies detected in critical information assets state, which could either indicate human error or possible threat targeting the assets and thus operative continuity
- *C&C Co-operation process* is an if-then –process, describing prototype processes of how outside party, monitoring the organization's data

quality, might react when organization's Data quality anomaly process messages them that the organization's critical information asset is compromised.

Further elaboration follows for the parts of the model.

7.5.1 Principles

The principles listed are few of the guidelines and organizational change management rationales, why the model presentenced is at the same time practical, leverages existing resources and (perhaps) already existing capabilities (like information security incident management –process). Principles describe the benefits (e.g. control over information assets) the organization gains from its implementation and promotes to align and join otherwise silo-operations (e.g. ISG and DG) for synergy-benefits of both efficiency. What is perhaps even more important is the ability to gather the needed change momentum for common targets' realization. Something those operations (e.g. ISG and DG) would otherwise (on their own) reach for without success.

7.5.2 Continuous model

This part of the model describes the build-up (or leveraging of existing capabilities and enhancing them) of the continuous operations needed for building up and maintaining solid control over critical information's change-processes as well as quality and any anomalies in those, which will in turn trigger the *data quality anomaly process*.

1.1 *Form shared strategies policies* […] is a sub-process in which the principles presented are addressed by management and decision to establish the operative model has been made. Its main target is to build synergies from leadership and efficiency perspective, e.g. join (part of) operations of

different governance structures (if separate for data governance and information security governance and/or risk management). Through (possible) reorganization the policies and sub-strategies of formerly separated functions are combined for those parts that gain synergy and/or are overlapping and thus sub-optimization.

1.2 *Integrate DG, MDM […]* sub-process is where the targets and organizational new models are deployed and start to work for targets set by the requirements of the model as a whole.

1.3 *Identify critical information[…]* sub-process is the first and foremost task of the newly (re-)organized operation. Understanding of the information asset held by the organization (directly or indirectly) is formed, master- and critical information is defined out of it and standardized, i.e. bought to standard meaning and form. The controls over different information assets are established, of which the critical ("master") information asset is rigorously change controlled, preferably via earlier defined segregation of duties-based data management process. As a key output of this challenging process phase is the standardized and business validated critical information asset, which is validated against DQ metrics like mentioned in Chapter 4.2. Once the baseline data quality is in place, process can proceed to "business as usual".

1.4 *Provide real time DQ-visibility[…]* Sub- process is the "everyday business" control process over data quality. It ensures that critical information is created and changed as per the defined rules and roles. The most important metrics, for the anomaly process are the mentioned *integrity* and *consistency,* which are there in place to detect, if any uncontrolled information change is taking place in the

system landscape as whole. Should it happen, exception handling process for data anomaly is initiated → 2.1. Otherwise the cyclic process continues on decided time interval or is triggered by C&C: Co-operation process or internal need, which transforms the control to 1.5.

1.5 *Continual model improvement[…]* sub-process is there to ensure that the controls and capability once established in 1.2 is kept up with changing business environment, e.g. new regulation, merger, de-merger or change of business model. This process receives input also from external Co-operation function, especially, if Anomaly process continuum proceeds to Co-operation process, which in turn will thrive to enhance the co-operation working practices through the experience gained from exception handling jointly executed. The circle closes to 1.2 and possible adjustments and for example new capabilities are brought into the model for iteration.

7.5.3 Data quality anomaly process

When 1.4 sub-process detects data anomalies, it initiates an exception handling process, border lined as *Data quality anomaly process*. The nature of this process is reactive and it receives the triggering input of DQ –anomaly and takes the responsibility to investigate its nature. Further, it will guide the process outcome to normal data management change processes or escalate it (in case of intended anomaly, e.g. cyber threat) to C&C Co-operation process-group and possibly e.g. organization's risk management function.

2.1 *Communication and possible SME consultation* sub-process is continuously involved in all the sub-processes of 2.x process group. The formalized and two-way verified Communication with clear roles is essential to involve the right people with right tasks to solve the anomaly. 2.1

receives communication from C&C Co-operation process execution also, i.e. across organization's "outer perimeters".

2.2 *Establish context and differentiate […]* sub-process is where the analysis of the anomaly's nature is investigated. It naturally involves setting priorities, resourcing accordingly etc., however the main responsibility of it is to distinguish, whether anomaly is due to e.g. failed reporting or clear system failure. Communication (2.1) and Monitoring and reporting (2.3) are involved to maintain clear picture of the process status (anomaly process can be understood as "internal SA" over DQ).

2.3 *Monitor, report and build[…]* sub-process is an integrated part of 2.2 through 2.4.x. Its responsibility is to provide monitoring over progress, report it to needing parties and build knowledge base so that next time similar cases are triggered, the whole of the exception process should have more knowledge and thus efficiency on how to react.

2.4 *Incident management* Sub- process further analyses the possible effect of the anomaly to critical services(2.4.1) and takes needed mitigation or continuity management activities as agreed. It then further analyses (2.4.2) the anomaly to form a strong opinion on the anomaly's nature of being intended (attack) or non-intended (internal process failure). At this stage the 2.4 –process is forked to 2.4.3, i.e. internal issue to be corrected (and escalated back to data management process e.g. 1.3), or if the nature is intentional, 2.4.4 is initiated. From 2.4.4 agreed parties are given control (e.g. risk management) and escalation to external C&C Co-operation process SA –process is triggered.

7.5.4 C&C: Co-operation model

C&C Co-operation process group is the Situation awareness process of the external data integrity monitoring party (e.g. Cyber Security Command Center) and its intention is to detect the trigger (e.g. changed information or new information received from 2.4.4), i.e. perceive it in context, comprehend it, form a projection for decision making and then make decision to either act or not act and in "act", perform the actions deemed needed. The process group is also responsible to communicate back to 2.1. and to provide feedback on overall process execution to 1.5, for possible Co-operation process improvement and knowledge sharing.

With closure of the model description and a note that the model and its processes are not intended to describe formal process input-output-role – model as it is a conceptual prototype and needs thus rigorous scientific improvement (e.g. usage of established incident management process-models) and empirical evidence and enhancement, author will close the Chapter in a form of a summary.

7.6 Summary of developed model

The presented model(s) draws from the knowledge base (both theoretical, as well as from industry best practices) combining those with author's systems thinking and wide cross-domains experience on information management, business development, information security management, data and information governance and intermediate skills in information security governance – all this combined with practical experience and academic research done on process development, deployment of IT-artifacts, and on understanding the relevance of organizational change management for any development endeavor's success.

The model identifies synergies with its components (Chapter 5) for purposes of more easily establishing the operational capabilities of holistic of the model.

As the model is process driven in nature, a prototype of more formal presentation of the model, with process –thinking dimension heavily involved, was provided in addition to the visualizations shown earlier. It is worth noting that by nature the key components of the model are greatly process –oriented, hence compatible with process thinking of the model.

In this chapter, it was also identified (as highlighted already in 6.5) that an IDS like HAVARO is practically helpless to those threats, which are happening inside the organization (even if HAVARO implemented to protect it), which execute on low profile, do not converse with outside world – instead it aims to degrade the critical information (advanced and targeted attack) of the organization slowly and undetected. With union of visibility to "what is happening outside" and that combined with the model's "what is happening inside to our most valuable information assets", a nation would have much covered. Added with the model's active participation in maintaining information quality and controlling changes to critical information, emerging threat would be detectable and their escalation stopped at the very starting point of the threat realization. This would provide a paradigm change of current reactive threat handling to proactive, where the threats can do little, if any damage – a sure asset for business and national continuity.

With this summary the theoretical part of the thesis is closed and focus moves to empiricism, as the concepts investigated and model produced are tested via interviews of cybersecurity veterans.

8 EMPIRICAL RESEARCH

This thesis has been based on the author's intuition that the research subject is relevant, up-to-date and the research is bringing value to both practice of science and industry practice. A strong convergence can be found in the research, as several domains and concepts (ISM, MDM, DG, ISG, DQ, SA) need to be knitted together to understand larger motivations and causes.

In the empirical part of the research these seemingly stand-alone concepts and constructs are merged together, their interconnections are investigated, differences in importance are identified, the model created tested and research questions are answered. The empirical part is based on the qualitative research method using the approach of semi-structured interview, theme interview. This Chapter will also elaborate the background of the empirical research, the methods used, introduce the interviewees and explain the data gathering process and analysis of the data.

8.1 Used research methodology and approach

A general guideline for empirical studies, suggested by Hirsjärvi and Hurme, is used for executing the research. It comprises of four main stages (Hirsjärvi & Hurme, 2008):

1) Defined research problem/question (select one with relevance for the community, not one which is just "easy" to cover);
2) Further study of the research problem/question, further refining it and looking into literature and existing research;
3) Collecting the data and analyzing it (observation, interview, databases, ...); and
4) Forming the conclusions and reporting the findings.

The research method used in the empirical part is qualitative and the approach was selected, as the target in the research is to consider also the past

of the interviewees, the evolution in their expertise, and their notions of the research phenomenon (Hirsjärvi & Hurme, 2008). Unlike often with quantitative research, there is no expectation set for clear causal relationships between the interview themes and questions, although many are identified in the research.

Interview, as the data gathering approach, was selected for several reasons, the first being that the subject of the research with its many dimensions and domains is so complex that trying to gather data via, for example, surveys would be very error prone and require a lot of elaboration in the questions, and most probably result in a very low response rate and mixed data. The second important reason is that there is a need to get further clarifications and "why so"s from the respondents and there is a need to deepen the received answers with opinions and free elaborations. The interview technique used can be categorized as half-structured interview, *theme interview* as per Hirsjärvi and Hurme (2008), which is based on *focused interview* presented by Merton, Fiske and Kendall. Most fundamentals of focused interview are well suited for this research as it provides the following characteristics (Merton, Fiske & Kendall, 1956, pp. 3-4):

- It is known in advance that the interviewees have experienced certain situation;
- The researcher has researched certain phenomenon's presumably important aspects, structures, processes and holistic nature;
- Based on the analysis, researcher has reached certain assumptions about the ruling factors of the researched situation and causes of it to ones experiencing it; and
- The interview is directed on the subjective views of the interviewees, those that the interviewer has earlier researched.

Most of the characteristics fit well into this research's design and purpose, although in this research, one similar "certain situation" (experimentally produced) does not exist. The situation (experiencing cybersecurity related

novel concept development via connecting existing constructs and models), although it could produce similar conceptual models from all interviewees, is still a situation, which varies a lot. Because of this "shortcoming" of a clinically correct focused interview, theme interview is chosen. Although very similar to focused interview, it still allows all the interviewees' experiences, thoughts, beliefs and feelings to be researched without an experimentally produced "certain situation" (Hirsjärvi & Hurme, 2008). This interview approach can also be recognized as "the general interview guide approach"(Hirsjärvi & Hurme, 2008).

8.2 Background of the respondents and the interviews

Five subject matter experts were selected for the theme interviews. Respondents were selected by the author recognizing their work history as very considerable in cybersecurity and/or information security management strategical and/or tactical development both in practice as in academia. The background details are kept to minimum as through them, it would be very easy to identify the responds, as the scene is small and professionals of this caliber are few. Some elaborative points on respondents' backgrounds are presented in Section 9.3. All of the respondents are active on the subject currently.

On the selection criteria, the author has also acknowledged personally that the selected persons have been very successful in their activities. This fact even further assured the author on the selection choices as he wanted to investigate, what "recognized names" value and see important in current and future cybersecurity scene. To summarize - all respondents have experience in endeavors very few of us have the opportunity to participate in.

Possible shortcomings of the selection criteria are explained in the following Section 8.3: Reliability of the selected interview approach. At this point, the author wants to recognize the fact that the interviewees are considerably

experienced, they are perceived as being successful, and their view on the subjects interviewed is broad and holistic. Therefore it is quite possible that selecting respondents with different criteria, e.g. “not experienced”, “not being successful” and “not contributing as holistic thinkers” would produce different data than the one presented in this study. This was acknowledged already at the very planning of this study and the selection criteria was formed already back then.

All respondents were asked for their permission and were given a very easy and discreet option to back off from the interview. Care was taken not to build any assumptions or expectations about the interview considering the topic of the study. The respondents were given general description of the interview; that it considered cybersecurity, information management and situation awareness. They were also told that they were selected based on their perceived experience on the subjects covered in the study. Even the title of the research was “kept secret” to ensure minimal bias on the answers. The respondents were told that the study does not compromise any laws and is kept strictly confidential and they are free to end the interview at any point, if they felt it being inappropriate. All the interviewees accepted the interview.

Three of the interviews were conducted via phone (for reasons of persons’ availability for a meeting was limited) and two on face-to-face –basis. The phone calls were recorded as were the in-person interviews. This was told to the respondents, and as the subject is somewhat delicate, interviewer explained the data analysis process as: interview is recorded on a factory-reseted cellular phone with no SIM-card or WLAN-connectivity. Interviews are processed on the same phone, interview files crypted and archived on the phone’s SD-memory card, which is removed and stored at secure place the interviewer only has access to. Memory card is physically destroyed, after author’s perception of adequate retention period of three years from thesis possible approval.

Where physical meeting was possible, the ambience for the interviews was selected as open and informal. The interviews were conducted in the respondents' work place or a restaurant, generally in places, which would not pose any feeling of a too formal ambience to keep the conversations easy and fluent. The interviews were carried out mostly in a very friendly and open atmosphere and in a very open-minded mindset. The interview meetings were started with casual chatting about "this and that" to take the edge off and to reduce any possible excitement of the interview situation itself. Average interview duration was 1 hour and 29 minutes – shortest being 58 minutes and longest 2 hours and 11 minutes.

To aid the verbal interview, author presented a thin slide deck, which had elaborations of the questions in forms of text and very simplified figure of the proposed prototype model. The slide deck is attached as APPENDIX I - Interview slides.

The author was left with impression that all the interviews were held in a open an honest spirit. It was also perceived that the interviewees did their best to be as precise as possible with their answers to provide maximum feedback. They also provided plenty of opinions and elaborations on their answers, which can be perceived as a sign that they were interested in the interview and thus probably provided their best possible answers. They showed their expertise with criticism and by enhancing the presented themes.

8.3 Reliability of the selected interview approach

Apart from the time consuming nature of interview approach, it is commonly recognized to have the shortcoming that the interview itself has the risk of possessing several error sources. These errors or faults can derive from the interviewer or the interviewees'. As an example, the reliability of the interview can be compromised by the interviewees' tendency to provide

socially "correct" answers and please the interviewer. (Hirsjärvi & Hurme, 2008).

Another possible reliability factor is the selection of interviewees. It is possible, although it has been consciously avoided by the author, that the author has selected such interviewees, which he recognizes as respondents favorable to his opinions and views and thus produce research data, which is favorable to the researcher.

