LAUREA
UNIVERSITY OF APPLIED SCIENCES
Together we are stronger

Security Management systems for global high technology corporation, case Wärtsilä corporation.

Sarkkinen, Perttu

2016 Laurea Leppävaara

Laurea University of Applied Sciences
Leppävaara

Security Management systems for global high technology corporation, case Wärtsilä corporation

Perttu Sarkkinen
Degree programme in Security Management
Master's Thesis
January, 2017

Laurea University of Applied Sciences
Leppävaara
Degree Programme in Security Management

Abstract

Perttu Sarkkinen

Security Management systems for global high technology corporation, case Wärtsilä corporation

Year 2017 Pages 54

The thesis aims to research what would be suitable security management system for the case corporation. The research is done on qualitative methods as a case study to solve the specific research question in the specific context.

On the first chapters of the thesis the organization of the case corporation will be evaluated while also establish general context of risk, security management and management systems. In the theoretical part several security management systems will be evaluated and their usefulness and applicability to the case corporation are assessed. Also literature regarding risk and security management will be used as a secondary material to create basis for later chapters.

On the second phase of the thesis information will be collected from the assessed key members of the organization with theme interviews, which will focus on their viewpoints of risk and security management and especially to understand their internal customer focus for security management. This information is the primary material of the thesis, which is analyzed in combination with the secondary material, the information of security management systems and how they are implemented in different organizations and situations.

The conclusions will be divided to two main concepts; firstly what would be the correct management system or combination of management systems that would best suit the case corporation in advancing security management and secondly what kind of organization model is required for effective implementation of the proposed management systems.

The thesis conclusions and results can be repeated and generally applied in similar corporations or organizations however bearing in mind the local and organizational specific limitations and especially the type of the organization.

Security, Security Management, Management Systems, Standards, Risk Management, Corporate Security, Information Security, Security Awareness, Security Culture, Authorized Economic Operator

Laurea-ammattikorkeakoulu
Leppävaara
Turvallisuusjohtamisen koulutusohjelma

Tiivistelmä

Perttu Sarkkinen

Security Management systems for global high technology corporation, case Wärtsilä corporation

Vuosi 2017 Sivumäärä 54

Tässä opinnäytetyössä tutkitaan tapaustutkimuksena case yritystä ja etsitään sille sopivaa yritysturvallisuuden johtamisjärjestelmää. Tutkimus toteutetaan laadullisena tutkimuksena, jossa tapaustutkimuksen keinoin ratkaistaan tietty ongelma rajatussa kontekstissa.

Ensimmäisessä kappaleessa esitellään tutkittava yritys ja sen organisaatio. Samalla esitellään yleisesti käsitteet riskistä, turvallisuusjohtamisesta ja johtamisjärjestelmistä. Edelleen teoreettisessa osuudessa arvoidaan useampaa turvallisuuden johtamisjärjestelmää ja arvioidaan niiden hyödyllisyyttä ja soveltuvuutta tutkittavan yrityksen käyttöön. Kirjallisuutta riskienhallinnasta ja turvallisuusjohtamisesta käytetään toissijaisena kirjallisuuslähteenä, johon myöhemmissä kappaleissa tullaan viittaamaan.

Tutkimuksen toisessa vaiheessa toteutetaan teemahaastattelut valituille avainhenkilöille tutkittavasta yrityksestä ja kerätään tällä tavoin tutkimuksen pääaineisto, joka muodostuu haastatteluista. Haastatteluihin valitaan erityisesti henkiöitä, joilla on näkemystä ja ymmärrystä turvallisuusjohtamisesta tai riskienhallista sekä erityisesti sellaisia henkilöitä, jotka ovat turvallisuusorganisaation suunnasta sisäisiä asiakkaita. Aineistoa analysoidaan ja yhdistellään teoreettisiin kirjallisuuslähteisiin turvallisuusjohtamisjärjestelmien toteuttamisesta erilaisissa organisaatioissa ja tilanteissa.

Johtopäätöksissä käsitellään kahta pääkokonaisuutta, ensimmäisenä mikä tai mitkä turvallisuuden johtamisjärjestelmät soveltuvat parhaiten tutkittavalle yritykselle ja kehittävät turvallisuusjohtamista ja toisena minkälainen organisaatio tarvitaan tällaisen johtamisjärjestelmän luomiseen.

Tutkimuksen johtopäätökset ja tulokset ovat toistettavissa ja yleistettävissä samankaltaisissa organisaatioissa, mikäli toistettaessa tai yleistettäessä ymmärretään ottaa huomioon eroavaisuudet ja organisaatioiden vaihtelu esimerkiksi paikkakuntien, organisaation rajoitusten tai liiketoiminnan luonteesta johtuen.

Security, Security Management, Management Systems, Standards, Risk Management, Corporate Security, Information Security, Security Awareness, Security Culture, Authorized Economic Operator

Table of contents

1 Introduction

Purpose of the thesis is to study various security and risk management systems, compare and understand their management aspects and differences and find a suitable management system or combinations of management systems to find a comprehensive security management system with case study method to high technology corporation, Wärtsilä Corporation.

First part of the thesis will focus on theoretical review of risk and security management systems and literature of risk, security and management systems itself. After the theoretical base has been formed with understanding of the advantages and disadvantages of different risk and security management system, the thesis will present the case organization, Wärtsilä Corporation in brief.

Second part of the study aims to create a plan for implementation of how and in what order should the management systems to be implemented into the corporate management and what are the key elements in the implementation plan. The actual implementation will be limited out of the scope of this thesis.

After the brief introduction of Wärtsilä Corporation and analysis of the selected security management systems in relation to operations of the case corporation the author will advance on collecting information from selected stakeholders and decision makers of the case corporation. The interviewees will be chosen by their position and possibility to influence security decisions or they are internal customers for security function. Information collection method will be theme interview. Theme interview is semi structured method of interviewing the subject with the possibility to change the order and wording of questions depending on the theme of the interview, where one of the greatest advantages of theme interview is the possibility for deeper interaction between the researcher and the subjects. (Hirsjärvi & Hurme 2000, 47 - 48.)

The interview will focus on the subjects of risk and security management systems and target of the interview is to gain information from different corporations with similar management systems and to understand what the different aspects of different system or standards are. Secondly the interview is designed to gain insight and opinions from the top risk and security executives what would their choice for the management systems be, and why.

The theme interview focus on the subjects of risk and security. The author will try to establish the internal customer viewpoint on earlier mentioned management systems and try to understand what internal customers, the corporation leaders, expect from risk and security management.

Finally after analyzing the primary material, the thesis will move on to conclusions, which will contain a proposal of risk and / or security management system and organizational model proposals for Wärtsilä Corporation and brief description on how the management system could be built.

1.1 Background of the thesis

The need for the thesis was identified on many of the following facts. Wärtsilä Corporation hasn't had a systematic global security management system so far and there hasn't been any global resources until 2015 designated to be responsible of security; country organizations have instead had the responsibility to organize security management on their own without corporate guidance or requirements.

Second background of the thesis derives from risk management perspective and as risk and security literature often suggest that security management is actually functionally corporate risk management. However the current management setup in Wärtsilä Corporation doesn't too strongly support this view and the author's hypothesis is that after studying the management systems there is significant synergy available in combining risk and security management more closely together.

1.2 Previous research in the field

The recent research in risk and security management system has been numerous in the past few years. Most often the studies have been made as either as case studies or general overview of the standards and management systems for risk and security.

There has been numerous doctorate level theses and academic publications regarding corporate security and management system and many of them are relevant as sources and referrals to this thesis.

Marinka Lanne has written doctoral thesis on "Co-operation in corporate security management (2007)" where she researched and described elements of communications, security culture and roles and responsibilities of different organizational functions. The doctorate thesis is likely to be useful source for this thesis due to its nature on creating corporate risk and security management models.

Kalevi Mäkinen wrote doctoral thesis on strategic security and strategic security model on 2005. The thesis itself doesn't provide information to this thesis in the theoretical or man-

agement system aspect, but it provides interesting viewpoints on research methodology and how for example theme interviews were conducted in large scale and how the results were applied (Mäkinen, K. 2005, 158 - 161). Also the connection presented in the thesis between security and the organizations strategy is interesting while deliberating management systems.

The following bachelor thesis' are the most relevant from this thesis point of view and therefore are shortly reviewed. They are included in the review due to their relevance in security management system study.

Esa Kukkonen has made a bachelor thesis for security management systems for Vacon Corporation and chose ISO 28 000 and supply chain security point of view in the thesis. (Kukkonen, E. 2015.) Some of the viewpoints presented are likely to be at least partially applicable in this thesis, since there are similarities within Vacon and Wärtsilä corporations. Both corporations have significant volumes on international supply chain and therefore security of the supply chain should be of specific interest in risk and security management.

Mika Karjalainen has studied information security management systems in his bachelor thesis for Laurea 2014. The approach for his study was to understand the level of information security in Finland as a literature study and understanding information security as a phenomena. (Karjalainen M, 2014)

Joel Ruippo's bachelor thesis is a case study of creating risk management system for The Governing body of Suomenlinna and it describes the process to create four different management plans for the organization (Ruippo, J. 2015). As the governing body for specific differs so greatly from large global corporation, it is likely that the conclusions aren't applicable in this case study.

1.3 Objectives and limitations of the study

First and most important objective of the thesis will be to understand what kind of or combinations of security management system or standard will suit the target organization. Second as important objective is to describe an implementation plan how the management system should be built and give out scenarios what kind of organizational structures and resourcing would be suitable to support in the implementation.

Third objective is create a link between risk and security management, however the risk management systems will be studied very briefly in comparison to security management systems and the focus is to take ISO 31 000 related risk management terminology for granted and apply them in relation to security management.

Wärtsilä Corporation has long traditions in quality, health, safety and environmental management and therefore all management systems and aspects of quality, health, safety and environment management are excluded from the scope of the thesis. Only exception to this exclusion is the general similarities that are common to all management systems in the top context.