The third possible shortcoming is the number of interviewees. How can the author say that an adequate number of people have been interviewed? The answer is: "He can't". There is no scientific nor commonly agreed minimum or maximum number of interviewees a theme interview should have (Hirsjärvi & Hurme, 2008). As the interviewees all are unique in nature, there is always a clear possibility that saturation of answers (i.e. answers from further interviewees would not probably produce new data) has not been reached, although the author is quite confident that the key findings are already presented in the answers of the interviewed people. Of the five interviewees all shared opinions on the critical research questions. The author deems this as a relevant finding in the study. A fact, which would not be altered by 10+ more interviews, even if the 10+ next interviews would produce different results. The findings still remain significant. The author concludes that the accuracy for the purposes of this research is adequate and the data gathering committed is of good scientific rigor when considering the availability of the author's resources. Still, the possibility for undiscovered, fruitful data is recognized as a possible shortcoming.

The fourth possible hindrance for the reliability is the experience of the interviewer with interviewed persons. Although the author has executed several interviews (formal and informal) during his professional career, he is not a professional interviewer. Hence it is possible that the author has missed one or several new aspects to the researched topic when interviewing the

respondents. One possible outcome of this would be too early and incorrect notion of reaching saturation and not interviewing further interviewees.

Lastly, four of the interviewees and the interviewer were acquainted, although only by one or two meetings or phone calls, to each other, which is not commonly favored (neither forbidden) in interview guidelines (Hirsjärvi & Hurme, 2008). For the purposes of this research, as it compromises between several areas of expertise and requires acknowledged high experience in information- and cybersecurity, the possibility, within the resources of the author, was to identify the interviewees from his personal network to ensure an adequate level of expertise and know-how from the respondents.

8.4 Summary on research approach

The selected empirical research approach was presented and justification for the selection elaborated. Interview and especially theme interview was seen as the research method to collect the primary data from the presented respondents. The main reasons for the interview was that the concepts investigated are very complex in nature and the possibility for misunderstanding without effective dialog is high. Also, it was needed to get elaborations and discussion on the themes from the respondents, not statistical data.

9 INTERVIEW STUDY ANALYSIS

This Chapter will continue from Chapter 8, where the settings and background of the research approach and interviewees were elaborated. The analysis of the primary data collection (interviews) is presented with most of the themes and questions already reduction processed and initial findings provided (interpreted via meaning).

The data collected is thematized and coded and this thematization and classification of data is first explained. Later the identified themes are covered one by one, each in its own subsection with relevant coded entities attached to the theme.

At the conclusion Section of each theme the author will provide his personal synthesis and key conclusions on the theme. This is to reflect the findings to his own extensive information-, master data management, business development and information technology knowledge added to authors (subjective, naturally) perception of possessing at least adequate information security knowledge – all this will further enhance the reliability of this research. The author will also, when needed, ground the findings back to the theoretical part of the thesis, i.e. the literature study of Chapters 2 through 6. A further concluding analysis is provided in Chapter 10: Conclusions, limitations and future research.

9.1 Analysis approach

The initial analysis of the data collected has already taken place at the interviews. The interviewer made remarks of relevant entries and summarized some of his interpretations to the interviewees, who then commented, whether the summary and interpretation was what they meant or corrected the interpretation. The approach could be classified as “self corrective interview” (Hirsjärvi & Hurme, 2008).

Apart from the initial analysis started during the interviews, the analysis was executed after the collected primary data was decomposed**.** The author proceeded immediately after the primary data decomposition to the analysis of it, trusting his intuition. Only part of the primary data (circa 35%) was transcribed, and some of classifications and interpretations were made from the recordings directly and analyzed and reported.

The reasoning practiced during the analysis phase can be considered as inductive reasoning. A considerable amount of interpretation of meaning has been applied and is always speculative in nature. This being especially the case, as the author had a personal view to the research subject and he is interpreting the data from this personal angle (Hirsjärvi & Hurme, 2008).

9.2 Identified themes, classification and coding of data

Although the approach utilized is that of a semi-structured theme interview, the author had quite a clear classification, or sub-themes, identified in his interview frame. The findings are classified under these identified sub-themes in the analysis. The used classification/sub-themes can be summarized as follows – to an extent they follow the general structure of the research's literature structure:

- Experience of the respondent in (cyber) security or information security
- Cyber?
- Cybersecurity 2014-2015 and Finland's capability to answer to cyber threats on critical infrastructure
- Information security management
- Information management and data quality
- Situation awareness and the relevance of the created model of critical information asset integrity-information sharing

A certain order of presenting the sub-themes is also applied. In the interviews the general idea was to first get the respondents own free definition of each item (e.g. "cybersecurity", "information security management") and then cross check those against the perceptions made in literature study. Then, only after this alignment, the most relevant questions concerning this research were posed. The order of themes getting discussed in the interviews corresponds to the order of the theme Sections following.

Data coding varies from a sub-theme to another and is question/area specific. The used coding is elaborated with each usage. Generally, no numeric scale is used. However, if the importance of phenomenon is investigated and coding can describe the views of the respondents with reasonable certainty - decipherable in comparable terms - then comparison is done (e.g. "*not important, somewhat important, important, and very important*").

9.3 Theme: experience of the respondent in (cyber) security or information security

To understand the answers later provided by the respondents, it was important to first get background information on the respondent. It was also important to validate the respondents' background as *subject matter experts (later SME)* on the researched topic. From the theme several classifications were produced:

- Experience in presented topic;
- Focus of experience
- Experience divided as either a practitioner or academia member

9.3.1 Experience in presented topics

A coding **experience in presented topics** was established to understand how many years they registered had been working (practice or academic) on the presented topic. All respondents registered a average of 15 years of (cyber)

security, ISM or information management experience. This means that they had been involved in work assignments where security or security of information management has been a central part of their work profiles.

9.3.2 Focus of experience

It was relevant to investigate the respondents' work and academic history to further validate the interviewees fit for the research. This was enquired by investigating on which broad category the respondent belonged, when investigating through classic dimensions of operations – strategic, tactical & operations. It was coded as **focus of experience**. As the concepts presented required mostly strategic and tactical thinking (relevance of the presented model to national cyber security), it was essential to check needed strategic and tactical know-how was included.

Three of the respondents can be perceived as belonging mostly to the strategic –class, one as a mix of strategic-tactical and one as mix of tactical-operational. For the purposes of validation of the respondent group's relevance, this was very assuring finding.

A further distinction was made, if the respondents were more on technology-know-how or managing and development-know how. This was coded as a binary **Technology focused**, in which three of the responded were perceived "no" (SME1, SME3 & SME4), one "yes" (SME5) and one mix between yes/no (SME2), which author later perceived as no, resulting in four non-technology-focused and one technology-focused respondent. The one technology-focused respondent was a good contrast to the strategists and provided a different perspective to the topic.

9.3.3 Experience divided as either a practitioner or academia member

For ensuring that respondents had enough practitioner experience on the topics a coding of **Academic or practitioner** was created with a rough

classification of “practitioner”, “academic” and “both”. None of the respondent belonged to academic per se. Four of them classified as “both” and one as “practitioner”. For the purposes of the interview this was encouraging.

9.3.4 Summary of theme’s findings

The target of the theme was to investigate, whether the respondents’ experience and background can be considered adequate for the purposes of the research. The author is convinced that the respondents have solid experience for providing *subject matter expert* opinions and views to the researched subject with their considerable involvement in high-profile security and cybersecurity strategic and tactical exercises. That, added with one respondent bringing in views of a more technical and operations –based role is strong base for expecting interesting results delivered.

9.4 Theme: Cyber?

The foundation of this theme was to explore the respondents’ own conceptual models and definitions for cybersecurity, cyber defence and information security for purposes of validating that what was found in literature study either correlated with the interview’s concepts or were totally different. Following classification is used:

- Cybersecurity defined
- Difference of cybersecurity and cyber defence
- Difference of cybersecurity and information security
- Cybersecurity in scope of single organization

9.4.1 Cybersecurity defined

Before posing the respondents any clues what the interviewer had defined for cybersecurity, their own definition was asked, which has the classification of

cybersecurity defined. The author was satisfied with the answers, because they were tuned in enough conceptually with the author's own conceptual model and those found in literature (although no commonly agreed definition exist to this date). Hence, it was reasonable to proceed with the interviews.

SME1 saw cybersecurity through the effect is can have:

> *"It affects all the sectors of the society, those witch need to be also involved in it […] cybersecurity is a holistic concept with five dimensions political, technical, military's involvement […] and the person or citizen must be seen in the picture[…] and the economical layer"*

SME2 also highlighted the effect factor:

> *"Were talking about large-scale things, like the effect the (mis)information has on this physical world...like how this cyber environment, which consist of these information systems, and people that use those is safe and trustable, but how it guides things like trains and electric are controlled that this environment is safe – so, were not talking like information systems' reliability but the whole of the things. Central is how the cyber assets are focused on to what, like that they should be put to functions which are critical […], people being the most important and that core information assets are secured. Information is the thing, not systems."*

SME3 saw it as a state of trust:

> *"It is about citizens, businesses, and public sector operators – about their possibility to operate in the network and its digital services with a feeling of trust and that they are not themselves cause for troubles. From the national perspective, there is a feeling of safety involved"*

SME4 saw it as an enabler:

> *"For me cybersecurity is much along the official [Finnish Cyber Security Strategy], where citizens, officials and business can do their things effectively and safely… but, it is also something like whole of the information systems, a structure of those, which impacts the society as a whole"*

SME5 put it very shortly as a holistic phenomenon:

> *"Something affecting everyone of us - a state of mind, which is not technical alone and it cannot be black and white told, when it is good or bad."*

9.4.2 Difference of cybersecurity and cyber defence

To investigate how the respondents differentiated the concepts of *cybersecurity* and that of *cyber defence*, a question was asked to make a difference between these two – provided one existed. This was relevant to study as cybersecurity and cyber defence seem to mix up somewhat as was noted in literature study in Section 2.1.

An open ended question, classification of **difference of cybersecurity and cyber defence** is investigated with coding *conceptually the same* & *differ significantly.* None of the respondents' elaborated can be perceived as *conceptually the same*. All of them considered the concept different enough to code the answers as 5/5 *differ significantly*.

SME1 highlights the difference with:

> *"Cybersecurity is the big picture, where cyber defence is a part of it only […] cyber defence is more of a military issue, although borders are not that clear."*

SME3 recognized the difference yielding from authorities perspective :

> *"Cybersecurity is other officials, like the police.. the operations police and other security officials, which are to ensure that the cyber environment has nothing criminal going on, be it hackers, terrorists.., while cyber defence is part of cyber warfare involving armed forces utilizing cyber capabilities as part of armed operations […] so, it is about the line between these, but the border is not clear and neither responsibilities are all agreed yet."*

SME4 sees cyber defence as military action and CS as the rest what is left:

> *"Cyber defence is something belonging to armed forces and is part of its statutory responsibilities. Cybersecurity is then all the other problems too, which are happening in the cyber environment."*

SME5's interpretation is also along the line drawn between civil and military:

"Something involving and affecting us all, where as cyber defence is military force's stuff."

9.4.3 Difference of cybersecurity and information security management

Once the difference of cybersecurity and cyber defence was investigated, it was interesting to know whether the SME's felt cybersecurity strongly corresponding to information security management. Classification of **difference of cybersecurity and information security management** is presented, which is studied through the viewpoints presented by the SMEs

SME 1 draws the line:

"Cybersecurity is holistic, information security management is in smaller context, so the context is the variator"

SME3 is on similar thoughts with:

"Cybersecurity is a larger concept, while information security is about elements of information and the C-I-A of those, so it's about information whereas cybersecurity is also about physical networks, physical environment and add human cognitive understanding and trust towards operation of the cyber environment – hence, it's abit more than information security"

SME5 takes a view that cyber security crosses the lines of information being processed:

"Difference is cyber can relate to much more, where information is not used"

9.4.4 Cybersecurity in scope of single organization

As the interviewees' opinions on terms was investigated, it was interesting to hear , if they see previous sub-themes differently, when looked from the perspective of a single organization (e.g. corporate or educational institute). Possible difference from instantiated viewpoint of single organization was

studied by asking whether the respondents felt that *information security management* was actually the same as *cybersecurity*, if one had the goggles of e.g. information security manager, risk manager or CEO of a corporate/institution on, through which they would perceive the theme.

This classifies as **cybersecurity in scope of single organization** and is coded with *in practice the same, mostly the same & differ significantly*. Results as per coding used are in TABLE 5.

TABLE 5 . Cybersecurity materializing as ISM in single organization

Respondent	*Answer*
SME1	*in practice the same*
SME2	*in practice the same*
SME3	*in practice the same*
SME4	*in practice the same*
SME5	*in practice the same*

SME1 commented on the *in practice the same* with:

> "*Cyber and information security [*management*]are in practice the same things, when looking from the operational point of view. The difference is that cybersecurity must concern, what information security management does not, that if there are holes in information security, there might be implications and effects cyber domain[…] so cyber must consider the risks of connected things, the causality[…]".*

SME2 summarized that cyber is something present in the big picture:

> "*Yes, I'd pretty much sign that they are the same. As the cyber-aspect is brought into picture it comes present only in the totality and society's scope and on the scope of a single actor it is more on securing critical systems"*

SME3 differentiates between different sorts of companies, nevertheless stating that:

"It depends on the company, but in many cases it is the same, especially, if one is not high information-intensive IT company with lots of IPRs and so on"

SME4:

"Depends naturally on the company or organization, if it's a company offering connectivity for critical infra companies, then it is cybersecurity, but if the same company provides network cable to my summer house, then it's not – so depends on the context. More it is anyways the classic ISM, but it can become cyber, if all the small companies in Finland are affected by it."

SME5:

"Much the same thing. And physical security should also be connected here [mentions cases, where physical premises have been breached in otherwise strong information security places and monitoring software installed in server rooms]."

9.4.5 Summary of theme

It was found out that all the respondents shared compatible enough understanding of what "cyber"-related concepts were about and could build context for them, when needed. As it was found out in literature study, there exists no clear and agreed definition for cybersecurity and author found that quite confusing and actually a hindrance for future development of cybersecurity study. A clear definition is needed so that e.g. corporate can distinguish, whether to decide, if "cybersecurity"-related news, events, ways of working etc. were supposed to affect their organization or not. From the interviews, a good rule of thumb for telling apart *cybersecurity* and *information security management,* is by the impact and effect the possible threat has or can have.

On the differentiation of cybersecurity, once investigated it from single organization's point of view, with information security (management) - there is mostly no practical variance. This messages that although "cyber" has been here for some time already, the terms are not rooted enough and cause

misunderstanding and perhaps even waste of resources on activities/information processing, which is irrelevant for the observing party. Although it would be easy to blame scandal and hype-driven reporters, it is ultimately for academia and educated practitioners to "remove the noise" and by educating the public, make a distinction between *cybersecurity* and *information security management* of a single actor.

Findings do support the literature study findings that cybersecurity and information security could and in some cases even should be considered the same in single organization's case. Benefit of doing so, is realized by not confusing the organization with phenomenon, which is hard to understand, instead to handle it through normalized terms and frameworks. Things are not this black and white, naturally, and the organization must understand its place in possible value and supply chains, which can have society-wide effects, if impaired.

On the personal record of the author the findings are in line with personal conceptual models. The author has been even a bit annoyed of the scandal-driven reporting and providing public with a clear bias-of-availability added with perhaps not so relevant threat scenarios of uncontrolled cyber-wars and so on. It is true that the "cyber-era" is still trying to settle itself in and the wisest prophet on this scene is the one that admits having no visibility to the future. Nevertheless, author strongly promotes the education need identified and encourages companies and institutions, especially, when they are not part of critical national services, to best prepare for cybersecurity by first identifying the assets they need most protecting and then utilizing already well-working information security frameworks – to start with.

9.5 Theme: Cybersecurity 2014-2015 and Finland's capability to answer to cyber threats on critical infrastructure

This theme is about getting the latest trends from SMEs riding the highest waves in *cybersecurity*. Viewpoints on 1) what have been current year's cybersecurity hot topics for Finland, 2) what might the focus be in 2015 and last - definitely not the least: 3) how do the SMEs perceive Finland's capability to answer to cyber threats, when narrowing the scope of function to those of critical infrastructure service providers (CISP). Further still asking the SMEs for their subjective view on 4) CISPs capability to maintain their technical defence perimeters. Hence the classifications are:

- Top cybersecurity challenges in Finland year 2014
- Possible hot topics for 2015
- Finland's capability of answering to cyber threats on critical infrastructure scope
- Critical infrastructure operators' capability to maintain their perimeters?

9.5.1 Top cybersecurity challenges in Finland year 2014

The interviewees were asked to identify, if they had some in mind, the most discussed or otherwise worth noting cybersecurity challenges of 2014 in Finland. Similar classification was formed. i.e. **top cybersecurity challenges in Finland year 2014**. This classification has no coding, instead open comments are presented.

SME1 remembered the year back with:

> *"Sure things to remember have been the state administration's vulnerabilities in public […] plus then this risk assessment, which we still have lots to do in. Also, this year has shown well the effects of information warfare, where this cyber is present – as Russia is it information warfare and other cyber warfare[…*with these*] 2014 will be remembered in the history as the year, which will change our long run security thinking plus European security*

political architectures[…] although not much of this is yet discussed in the public"

SME2 elaborated the topic with:

"We more and more awaken to the fact that these threats are real and they can have significant consequences and this has brought the topic more onto agenda".

SME3 does also highlight the incident with the department of state:

"Incident with the Department of State and the espionage happening there, which shows that somewhere the control over the environment is not working as it should. From which we can naturally start big questions that how much we should be interfering…"

SME4 is on practical implementation actions:

"What are the practices we must take, when something go wrong, how to detect something being wrong and further how to pinpoint the partners who should be informed, SA over problems."

SME5 does also bring in the department of state –case and does see the positive side of the incident getting publicity:

"Perhaps the biggest thing has been the case of department of state's attack, which has opened eyes and especially the thing that it has most probably been there for some time. In that sense it is good that these are brought to public, so we can better prepare for these in the future – there has been this [paradigm] that one has not been able to say what the threat is, if one has not been able to name the threat. This does not necessarily mean that there are more threats happening, but that the ability of detecting threats has improved-"

9.5.2 Possible hot topics for 2015

Having formed a view on status of the current year and its cyber –topics, it was interesting to hear, what SME's saw as rising future trends for 2015 or otherwise noteworthy scenarios, which might emerge. Classification was presented: **possible hot topics for 2015**.

SME2 predicted that the challenges will be on really getting things done and showing results out of cyber strategy:

> *"Challenge will be to see how we are driving these things forward on national level. Cyber operation plan, which came one year after the strategy, which I see as very bad thing – it has lots of things listed and those have been categorized to logical packets… but… one cannot still see how the different functions will contribute to some designated target state […] there is no coordination between functions […] it still seems that we are trying, on the national level, define what this cybersecurity really is about on the concrete".*

SME3 is pondering the balance between enough control and that of too much control – an Orwellian perspective:

> *"There will probably be discussion on how much we can control and how we can control that the information that should stay within this country stays here, … so more talk will be on the situation awareness and how to improve that. Third aspect might be the confidentiality of citizens' personal information and how to ensure it stays where it should"*

SME4 is promoting that the role of intelligence operations will be discussed

> *"It's the same as 2014 with more emphasis being put to it. Possible very Finnish-culture-thingie will be discussion on what is the role of intelligence operations in the cyber security context and how national cyber security can be improved via efficient intelligence."*

9.5.3 Finland's capability of answering to cyber threats on critical infrastructure scope

To grasp something really precious, i.e. topnotch SMEs' -hopefully unfiltered- view on national capability to answer to current and near future cyber threats on critical infrastructure, a direct question: "What is Finland's capability to answer to cyber threats on scope of critical infrastructure service providers" was asked and coding formed from the question: **Finland's capability of answering to cyber threats on critical infrastructure scope**.

A question like this can to a decent degree be coded, and thus a coding of *poor, decent, good* was provided, although the stress is on the comments themselves. Coded answers are presented in

TABLE 6.

TABLE 6. Finland's capability of reacting to cyber threats

Respondent	*Answer*
SME1	*decent*
SME2	*decent*
SME3	*good*
SME4	*good*
SME5	*decent*

SME1 noted on the capability through capability to recover and how it should be it should be enhanced:

> *"[…] capability to predict, prevent and recover – this is what it is much about that the time to recover has be seen at large as surprisingly long, that companies target of cyber attacks … we've been talking months of recovery time, which is far too long for business and it even more far too long time for critical functions in the society. So, that the time can be shortened we must focus on prediction and prevention […] much of this comes down to situation awareness".*

SME2 saw that single operators are on almost a good level, however understanding the dependencies and chains of reaction is something needing improvement:

> *"Basic level is pretty good for critical functions, but there is much to improve and develop on that the value chain is scattered and longer that… well… like who owns what activity or is responsible of the operational security of it, is kind of blurring. I'd say it's pretty scattered now and then we come to this shared situation picture and awareness and I think there is no such thing at the moment, and I do not see it as a technical problem but it all comes down to sharing understanding and definition of master information and operations and their criticality".*

SME3 estimates the capability as "not bad". Still he identifies that we have much of history's burden still to carry with us:

> *"I don't know this topic so I' could tell that here things are ok and here they are not, but with a finger in the air, I'd say that the situation is not bad. As it is everywhere the situation with automation in industry and critical infrastructure is perhaps not any better that it anywhere else – there is lots of legacy still left and we are living a stage in evolution, where there are the new systems designed to answer to cyber threats and then old systems, which are not."*

SME4 seems that critical operations will withstand:

> *"I think we can maintain supply network Finland yes, but if major aggressive cyber activity is taking place, then I think we'll lose some of the well-being-Finland for sure… lot's of "ifs" here, but it's still far from optimal, anyways."*

SME5 brings in the fact that there are no metrics yet to tell the capabilities apart:

> *"Well, there are many factors involved here, which should be taken into consideration as unlike analog world, cyber environment loses meaning of time and space, so that we can be attacked by the best in the world, not just that is the "neighbor", in which case we should be able to define how good the best of the world is and in that sense I'd not say we are at very good level."*

9.5.4 Critical infrastructure operators' capability to maintain their perimeters?

The author asked the respondents for their opinion on how well they felt Finnish critical infrastructure service providers are able to maintain their technical perimeters in context of information technology security (i.e. not physical premises) or had the battle for "absolute defence" already been lost.

This is classified as: **critical infrastructure operators' capability to maintain their perimeters.** Coding presented is simple *poor, adequate, good* –scale, although the perspectives themselves are of interest as is also the "tone" or "dramatics" of the answer as they convey much information too. Coded entries follow in TABLE 7.

TABLE 7. CISPs' capability to maintain IT perimeters

Respondent	*Answer*
SME1	*adequate*
SME2	*poor*
SME3	*adequate*
SME4	*adequate*
SME5	N/A

SME1 saw the capability established at decent level, nevertheless commented that:

> *"They will be coming through that is for sure, there is no such thing as absolute security […] There are weak links in the chain, but then again, those are the links anyone planning to paralyze Finland are looking for."*

SME2 observed a rat race - the defender is always on the losing side:

> *"No, I'd claim that as some BYOD, Dropbox or something is closed out, something new will soon pop up, it's a rat race and I'd not be certain at all that it is worth investing, at least on a longer run. It's better to just raise your hands in the air with trying to be 99% protected and focus on the information, which matters the most. It at the same time means an ongoing capability to define, which information at which point is the critical one".*

SME3 brings in the Finnish nature of character not being perhaps best fitted to harsh realities of cyber threats and is realistic about absolute defences:

> *"I cannot say for even close to sure… I guess there are operators through the whole spectrum, but my hunch is… little pessimistic on this perhaps. Just that is it some Finnish national trait to believe in goodness of the world and then wake up as things happen, which should have not happened. And fact is that bomber always gets through, means we cannot build such a defence, which would not be penetrated. Attack will get through, it is more on continuity management, resilience and risk management – these are parts of company's safety policy"*

SME4 is on similar lines of thought:

> *"Can't think anymore as something absolute… something will come through that is for sure, so thinking should start from there that there will be things happening inside and prepare for those."*

SME5 seems the topic multifaceted and highlights that although new threats are immune to defences of 90's they still prove their place, e.g. firewalls are needed:

> *"Several things here, first that this security is in that sense an interesting phenomenon that we have to drag along all the things from the 90's although new stuff is constantly flowing in. Like there is discussion that new malware is on the rise which these [*90's stuff*] have no effect on –still a firewall is a good network hygiene product … we can increase the [*attack*] cost with all of these* [perimeter defence tools] *and have an effect that attacker needs to spend more time and resources … to make it as difficult as possible … so the co-operation of these* [old tools and new tools] *is essential, not single tools per se."*

9.5.5 Summary of theme

In this theme the current landscape and topics of discussion about cyber-scene were first interviewed and possible future trends identified. This was done for a reason of general interest and also to build insight into topics at the very surface, if situation awareness or other this researches topics would appear. Actually, interesting items popped up, especially the case with department of state, where a persistent threat had compromised information for a long time at the very core of national operations. Although not a good thing in general, it still brought implicitly more value for the proposed model, which is targeting to identify this sort of "planned longer time presence" – threat at the very early stage. In general, the threats getting publicity have been also as eye openers for more attention to prevent future threats doing similar damage. Interesting note was that although (in later Chapter) operational plan execution is seen as producing results, it was noted here, as it will be noted later that a different view of not really observing any results from the strategy prevails too. A sure sign for the operative plan execution group to facilitate more communication and awareness building.

From the interviews coding on Finland's capability to answer to cyber threats in critical infrastructure the insight and feeling (there are no meters, though) is

that the general capability is between decent and good. Emphasis was put on accepting that attacks will come through and accepting that, to invest into fast recovery from the treats, which is asking for more rigorous risk management and business continuity management in general. A clear problem, which is emphasized many times later is that the control of supply chains is not at adequate level, which is something a serious harm meaner will be sure to exploit.

In literature part it was brought to attention several times that absolute defence is impossible. This was nevertheless enquired from the respondents. The coded answers of "adequate minus" tells that although there is trust in the operation of the critical infrastructure network continuity, it sure is not based on trust of their perimeter defences capability to keep threats out. In fact it was again brought to attention that chain has weaknesses, which will be exploited, if not filled. Also, assurance for the literature part was presented with notions that the complexity is raising at such rate with BYOD, cloud services etc that is virtually impossible to maintain decent perimeter defence. This signals that the resilience must come from something else than perimeters. Some hint was already given about risk management and business continuity management, which might prove out worth more emphasis.

9.6 Theme: Information security Management

Of the main concepts the created model in Chapter 7 consist, the next one studied and to which SMEs views are concepts close to information security management. Indication on how *ISM* and *cybersecurity* differ and on what parts they are the same, was discussed in Chapter 9.4.3. This theme investigates ISM further with gaining more insight into the concept.

Of interest is to have insight into on how efficient organizations in practice are in conducting ISM, does the information security policy(-ies) play significant part and last, where should the operational management of information

security and the governance of it reside organizationally for best results and lack of conflicts of interest.

The following main classifications were identified and will be covered next:

- The term Information Security Management
- Organizational location of ISG/ISM
- Relevance of information security policies
- Organizational location of ISG/ISM for most efficiency

9.6.1 The term Information Security Management

Few definitions and characteristics for ISM were researched in literature study to form a concept to be used in model-building purposes (Chapter 7) and also to compare the definitions/characteristics of literature with those of the practitioners' – how similar would they prove out to be?

The classification for this is **definition of Information Security Management**. It does not have coding as such, however similarities are identified from SME-comments and quotes provided for showing the alignment and/or lack of it.

SME1 seems things through processes:

> *"Information security... --- …I see it as a process, like that it is made from securing the information, securing the process, it involves educating people and then that there is this technical side to it. It will not turn into flesh, if the significance is not understood at the top of the company – much more must be put effort onto this"*.

While SME2 is underlining classic C-I-A –approach:

> *"Oh. Heheheh! Pretty much the CIA model, especially the availability… and sure integrity is important as well as confidentiality"*

SME3 perceives also the security management by a state to be achieved:

> *"I'd again throw in the feeling of safety here, that I trust the systems being safe like some online banking system, i.e. I trust it and thus consider things safe"*

SME4 was a bit taken by surprise and had to align his thoughts:

> *"Well, is it not information integrity, confidentiality, usability – these things, right? I'm thinking … … … that it could be the system level things too, or is it the information; have to think a bit about this."*

SME5 presented a rather interesting and anti-dogmatic view:

> *"Well, doh – it's the security of the information. I've not in my own work been thinking too much of information security [*tietoturva in Finnish*], as we only have one word where in English there is security and safety and in that sense, when thinking about critical infrastructure, like energy plant, then safety is of utmost importance there as it means that people will die if it fails and information security can play a smaller role there."*

9.6.2 Organizations' capability for efficient information security management

In short, this classification of: **organizations' capability for efficient information security management** drills into subjective views of the interviewees on how well they felt ISM practices are practiced in CISP – organizations. Coding of *poor, decent, good N/A* is used and coding results presented in TABLE 8.