As Wärtsilä has operations in over 200 locations in more than 70 countries around the world and therefore all national and local management systems will be limited out from the scope of the thesis and the focus will be on internationally recognized security management systems. Regional management systems will be included only in supply chain security, because of its relevance to the corporation.

Finally a top level corporate implementation plan with few organizational models will be presented in the conclusions, anything related to the actual implementation will be limited out of the scope.

1.4 Crucial concepts and terminology

The most crucial concepts and terminology during course of the thesis will be explained and reviewed in brief in this chapter. As management systems and risk management vocabulary is relatively standard and cohesive throughout the international standard industry, the definition of security will vary depending the source.

Edward Borodzicz (2005, 50) considers the term security in two contexts, either freedom from danger, or a show of force (or strength), able to respond to or deter threats. Another widely used term for security is resistance to intentional, unauthorized act(s) designed to cause harm or damage to, or by, the supply chain (ISO 28 000 2007, 2).

Risk is the most established of the concepts presented on this thesis and most commonly used term and methodology of risk is that risk is related to the uncertainty of outcome or effect of uncertainty of objectives (Hopkins, P. 2012, 13) and (ISO 31 000 2009, 1).

Risk is often used also in negative context to describe the negative outcome (Hopkins, P. 2012, 3), which often applies when thinking risk in security management context. However it should be clear that when establishing mind set for corporate risk management program, the possibility of positive outcome in risk management should not be disregarded. Positive aspects and understanding business operation as a risk which can have positive outcome must also be considered. (Ilmonen, I., Kallio, J., Koskinen J., & Rajamäki, M. 2013, 15).

Most used definition of security management in the scope of this thesis is that security management is coordinated activities and practices through which an organization optimally manages its risks and the associated potential threats and impacts therefrom. (ISO 28 000 2007, 2)

Information security is very specific part of security, but due to the nature of the thesis and case corporation, the concept earns to be explained separately. Information security is according to ISO 27000 (2014, 4) preservation of confidentiality, integrity and availability of information.

1.5 Research and information collection methods in the study

The thesis will be conducted in qualitative methods. The selected method for the thesis will be case study, since the thesis is aiming to understand specific problem in specific context. Case study is often used in this type of thesis. (Kananen, J. 2015, 76).

Information will be collected in few major methods, first part of the thesis will concentrate on literature review and analysis of selected security and risk management systems and literature addressing security and risk management.

Second part of the thesis will be conducted as a theme interview to selected target group. Theme interview is one of the major methods of information collecting in qualitative research (Kananen, J. 2015, 131). These interviews will form the primary material for the thesis and the primary material will be interpreted in reflection to the results of the literature review. In addition to the interviews, author's observations will be another, yet more subjective part of the primary material. As Kananen, J (2015, 132) states, observation isn't always enough since interpretations made by the author can be misleading.

After the collected primary information has been analyzed, the information will be combined with secondary material, which mainly consist of management systems and literature in security management. After the final analysis conclusions and possible solutions will be presented in the final part of the thesis which will answer the research questions:

- What or which management systems would be best suitable for the case study corporation globally?
- What kind of organizational model would best support the management systems?

One of the major questions in qualitative research and specifically in case study where the author tries to create understanding of the interviews and views or other people, while reflecting in from his personal subjective view? Since the importance of people actions, their

choices and part to play in the organization will be crucial in the theme interviews, it can be said that “Aristotle point of view” will be used in the thesis to emphasize the meaning of subjectivity in the choices of the people. (Tuomi, J. & Sarajärvi A., 2009, 27-30 and 68-70)

2 Wärtsilä Corporation

Wärtsilä Corporation consist of three business divisions, Energy Solutions, Marine Solutions and Services. Wärtsilä had net sales of 5 029 Million Euros with operating result of 12.2 % or 612 Million Euros during 2015 and Wärtsilä employed 18 856 persons at the end of fiscal year 2015. Wärtsilä has operations in over 200 locations in more than 70 countries around the world (Wärtsilä Annual report 2015, 5-6).

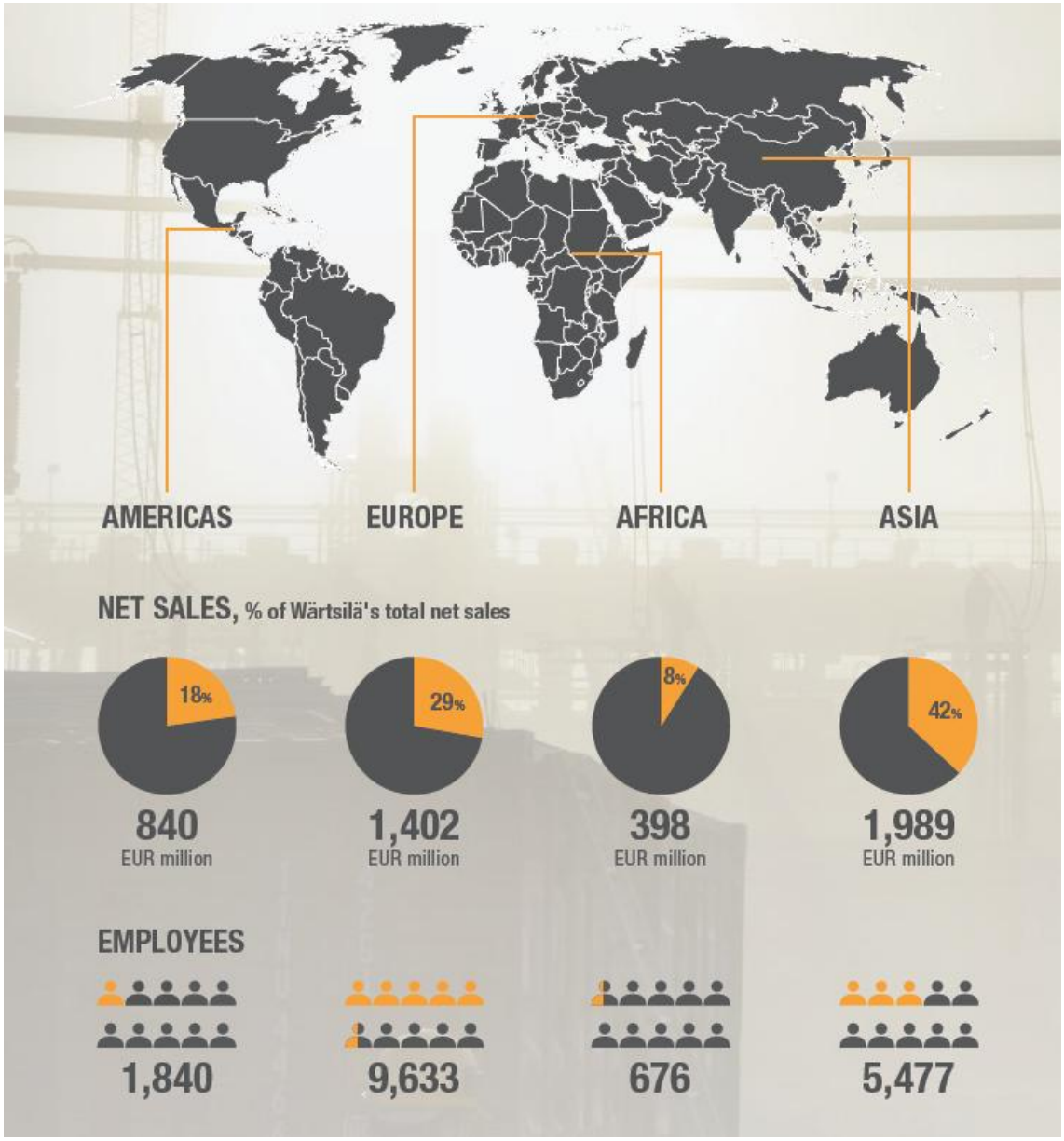

Figure 1 Wärtsilä global reach in brief, with personnel and net sales divination to global areas.

As the case corporation has numerous locations in different countries, cultures and environment, first rule of success for management system is, that they should be on very general level on the highest level. The global level should be on creating corporate policy on management and creating guidelines, directives and boundaries which global business units can follow.

Corporation can choose the level of internal control and management on specific part of management by establishing and implementing management system, directive or way of working for the corporation to follow.

2.1 Corporate Strategy, Sustainability & Management

The case corporation aims at profitable growth by providing advanced technologies and lifecycle solutions to its marine and energy market customers. Wärtsilä aims strongly to profit from digitalization and continue to stay on top of the technological competition in marine and energy markets, while also offering top of the line service network for the markets. (Wärtsilä annual report 2015, 6).

Wärtsilä operates with three business divisions; Energy Solutions, Marine Solutions and Services; which all have end to end responsibility of their profit and loss targets and can execute decisions on all levels with little corporate control from HQ. Generally the corporate framework is in place only for selected management systems or functions where for example Information Management is one of them.

Wärtsilä has wide listing of sustainability tools and policies in place which include for example: “Code of Conduct, QEHS policy, Anti-corruption, compliance reporting and many more”. In systems and processes mentioned are Quality Management, Environmental Management, Occupational Health and Safety and finally Supplier Management Systems. Proportion of Wärtsilä legal entities with management systems are 82% on quality, 66% on environment and 65% on occupational health and safety. (Wärtsilä Annual report 2015, 69-70)

Risk management is mentioned only as risk management processes at sustainability and it clearly reflects that risk management is placed in different part of the organization that management systems.

Security Management is mentioned only briefly with one paragraph which states only six sub-categories of security management, but doesn't contain any management system, goals or objectives for the security management system. It is also stated that security is done on the business and local level, but in practice this has been obviously voluntary at local or business level. (Wärtsilä Annual report 2015, 77)

Risk and Security management which are the main focus for this thesis are currently dispersed or fragmented and only recently the case corporation has taken slight interest in developing globally unified risk or security management systems or guidelines.

Case Corporation should have specific interest in supply chain and managing risks and security supply chain due to the nature of the business, main focus still comes from two activities, bringing services and spare parts to the customers at their chosen location or main assembling engines at production facilities from numerous supply sources and delivering them to customer at their designated location.