TABLE 8. Capabilities for efficient ISM

Respondent	*Rating*
SME1	*decent*
SME2	*poor*
SME3	N/A
SME4	N/A
SME5	*decent*

SME1 seems the maturity varying a lot and challenges not as technical ones:

> *"Difficult question… there are good and bad examples, but I think we are heading the right direction here. Challenges are more on governance, not technical, this is seen too much as an technology issue, but ignorance is one important driving the society…"*

As well as does SME2: :

> *"On the paper, it works well, but in practice there is much disparity between information security management's and that of top management's as well as even functions expectations and views. I see it very much as low efficiency and the thing is the perspective differences of operations and those of information security management".*

SME5 notes that in theory education is there - still action is not yet realized:

> *"The principles are quite well understood, but the problem is they do not materialize from the slideware."*

9.6.3 Relevance of information security policies

A certain understanding can be already formed from the earlier chapters' comments on ISM's role. However it is worth investigating, how much on SME's opinion do policies have effect on the capability to deliver ISM. Classification for this is: **relevance of information security policies**, and coding of *low, medium, high & N/A* is used, while results follow in TABLE 9.

TABLE 9. Relevance of IS policies

Respondent	*Rating*
SME1	*N/A*
SME2	*medium*
SME3	*high*
SME4	*medium*
SME5	N/A

SME2 seems that much more commitment is needed from management:

> *"Improvement is seen and ownership has gotten more attention, but still it should be more CEO signed paper, which she communicates and shows management's commitment and form a target state… but then the ball drop to the floor* [and if someone picks it]*that there should be management of the policy more and this varies a lot"*

SME3 states the policy as the very fundamental needed:

> *"The existence of the policy is whole basis for efficient ISM, but it requires that it is a living document and tied closely to practical activities of everyday business, not just a paper or declaration, but a process and which unites the different layers of the organization. This is essential to do to get the different operations like ICT and management to talk to each other and see common goals."*

SME4 uses general reasoning and brings it into context:

> *"I'm not from this scene, but I feel that if there are commonly agreed practices and targets with policies, where the process owners, IT, risk and continuity management are involved, then things will work. If information security is done from only one perspective, then it gets worse."*

SME5 calls out for practical approach and something everyone can utilize:

> *"Depends on the policies established, like there can be those of 80 or 180 pages with very detail information in them, but they do not necessarily flow through the organization. They must be and good precise and fit to the business where they are used in. Further they must be such that one does not need 20 years of security experience to execute them – so, understandable and actionable"*

9.6.4 Organizational location of ISG/ISM

Last on the ISM-theme, as it was found out in literature study, there are indications that information security and governance are not perhaps always best placed in organization for them to be efficient and ISM and ISG can even compete on different targets, e.g. ISG and ISM were not good to be seen in for

example CIO-office as ISG should be able to audit compliance etc. and no organization should be made possible to audit its own operations.

A classification of: **organizational location of ISG/ISM for efficiency maximization** is made and is presented with no coding, instead open comments are seen more relevant.

SME1 has a view that:

> "[Long pause] *one cannot just see that it place in somewhere, but it must be able to affect the processes of the organization, where it matter. Risk management and risk analyses… that is where we are not yet good at … that exactly should be the tool for the upper management, from which understanding is drawn from. Without question, we are to ICT-centric on this one.*

SME2 seems this needing to happen as close to the operations as possible:

> *"It is essential that these activities link close to the operations, which they are supposed to support. So, data ownership could come reality and the dialog real. I see data ownership here as most important thing – A and O – and also the greatest shortcoming and if that would be ok, then* [ISM] *could dramatically improve. Information integrity, information security and ownership of these must be part of the process so we can tell, if the process is secure and trustable or not".*

SME3 is thinking possible paradigm change as new possibilities:

> *"Hmm… a thought rises that could they be organized somehow different than they now are, i.e. usually in the IT. IT being considered as a support function and this is the essence of the problem as it will, through being in IT just like that to top management – support function and operative business processes are more of interest and importance. […] The cyber officer in the company should understand the business and that it is more than just about email working[…] A good topic for further study for someone to find a model, which would work well here. Anyways, the security personnel like this should reside as close to the top management as possible, possibly as part of the executive board and then the dialogue would work"*

SME4 seems supporting function (IT) as not the best possible location:

> *"Well, everything should be upper management's business like this, but they are short on time. It might be good to reside in risk management. Definitely not good to be in IT as if the CIO is put to save money and he tells the security guy to save on security, he'll probably will do so, but if it's in the risk management, then they can come and say that you guys are breaking the jointly agreed rules, this will not do – these risks you are taking are unbearable."*

SME5 experiences the subject as very context sensitive:

> *"There is no one sure location, because it depends so much on how the company operates. It should still have much of linking to what the upper management is doing, consider the size of the company, e.g. large companies could need more mandate and approvals."*

9.6.5 Summary of theme

Information security management was investigated to better understand the findings behind the main research questions and to be able to answer to RQ3. It turned out that respondents had very different conceptual models of information security (management). One saw it as a state of mind (trust), some classic CIA- views were presented with emphasis on integrity (which is promising finding for the model) and it was also observed from perspective of human safety, which was an interesting (and valid) viewpoint – actually worth further investigation as a perception angle to safe information.

Quite dramatic coding results were received for CISP-organizations' capability for efficient ISM. There the verdict is (with three answers, which could be coded) a "decent minus", which indicates this should be put more attention in both research and practice. One reason was observed as lack of management commitment and seeing ISM as technical exercise, which it is not. The notion was twice made that general knowledge exists, it's a problem of commitment and governance.

The mentioned is getting support when the importance of shared and agreed security policies were investigated. They were seen as important and the same

need for management support was encountered again. So, the policies must exist, they are seen as fundamental – however, they are in many cases just paper without action and sometimes made not fit-for-purpose. Some of the reasons, which might explain this and the previous problem could be due to how ISM is organized.

Where ISM/ISG should reside in the organization gave no clear "department". Nevertheless a good indication was detected on what might be the problem. From the interviews it seems that IT is not the place for ISM/ISG to reside, it is in these cases left with little attention and could even provoke conflict of interests of the organizations' security interests and those of CIOs need to reduce costs. It was also suggested that ownership should either be in e.g. risk management, or then the ownership should be tightly integrated to processes. Data ownership was seen important and it was suggested that processes could even own the data as well as the security of it and the risks associated and their management.

Findings also indicate that it would be valid to understand ISM as a continuous process (just like described in Model creation in Chapter 7) and several highlights combining all the three – ISM efficiency, policies and organizational position of ISM/ISG indicate that IT is not the best possible place and that management support is more than crucial. Findings, which further underline the synergy-indications earlier in the study between ISM-MDM, ISG-DG.

The author's personal views are much in alignment with the findings and thus, once again, more enforce the hypothesis that the author had, once he planned to conduct this study. Hence executing this research has educated the author much more and put words to meanings, which earlier did not have solid concepts, and names for the concepts the models already existed.

Justification of this theme lies also in the fact that the findings are very relevant for possible further study and development of the created model (Chapter 7). The possibilities of this are discussed more in Chapter 10.8.

9.7 Theme: Information management and data quality

As information as an asset and its quality have been very central themes and the fundamental basis for the model created in Chapter 7 , it was more than necessary to get interviewees' conceptual models opened up on management of information and their concept of good quality data.

Further it was worth investigating CISP's capability to both identify their whole of the information assets and locate the information in system landscape, their ability to tell apart the critical part of the information asset and reactivity of the data quality-approach of the CISPs. Last, SME's were inquired about how important they saw information quality as component of CISPs' ability to operate in crisis situations.

The classification of the theme is divided as:

- Information quality conceptualized
- CISPs ability to name their information assets, locate them and further segment critical assets
- CISPs information quality management approach – reactive/proactive
- Importance of information quality for CISP to operate in crisis situations
- SME's view on relevance of named information ownership

9.7.1 Information quality conceptualized

Classification is **information quality conceptualized** and it investigates the SMEs' concept of what information quality meant for them, e.g. how they

would describe operation-, decision making- and analysis information of good quality. This is best described just with open comments.

SME1 does not go into defining what it really means, instead he just describes good quality information through short and to the point comment:

> *"Information's quality is defined by its[information's] usability .*

SME2 sees DQ through criticality :

> *"Well, what is the information needed to perform a function and those owning those functions should be able to tell how they weight what is important for them [*respondent refers to C-I-A, i.e. function owners should define the risk with each "dimension" that they are willing to accept] *That information owner also must be better to define what, like integrity, is important – they should be able to do that better than they do it today".*

SME3 underlines the availability of information:

> *"Availability is closely linked to quality – timely, so it for the right moment for decision making, meaning it is relevant and that is enough in volume."*

SME4 seems quality as something, which has processed the raw data:

> *"Good quality information.. hmmm…. Trash or noise has been removed from the data and it's thus material one can build upon, be it person of software."*

SME5 observes many views on the matter and he highlights relevancy:

> *"Again, many dimensions here […] it must be valid and up-todate so that I know that it is relevant or I will know when it WILL be relevant […]and in many organizations there are decisions made based on the information, which is thought to be the whole of it, when it has in fact not been – the information can be a lie, it might require correlation and enrichment and in my mind all of these are linked to data quality"*

9.7.2 CISPs ability to name their information assets, locate them and further segment critical assets

This classification explores the fundamentals of information management as well as those of information security management with relevant governance functions attached, e.g. data governance and information security governance. Some organizations exercise operations much through risk management, so it should be considered also the included in the list. The very point of this enquiry to SME's is that if CISP cannot tell what information they have, which part of it is critical (to be able to produce critical services) and to tell where this information resides (be it CISP own systems, outsources systems or cloud services, where information resides) they practically cannot have any control over their information assets and logically to its quality.

Classification of **CISPs ability to name their information assets, locate them and further segment critical assets** is presented with coding of *low, adequate & good* and for clarity's sake are presented combined in TABLE 10.

TABLE 10. CISP's capabilities over information management

Respondent	*Identify assets*	*Locate assets*	*Crit. Assets identification*
SME1	*low*	*low*	*low*
SME2	*adequate*	*low*	*low*
SME3	*adequate*	*adequate*	*low*
SME4	*good*	*adequate*	*low*
SME5	*N/A*	*low*	*N/A*

SME1 seems that CISPs capability for each area is pretty low and there is much room for improvement:

> *"Altogether bad … that is the situation, have to admit. Information is taken as granted and the criticality of it is not generally understood. […] one could describe it as social vulnerability. […] As a needed trend I see that more and*

> *more we must be able to tell what information is mission critical and what is not and what can be even open. The amount of information is increasing at the speed where we cannot and should not try to protect all information, but focus on identifying the critical part of it and secure it, that A and O of it – knowledge and skills at this are not at the needed level yet, much due to fact that this is seen as a technical problem, which is it not"*

SME2 sees the same possibility for major improvement:

> *"Perhaps they know the information in their own systems, if they anymore have 'own systems', but as we move any further towards the outer rim, then especially the lack of information ownership presents problems, and it is no more know, to where the information is going or from where the information is coming and especially for critical information that of what does it actually consist of[…] then it becomes very unclear. It comes to information ownership as mattering the most, or otherwise I do not even see that we could reach any situation even remotely close to safe."*

SME3 does not observe things being much any better and sees future as challenging:

> *"Hmm.. I think there is a gap here, to be able to describe to people where the data is, what these virtual places are, what part of the information is transmitted and to where […] to further complicate if there are cloud services it get's difficult… here is a problem to understand the big picture well enough, there are discontinuities and these discontinuities are naturally what the attacker is seeking.*

SME4 understands limitation of the perceived cases. However he still highlights the lack of visibility in networked operations:

> *"It's a hunch only, it could be that I've heard one story and not the one hundred others. I guess they know their own assets and some governmental bodies are probably better at this who have worked in security related responsibilities than other are. But the visibility to the guy next to them is probably very low, which I see as a problem."*

SME5 comments on the very basic of things – can the CISP even locate their assets:

> *"[*To a question on if CISP can locate their assets*] – not taken into control well enough"*

9.7.3 CISPs information quality management approach – reactive/proactive

Usually, when information management and especially information quality management maturity is low, there is hardly any room for proactive information quality management, i.e. capability to observe information quality as per quality dimensions described in Chapter 4.2 with lifecycle management of the information to prevent non-compliant information (information definitions, technical quality rules& business rules) from either being created/changed or at least preventing it from flowing in system and operations landscape further than the point of control, where the quality is assured.

The view of how SME's saw CISPs capability to execute proactive information quality management or was it more on the reactive is classified as **CISPs information quality management approach – reactive/proactive** and coding is simple *active / reactive*. The answers are reflected in TABLE 11.

TABLE 11. Information quality management approach

Respondent	*Reactive / Proactive*
SME1	*reactive*
SME2	*reactive*
SME3	*reactive*
SME4	*reactive*
SME5	N/A

SME 1 noted the general trend being:

> *"Unfortunately it is reactive, but we get proactivity out of it later […] but too much reactive we are at the moment".*

While similar general view on the approach exercised is elaborated by SME2: :

> *"I see it, without naming any parties, that even critical infrastructure operators are some in the reactive mode that it means that there must always first come the 'stop', before anybody does anything to the thing. This is, especially considering continuity, everything but an optimal situation. I see this a critical risk, which will more and more grow as different systems are increasingly linked to each other[…] we should be able to constantly monitor the situation and understand it and implications and interfere fast when needed, not only once we are at zero operations".*

SME3 same thoughts as previous – reactive mode prevails:

> *"An impression, not a hard fact, but I'd say it is reactive.. an improvement is through a list of cases that happened and try to learn from these and thus become more active"*

SME4 further brings in the view of current mode being reactive:

> *"My general view on the thing is that it is on a reactive mode."*

9.7.4 Importance of information quality for CISP to operate in crisis situations

When things go wrong relevance of things can almost turn upside down. Hence, hearing out, if information quality had different importance in crisis-situations (e.g. national emergency) than it had in day-to-day business was done. This is classified as **importance of information quality for CISP to operate in crisis situations** and as open comments are of most interest, the coding of *lower than normal, same as normal & higher than normal* was used, where "normal" refers to average state operations of business. TABLE 12 summarizes the coding results.