2.2 Risk and Security management

Case Corporation states that risk management is in place to ensure that the corporation can effectively execute strategy and reach set targets. Risk Management actions listed are either to avoid, mitigate, transfer or monitor identified risks. (Wärtsilä Annual report 2015, 145-146)

Risk Management actions at the case corporation follow quite widely accepted 4T methodology, where the four T's stand for Tolerate, Treat, Transfer and Terminate. (Hopkins, P. 2012, 225 - 226)

Case Corporation also states that its risk management vocabulary and methodology for risk management is in large extent conforming to ISO 31 000:2009 standard on risk management.

Risk radar 2015 is listed on the following picture.

Figure 2 Risk Radar 2015 (Wärtsilä Annual Report 2015)

At short listing in security related risks are found under hazard segment of risk mapping, which include personnel security risks, fire, cargo and other accidents and finally information and cyber security risks. At the same the list of risk management processes states that all management systems in place are protective methods in risk management. (Wärtsilä Annual report 2015, 151-152)

Information and cyber related risks management are explained briefly by stating that cyber security governance model is tied together with traditional safety and security functions with cyber security operations (Wärtsilä Annual report 2015, 155), however it is clear that there is no management system in place for information or cyber security related risks and the management is on fragmented level. This seems contradicting with objectives of the corporation since it is stated that information and automation related risks have exceeded physical and personnel risks even though Wärtsilä operates on over 200 locations on 70 countries. (Wärtsilä Annual report 2015, 6 and 155)

Finally on security management point of view, the risk management doesn't explain what the mentioned physical or personnel risks are, expect on side note with travel security measures which seems to derive on idea that travelling is risk for Wärtsilä, as this was also mentioned in the six categories of security. Also it is describing that in risk management section premises safety is mentioned as one of the control methods under personnel risks. (Wärtsilä annual report 2015, 158)

Short conclusion based on analysis of the security management in the case corporation is, that there isn't any corporate framework, organization or policy in place on corporate level that would guide the organization, set requirements or management commitment in security

management, but instead it is just stated that security is run in businesses or locally. From internal control point of view, the corporation does not know how security is being managed across the different sites and locations.

3 Risk Management

First and foremost in this thesis a general assumption will be carried throughout the thesis that security management or corporate security should be considered as a risk management process or management process of an organization. Secondly the risk management aspects shall be handled extremely briefly in this thesis and only to link security management and risk management together. All further risk management aspects are limited out of the scope in the thesis.

When thinking the risk and security management, enterprise risk management content will be the main approach due to the nature of case Corporation already selected risk management approach, large size and global nature of the organization. (Hopkin, P. 2013, 42-43)

Generally in enterprise risk management there should be three elements present:

1. Description of the process that underpins the enterprise risk management
2. Identification of output of that process
3. The impact (or benefit) that arises from these outputs

(Hopkins, P. 2013, 225-226)

Secondly the enterprise risk management approach can be combined with ISO framework whose purpose is to integrate the process for managing risk into the organization's overall governance, strategy and planning, management, reporting processes, policies, values and culture. (ISO 31 000:2009 E, V).

Finally the risk management actions at the case corporation follow quite widely accepted 4T methodology, where the four T's stand for Tolerate, Treat, Transfer and Terminate. (Hopkins, P. 2012, 225 - 226) Therefore in risk management this type of approach is applicable and feasible choice in this particular case study, to solve the case study problem at hand.

4 Management Systems

The thesis is following general principles of management systems that are established on "plan do act check" methodology.

- Plan: establish the objectives and processes necessary to deliver results in accordance with the organization's security policy.

- Do: implement the processes.
- Check: monitor and measure processes against security policy, objectives, targets, legal and other requirements, and report results.
- Act: take actions to continually improve performance of the security management system.

(ISO 28000:2007, VI)

Management system is described as set of interrelated or interacting elements of an organization to establish policies, objectives and processes to achieve those objectives. The scope of the management system can be whole organization or just a part of it. (ISO 27000:2007, 6)

Purpose of this chapter is to map relevant management system for the case corporation and while doing so keep in mind what could be the benefits and implications the management systems would bring to the organization. The thesis will review most applicable pre-selected security management systems from the case corporation point of view, ISO 28 000 and Authorized Economic Operator (AEO) for general security management and security management in supply chain and finally ISO 27 000 for information security management.

4.1 Security Management system - ISO 28 000

Definition and scope of security management system according to ISO 28 000:2007E standard is: "This International Standard is applicable to all sizes of organizations, from small to multinational, in manufacturing, service, storage or transportation at any stage of the production or supply chain that wishes to:

1) establish, implement, maintain and improve a security management system;
2) assure conformance with stated security management policy;
3) demonstrate such conformance to others;
4) seek certification/registration of its security management system by an Accredited third party Certification Body;
   Or
5) Make a self-determination and self-declaration of conformance with this International Standard."

In other words, security management systems are management systems which ensure that certain corporate objectives are met. As stated earlier in the case corporation chapter, the case corporation hasn't had so far any specific interest to develop security or risk management through management system, unlike for example in quality, safety and environment.

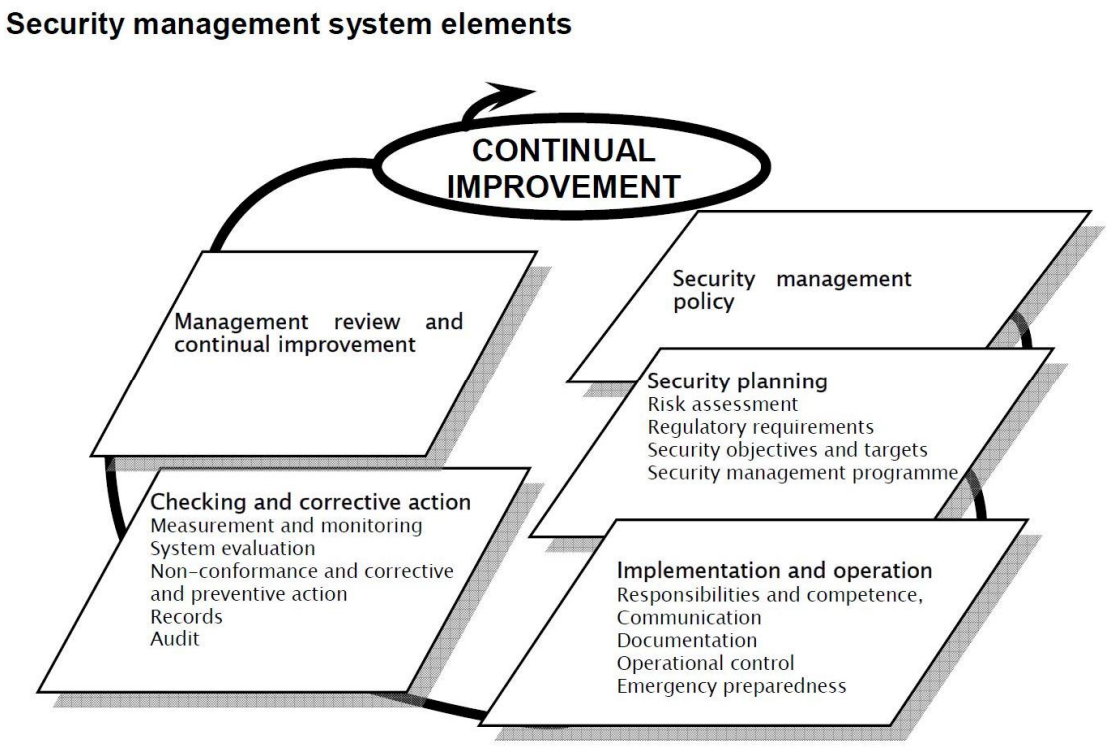

Figure 3 Security management system elements (ISO 28000:2007E, 3)

4.1.1 Security Policy

Setting suitable security policy for the organization is one of the key elements in management system to define, communicate and visibly endorse top management commitment to the policy. The policy must provide framework for security management objectives, targets and programs and be consistent with the overall security threat and risk management framework. The policy must also clearly state overall security management objectives and include commitment to continual improvement of the security management process. (ISO 28000:2007E, 4)

Wärtsilä security policy has not been publicly stated, even though its existence is mentioned in the annual report (Wärtsilä annual report 2015, 77). The policy exists in internal communications material and the policy is: "Security in Wärtsilä is the responsibility of all personnel. The security objective is to obtain a business environment for Wärtsilä, which is without interference and to guarantee a continuity of the business" (Wärtsilä Corporate Manual chapter 17, 2015, 1)

One observation from the author is clear when comparison is made between quality, health, safety and environment policies against security policy; there are numerous plaques, noticeboards and statements visible around case organization public and internal premises where top management commitment to quality, health, safety and environment are clearly stated and presented visibly, while for security policy there are none. The lack of actual implemen-

tation of public statement and endorsement of security policy makes it obvious that there isn't security management system in place in the case organization.

The first and foremost role of the top management of the organization is to decide commitment, resources, targets and policies for the organization. (Kerko, P. 2001, 44) In the case organization the top management should first focus on setting the commitment, roles, resources and targets for the organization. Abovementioned are the first steps in implementing the security policy in the organization. However current security policy should be reviewed before these in the organization, since the current policy states that security is responsibility of everyone and quite often this kind of statements leads to a situation that no one is actually responsible.

Implementing security policy will require tangible and concrete actions from the top management and security must be integrated to the business management with terminology and terms that are applicable to the organization and its business. Implementation requires strategic terms for security and at least following should be described: Principles for security in the organization, critical success factors for security, security policy, concrete goals and targets and finally actual action plan for security. (Kerko, P. 2001, 45)

When defining security related policies, they should be defined by few most important categories. For Case Corporation the categories should be at least general security policy, information security policy, cyber security policy for corporation end products and travel and premises security policy. (Kerko, P. 2001, 46)

4.1.2 Security risk assessment and management

Second part of security management system element is establish and maintain processes for security risk assessment, in order to identify, assess and manage security related threats and risks that are relevant for the organization. The system must be designed for the organization and take into account what is relevant for the organization and to understand what risks threaten the business operations. (ISO 28 000: 2007E, 4)

The security risks assessment results are used in creating security management program with objectives and targets for security and assist the organization in designing specifications and requirements for the organization security management system. The security risk assessment should provide input for the organization to identify what resources and staff is needed for security management and finally also to identify training needs and required skills for the organization. (ISO 28 000:2007, 4-5)

All the security risk assessment elements and results must be documented and kept up to date for the adequate control of the management system. (ISO 28 000:2007, 5)

Security risk assessment is the most vital and suitable tool for creating corporate security information and large part of decisions related to security should be based on security risk assessment information. (Kerko, P. 2001, 57) Designing suitable security risk management system for the case corporation requires that the risk management will be done on several organizational levels.