TABLE 12. Importance of DQ in crisis situations

Respondent	*Perceived importance*
SME1	*higher than normal*
SME2	*higher than normal*

Respondent	*Perceived importance*
SME3	*higher than normal*
SME4	*higher than normal*
SME5	*higher than normal*

SME1 noted on the change of importance over "business as usual" with:

> *"That is totally fundamental and centric. If we think for example leading and administration … or that we are doing business… we're talking possibly millions wasted, if information quality is low [*for decision making*] or there is not enough of it – definitely core thing on".*

SME2 sees this through "business as usual" being optimization, crisis totally different situation relying on high quality decision making information:

> *"Good that you asked. When in normal day we are talking about optimization, then in crisis situation this plays [DQ] greatly larger role, when we need to do hard priorization choices and if you start doing wrong decisions in that situation, where the scarce resources are even fewer, well then the impacts of that will be exponentially higher and more serious".*

SME3 sees the quality of information even existential:

> *"It is utmost important for the company's survival in crisis, where those who survive and will not are decided much on who had control over their information quality and who did not. We are missing this one big cyber tsunami, so cannot tell for sure how things are, but sure there are lack in preparedness"*

SME4 is promoting a need to further enhance the quality-aspects of assets:

> *"Definitely in the center. If the information is distorted, then the conclusions drawn from it and the decisions made are compromised or wrong. We must struggle harder to get the raw material of better quality."*

SME5 needs putting concepts into context with still agreeing on the importance:

> *"It's very important, but it much depends also of the organization so, organization should educate their personnel in a way that they can suffice with*

information of not perfect quality, which still "works" and can take actions based on it or correlate it some more"

9.7.5 SME's view on relevance of named information ownership

In general, one critical facilitating factor for data quality improvement is establishment of ownership over information assets. Ownership brings responsibility and neglecting of responsibilities brings consequences.

SME's own concept of information ownership's relevance was asked. Ownership was told to include also responsibility over set scope of information's quality and e.g. change management (only persons and systems explicitly having a role in the change process can affect it, other changes are violations of data quality). This was classified as **SME's view on relevance of named information ownership** and rough rounding was done to tell it apart by *not important*, *N/A* and *important*. TABLE 13 provides the coded answers.

TABLE 13. Relevance of information ownership

Respondent	*Perceived relevance*
SME1	*N/A*
SME2	*important*
SME3	*important*
SME4	N/A
SME5	*important*

The answer was not coded for SME1 due to much of interpretation bias possibility – on the one hand it was seen important, then on the other also as a possibility of misusing the ownership-concept. In the end it was tied to process ownership, through which it could be perceived of relevance - the quote is left open for interpretation:

> *"Well, it matters, but it cannot be a thing we cannot proceed without, but the information management and the security management of it must be things happening automatically by the functions. […] but I would not stress this ownership too much as there are always those, who use this position for their own purposes and get zealous of it [as it should be the organization, which owns the information]. Process owner should own the information and thus the information ownership is not important but the ownership of the processes".*

SME2 had a view on the matter and tells:

> *"A & O! Greatest shortcoming and if this would be in good shape … we'd receive most* [general] *benefits from developing the information ownership".*

SME3 is presenting an approach, where ownerships of concepts would be joined and sees IT as a bad home base for the ownership:

> *"One solution could be that the ownership of the information is taking place at high enough level in organization, like that if I own some process, I also own the information in that process, data quality, information security and risk management related would be on my responsibility. That might work, but it should not reside in some support organization like IT."*

SME5 seems also lifecycle-management perspective of the ownership:

> *"This is very important in my opinion. In fact a thought popped up that if I am an owner for some information, what happens, when I leave the company, is the responsibility over it transferred to someone else?"*

9.7.6 Summary of the theme

Firstly it was checked how the respondents had formed their conceptual models of information management and especially data quality. It turned out to have similar characteristics as secure information, i.e. C-I-A was presented several times, and also novel viewpoints were presented, which eventually all translate into earlier presented DAMA quality dimensions in Chapter 4.2.

As one of the key themes in the thesis has been the "information as an asset", it was needed to get a view from the SMEs on how they perceived CISPs

capability to identify their assets, locate them (physically) and identify which part of the asset is critical. Generally, the results were devastating. Not only do the CISPs seem to be unable to tell the critical information (which they should do at minimum via critical processes' information needs) - generally they are perceived not to know, where the information resides, which is not good at all and last. Neither do they seem to be very good at even identifying what information they possess in general. Although the details are presented in the quotes, the author still wishes to underline and stress the dire need of addressing this issue, which presents the CISPs to not just one or two threat vectors, but a army of them. On the positive side this indicates that the created model could very well be welcomed with pleasure to remedy a situation like that. Re-quoting SME1 to emphasis this one more time: "*Altogether bad … that is the situation, have to admit. Information is taken as granted and the criticality of it is not generally understood. […] one could describe it as social vulnerability. […] As a needed trend I see that more and more we must be able to tell what information is mission critical and what is not*"

It does not come as an surprise - more of an expectation from observation like just made - it was noted that the CISPs are in reactive mode for their data quality management. Logically sound, as if they are not able to tell their assets and critical parts of or where it resides, how could the proactively manage data quality? More evidence for the need of the model and its capabilities to remedy this situation. In times of crises this is even more critical as the CISP need to act fast, there is no time for anything but the essential and decisions must be made fast, which might provide cascading and dramatic results, if based on data and information not fit to be used for decision making. This was well formed by SME2: "[…] *when we need to do hard priorization choices and if you start doing wrong decisions in that situation, where the scarce resources are even fewer, well then the impacts of that will be exponentially higher and more serious*".

One last thing studied was the data/information named ownership. Something, which is quite in the center of discipline like MDM for ensuring the responsibility over quality of the critical data. SMEs responded that it important. The view presented by another SME was brought to surface again that the ownership could be on the process level. It was also noted that the best quick wins could be achieved by establishing rigorous information ownership. IT was seen as not optimal place for the information ownership, which should be on high enough level. Findings present more expectations for the model as they underline many times the fundamentals the model is based on.

The author's personal perception, from tens of corporate and public institutions, in short is that a very small part of Finnish organizations have clear understanding of what information they have at their hands, yet alone tell, where it resides in functions or system landscape and as usage of cloud services is getting more common, the visibility is dim, if not close to totally vanishing – not to mention what happens to controls over information in such a state of asset management maturity.

Data in the systems is of mediocre quality by any metrics – redundancy, conflicts, shortages in content, lack of ownership, zero quality metering, definitions of data much missing or in form of architects' diagrams, which could interest business less than number of stars in the universe. The only short glimpses of "understanding" are seen, when things go wrong, but as "business as normal" (although through heavy casualties of time and money to recover the business) resumes, there are "more important" things to consider, and the experienced relevance of DQ is forgotten.

There are exceptions, nevertheless the general situation is as described. Best driver the author sees for "dramatic and general" improvement of the situation is drive of regulations and compliance. Although compliance for its own right everything but ensures things improving significantly, at least it

opens a door for considering the business opportunities available through really taking the best out of information assets and ensuring quality for e.g. predictive analytics of production or business in general. The author wishes to give special credit to Solvency II and its Technical Provisions data quality requirement. Although much abstractions and absolutes, they still – even partly explicitly – require the insurance company to form some mock up at minimum of data governance and data quality management. The author has perceived MDM –principles and model working great for Solvency II – purposes.

9.8 Theme: Situation awareness and the relevance of the created model of critical information asset integrity-information sharing

Although all the themes presented and analyzed are important in themselves, they all are building blocks for this "theme of themes" and the ultimate research questions Q1 and Q2. First, this theme covers situation awareness as a concept. Second, it places the role of SA into context of Finland's Cyber Strategy and operational execution of it.

As a climax, it introduces the model created from the pieces of presented common concepts to provide a novel and innovative, yet "low entry cost" solution for both the organizations of critical infrastructure for establishing control and visibility of critical information assets integrity, sharing that information and for Cyber Defence Command Center to have situation awareness over organizations' critical information assets for early warning and control of cyber threats directed to degrade information. This represents the real core of the whole research.

The classification of the theme divides as:

- Situation awareness - defined

- The role of situation awareness in Finland's Cyber Strategy and in overall cyber security capability
- Maturity of situation awareness of critical infrastructure service providers' objective view on their critical information quality
- The created model – significance of the presented capability, novelty and value of further development

9.8.1 Situation awareness - defined

Before the Grande closure of the theme interview with its most significant questions yet to be asked, it is still needed to align the concept of the respondents' on their observation of what *situation awareness* means and perhaps of what it consists of or what is of utmost importance for it,. This classification is: **situation awareness – defined**.

SME1 concentrates on the characteristics of situation awareness, which are of importance.

> *"SA is a critical factor [*for cyberdefence*], and I see it as something, which should scale to multiple levels, so that decision makers on each level can make their decision [*this implicitly defines the SA for the person*]base on it – that there is no as one static situation picture. It is.. it is one of the most critical handicap we have here in this cyber world, the lack of these* [SA capabilities] *, that we have so many areas, where situation awareness just does not work. There are nations, who do not even know that they are stolen of information constantly, which is the saddest state, naturally"*

SME2 seems things rather similarly, although on the function of SA he elaborates:

> *"Definition the situation awareness in the context is crucial, i.e. what is the situation awareness we need build and what do we get out of it. Situation awareness's only function is to support decision making, meaning producing information to the decision maker that is needed. Situation awareness must support a decision – if it is only situation awareness for the sake of having one, I see little value for such."*

SME3 sees the layers of SA as situated and context and information need-based stacked pictures:

> *"SA comes in different forms for different people, there is technical SA, operative SA, i.e. where we are in the situation. It's a stack of things, sensor data at the bottom, technical analysis layer next, own picture for the management. So, it's stack of these pictures with at the very bottom information sources, and information travels through these layers to produce the picture level needed."*

SME4 observes the key point of improving understanding (and thus building more knowledge too):

> *"It's a composition from different sources with possibly different methods of an situation, based on which a professional or a decision maker can either improve his understanding of the situation or make other conclusions. Situation Target of it is to enhance situational understanding."*

SME5 differentiates awareness from knowledge:

> *"This one is interesting… like at NATO there might be this SA in use, which tells that there are these 50 battle tanks here and here, but it is missing the situational knowledge of how to use the tanks. I make these stand apart as many forget that knowledge does not automatically pop up from the product itself* [e.g. command and control battle SA-system]*"*

9.8.2 The role of situation awareness in Finland's Cyber Strategy and in overall cyber security capability

Although it was noted in literature study that many countries (like USA) stress the importance of situation awareness in their cyber strategies and guidelines, as does Finland, it remains still to be asked the SMEs for their weight of SA for overall Finland's Cyber Strategy and the capability the strategy should through operational plan achieve.

Classification of **the role of situation awareness in Finland's Cyber Strategy and in overall cyber security capability** was provided and coding is familiar: *low, medium, high, N/A*. First the question about role's relevance for strategy is

posed and presented in TABLE 14, which has the coded answers for the relevance of the role in overall cybersecurity operational capability.

TABLE 14. Relevance of role of SA in Finland's Cyber Strategy and in overall operational cybersecurity capability

Respondent	*SA in strategy*	*SA in operational execution*
SME1	*high*	*high*
SME2	*medium*	*high*
SME3	*high*	*high*
SME4	*high*	*high*
SME5	*high*	*N/A*

Few open comments are presented starting with SME1:

> *"Situation awareness and forming the situation picture are central and it must be a multi-stakeholder process that everyone involved, produces information and on the other hand the system produces information for the same stakeholder – two-way street. Only then we can start talking about really working situation awareness".*

SME2 takes a skeptic view on part of the topic. In his previous comments he sees SA important, however he states that current execution is uncoordinated and without set target (relevance is thus coded from previous and later following comments):

> *"Well, it is there in the paper and I guess even ranks as number one and what that means in the field is that everyone's now building their own situation awareness or trying to define what it is. But, it is characterizing that one bureau even had a project called 'Situation awareness of situation awareness project', which describes the confusion we are having in the society over this matter […] at least there is no common understanding that what the heck this situation awareness should now be and what is supposed to do – things are really loose here."*

SME3 sees the role of Cyber Security Command center as very centric:

> *"It's high already through being in the strategy and driving the imperative of Cyber Security Command Center, which has the primary mission of providing the SA based first on Cert-FI and later expand it to cover a 24/7 situation picture for this internet world of ours. I would feel very hard to establish any operational defences or structures without knowing where we are."*

SME4 has seen already results from the strategy's implementation:

> *"Important yes and as first outcome the establishment of Cyber Security Command center, which has already improved the co-operation between different departments."*

SME5 on the contrary is still standing by for the strategy to get realized:

> *"At least it has been underlined a lot in the strategy and its execution plan, then all we are missing is the implementation."*

9.8.3 Maturity of situation awareness of critical infrastructure service providers' objective view on their critical information quality

Earlier in Information management-theme, it was investigated, how mature was the critical infrastructure service providers' capability to identify and control their critical information assets. Here, that overall capability to manage the information assets is viewed through lens of situation awareness.

Two main assisting questions were presented – one to have a general understanding of the CISPs capability to form situation awareness over their own critical information assets. Another to form an opinion on the CISPs visibility to data quality into their supply chain for critical services. These combined are coded as **visibility of own and value chain's objective information quality**. It is coded to be presented via coding of *poor, adequate, good & N/A*. Results are shown in TABLE 15 and comments further will elaborate the status of SA.

TABLE 15. CISPs' SA over their own and supply chain's critical information

Respondent	*SA on crit. Inform.(CI)*	*SA over supply chain CI*
SME1	N/A	N/A
SME2	adequate	poor
SME3	adequate	poor
SME4	poor	poor
SME5	adequate	N/A

SME2 has already commented on the matter in information management-theme, and further elaborates::

> *"There is some reactive situation awareness capability, but is more on like reporting on quarter –basis, but as it should, like for master information, be continuous operation. These things like SOX and so on are not just not sufficient. There is not enough of this and it is outdated".*

SME3 sees that there is no general capability to tell data either corrupted or being what it should be and seems holes for possible attacks left unfilled:

> *"It's just an impression I have not hard evidence, but I'd say that they [CISPs] are having hard time identifying corrupted information of theirs, if it has not been thoroughly thought and implemented that how can they tell if the data is correct or not. And when we go to a company [not CISP] then there is a high risk that they cannot tell if their data is corrupted or not. Classic way has been to put it into some silo and protect the silo. Visibility to supply chain.. most probably even worse, I's say this is not in control, which does not mean that things are all problem, but that there pretty sure are gaps and holes, but if someone at some point in time wants to leverage this situation, it is possible. We are not on the right level with this one."*

SME4 has a more positive view that there would be visibility over the quality, however he sees clear need for establishing more visibility for the internal monitoring:

> *"An educated guess but I don't believe they can form it… No, they'll have no understanding of the quality of the data. This is due to this belonging into internal monitoring of those parties, and they do not do that too much, really. In the supply chain – even less! Close to zero. Even in the best cases visibility is restricted to immediate chain loops, not further."*

SME5 seems linear problem solving as not innovative and is asking for more innovative answers:

> *"Not perhaps too mature as such. Many think this in a linear way so we need to find a solution to a problem instead of investigating what else might exist* [instead of the problem solution per se]. *Like in ISM-scene there is this HAVARO, which has produced some success stories and in which the importance of sharing information has been understood."*

9.8.4 The created model – significance of the presented capability, novelty and value of further development

Much of this research's literature study have been ensuring that the author's conceptual model is in line with the one found in science and practice. Most of the interview questions have been targeted to ensure compatibility of the interviewees' conceptual models of scope management and change management to the ones of the author. All this has driven the work done to the ultimate research question presented: Was a model, asked for in Research Question Q1, doable, which partly was evidenced in Chapter 7 and later concluded in Chapter 10.