One possible solution for the case corporation is to manage security in three layers;

1) Corporate wide top level where risks and targets are followed globally by top management.
2) Business operations level, where risks and targets are followed at business division level by business stakeholders or area ownership level, where these are monitored regionally
3) Local level, where risks and targets are followed locally with hands on perspective to physical surroundings and local aspects.

This solution would ensure that the case corporation will take into account relevant objectives, requirements and specifically allow the views and requirements of the business stakeholders. The solution would also be compliant with the management system requirements for optimized and prioritized system and allow designating appropriate authority and responsibility for security management objectives and targets and finally state the means how the targets are to be achieved. (ISO 28 000:2007, 6)

4.1.3 Operational structure and implementation

The case corporation will need to establish and later maintain organizational structure of roles, responsibilities and authorities that are consistent with the earlier set security management policy, objectives and requirements in order to successfully implement the security management system. The system must contain at least following documented elements:

1) Appoint member from top management who is responsible for overall design, maintenance, documentation and improvement of the security management system.
2) Appoint member(s) of management with the necessary authority to ensure that the objectives and targets are implemented.
3) Identify and monitor the requirements and expectations of the organization's stakeholders taking appropriate and timely action to manage these expectations.
4) Ensure the availability of adequate resources

5) Consider the adverse impact that the security management policy; objectives, targets, programs may have on other aspects of the organization,
6) Ensure any security programs generated from other parts of the organization complement the security management system.
7) Communicate to the organization the importance of meeting its security management requirements in order to comply with its policy.
8) Ensure security-related threats and risks are evaluated and included in organizational threat and risk assessments, as appropriate.
9) Ensure the viability of the security management objectives, targets and programs.

(ISO 28 000:2007, 7)

As the case corporation expands all continents with over 200 locations, implementation of security needs specific attention from the corporation and it will require specific attention to several targets in order to meet the targets. The solution provided for the case corporation must have several enterprise wide dictated elements that are always implemented globally in a same manner, all the time, all locations. When these elements of the program are implemented there are also local and business wide elements as well, that are implemented locally and can wary between the locations, according to the security risk assessment results locally.

4.1.4 Internal monitoring and auditing

The case corporation must monitor and measure the performance of the security management program. Monitoring must contain elements to that help to measure how security management policy, targets and objectives are met. Organization should monitor and measure both proactively and reactively how security management system is performing and how changes in legal, statutory or other regulatory requirements will affect the system. (ISO 28 000:2007, 10)

The audit program, including any schedule, shall be based on the results of threat and risk assessments of the organization's activities, and the results of previous audits. The audit procedures shall cover the scope, frequency, methodologies and competencies, as well as the responsibilities and requirements for conducting audits and reporting results. (ISO 28 000 2007, 11)

Security management must contain audit program in order to be compliant with management system requirements and the audit program should be where possible, audits shall be conducted by personnel independent of those having direct responsibility for the activity being examined. (ISO 28 000 2007, 11)

The independence requirement does not require the person to be external for the organization (ISO 2007, 11). From management point audits are beneficial to be divided into internal and external audits, since the management scope can be quite different.

When creating organizational model for global security management, the auditing must be organized so that it can audit the requirements that derive not just only from the management system point of view but also ensure that the business requirements to security managements are fulfilled. This will be one of the many major points that should dictate the organizational model when considering actual implementation and resourcing the case corporation security management system.

4.1.5 Management review

Top management of the organization must review the management system at decided intervals in order to ensure suitability and effectiveness of the system and also to periodically review improvement opportunities and need for changes for the security management system. (ISO 28 000 2007, 12) Management reviews are great opportunity for the organizations top management to show commitment for the management system and see the status of the security performance of the organization.

In addition to formal security management system compliant management reviews, the presence and personal commitment of top management is needed more often as the requirements for security management are increased. Organizing reviews, security walks and other means enabling visible presence and interest of the top management towards security are necessary to positively affect security culture in the organization. (Kerko, P. 2001, 27)

Organizing suitable management reviews and showing commitment in case corporation will be vital to the success of the security management system due to diverse and complex nature of the case corporation. Since the organization is in multiple parallel matrixes setting responsibilities and showing management commitment for security management are crucial for success of the program.

4.2 Security Management system - Authorized Economic Operator (AEO)

The Authorized Economic Operator (Further AEO) concept is based on the Customs-to-Business partnership by World Customs Organization. The concept is to create partnership between companies and customs official to together ensure security of the supply chain and follow principles of mutual transparency, correctness, fairness and responsibility. The European Un-

ion established its AEO concept based on internationally recognized standards (Authorized Economic Operator Guidelines, 2016, 8)

The AEO program is open to all economic operators including small and medium sized enterprises and regardless of their role in international supply chain. The AEO status itself consists of two different types of authorizations; AEO for customs simplifications (AEOC) and AEO for security and safety (AEOS). (Authorized Economic Operator Guidelines, 2016, 9)

AEO contains following common requirements:

- Record of compliance with customs legislation and taxation rules, including no record of serious criminal offences relating to the economic activity of the applicant
- Demonstration of a high level of control of its operations and of the flow of the goods, by means of a system of managing commercial and, where appropriate, transport records, which allows appropriate customs controls,
- Proven financial solvency.

Requirements depending the type of AEO status:

- practical standards of competence or professional qualifications directly related to the activity carried out (AEOC),
- Appropriate security and safety standards (AEOS).

Finally the AEO status granted by any member state of the EU is recognized by the customs authorities in all member states and partially with countries with Mutual Recognition Agreement in place with EU. (Authorized Economic Operator Guidelines, 2016, 8 and 109)

4.2.1 AEO Benefits

AEO program differs from ISO family security management systems in one crucial aspect, since the program has EU granted benefits in place for all organizations with AEO status. Benefits and relevance to AEOC and AEOS statuses are listed in the following table.

Benefit	AEOC	AEOS
Easier admittance to customs simplifications	x	
Fewer physical and document-based controls - related to security & safety - related to other customs legislation	 x	 x
Prior notification in case of selection for physical control (related to safety and security)		x

Prior notification in case of selection for customs control - related to security & safety - related to other customs legislation	 x	 x
Priority treatment if selected for control	x	x
Possibility to request a specific place for customs controls	x	x
Indirect benefits	x	x
Mutual Recognition with third countries		x

Table 1 AEO Benefits (Authorized Economic Operator Guidelines, 2016, 27)

Most of the benefits are self-explanatory and revolved around getting priority, more information and easement in supply chain within customs procedures in EU member states.

Indirect benefits however contain more general benefits of increased security and internal control such as reduced incidents, fewer delays of shipments, reduced thefts and losses and all the general benefits of management system such as improved management and relation to customers. (Authorized Economic Operator Guidelines, 2016, 27) and (Kerko, P. 2001, 32-33)

First minor one of the benefits in international supply chain is related to civil aviation legislation and in there specifically if the AEOS certificate holder applies for Regulated Agent or Known Consignor status, the respective security requirements are deemed to be met and are mutually applicable when assessing the fulfilment of these security requirements. (Authorized Economic Operator Guidelines, 2016, 28)

One of the greatest benefits of AEO certification for Case Corporation is, that AEO program recognizes corporation structure with common system and procedures and it is recommended that large corporate processes and systems are checked only once in application phase and subsequent application(s) of different legal entities inside the corporation can then done with smaller scope. (Authorized Economic Operator Guidelines, 2016, 83)

Another benevolent factor for Case Corporation is if a specialized unit produces certain services for entire corporate structure with shared services. Currently in Case Corporation information management is done with centralized corporate support function model and invoice handling is done by a global shared service center. (Authorized Economic Operator Guidelines, 2016, 83-84)

One of the greatest possible advantage of AEO program is the recognition of international standards related to security management. Mutual benefits in acquiring AEO status are available for organizations who are holding ISO 27001 certificate (Authorized Economic Operator

Guidelines, 2016, 82) and especially in large corporate structure with centralized information management holding ISO 27001 certificate can be greatly beneficial when acquiring AEO for several legal entities in various locations or countries.

Finally in security management systems there is benefit available for ISO 28 000 series certificate holders; whereas ISO 28 000 requirements are very general and on top level while in ISO 28001:2007 requirements for supply chain security are very specific and these should be reviewed in context with AEO requirements. (Authorized Economic Operator Guidelines, 2016, 82-83)

Mutual recognition agreement has been concluded and implemented between EU and following countries: Norway, Switzerland, Japan, Andorra, the United States and China. The agreement is in place to ensure compatibility of the AEO programs of the two parties, states the reciprocal benefits granted to the operators and furthermore it contains procedural rules for customs (Authorized Economic Operator Guidelines, 2016, 109)

As stated in the benefits earlier in chapter, generally the mutual recognition agreement offers the same benefits as inside EU and contain:

- Fewer security and safety related controls
- Recognition of business partners during the application process
- Priority treatment at customs clearance
- Business continuity mechanism
- Future MRA benefits

(Authorized Economic Operator Guidelines, 2016, 110)

4.3 Supply chain security in Case Corporation

As earlier stated in Chapter 2, Case Corporation has large dependency on international supply chain and when assessing AEO benefits, it seems likely that the Case Corporation would benefit greatly of acquiring AEO certifications to all sites and / or legal entities with manufacturing or logistics function. Unified standards and security management system on corporate level would most likely simplify processes and acquiring AEO certification would be definitely be a lot more cost effective than without common processes and corporate level standards.