The previous classifications of this theme have been there to build evidence on need for a created model or decide that the model as such is not answering the challenges Finland's cybersecurity is facing via perceived lack of actual SA, although many people talk of it and its importance.

As the last concept of SA was interviewed, the model was presented to interviewees and they were given the chance to tell their opinion on 1) significance of the presented capability model is arguing to present, 2) novelty of the model and last 3) value of further developing the model. These questions have a shared classification of: **the created model – significance of the presented capability, novelty and value of further development** and although quotes are of most relevance a summary of answers was coded to TABLE 16 with coding of, *low, medium, high & N/A*.

TABLE 16. The Model – Significance, novelty and relevance of developing

Respondent	*Significance*	*Model's novelty*	*Relevance of future dev.*
SME1	*high*	*high*	*high*
SME2	*high*	*N/A*	*high*
SME3	*high*	*high*	*N/A*
SME4	*high*	*high*	*high*
SME5	*N/A*	*N/A*	*high*

SME1 seems the connection with his earlier views realized here:

> *"This is thoroughly central and I think this as a good idea. And I think we need also this interaction between the parties* [...it is important, because...] *we have no current capability to know if our information is degrading, but we think… well, we come back to this that we have the whole process and the situation picture with it and then should be able to predict the implications to own processes and.. .. yes, you are on the right tracks with this one here. My hunch is that this is not yet researched as presented and should be researched further, and should be done… this is on the very core of what this cyber world is.*

SME2 is rather excited about the model and its potential:

> *"Yes… if we take the threat you described* [as per threat –description in Chapter 7] *then the ice cold fact is that we are totally defenceless against such threat with existing processes and systems and it would be sheer luck, and very lucky sheer luck, to detect such a treat when the need would be. This model is see it as stupendous and especially for business continuity management too. All in all, I'm really excited about this model and its potential."*

SME3 seems the model as valuable and possible helper for national resilience – he also observes the mode in which model work (prevention) as good approach and the threat described, which the model is addressing as very nasty and difficult to control:

> *"Definitely this is valuable – protecting the critical infrastructure and working on national level, so this is in the very core of national cyber security and national safety […] offering true national resilience, which is based on the situation picture – and for purposes like that, this model is very much supporting that sort of activity. If operating well and we can step in very early*

> *in the threat detection, which if managed (or not managed in practice at all) poorly would lead to major escalation, we could tackle that sort of threat [persistent and difficult to spot through slow data corruption not detectable easily], which I see essential for the security measure to be efficient. […] I have not encountered this thought this far to the date, so you definitely have something here, mostly there has been questions what we should do […].*

SME4 is promoting the further development and sees the potential (although also the possible of barriers hard to collapse) of having some visibility into inside of operations:

> *"With [a model like] this we'd be able to catch the strange things inside the borders of the organization I say this is very good idea, especially as it forces to things happening also inside and their status, which is missing at the moment. Thumbs up on this, carry on researching too and think, how this could work perhaps even better in the context of public authority departments* [as there is less legislation challenges to tackle]."

SME5 is supportive for the model and highlights that it should be done simple to adapt and sees much value in the continuous exchange of information, not just incidents a driver for building trust:

> *"There are many things here again – reflecting against the presented threat scenario* [per Chapter 7]*, this brings the added value that there is more of information exchange than mere incident information[…] as when you exchange information on a regular basis it pays back for a longer period […], and when sharing more than just the incident information it build trust, which is important once things start happening […]– this would be good to highlight here. Yes, it's worth developing further and it should be kept as simple enough, which would ensure that it's taken into use – so easy that one cannot say "no"."*

9.9 Summary of the theme

This theme was to investigate the most important research question Q2 by first aligning *situational awareness*, significance of it for Finland's Cyber Strategy and cybersecurity capability. Then the model created from bits and pieces was submitted to SME's verdict over its relevance. Last it was investigated, if the model was innovative and worth more development.

The conceptual models the SMEs had on situation awareness itself were pretty aligned with one observing it from functional view, one from characteristic's of it one through the layer of pictures SA consists is consisting of, SME 4 underlines the understanding presented by SA and SME5 highlights that there is a significant difference with awareness and knowledge, which is as per SA-model (i.e. the observer brings her knowledge into the model).

The importance of SA for Finland's cyber security was asked and the answers were aligned as high with one medium, which was due to scientism that does anyone now know, what the SA should do or what purpose it should fill – a solid point presented, which needs focus from Cyber security command center – obviously there is lack of direction for the execution at the moment. Also the importance of SA in operations was deemed systematically high, i.e. it is needed for efficient cybersecurity capability. A good summary on the importance is presented by SME3: "*I would feel very hard to establish any operational defences or structures without knowing where we are.*"

For purposes of double checking previous (there was many double check in the interview, asking the same things from a different viewpoint) data quality and information management –topics, the SMEs were asked for their opinion on the SA capability of the CISP on DQ of their own information and possibly the SA of their supply chain's DQ. Although the answers show an mediocre status (confirms the previous findings), it builds more momentum for the model to be presented. It is observed that generally CISPs have "adequate minus" –SA on their own critical information quality, however to the supply chain's DQ the SA-capability was seen "poor" systematically. Observation is naturally good emphasis for the model and at the same time bad for national continuity, as this implies that it might prove out to be pretty easy feat to corrupt some of the CISPs' critical information assets. The presented is just an easy and obvious possible attack vector, however a more alluring vector would be to influence the service production operations of the CISPs on the

light of the fact that they have no visibility on their supply chain's information quality.

SA's significance for Finland's Cyber strategy and its deployment as well as for effectiveness of cybersecurity efforts made was deemed as of utmost importance and one thing to focus on. It was noted at the same time that although situation awareness has been there (in the strategy and plans) for some time already, very little concrete exist on it yet. A pick from SME3: "*It's just an impression I have not hard evidence, but I'd say that they [CISPs] are having hard time identifying corrupted information of theirs, if it has not been thoroughly thought and implemented that how can they tell if the data is correct or not. And when we go to a company [not CISP] then there is a high risk that they cannot tell if their data is corrupted or not*". This quote summarizes the hole through which many threats could crawl, or even walk in head held high no-one noticing.

As a climax the SMEs were presented with the model and explained through the high level concept of it and on what it is based and it might provide. They were asked for the possible significance of the model to enable targets set in cyber strategy and its operational plan. The ones being able to comment on this all ranked the value as "high". A quote from SME2: "*This model is see it as stupendous and especially for business continuity*". Similar support for the significance was through received through e.g. SME 3's quote: "*Definitely this is valuable – protecting the critical infrastructure and working on national level, so this is in the very core of national cyber security and national safety […] offering true national resilience, which is based on the situation picture – and for purposes like that, this model is very much supporting that sort of activity*".

On the novelty of the model the comments, which coded were "high". It was seen as not yet researched and developed to even this maturity level e.g. SME3: "*I have not encountered this thought this far to the date, so you definitely have something here*". Last it was asked, if the model should be developed further, i.e. was there enough value potential included. It was concluded "high" for

relevance of future research, which is very encouraging and best summarized by SME4's comment: "*I say this is very good idea, especially as it forces to things happening also inside and their status, which is missing at the moment. Thumbs up on this, carry on researching too*".

On a personal note author does not have too much to elaborate. The most important things this study was pursuing after, have been proven with this limited scope to stand examination by SMEs very skilled in security and information security. Feeling content, it is just better to proceed to closing part.

9.10 Closing the analysis part

The most relevant part of the interview data was classified, coded and the findings were presented in the previous theme Sections. A notion should be made that much more data was gathered in the interviews, however in the author's judgment the data does not provide relevant addition of insight into main research questions, although they are surely interesting and can be utilized in later studies. Subjects, which were not covered are listed along the covered subjects in the interview frame, which is presented in APPENDIX II – Interview frame.

The analysis part of the research has broken the "big picture" down into smaller pieces, themes, and classified the theme key elements with the appropriate coding, and made a comparison with the secondary research data, the literature study data, where applicable. The following Chapter 10: Conclusions, limitations and future research will proceed back to the big picture with interpretation of the holistic findings.

10 CONCLUSIONS, LIMITATIONS AND FUTURE RESEARCH

Much of the conclusions from the primary data (interview data) and its analysis were already presented in the interview study analysis in Chapter 9. Possible repetition of those in this chapter would be exactly that: repetition and thus not done. The summaries in the interview theme Section capture well the conclusions drawn. Neither are systematic comparisons to the secondary data (literature study) presented as it is also made familiar in the previous chapter, where special mention provided value. Otherwise, as it was noted earlier, the interview questions grounded back to literature and model building parts of the thesis.

This chapter concentrates on concluding the answers to the research questions, although it will additionally provide some further conclusions. It will also comment on the reliability of the study, possible limitations and also to the significance of the research. Later on, the author will express his personal view on the findings. Lastly, further research possibilities provided by findings of this research are suggested.

10.1 Concluding research question 1

The first, and most important, research question was presented as:

Q1: Can a novel model be built leveraging from established disciplines of master data management (and data governance), information security management (and information security governance) combined with situation awareness for purposes of:

1. **providing organizations capability to identify their critical information, build controls over it and identify any attempts to tamper the critical information assets**
2. **presenting command and control -type operator (like Cyber Security Command Center) with a situation awareness and early warning capability over threats compromising information assets of identified critical service providers?**

Both "1." and "2" of the Q1 were answered through the literature study's secondary data findings utilized in Chapter 7, where the actual model was built and proofed for concept. The components (disciplines) presented were capable building pieces for combining them for something, where the holistic value of them was more than mere sum. As a conceptual model, it needed to be presented to SMEs in cyber security to have **initial validation for the model. This was done in Chapter 9.8.**

The author was not left into doubt that the respondents would not have had similar enough conceptual models of the presented concepts as presented in this research and owned by the author.

The conclusion is that a model like presented could be made and the prototype proofed that the conceptual model is feasible and it should be developed either to a working prototype or further formalized via e.g. ISDT-theories for building a design science –based model of system of systems.

The direct implication from this finding is that both practitioners as well as researchers should think with wider scope than their own silos of e.g. MDM or ISM. It was noted several times in interviews also that silos in general are bad and synergies should be sought out from combining the disciplines. Four of the SMEs commented that information security and data management/-quality overlap in a way that there would be synergy-benefits expected, if organized accordingly. This would provide potential for both cost savings as better management of resources to activities, which matter the most and provide momentum and organizational change management "muscle" for the combined forces.

Another direct implication is that universities and applied science universities, especially those providing cyber security education, should consider their scope of education to consider a fusion like presented here to

establish novel new models of operations for an industry sector which is growing rapidly and has huge potential for society benefits.

The mentioned will be done with a tactical mindset, not rushing into conclusions, instead promoting the concept, gathering requirements, assessing its feasibility on larger scope of experts and via promoting the possibilities to both university for rigorous scientific study as well to applied university for technology demonstration or pilot.

10.2 Concluding research question 2

Second research question was aimed to validate through empirical study, whether the possibly, theoretically feasible, model created for Q1 was on high conceptualization level valid, of value and of further research. This was done via theme interviews of considerable track record security and cyber security professionals, both researchers and practitioners. Levels they operated were mostly strategic, some tactical-strategic and one of tactical-operational.

Q2: If such a novel model (as per Q1) could be built, what would be its potential value for national cybersecurity capability of Finland?

As the model is not build per e.g. design science theories, it needed to get either confirmation for its possible initial applicability as well as the value it might present to Finland's cybersecurity development, if studied further. This was done in Chapter 9.8.4. **The comments from some of Finland's leading cyber strategists, tactician and operational experts were confirming that the model made sense, it could potentially solve a dramatic current problem having direct impact on safety of the Finnish society, and it was definitely worth more research and development**. It was also encouraged to develop it further fast and present it to Finland's Cyber Security Command Center and several other governmental bodies.

Direct implication of this is the same as in Q1.

10.3 Concluding research question 3

Last of the research questions was a "added value" research question to further provide insight into topics, which are of relevance for the model and for providing insight to build momentum for its possible further development.

Q3: In Finland's cybersecurity context, is information understood as an asset by critical infrastructure service providers:

1. **Are these assets identified and protected accordingly?**
2. **Are there decent controls over information assets?**
3. **Is the concept of data quality and its monitoring present?**

Answers to these questions were already covered in Chapter 9. As the details are there – especially in the Summary -chapters, no repetition is made. Instead a summary of summaries to questions is presented as follows:

Are these assets identified and protected accordingly?

They are not – capabilities are at level "decent" at their best.

Are there decent controls over information assets?

No, the controls seem to be missing and even monitoring capabilities of data quality are at their best minimal – note, technical controls like system administration etc. are not of concern in this scope. The answer is provided only for purposes of the presented concepts of data DG, DQ, MDM and partly for ISG and ISM.

Is the concept of data quality and its monitoring present?

As per previous answer – no, they are not in place for even decent level.

First direct implications of this is further to migrate the best features of these disciplines into the created model development.

Another direct implication, on wider scope, is to promote the wide gap Finland has in its cyber security defences, which, if (when) exploited, could tax our cyber resilience to its maximum of beyond, seriously endangering national continuity or at least locking up key continuity resources, which would be needed elsewhere. This will be made aware to Cyber security command center to consider in their operative and tactical plans as well as promoting critical information's relevance.

It could prove out that although findings are very much in line between the respondents that very different views are provided by different set of people. Things are not black and white, however the shade of gray needs to be found out first before any major activities can be taken.

10.4 Other conclusions

The author would like to highlight few additional conclusions. First is "the not presented hypothesis" of the author (motivating for this large research) that complex disciplines like DG and ISG, MDM and ISM as well as DQ and SA could be combined for holistic benefits. A hypothesis was also present in author's mind that mentioned concept overlap both positively and negatively. From the positive overlaps would synergy benefits rising and the negative overlaps could be eliminated through efficiency thinking. It seemed there is a big picture which is relevant for the large scope of this research. This was proved implicitly in Chapter 7.

Another conclusion is that the same disparity, which seems to exist in so many other disciplines does show up in this study too. The business operations and IT (or even ICT) do not either want to or just cannot comprehend each other. The only remedy the author has is to educate CIOs to

be really *Chief Information Officers*, not *Chief Technology Officers*, which they more to author's perception are. It would mean either business oriented CIOs or tasking CIO-offices with direct development responsibilities over e.g. business process development instead of sourcing new, neat, tools. Only via the understanding of business and its needs could the CIO –operations be something else than mere "support organizations".