Unified management support of AEO certifications in the case corporation would most likely be very beneficial and help local business and country organizations in supply chain management.

4.4 Information Security Management system - ISO 27000

Generally speaking all organizations handle information by collecting, processing, storing, transmitting information and in many cases the collective information that the organization holds creates the value of the organization.

Information is an asset that, like other important business assets, is essential to an organization's business and consequently needs to be suitably protected. Information can be stored in many forms, including: digital form and material form as well as unrepresented information in the form of knowledge of the employees. Information may be transmitted by various means including: courier, electronic or verbal communication. Whatever form information takes, or the means by which the information is transmitted, it always needs appropriate protection. Finally information security includes three main dimensions: confidentiality, availability and integrity. (ISO/IEC 27 000:2014(E), 2014, 13)

As in earlier chapters of security management systems, the information security management creates framework in information security management and specifies requirements for establishing, implementing, maintaining and continually improving the management system in the context of the organization. The requirements for assessing and treating information security risks have been specifically mentioned. (ISO/IEC 27 001:2013(E), 2013, 1)

By using ISO 27 000 standard family organizations can develop and implement a framework for managing the security of their information assets including financial information, intellectual property, and employee details, or information entrusted to them by customers or third parties. (ISO/IEC 27 000:2014(E), 2014, 1)

The case corporation has strong emphasis on research and development and the aim of its R&D activities is to continuously strengthen the technological leadership position and future improve the competitive edge in global marine and energy markets. The significance of information security cannot be emphasized strongly enough, as the annual R&D expenditure has been between 135 and 180 million Euros per year between 2011 and 2015. (Wärtsilä Annual report 2015, 50-51)

The competitive edge the case corporation gains through R&D is significant and therefore the information security risks the case corporation faces are likely to be equally significant.

4.4.1 Leadership, commitment and policy

The top management commitment is required to effectively influence information security management and it should at least include the following:

- Setup information security policy and objectives that are aligned with strategic direction of the organization.
- Ensure the management system integration into organization processes.
- Ensure the resources for the management system.
- Communicate and promote importance of information security and continual improvement for the management system.

(ISO/IEC 27 001:2013(E), 2013, 2)

One member of senior management should be given the overall responsibility for protecting the organizations information assets. The top management commitment is crucial to success in setting leadership for information security and to ensure the resources it requires. (Taylor, A. 2013, 44-45)

When the organizations top management has reached decision on ownership and overall responsibilities for information security, policy for information security should be set. Information security policy must contain at least following:

- Appropriate and suitable for the organization
- States objectives or framework for information security objectives
- Commitment to achieve information security requirements
- Commitment to continual improvement of information security management system

The policy should be available to all stakeholders as documented information and communicated throughout the organization, and the policy should contain following practical statements to be successful: How the organization will manage information assurance, the protection of information assets in accordance with their criticality and that the policy has the support of the board of management and senior executives. (ISO/IEC 27 001:2013(E), 2013, 2 and Taylor, A. 2013, 46)

4.4.2 Information security risk management

Assuring information security is almost entirely about management of information security risks. The key concepts in information security risks are threats, vulnerabilities, impact and finally assessment of likelihood or probability. (Taylor, A. 2013, 21-23)

The requirements for information security risk management plan contain that they must planned and periodical, should be conducted when significant changes are proposed or occur. Finally documented information of the results of the information security assessment must be kept and finally information security risks treatment plan must be implemented to comply with the requirements of information security management system. (ISO/IEC 27 001:2013(E), 2013, 7)

Risk management plan should contain the 4T principle or similar structured way to document and plan what risk management decisions the management will do with each risk item. As stated in the risk management chapter, risks can be treated for example with hazard risk 4T principle, which stands for options tolerate, treat, transfer and terminate. (Hopkins, P. 2012, 165-166)

As assessing information security risks can be highly theoretical and the assessment of impact can be quite imprecise, the scale should be set according to the organizations side. Since the case corporation has such huge spend in R&D for example, the information security risk impacts should be compared to the R&D spend to make the risk effects more quantifiable and tangible to the organization.

All information security policies and processes are part of organization-wide risk management and business continuity program and therefore they will need the resources and attention of the top management with suitable resourcing and commitment. (Vacca, J. 2009, 70)

4.4.3 Implementation

Implementation of information security management system can be done according to many standards or guidelines. Organization can choose to implement the system for example according to specifications in the Federal Information Security Management Act or follow ISO 27000 family framework. (Vacca, J. 2009, 55-56) The most important aspect of the implementation is that the framework is suitable and applicable to the organization. (ISO/IEC 27 001:2013(E), 2013, 2)

The differences of ISO 27 000 family of standards and FISMA are compared in the following table.

ISO 27 000 family	FISMA
Security policy	Standards for categorizing information and information systems by mission impact
Organization of information security	Standards for minimum security requirements

	for information and information systems
Asset Management	Guidance for selecting appropriate security controls for information systems
Human resources security	Guidance for assessing security controls in information systems and determination of their effectiveness
Physical and environmental security	Guidance for certifying and accrediting information systems.
Communications and operations management	
Access control	
Information system acquisition, development and maintenance	
Information security incident management	
Business continuity management	
Compliance	

Table 2 ISO 27 000 family of standards and FISMA (Vacca, J. 2009, 55-57.)

The actual implementation should take account of all the relevant elements for the case corporation and make sure that they are covered in documented manner. From information security and risk management point of view it's crucial to cover all elements that are found to be relevant in the security risk assessment phase.

As information and technological advantage is vital to the case organization, information security seems to be one of the most important parts of security that the case corporation does need to develop.

5 Theme interview, corporate security management

Theme interviews were conducted during autumn 2016 to preselected group of internal stakeholders who either had possibility to influence security decisions or were internal customers for security function. All interviews were recorded and transliterated by the author, the records are kept by the author.

The interviewees were selected based on few criteria. The type of selection chosen was elite sampling. First and foremost selection criteria was that the person was in place of authority and could genuinely influence security related decisions in one or multiple ways. Second selection criteria was based if the person could be internal customer for security and finally persons participating were shortlisted on many occasions to ensure the quality and depth of

knowledge related to security and risk management. Finally the distribution between different Wärtsilä business divisions and support functions was chosen to be kept even, with target of 25% to each three business divisions and last 25% to support functions; such as human resources, finance or quality. (Tuomi, J. & Sarajärvi A. 2009, 85-86)

When assessing the size of the primary material; interviews in this case;, it is often stated that only 1 out of 100 theses below doctorate level is scientifically significant and rather usually they are in place to bring evidence that the author has mastered the area of expertise he studies. Usually the size of the primary material is quite small in qualitative research at this level. Finally since the aim of the thesis is to try to find answer to a specific question, the relevance of the primary material and its interpretations are far more important than size of the sample. (Tuomi, J. & Sarajärvi A. 2009, 85)

Information collection method used was theme interview. Theme interview is semi structured method of interviewing the subject with the possibility to change the order and wording of questions depending on the theme of the interview, where one of the greatest advantages of theme interview is the possibility for deeper interaction between the researcher and the subjects. (Hirsjärvi & Hurme 2000, 47 - 48.) One of the practical examples in that in cases of misunderstandings, the questions can be repeated, clarified and rephrased and the same applies to understanding the answers. (Tuomi, J. & Sarajärvi A. 2009, 72-73)

The interview was organized to understand most vital questions and viewpoints that were for example:

- How effective is the current security management system (if any)?
- How does the system suit the corporation?
- What type of security risks the organization usually encounters?
- How security culture was seen from their viewpoint?
- What would be the most important development areas in security
- How did they feel that security should support their business

The interview thematic picture and topic list is provided in Appendix 1.

5.1 Qualitative content analysis

In the content analysis qualitative research methods and specifically subject referenced analysis method was chosen since it supports the framework of the thesis with the ability to emphasize the interview statements and work with inductive methods towards cohesive understanding the problem at hand. (Tuomi, J. & Sarajärvi A. 2009, 95)

As is stated in the literature and in qualitative research in general, the framework, research methods and subjectivity are always derived from the author and the problem of subjectivity is even greater in subject referenced analysis, since the questions is, can the author control that the information gathered is not polluted by and stay outside of authors set framework and prejudices of the subject. (Tuomi, J. & Sarajärvi A. 2009, 95-96)

The problem can be solved by using theory guiding analysis method where analysis begins with subject references and is guided by the selected framework of theory to combine the interpretations of the primary material and the theory. (Tuomi, J. & Sarajärvi A. 2009, 95-96)

In the content analysis the information was classified and themed to pick out relevant contents and topics from the fields of security and risk management to form the grounds for conclusion and proposals how the thesis problem should be addressed. (Tuomi, J. & Sarajärvi A. 2009, 92-93)

The theory guiding analysis was chosen for the thesis, since the theory of security management and security related knowledge was already known and established information and the focus of the thesis is to study the specific problem at hand, Case Wärtsilä Corporation. In the content analysis main elements that effect security management or are relevant for the case corporation in security management are quantified and further content analysis is based on the verbal comments and views of the interviewees.

Main points to understand reside around the aspects of corporate security management models and management systems or what would potentially be most efficient and suitable corporate security organization to support the business organization in security and finally what areas of security would need development.

Following main themes were found in the content of the interviews and they were mentioned or deemed important aspects in the interview:

Theme	Mentioned in the interview as key element or focus area
Security Awareness	6 / 8 times
Security Culture	7 / 8 times
Global or Area Security Management Model	4 / 8 times
Premises Security & Physical Access Control	4 / 8 times
Information Security	4 / 8 times
Information Security with Cyber security and Industrial control systems	6 / 8 times

Personnel Security	2 / 8 times
Travel Security	3 / 8 times
Crisis Management	2 / 8 times
Analysed Security Information and situation updates	2 / 8 times

Table 3 Theme interview key elements

In addition to these main themes, two specific themes were discussed in each interview:

- What Security risks the participants see that the case corporation faces?
- What is the biggest development area in Security?

These topics will be covered in the following chapters, to understand the concepts and their importance. All topics with four or more mentioning will be addressed in the following sub-chapters.

5.1.1 Security risks

As stated in crucial concepts of the thesis in earlier chapters, in security management risk is by default a negative event, although risks can also have positive effects. Within the interview this approach was used to gain the insight the interviewees had on the risks that the case corporation faces.

Following security risks were mentioned as the most important:

Risk Category	Threat, consequence or trigger
Information Security	Information or material theft Digital access control failure Human error Poor Security culture Research & Design data leak
Premises Security	Crime Material thefts Information thefts Violence External users with authorized access to premises
Personnel Security	Crime Violence against personnel and expatriates Terrorism Hostage situations

Travel Security	Crime Violence against personnel and expatriates Terrorism Political, war or military risks to travellers Hostage situations
Cyber Security and Industrial Control systems	Integrated ICS solutions Internal Cyber Security risks Digital access control failure
Crisis Management	Natural disasters Fire

Table 4 Case Corporation security risks

Understanding and evaluating the security risks is the first and foremost action in any security related management and only risks that are significant to the organization should be actively managed (Kerko, P. 2001, 57-58).

The risks landscape varied heavily depending on the interviewee and especially important factor seemed to be their position in the organization and how global role they had in the organization. However in similar positions across the globe same risks were repeated and therefore it can be assumed that the risk landscape for the case organization is well known and established. The interpretation is further supported in the upcoming analysis of the theme and development areas.

5.1.2 Security awareness and culture

Security awareness and culture was mentioned most often in the themes of the interviews. Generally security awareness program will increase the amount of eyes in the organization to report where security personnel are then needed. (Wayland, B. 2014, 50). On the other hand security awareness can be understood as the general knowledge level of the personnel regarding risks and informing, management commitment and training are key elements in creating this awareness, which can also be called security culture. (Kerko, P. 2001, 25-29)

One of the interviewees stated: “It’s not like you can build the awareness in a day and then be happy, situations develop and keeping security awareness up needs constant reminders and the risk landscape is evolving all the time. When people are aware what the risks are, then we can more easily keep the awareness up. This will change behavior and when we do things differently this will build new culture. We must make people aware of the risks. It’s like vegetable, fresh one day and gone few days after. “

Another interviewee pointed out that: "the premises security changes since it's so concrete and I think it is more effective than official trainings for example even though those are important as well. Same as in any area where you want to increase awareness, you need to have trainings, info's, news and this and that and remind people about the issue. I really think the premises security changes are doing the trick here. "

Information security awareness was mentioned specifically in one interview and it was stated that even most basic e-mail fraud or false invoice is currently possible risk for the organization and that the employees are sometimes far too trusty.

Awareness plan should contain basic training of security concept to personnel so that the implementation of the security awareness program can be ensured (Wayland, B. 2014, 50.) Both of the interviews support the idea of constant awareness program with continuous reminding of the organization and its employees of the importance of security, but two of the interviewees also point out that actual physical changes in premises and ways to access the facilities will also impact culture and awareness and be catalyst in the change of behavior.

When evaluating the security culture many of the interviews stated that our culture appreciates reacting to incidents but not prevention of the risks and another stated directly: "…currently they (our employees) are coming in like cowboys. They are usually being fooled when it comes to the prices and such." One person stated: "Earlier we were proud about taking risks and being the doers…" the same person also stated that this has been improving during the past five years.

As it can been seen from the interviews, the security culture level is quite different depending on the location, business line and country where the case corporation operates.

Some of the remedies that the participants pointed out and were committed to actively develop was top management commitment and actively influencing the change in culture, for example one statement was: "What can I do and what my organization can do. For me the approach is the same as in safety. In every leader and leadership theme we must have same focus to security as we have on safety. For management in general in company this is our role to play. And we must ensure that the mechanics are in place."

Finally in security culture, how can it be lifted to same level with safety management in top management commitment and in general awareness? One of the answer can be sought from earlier safety management system in the case corporation review; proportion of Wärtsilä legal

entities with management systems are 82% on quality, 66% on environment and 65% on occupational health and safety. (Wärtsilä Annual report 2015, 69-70)

It seems that one of the answers is to utilize security management systems and their implementation of gaining the much needed focus for security. Currently only 5 legal entities inside Wärtsilä corporate structure have a security management system, all of them Authorized Economic Operator. It should be noted that they only cover small portion of the legal entities and do not represent a corporate security management system.

5.1.3 Global security management model & organization

First and most important conclusion could be drawn either directly or indirectly from all of the interviews. Currently there isn't strong enough organization, not in amount of resources, visibly, mandate or top management commitment to adequately manage the risk landscape the case corporation is facing in its 170 locations across the globe.

Many sources in security management literature and study fields support the view that security management should be considered as one of the main functions of any large organizations and the person responsible for security or corporate security should report closely to most senior executive of the organization or very close to this most senior executive. (ANSI/ASIS CSO.1.-2013. 2013, 4)

Lanne, M. takes stricter stand in reporting hierarchy by stating: "Director responsible for corporate security must report to the most senior director." She also supports the view that security is one of the main functions in any organizations and should be managed in similar way. (Lanne M. 2007, 24)

One of the interviewees stated quite effectively: "How do you make the security global? It has to be centralized and there must be a system. That's the challenge. How do you really get this through all the organization?"

First and foremost statement and conclusion is that security management must be centralized globally in order to effectively coordinate organizations resources, senior management commitment and start the change management in security culture to change the organization-wide security management.

However with organization spanning to over 200 locations in 70 countries globally, one centralized position isn't surely enough. This is fully supported with all comments that address the issue in the theme interviews, take following comment for example: "It's about security

as a function to support to business. The direction with area or regional security managers is the right type of setup for us. Security experts in the local environment are the key to make their expertise accessible to the local organization and people and second to understand what I was touching earlier. They are the key to understand the risk scaling in the local regions. I think this is the right direction and I really want to mention this."

Second comment that supports the view is: "we need to have more guidance, more structures and once we have that information available we must have good organization to back that up and make (those) difficult decisions. (We need) fast, correct and mandated decisions." The same interviewee continues: "We are in firefighting mode. When decisions need to be made it is very slow since mandate isn't clear. It is not clear what you can do. Also whenever any cost item comes up in security, it is very difficult…"

Finally, one related comment to negative impact caused by wrong type of security setup is worth considering: "We used to have system that each country had a security coordinator assigned in the network companies but it has never been really worked in any ways as it was supposed to. The security coordinators were not up to date, especially in project (security) work. Often it was just managing director of the country or some assistant. Either of them didn't have time or competence for that so it's kind of false security, especially for the projects."

One of the greatest research problems to solve in the thesis will be the organizational setup that would address in an effective, suitable and flexible way to suit the business needs of case corporation security management needs. However the following key requirements are seen quite clear already in the content analysis of the interview:

- Centralized ownership, responsibility, strategic direction and leadership with cost and overall budget responsibility
- Reporting line from responsible security director to the most senior members of the management
- Suitable area organization with mandate and understanding to make locally sound security decisions
- Local presence of the security organization with local and hands on understanding of local and practical security issues
- All levels of organization must have competent subject matter expertise in security and risk management

All these aspects must be taken into account of the requirements of the solution for the security management system and organization for effective and suitable risk and security management for the organization.

5.1.4 Premises Security

Unified premises security policies and ways of working can be utilized as an effective change catalyst for change management and increase in security awareness and culture. Furthermore cost effective and globally unified identification and physical access management offers suitable convenience in security for the organization and can be effective change tool by making the most secure choice also most convenient choice for the user. This will greatly increase the likelihood that the most secure solution will be chosen when individuals makes the choices. (Benson S, 2016. Security Management September 2016, 58-60)

One interviewee stated: "… There was someone in my office and they actually quite spontaneously started conversation about information security. I think that trigger has been more controlled premises security and they are also taking the information security more seriously so there is a cultural change so far."

The situational awareness offered by centralized monitoring can be utilized to entire Case Corporation with suitable analysis and dissemination of the security information and its potential to support business management are easily captured by cost efficiency and simplicity brought by unified systematics. It is likely that the systematics can be used to support information flow from the introduced security management organization to the business organizations, bearing in mind that implementation for that type of system will take several years.

One of the observations of the author regarding premises security of the case corporation is, that it is widely diversified without any centralized systematics, policy or way of working and all physical security solutions have been invented and implemented locally. This is one of the easy wins that should be unified when building up the global organization to point out the benefits of global security management system.

5.1.5 Information Security

Information security was addressed as the biggest development area by half of the interviewees and it was second only to development issues with global security organization. Since the case corporation is effectively high technology Corporation the biggest information security risks cannot be measured while they realize, but instead their impact is likely to be divided on many consecutive following years, due to long term impact of R&D information loss.

One interview specific addressed huge information security risks: "The leaking information from R&D and how easy it is for the information to leak out before it is supposed and this will

often give our competitors advantage to use." Another interviewee continues: "In information security area we still have things to do especially drawings, in electronical sharing and digital access control."

Finally one of the most senior interviewee's states: "Firewalls and that kind of stuff are really the cornerstone and basic stuff in security, this was adequate before. Earlier segmenting the network to internal and external was enough but not anymore. The key point has changed from these to identity and access management. … This is also relevant for the ICS part. We must be able to identify in digitalization that is this part actually the part it claims to be and how their identities are managed."

As the examples state, at least most parts in the requirements of any information security management system are not met or in place. As earlier already mentioned when comparing information security management systems, at least policy, targets and requirements should be stated out in the policy, for an effective start. (Taylor, A. 2013, 45-46)

The identified and mentioned risks that involve identity and access management and information classification are undisputedly the hardest to manage, especially when keeping in mind their importance to the organizations due to its nature as a high technology corporation.

The general risk landscape the organization phases in the field of information security seems to be largest of all risk landscapes in risk magnitude to the organization. There isn't any centralized management system in place for information security and throughout implementation of information security management system to the organization should provide tools and means for the corporation to manage information in structured way. It is likely that high technology corporation with almost 20 000 employees cannot control information security in desired way unless management support and commitment is demonstrated by selecting and endorsing information security management system. (Taylor, A. 2013, 45-46)

Also another issue to be considered is, that if information security management system should be assessed and perhaps implemented after general security management system is in place to overcome the change resistance of the organization and secondly to prove to the organization first the value of centralized security management system and organization.