A more of a secondary conclusion is made to further underline the fact that the terms definition for cyber- prefix terms is rather in-mature and this causes lots of misunderstanding and could complex further the high speed evolving phenomenon. Cyber security control center and its operations as well as education bodies in co-operation, have a task to formalize the terms into Finland's context maintaining the compatibility with the wide array of terms outside Finland's perimeter.

10.5 Significance of the findings

The conclusions and findings presented can be considered very significant, as cyber threats are coming more eminent, advanced and target to specific purposes and organizations. The complexity of cyber environment is getting even more complex with introduction of e.g. internet of things, industry of things, BYOD, BYOA –concepts and no set international rules for nation-scale operators on what can and cannot be done and with what possible consequences. Nations, as well as single organizations are sprinting fast to stay onboard and be a bit ahead of others in cyber capabilities.

The research is rather unique, with the innovative and novel model presented and verified for significance by Finland's leading cyber strategists and tacticians and operative persons. It encompasses many complex concepts to facilitate the understanding of their dependencies, interactions and holistic sum and makes a fusion of those. A similar study has not been made earlier and the research conducted is expanding both academic doors for further

research. More importantly it could provide an instrument for solving some of the Finland's national cybersecurity challenges, which have direct implications on large society context. Should the model prove out valuable via the upcoming iterations, it could perhaps presenting Finland and its CISP as well as e.g. national emergency supply network as a whole, something that few countries (if any) in the world have.

10.6 Reliability of the study and limitations

Much of the limitations have been explained in Section 8.3: Reliability of the selected interview approach. Scientific rigor in both the research setting and conducting the interviews has been exercised to the author's best ability and requirements of applied university's thesis. As it has been noted many times, things are only perceived for their value in the right context. Hence, this thesis must be perceived in the context of applied sciences, where theory is in lesser role than practical results. For real scientific rigor, the model should be further investigated via e.g. design science models like ISDT.

Worth noting is also that the sampling strategy is limited both in the number of interviewees as their possible self bias on some of the interviewed themes. The author has done his best (with the given resources) to ensure the needed data saturation and receiving as accurate data (not biased) as possible.

Also, the study is aimed to explore studied concepts only in context of cybersecurity. Nevertheless, many of the findings as well as the general basic model are probably well worth considering in e.g. supply chain risk management outside the scope of critical infrastructure service providers. In general the findings and conclusions should only be viewed in the context of the given research setting. The author does not claim for any outright generalization of the findings and conclusions - on the contrary, encompasses to critical utilization of the conclusions with the given limitations in mind.

For the purposes of the model creation, SA-approach was in author's perception, ideal as it is well recognized model used in for example tactical and strategic systems, where users are taxed with highly complex cognitive duties requiring high performance in decision making. The author argues that the presented model is best *perceived* (as well as *comprehended* and *projected*, although these "steps" of SA or situation assessment are out of scope of the study) via SA. Partly this is due to a perceivable analogy with large-systems operations like nuclear plants (Endsley, 1995) and that of a cyber command & control. At the same time author recognizes his familiarity with SA-theory-in-depth knowledge missing. Thus it could prove out that SA is not a fit theory to serve the information sharing purposes required by the model.

Further study is required to validate the findings with a larger count and more heterogeneous data sources, and more detailed research and interview questions. The author proposes adhering to the interview approach as the concepts are quite complex and survey research can easily lead to misconceptions and corrupted data, if not elaborated to the very last extent of the concept and validated the conceptual model of the respondent.

10.7 The author's professional view on the findings and improvement suggestions

The author would like to use the opportunity to encourage both academic as well as practitioner organizations (especially critical infrastructure service providers) to put special attention to understanding cybersecurity and its connection with classic information security management. The author also encourages all, especially service provider for critical infrastructure to pay much effort into understanding the critical information asset and establishing controls over it. It was already noted in literature study and further underlined by interviewed subject matter experts that there is no absolute defence and focus should be more on the information, not technology. The

author proposes some concrete steps forward and will later summarize his personal "free word"-thoughts on the findings.

10.7.1 Few suggestions by the author on the conclusions

From my experience and perceptions from the interviews one thing can be considered as a fact: information management, be it MDM or other discipline and information security do not work well together with current models. In author's experience, there has always been mixed responsibilities, which eventually end up in situation of no-one taking the responsibility. Also, these disciplines are making half-futile effort for goal far beyond their reach and fail, where they could consider combining forces for joint goals. This notion was one of the basis for this research and this research thrives to offer advice and guidance for developing possible co-operation.

Another suggestion the author wants to make, is data quality as a whole. The analysis findings state that the situation is not on the needed level and the author can only agree. What could organizations and educational institutions do to enhance the situation?

Organizations: Management must recognize first the importance. This can be done via studies like this and further evidence. The importance must be grounded to money and efficiency lost, which is partly already evidenced in this study.

Organizations can and must also consider the time of their information security professionals. Studies have shown in the theory part and interviews confirmed the findings that the professionals with latest know-how are few. It should be really considered, where to invest those resources. If the premises are somewhat in order, then sub-optimizing those and trying to tackle information leaks on device level could prove out futile effort. Perhaps it would be better to concentrate on the asset itself – the information, which is supposed to be protected. The author sees clear need for widening the

perspective of ISM professionals with at least basic data management and governance studies – these could result to new models of working and reducing some of the redundancy data management, risk management and information security management organizations currently do have.

Educational institutions: Institutions like universities and polytechnics must come to understand that the cybersecurity –education they provide is, naturally, relevant, however it is of very narrow scope. The author perceives that there is demand for generalists, who do understand basics of business operations, information management and information security. Could such a mix be created via co-operation of university's (unfortunately often very silo-operating) departments?

10.7.2 The author's "free word"

The author has always been a "big picture" -thinker and seeing connections and possibilities between concepts. The "pros" are precisely the things mentioned, but on the cons-side, details sometimes escape me or are of no interest. Hence, I call for supporters to continue parts of the work, which need eye for rigorous and pedant work and eye for details. I see the concept presented as very exciting and much loaded with potential. However, at the same time I must admit the facts that help is needed. This is a call out for co-operation on development of the model.

Although reading my "sharing"-experience view on the results, one could start to doubt the findings are being biased, I have to admit that, naturally, I have not agreed with all the interviewees' opinions and have done my best to stay as objective as possible, not putting words to their mouth. A possible reason for so many shared conclusions is that the findings really are a quite general phenomenon. That is to be validated by further research, which is covered next.

10.8 Further research possibilities

Several future research topics can be suggested on the basis of the findings, conclusions, and also the limitations of the study. The following could be considered:

1. Validating the findings of this research – do they withstand a larger audience and more heterogeneous research environments? If not, what are the limits of the findings environment where they do still apply?

2. Conducting design science study for the model presented for the purposes of describing it as a system e.g. according to ISDT –theory.

3. Prototyping a technical solution, which could source critical information inside the organization, take a stand on its quality, especially the consistency and form a "status message" as few of the data quality meters presented in this study and further send it out perhaps utilizing models and later standards being developed for threat information sharing. At the receiving end, react to the information received and present it at simple observation-view of an SA-tool or integrate it directly to existing SA-tools of Cyber security command center, police force or the military.

4. Further comparison of the presented concepts ISM and MDM for realizing more synergies and proposing operational models and systems, in which overlaps are removed and common goals foster commitment and "drive" as well as get buy-in from top management more easily.

5. As analyzed and concluded, there seems to be a disparity with business goals and IT goals. This leads to a situation where IT is not executing its activities efficiently for realizing business strategy and therefore the

best for the company. This might be much due to "not proper" governance structure of ISG/DG and ISM/MDM. A model could be researched, where (as suggested by interviews) process ownership takes ownership of information, its security as well as associated risks. It could turn out that this sort of model is not working due to same information utilized by several processes and ownership is getting scattered and thus vanishes. It might still be worth investigating

6. Also, a model, where all the mentioned disciplines are governed centrally by risk management, could be studied. This would fit more easily to institutions like banks, who already thing through risks.

7. What kind of learning programs and learning paths could be introduced for better combining ISM and IM education? At the moment it seems both work as their own disciplines, however many of the goals and responsibilities overlap, although perceptions could alter a bit or terms be different. The author is quite sure there would be pull for future professionals, who understand information as a key asset of the organization and at the same time understand the needed security measures and risk management

REFERENCES

107th Congress of the United States of America. (2002). *Sarbanes-Oxley Act of 2002.* Washington.

Ahmad, A., Bosua, R. & Scheepers, R. (2014). Protecting organizational competitive advantage: A knowledge leakage perspective. *Computers and Security* , 27-39.

Ahmad, A., Hadgkiss, J. & Ruighaver, A. B. (2012). Incident response teams - challenges in supporting the organization security function. *Computers & Security , 31* (5), pp. 643-652.

Antikainen, J. & Käkölä, T. (4. 11 2011). *Information System Design Theory for Master Data Management Systems: Designing and deploying MDM processes and systems for strategic enterprise and business process effectiveness.* Accessed on 28 November 2014. Retrieved from IFIPWG82 -OASIS 2011 Workshop Program: http://ifipwg82.org/sites/ifipwg82.org/files/2011%20OASIS%20PROGRAM%20SHANGHAI%20rev%201.pdf

Antikainen, J. & Käkölä, T. (2010). Relevance of Scope Management and Organizational Change Management in IT Deployment Projects. *International Research Workshop on IT Project Management (IRWITPM)*. AISeL.

Berson, A. & Dubov, L. (2007). *Master Data Management and Customer Data Intergration for a Global Enterprise.* McGraw Hill.

Choo, K.-K. R. (2011). The cyber threat landscape: Challenges and future research directions. *Computers and Security* (30), 719-731.

Cochrane, M. (2009). 5 Steps to Data Governance. *Computers & Data Base Management* , 33-34.

Council of Cybersecurity. (2014 (b)). *Council on CyberSecurity.* Accessed on 30 November 2014. Retrieved from Critical Security Controls: http://www.counciloncybersecurity.org/critical-controls/

Council on CyberSecurity. (10 2014 (a)). *Council on CyberSecurity.* Accessed on 29 November 2014. Retrieved from Council on Cybersecurity: http://www.counciloncybersecurity.org/

Crossler, R. E., Johnston, A. C., Lowry, P. B. & al. (2013). Future directions for behavioral information security research. *Computers & Security , 32*, 90-101.

Cukier, K. (2010). *A Special report on managing information.* The United States of America: The Economist.

DAMA (UK). (10 2013). *The Six Primary Dimensions for Data Quality Assesment.* Accessed on 30 November 2014. Retrieved from DAMA UK: http://www.google.fi/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CCYQFjAA&url=http%3A%2F%2Fwww.damauk.org%2FRWFilePub.php%3F%26cat%3D403%26dx%3D2%26ob%3D3%26rpn%3Dcatviewleafpublic403%26id%3D106193&ei=XYh_VP_XBKvXyQPZ8oG4CA&usg=AFQjCNErJKCVwWSfMcxqXQz0N

Das, T. K. & Mishra, M. R. (2011). A Study on Challenges and Opportunities in Master Data Management. *International Journal of Database Management Systems (IJDMS) , 3* (2), 129-139.

de Freitas, P. A., Michel, W. S., de Macedo Rodrigues, M. A., dos Reis, E. A. & Gronovicz, M. E. (2013). Information Governance, Big Data and Data Quality. *2013 IEEE 16th International Conference on Computational Science and Engineering* (pp. 1142-1143). IEEE.

Denning, D. E. (2014). Framework and principles for active cyber defense. *Computers and Security* (40), 108-113.

Endsley, M. R. (1995). Towards Theory of Situation Awareness in Dynamic Systems. *Human Factors , 37* (1), 32-64.

European Insurance and Occupational Pensions Authority (EIOPA). (2009). *Technical Provisions - Article 86 f Standards for Data Quality.* Accessed on 4 December 2014. Retrieved from European Insurance and Occupational Pensions Authority: https://eiopa.europa.eu/fileadmin/tx_dam/files/consultations/consultationpapers/CP43/CEIOPS-L2-Final-Advice-on-TP-Standard-for-data-quality.pdf

Franke, U. & Brynielsson, J. (2014). Cyber situational awareness - A systematic review on literature. *Computers and Security* (46), 18-31.

Gartner, Inc. (2013). *Definition: Cybersecurity*. Accessed on 1 December 2014. Retrieved from Gartner: https://www.gartner.com/doc/2510116/definition-cybersecurity

Hardy, G. (2006). Using IT governance and COBIT to deliver value with IT and respond to legal, regulatory and compliance challenges. *Information Security Technical Report , 11* (1), 55-61.

Henry, K. (2003). The Human Side of Information Security. In M. Krause & H. F. Tipton, *Information Security Management Handbook, Fifth Edition* (pp. 663-676). The United States of America: CRC Press.

Hevner, A. R., March, S. T., Park, J. & Ram, S. (2004). Design Science in Information Systems Research. *MIS Quarterly , 28*, 75-105.

Hinde, S. (2000). Do You Know Your Organization's Achilles Heel? *Computers & Security , 19*, 585-590.

Hirsjärvi, S. & Hurme, H. (2008). *Tutkimushaastattelu*. Helsinki: Gaudeamus.

International Telecommunication Union. (2014). *Definition of cybersecurity*. Accessed on 1 December 2014. Retrieved from ITU: http://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx

ISACA. (2012). *COBIT 5 for Information Security.* Accessed on 30 November 2014. Retrieved from ISACA: http://www.isaca.org/COBIT/Documents/COBIT-5-for-Information-Security-Introduction.pdf

ISO/IEC. (2011). *Information Security Incident Management.* Accessed on 2 December 2014. Retrieved from ISO/IEC 27035:2011: http://www.iso.org/iso/catalogue_detail?csnumber=44379

ISO/IEC. (2014). *Information security management systems — Overview and vocabulary.* Accessed on 2 December 2014. Retrieved from ISO/IEC 27000:2014(en): https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-3:v1:en

ISO/IEC. (2009). *Risk management — Principles and guidelines.* Accessed on 30 November 2014. Retrieved from ISO 31000:2009(en): https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-1:v1:en

IT Governance. (2014). *Cyber Resilience*. Accessed on 30 November 2014. Retrieved from IT Governance: http://www.itgovernance.co.uk/cyber-resilience.aspx#.VIJ-UsnV5yX

Kahneman, D. (2012). *Thinking, Fast and Slow.* Great Britain: Clays Ltd.

Knapp, K. J., Morris, R. F., Marshall, T. E. & Byrd, T. A. (2009). Information security policy: An organizational-level process model. *Computers and Security* , 493-508.

Kobielus, J. (2006). Master data management is key to compliance. *Network World , 23* (22), 35.

Kshetri, N. (2005). Pattern of global cyber war and crime: A conceptual framework. *Journal of International Management* , 541-462.

Lagus, A. J. (3 2013). HAVARO analysoi ja varoittaa. *Tietosuoja* .