6 Conclusions

In the conclusion chapter of the thesis main thesis questions will be discussed with possible answers. The research questions to answer are:

- What or which management systems would be best suitable for the case study corporation globally?
- What kind of organizational model would best support the management systems?

In addition to these large conceptual questions in the conclusions chapter few smaller aspect related to the implementation shall be presented due to their relevance and easy linking to the selected research questions.

First and foremost conclusion is that the case corporation does not know how its security is managed. All management system aspects are missing from the published corporate material and there wasn't any points in the primary material that would support that such management system exists. As important conclusion is that there isn't suitable organization with top management support, resources and operational responsibility to manage the security to the extent this size of organization would need.

However also few of the smaller details found out in the primary material point out that at some levels or part of the organization there is security management in place and there seems to be evidence that security management and awareness have been address and actual change in security management has been seen by the interviewees.

Finally it must be also pointed out that even though the organization does not know centrally how security is managed, it seems that local solutions are almost always designed and created to achieve some sort of minimum level of security to address the most basic needs. Their effectiveness in action or in cost will not be evaluated in this thesis.

6.1 Global Security Management Organization Model

Global security management model will address following concepts: the structure and position of most senior risk and security officer, global area organization structure, information and cyber security management. All of these areas will be discussed and conclusions drawn out to find suitable solutions for the case corporation.

6.1.1 Chief Risk and Security Officer

The first and foremost action to start the path to improvement is that the organization must establish one senior position with full responsibility in risk and security management. Without the organizations top management commitment to support such senior position, further improvement is likely to stop or is at least seriously slowed by organizational change resistance.

There seems to be consensus amongst security literature that this senior security management officer should report to the CEO or very close to the position of CEO. This will help to organize security as one of the main functions of the organization and enable the desired level of attention. (ANSI/ASIS CSO.1.-2013, 2013, 2) & (Lanne, M 2007, 24)

When designing the corporate security management model, all organizational aspects should be evaluated, such as size, organizational structure, culture, ways of working and key risks affecting the organization are most important factors to assess. (Lanne M. 2007, 74)

Senior management must be committed to the level of security decided in the organization. This should be measured by actions, not just words and verbal commitment, such as committing funding, resources and responsibilities to maintain security program. (Wayland, B. 2014, 36-37)

Since the organization functions with three very independent and autonomous business lines, who report to the CEO, it is likely that risk and security should be elevated to Board of Management position due to heavy reliance of future digitalization, and especially due to high risk profile cyber, industrial control system and information security challenges create to the organization. Only with full support of the Board of Directors and widespread understanding of complex security challenges in physical and digital environment this strategic risk management and ownership can be addressed in a way that it aligns with fast paced digital development.

When assessing the rest of the related board of management positions, the following supporting facts are found to previous conclusion:

- Board of management hasn't stated where risk, security or information security management are situated and reporting.
- Board of management has stated that sustainability, health and safety are reporting to Corporate Relations & Legal affairs.
- Board of management has stated that information management is reporting to Chief Digital Officer.

(Wärtsilä Annual report 2015, 129) & (Wärtsilä stock exchange release 24.8.2016)

Based on the earlier facts most suitable solution would be to establish Chief Risk and Security Officer Position who will report to Chief Executive Officer. The risk and security function should gather full ownership and responsibility of Enterprise risk management and security management with physical, information, cyber and digital domains of security.

From this position the organization should be divided three paths:

- Global area security organization
- Centralized risk management function
- Matrix management model of information & cyber security organization with direct reporting to information management

Finally health, safety and environmental management should be kept as they are; aligned with current setup with sustainability due to their maturity level and established management systems.

6.1.2 Global Area Security Organization

The case corporation operations are heavily weighed to Europe and Asia with over 75% of its workforce and turnover coming from these continents. It is equally important that these areas are covered with equal effectiveness in security management focus to enable full support to business operating at these areas. (Wärtsilä annual report 2015, 87 & 217)

In global and diverse organizations security management will be divided to many persons and organizational units, therefore the when applying to global solution all three levels; global, area and local must be taken into account when designing suitable security management solution. Full support to local business must be kept in focus all the time, to ensure that security is aligned with business goals. (Lanne M, 2007, 14)

With the setup of Case Corporation the area organizations should contain two director level positions, one in Europe and one in Asia and then two area manager positions to cover Americas and Africa respectively. Furthermore these positions should evaluate and establish the amount of personnel, resources and related competences they require to manage security in their respective areas to achieve organizations risk and security management requirements.

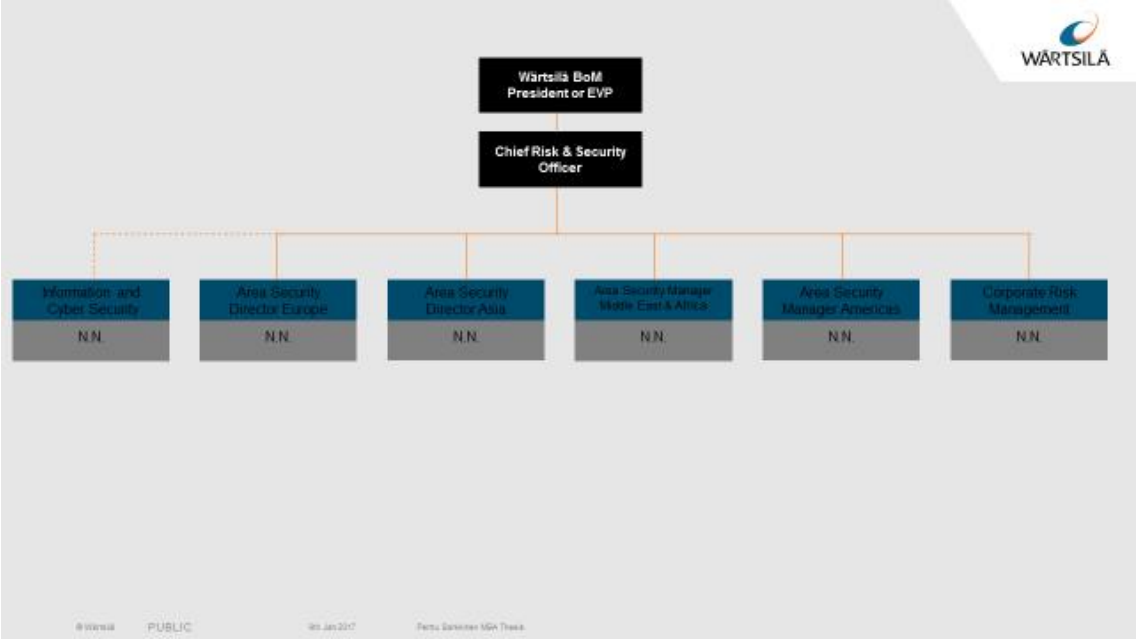

Figure 4 Area security and risk organization

One equally important aspect is regarding crisis management, how to organize cost ownership and funding for emergencies and different types of crises. As it was stated in the theme interview, there has been slowness in decision-making and misalignment in how crises are handled since the ownerships hasn't been clear. This should be another one of the easy wins the area security organization should achieve by establishing clear procedures, cost ownership and way of working for handling crises and emergencies.

The most important task for the area security organization would be to create, establish and maintain the framework for the security management systems, in order to provide the subject matter expertise for the global business organizations and provide support in the actual implementation of security management system to the line organization.

Lastly the area security organization should provide expertise and facilitation in enterprise risk management. Establishing communication with the business organization in enterprise risk management would create much needed link between the security and business organizations and provide support to the business leadership in risk management facilitation. It should be however extremely important that the risk ownership is clearly staying with the business organization.

6.1.3 Centralized Risk Management Function

As stated earlier in the thesis, the current setup of the case corporation doesn't provide any linkage between risk and security management functions. When deeply studying security

management and risk management and comparing their knowledge to each other it can almost be stated that in risk management there isn't clear picture how security is performing and vice versa.

In order to strengthen the connection between risk and security management the centralized risk management function should be situated under the chief risk and security officer, with same reporting level as the area security directors and managers shown in Figure 4.

This management model would ensure the cooperation and alignment in risk and security management and create the much needed link between different functions. Secondly the management model would ensure that the other relevant support functions that have role in corporate risk management are available and accessible to the risk management process. These include at least, finance, treasury, business continuity, internal audit, health, safety, security and environment. (Hopkins, P. 2012, 88-89)

Finally the centralized risk management function should be the subject matter expert in risk management and provide the chief risk and security officer the enterprise wide risk information in order to communicate required risk management decisions to the board of management and implement the required risk management decisions together with business units with the help of area security organization.

6.1.4 Information and Cyber Security Organization

As the ownership and management structure of information management and information security has been establish in the information management and the direct reporting line is clear, the most important thing is to create the link between chief risk and security officer and the information and cyber security organization in order to ensure that all aspects of security are managed in equal and suitable fashion.

Creating, establishing and maintaining the information and cyber security management system is the most important task for the function. Secondly improving information security awareness and culture are ever more important, since almost 80% of the data breaches are caused by employee negligence or maliciousness. (Ponemon Institute, 2012, 2.)

The area security organization would have the supportive role in information security management mainly in providing support in administrative information security such as training, communicating and the day to day awareness of the information security of the employees.

6.2 Management Systems

The case corporation has shown remarkable ability to grown, evolve and develop its business operations whenever the top management has decided to improve any area. For example the safety management has been corporate focus for several years and it has improved lost time injuries per million working hours from year 2011 level of 6.3 to all-time record low of 2.8 during 2015. (Wärtsilä Annual report 2015, 90)

This proves the point that when the corporation has set strategic goals, they have been improving remarkably and the way to achieve the goals has quite often done by building management system for the organization to implement and execute. In other words choosing to select and certificate security management system the organization top management can make an actual statement, strategic decision and show commitment that improving security is important to the organization.

6.2.1 Security Management systems

As is the case with the organization, there should be global business approach to align security through a management system. The management system should be built upon ISO 28 000 requirements and certified in global business management level and then to be further trickled down to Authorized Economic Operator certificate with locally establish legal entity whenever there are benefits available with AEO. (Authorized Economic Operator Guidelines, 2016, 83)

The goals of the selected security management systems for the case corporation should be at least the following:

1) establish, implement, maintain and improve a security management system;
2) assure conformance with stated security management policy and increase security awareness of the personnel;
3) demonstrate such conformance to all stakeholders, internal and external;
4) seek certification of its security management system by an Accredited third party Certification Body to ensure and demonstrate top management commitment

(ISO 28000:2007E, 1)

The importance of certification cannot be emphasized enough in such large scale corporate operations, where business targets can easily be misaligned with management system targets, unless they are designed, communicated and implemented correctly from top to down by the line management.

The top level ownership and responsibility of the security management systems and their global implementation should be on the chief risk and security officer, who can establish suitable regional and local management systems by utilizing the area security organization to communicate and implement the management system with local business units and support in creating the local security management framework, which should most often be Authorized Economic Operator whenever possible due to earlier mentioned benefits to international supply chain and customs easements.

Since the case corporation is large, diverse and dispersed to 170 locations globally, it is likely that the only feasible way to establish suitable security management systems is to use approach that covers global, regional and local aspects of security management.

The earlier presented area security organization is once again in key role in creating the security management systems for the case corporations and the subject matter expertise in risk and security management will be right approach to provide regional and local security risk assessments to establish correct and suitable security measures to different geographical areas.

The area security organization should be the spearhead in rolling out and utilizing earlier presented risk management approach and be the change agent in creating the enterprise risk management culture. As is the case with other change management issues brought up in the case corporation, it is likely that the enterprise risk management approach should be built by starting on easier risk management items, such as hazard and security risks and move on the more abstract risk categories only when the organization has matured enough in risk understanding.

6.2.2 Information security management system

The information security management system implementation is likely to be the hardest task of all the management system tasks the case corporation can face due to the high dependency to information, cyber and industrial control systems and the sheer volume of information and documents needed in the high technology environment.

Therefore from the management and change management point of view, the information and cyber security organization should concentrate on improving the selected industrial control systems while the area security organization implements the security management system to the organization. Only after the successful implementation of the security management sys-

tem the case corporation should start the implementation of the information security management system due to complexity and change resistance.

However it is of no doubt that the corporation would benefit greatly from certified information management system, but due to the nature and amount of change management people in an organization can tolerate in a certain timeframe, the changes should be completed after one another.

Also it should be noted that creating information security awareness and basic information security to all personnel of the case corporation should be on going simultaneously with the security management system implementation.

6.3 General Security Management Program Elements

In the theme interviews several general easy wins and essential security management elements were discovered which should be established together with the selected security management system because of their relatively easy implementation, effect on security awareness, effect on actual risk or security management and finally help the change management process by creating visibility and feelings of positivity in security changes.

6.3.1 Security Awareness program

Security awareness program is needed and at all locations some presence of security management and security related issues must be present in order to change the mind-setting so that actual change in security culture can happen. These changes can be supported and made more efficient if they are combined with actual changes in facilities, premises security and the most tangible ways of working that affect every day work environment of the personnel. The awareness program must be at least on global and local level, global to address the general security risks the organization phase and local to make it suitable for the country, culture, location and to address the specific risks at the local area.

The selected management system must contain elements that ensure security awareness of the personnel. Effective security awareness will ensure that the staff of the organization will be vigilant and understand when security personnel should be contacted. Second fact that must be admitted is that it is unlikely that security staff will be directly on the site when incident occurs. Awareness program will increase the amount of eyes in the organization to report where security personnel are then needed. (Wayland, B. 2014, 50).

Awareness plan should contain basic training of security concept to personnel so that the implementation of the security awareness program can be ensured (Wayland, B. 2014, 50.) From management system point of view the management must decide how often the training is organized and how comprehensive the training program will be. Also follow up and documentation are important part when considering the management system aspects of the awareness program.

6.3.2 Physical Security

The general physical security management is very diversified and fragmented in the case corporation and unifying physical security policies, ways of working and systems would be great change management catalyst to help communicate and make security management system implementation very visible and concrete to all employees in the case organization. When combined with the awareness training program with new tools and ways of working, it is extremely likely that the effect on security level will be positive. (Wayland, B. 2014, 50).

Since the case corporation is extremely global and has several thousands of its personnel traveling every day, one of the physical security change elements should be globally applicable access control and corporate identification system that should be implemented with several key requirements in mind:

- Make the selected and secure solution also the most convenient choice for the user
- Globally available information to the organization of the status of all its selected sites and offices
- Globally available information of many employees are present in the sites and offices and their last known location

(Benson S, 2016. Security Management September 2016, 58-60)

The benefits and cost efficiency in simplification of processes and ways of working alone are likely to greatly increase the positive attitude towards security, since the employees will notice the time savings when they know that they can behave in similar way in all locations globally.

6.4 Evaluation of the thesis

The thesis has brought solutions to the research questions presented in the introduction. The question how to create security management system and what type of security organization would be suitable for the case corporation have been presented and both of the solutions can be implemented immediately.

The solutions presented in the thesis for the case corporation are likely to be universally applicable to similar type of organizations. Most of the solutions are in general level and they can be applied to other environments as well bearing in my by always taking into account the nature of the organization is question.

The solutions offered are only one possibility of many options available, but the literature has been quite unanimous of the fact how risk and security responsibilities are implemented most effectively, so the most effective choice has been selected.

Overall in can be stated that the thesis has been a success and should provide actual improvement in the field of risk and security management for the case corporation if the proposed changes are implemented.

6.5 Future research opportunities

The subjects handled in the thesis provide many opportunities for future research for the case corporation. First of them is to research further how should information and cyber security management system to be tied to the proposed security management system when implemented.

Second interesting research topic would be to follow up how security culture and awareness are changing when the security management system is implemented and study the culture and phenomena of behavior changing in people choices.

References

ANSI/ASIS CSO.1.-2013, 2013. Chief Security Officer - An Organizational Model

Benson S, 2016. Security Management September 2016, 58-60. Virginia, Asis International.

Borodzicz, E. 2005. Risk, Crisis & Security management. West Sussex: John Wiley & sons.

European Comission, 2016. Authorized economic operators guidelines. Referred 12.5.2016 http://ec.europa.eu/taxation_customs/resources/documents/customs/policy_issues/customs_security/aeo_guidelines_en.pdf

Hirsjärvi, S., Remes, P. & Sajavaara, P. 2007. Tutki ja kirjoita. 13. uudistettu painos. Helsinki: Tammi.

Hirsjärvi, S., Hurme, H. 2000. Tutkimushaastattelu. Teemahaastattelun teoria ja käytäntö. Helsinki: Yliopistopaino.

Hopkins, P. 2012. Fundamentals of Risk Management 2nd edition. London: Kogan page.

Ilmonen, I., Kallio, J., Koskinen J., & Rajamäki, M. 2013. Johda riskejä, käytännön opas yrityksen riskienhallintaan. Jyväskylä: Bookwell.

ISO/IEC 27000:2014(E) International Standard ISO 27000 Information technology — Security techniques — Information security management systems — Overview and vocabulary

ISO/IEC 27001:2013(E) International Standard ISO 27001 Information technology - Information technology — Security techniques — Information security management systems — Requirements

ISO 28000:2007 (E) International Standard ISO 28000. Specification for security management systems for the supply chain.

ISO 31000:2009 (E) International Standard ISO 31000. Risk Management – principles and guidelines.

Lanne, M. 2007. Yhteistyö yritysturvallisuuden hallinnassa: Tutkimus sisäisen yhteistyön tarpeesta ja roolista suurten organisaatioiden turvallisuustoiminnassa. Espoo: VTT.

Kananen, J. 2015. Opinnäytetyön kirjoittajan opas. Jyväskylä: Suomen yliopistopaino.

Karjalainen, M. 2014. Bachelor thesis: Developing an Information Security Management System. Espoo: Laurea.

Kerko, P. 2001. Turvallisuusjohtaminen. Jyväskylä: PS-kustannus

Kukkonen, E. 2015. ISO 28000 – standardi kokonaisvaltaisena turvallisuuden hallintajärjestelmänä: Case Vacon Oyj

Mäkinen, K. 2005. Strategic Security. Helsinki: Edita Prima.

Ruippo, J. 2015. Bachelor thesis: Developing a risk and security management system. Espoo: Laurea.

Ponemon Institute Research Report. 2012. The Human Factor in Data Protection. Referred 2.1.2017
http://www.ponemon.org/local/upload/file/The_Human_Factor_in_data_Protection_WP_FINAL.pdf

Taylor, A. et al. 2013. Information Security Management Principles. 2nd edition. Swindon: BCS, The Chartered Institute for IT.

Tuomi, J & Sarajärvi, A. 2009. Laadullinen tutkimus ja sisällönanalyysi. Vantaa: Hansaprint.

Vacca, J. 2009. Managing information security. Burlington: Syngress.

Wayland, B. 2014. Security for business professionals. Oxford: Butterworth-Heinemann.

Wärtsilä Annual Report 2015. Referred 24.1.2016 http://www.wartsilareports.com/en-US/

Wärtsilä stock exchange release 24.8.2016. Referred 27.12.2017.
http://www.wartsila.com/media/news/24-08-2016-wartsila-appoints-marco-ryan-to-lead-digital-development

Figures

Tables

Appendixes

Appendix 1: Theme interview thematics and discussion list

Security risks, what type of security risks do you see in your business?

How can you see security in your daily work or business?

How would you describe good security culture?

How do you feel about security culture in Wärtsilä?

What is the most important factor to develop security culture from your viewpoint?

How do you measure security? Do you have ideas of what KPI's could measure security?

How do you feel and think that security should support your business?

Do you have examples of situations that security enabled or hindered business operations?

Where do you see biggest development areas in security?

How could you or your function contribute to enhancing the security level?