Merriam-Webster, Incorporated. (2014). *Dictionary*. Accessed on 28 November 2014. Retrieved from Merriam-Webster: http://www.merriam-webster.com/dictionary/cybersecurity

Merton, R., Fiske, M. & Kendall, P. (1956). *The focused interview: A manual of problems and procedures.* Glencoe,IL: Free Press.

Mesquida, A. L. & Mas, A. (2014). Implementing information security best practices on software lifecycle processes: The ISO/IEC 15504 Security Extension. *Computers and Security , 48*, 19-34.

Mitnick, K. (2004). *CSEPS Course Workbook.* USA: Mitnick Security Publishing.

Morrow, B. (2012). BYOD security challenges: control and protect your most sensitive data. *Network Security* (12), 5-8.

National Association of State Chief Information Officers (NASCIO). (4 2008). *Data Governance – Managing Information As An Enterprise Asset.* Accessed on 28 November 2014. Retrieved from NASCIO: http://www.nascio.org/publications/documents/NASCIO-DataGovernance-Part1.pdf

National Emergency Supply Agency. (10. 5 2014). *Varmuuden vuoksi*. Accessed on 30 November 2014. Retrieved from HAVARO turvaa yhteiskunnan huoltovarmuuskriittisiä toimintoja:

http://www.varmuudenvuoksi.fi/aihe/huoltovarmuuden_toteutuksia/106/havaro_turvaa_yhteiskunnan_huoltovarmuuskriittisia_toimintoja

National Initiative for Cybersecurity Careers and Studies definition. (2014). *Explore terms: A Glossary of Common Cybersecurity Terminology*. Accessed on 1 December 2014. Retrieved from National Initiative for Cybersecurity Careers and Studies definition: http://niccs.us-cert.gov/glossary#letter_c

National Institute of Standards and Technology (NIST). (12. 2 2014). *Framework for Improving Critical Infrastructure Cybersecurity.* Accessed on 28 November 2014. Retrieved from National Institute of Standards and Technology: http://www.nist.gov/cyberframework/

OECD. (2004). Principles of Corporate Governance. Paris, France.

Oxford University Press. (2014). *Oxford Dictionaries*. Accessed on 30 November 2014. Retrieved from Oxford Dictionaries - cybersecurity: http://www.oxforddictionaries.com/definition/english/cybersecurity

PwC. (30. 09 2014). *The Global State of Information Security Survey 2015.* Accessed on 30 November 2014. Retrieved from PwC: http://www.pwc.com/gx/en/consulting-services/information-security-survey/download.jhtml

QuinStreet Inc. (2014). *Webopedia*. Accessed on 1 December 2014. Retrieved from Webopedia -Term - cybersecurity: http://www.webopedia.com/TERM/C/cybersecurity.html

Rice, D. C. & Bucholz, G. (2003). Methods of Auditing Applications. In H. F. Tipton & M. Krause, *Information Security Management Handbook, Fifth Edition* (pp. 1287-1294). The United States of America: CRC Press.

Roebuck, K. (2011). *Data Quality: High-Impact Strategies - What You Need to Know: Definitions, Adoptions, Impact, Benefits, Maturity, Vendors.* Emereo Pty Limited.

Saha, B. & Srivastava, D. (2014). Data Quality: The other Face of Big Data. *ICDE Conference 2014* (pp. 1294-1297). Chicago: IEEE.

Secretariat of the Security Committee. (2013). *Finland's Cyber security Strategy*. Accessed on 28 November 2014. Retrieved from Ministry of Defence: http://www.defmin.fi/files/2378/Finland_s_Cyber_Security_Strategy.pdf

Silic, M. & Back, A. (2014). Shadow IT - A view from behind the curtain. *Computers and Security* , 274-283.

Siponen, M. (2006). Information security standards focus on the existence of process, not its content. *Communications of the ACM , 49* (8), 97-100.

Steward, R. (2008). A framework for the life cycle management of information technology projects: ProjectIT. *International Journal of Project Management , 26*, 203-212.

System Experts. (2004). *National Security Agency (NSA) INFOSEC Assessment Methodod (IAM).* Accessed on 25 November 2014. Retrieved from System Experts: http://systemexperts.com/media/pdf/NSAIAM.pdf

Talburt, J. & Williams, T. L. (2014). Information Quality Research Challenge: Predicting and Quantifying. *ACM Journal of Data and Information Quality , 5*, 1-3.

Teixeira, A., Dán, G., Sandberg, H. & Johansson, K. H. (2011). A Cyber Security Study of a SCADA Energy Management System: Stealthy Deception Attacks on the State Estimator. *Proceedings of the 18th IFAC World Congress, 2011* (pp. 11271-11277). International Federation of Automatic Control.

The Atlantic Council and Zurich Insurance Group. (2014). *Beyond Data Breaches: Global Interconnections of Cyber Risk.* Zurich: Atlantic Council & Zurich Insurance Company.

The Department for Business, Innovation and Skills (BIS) - Gov UK. (2013). *Information securities breaches survey 2013.* Accessed on 30 November 2014. Retrieved from The Government of UK: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/200455/bis-13-p184-2013-information-security-breaches-survey-technical-report.pdf

the European Commission, Directorate-General Home Affairs. (2013). *Special Eurobarometer 404 - "Cyber security".* the European Commission.

Tondel, I. A., Line, M. B. & Jaatun, M. G. (2014). Information security incident management: Current practice as reported in literature. *Computers & Security , 45*, pp. 42-57.

Trope, R. L., Power, E. M., Polley, V. I. & Morley, B. C. (2007). A Coherent Stratety for Data Security through Data Governance. *IEEE Security and Privacy* , 32-39.

UK Government - Department for Business Innovation & Skills. (2013). *2013 Information Security Breaches Survey.* Accessed on 28 November 2014. Retrieved from UK Gov: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/200455/bis-13-p184-2013-information-security-breaches-survey-technical-report.pdf

Walters, R. (2013). Bringing IT out of the shadows. *Network Security* (4), 5-11.

Wang, R. Y., Lee, Y. W., Strong L, P. & Strong, D. M. (15. 07 1998). *Manage Your Information as a Product.* Accessed on 30 November 2014. Retrieved from

MITSloan Management Review:
http://sloanreview.mit.edu/?content_type=research-feature

Webb, J., Atif, A., Maynard, S. B., & Shanks, G. (2014). A Situation awareness model for information security risk management. *Computer and Security , 44*, 1-15.

Wikipedia. (26. 11 2014). *Wikipedia - Corporate governance*. Accessed on 4 December 2014. Retrieved from Wikipedia:
http://en.wikipedia.org/wiki/Corporate_governance

von Solms, B. & von Solms, R. (2004). The 10 deadly sins of information management. *Computers and Security , 23*, 371-376.

von Solms, S. (2005). Information Security Governance Compliance management vs operational management. *Computers & Security , 24*, 443-447.

Yle News. (3. 3 2014). *Uutiset.* Accessed on 30 November 2014. Retrieved from Yli 600 punaista hälytystä verkkohyökkäyksistä – kohteena tärkeimmät yritykset:
http://yle.fi/uutiset/yli_600_punaista_halytysta_verkkohyokkayksista__kohteena_tarkeimmat_yritykset/7117056

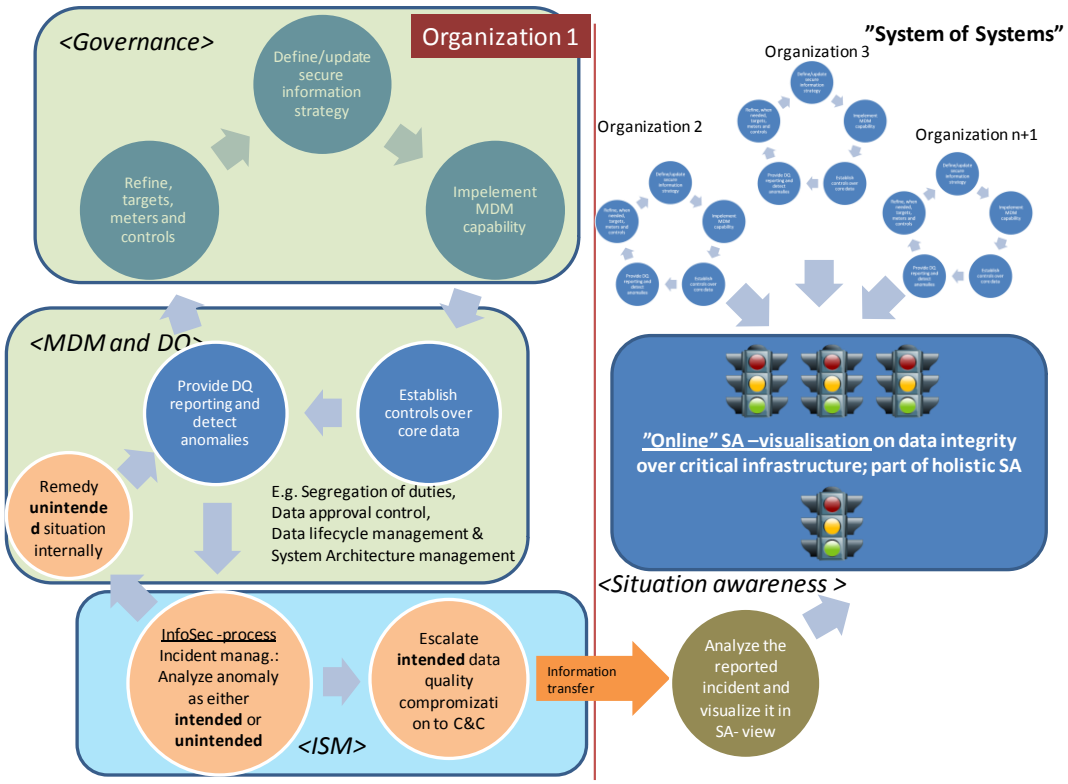
APPENDIX I - INTERVIEW SLIDES

Von Solms – Information Security – The Fourth Wave

- **1st wave:** "was characterized by Information Security being a technical issue, best left to the technical experts"
- **2nd wave:** " was driven by the realization that Information Security has a strong management dimension, and that aspects like policies and management involvement are very important"
- **3th wave:** "consisted of the need to have some form of standardization of Information Security in a company, and aspects like best practices, certification, an Information Security culture and the measurement and monitoring of Information Security became important"
- **4th wave (2006)** "This wave relates to the development and crucial role of Information Security Governance [...] drivers behind this Fourth Wave are closely related to developments in fields of Corporate Governance and the related legal and regulatory areas. Top management and Boards of Directors felt the heat as they started to become personally accountable for the health (read Information Security) of their IT systems on which they base their planning and decisions"

Threat description

- **Persistent Stealthy deception attack**, where organization's (and its supply and value chain's) data - critical operational and tactical assets - is silently degraded over longer period of time.
- Attack is advanced and targeted in nature and does not:
  - present e.g. significant network traffic trail
  - does not communicate with C&C servers,
  - nor create abnormalities in WLAN usage etc.,
- It masquerades itself as "normal user activity".
- Detection of the threat is difficult due to its silent nature and non aggressive attack philosophy.
- Characteristics of the attack, once threat either is detected by security measures or users' reports (strange data changes etc) or in an orchestrated larger scale attack on larger critical infrastructure composition (multiple parties of critical infrastructure affected by the threat realization), where threats existence becomes obvious, makes it dangerous:
  - Parties involved possibly could not, with required certainty, reference the point in time, the attack started, making back up recovery and business continuity challenging tasks.
  - Even though the degraded data could be identified and fixed, the impact to victim organization could still prove out to be enormous.


<Governance>
Define/update secure information strategy
Impelement MDM capability
Refine, targets, meters and controls
Organization 1
<MDM and DQ>
Provide DQ reporting and detect anomalies
Establish controls over core data
Remedy unintended situation internally
E.g. Segregation of duties,
Data approval control,
Data lifecycle management &
System Architecture management
InfoSec -process
Incident manag.:
Analyze anomaly as either intended or unintended
Escalate intended data quality compromization to C&C
<ISM>
Information transfer
"System of Systems"
Organization 3
Organization 2
Organization n+1
"Online" SA –visualisation on data integrity over critical infrastructure; part of holistic SA
<Situation awareness >
Analyze the reported incident and visualize it in SA- view

APPENDIX II – INTERVIEW FRAME

Basic information

- For the background of the data collection

ISM, Information management or security -experience

- For the background of data collection

Theme Cyber

- Difference between cyber security and cyber defence
- Cyberdefence defined
- Do cybersecurty and information security differ in which parts
- In a context of single company not CISP – what is cybersecurity and its relation to traditional ISM
- Von Solm's 4 waves –where are we riding as a nation
- How'd you perceive Finland's national cybersecurity capability
- What have been 2014' topics of discussion or relevance
- What about 2015

Theme Environment

- How'd you describe CISP's capability to govern and manage their information
- Do CISPs know what their info assets are
- Do they know where they reside
- Do they know the critical information apart from whole asset
    - How do yousee previous in context of data volumes arise
    - Where should the effort thus be on information based model or technology based model and why so

- What is CISPs capability to estimate their critical informations' quality e.g. consistency, CIA or other metrics on objective level?
    - How does this capability change (if it does) when moving in the supply/value chain?

Theme Resources usage

- Where is the bias currently – on technology defences building or managing the information and its security directly
- Do the CISP have what possibilities and capabilities defending their perimeters
- Where should the limited resources directed to

Theme Information and information security

- Definition information security
- Definition data quality
- How do you perceive information of good quality, characteristics etc
- Is the action to perceived information quality reactive or proactive by nature
- How do you see information quality in crisis situations
- What is the perceived efficiency of ISM in CISPs
- How situation aware CIPS are of their DQ
    - What about their supply chain partners DQ
- What is the relevance of information security policies and its effectiveness to operations
- Where should ISM and ISG reside in organizations for maximum efficiency and effectivity
- How important do you perceive information ownership
- What about ownership of information security
- Do you perceive ISM and IM as overlapped and if, on what parts
- Are they operating better separated or united and why so

- Could the functions receive synergy form uniting them for central parts if so, what synergy – what problems would arise
-

Theme: Situation awareness

- What is SA
- What is relevance of SA in F's Cyber strategy
- What is its relevance to operations via cyber strategy
- What could be the role of information quality in a SA, if the CISPs could transfer DQ information between them and cyber command or even among each other
- What value would it present
- Whast obstacles
- How could capability like this expand e.g. HAVARO concept
- Presented with the model and threat description how'd you describe
    - The relevance of the model as something solving an existing or future problem
    - Novelty of the model – have you seen similar concepts
    - What value could the model bring for SA
    - Should the model be researched further, e.g. do you see potential or should it remain as academic study
    - How much researched this topic is in genera
    - What requirements would you present to the model to be developed
    - What obstacles must it overcome