LAUREA
UNIVERSITY OF APPLIED SCIENCES
Together we are stronger

Preventing data leaks caused by employee error in organizations

Wrede, Axel

2016 Leppävaara

Laurea University of Applied Sciences
Security Management

Preventing data leaks caused by employee error in organizations

Axel Wrede
Security Management
Bachelor's Thesis
December, 2016

Laurea University of Applied Sciences **Abstract**
Leppävaara
Security Management

Axel Väinö Wilhelm Wrede

Preventing data leaks caused by employee error in organizations.

Year 2016 Pages 43

The purposes of this thesis is to investigate the effect of employee errors as a cause for data leaks occurring in organizations, and the preventive methods that can be used to reduce the likelihood of these errors occurring. The importance of securing a company's immaterial assets is motivated through analyzing the potential consequences of a leak, which in turn serves as the motive for implementing information security awareness programs. But what methods should a company implement to increase employee awareness about information security risks? Which methods are effective?

The theoretical solutions for improving information security awareness in companies are evaluated and analyzed in order to determine in what way the theory could be implemented in practice to reduce the likelihood of a threat to a company's information assets being compromised.

Nokia Corporation was the target for a case study, where four managers were interviewed and a focus group of 25 randomly selected individuals at the Nokia Corporation headquarters in Karaportti participated in an information security survey. In order to produce conclusions and solutions to the research questions, the survey and interviews were cross referenced to establish what expectations there are on the ability of employees of Nokia to handle information in their daily work, and how the awareness level of the employees correlates with the expectations of the management.

The results of the thesis suggest that although Nokia is doing well in their processes of controlling information security measures within the company and benchmark it well among other companies through certification, the process of determining which employees may face challenges with information security remains a challenge. Therefore, different suggestions for how the current information security awareness level in the company could be improved in the future are discussed.

Keywords: Data leak, information security risk awareness, behavioral psychology, social psychology, company information and immaterial assets

Laurea-ammattikorkeakoulu **Tiivistelmä**
Leppävaara
Security Management

Axel Väinö Wilhelm Wrede

Työntekijöiden virheistä aiheutuneiden tietovuotojen ehkäiseminen yrityksissä

Vuosi 2016 Sivumäärä 43

Tämän opinnäytetyön tarkoituksena on tutkia työntekijöitten virheistä johtuvien tietovuotojen vaikutukset organisaatioon ja tutkia ehkäiseviä menetelmiä, joita voidaan käyttää vähentääkseen näiden virheiden sattumisen todennäköisyyttä. Yhtiön aineettoman omaisuuden turvaamisen tärkeyttä motivoidaan analysoimalla mahdollisia tietovuotojen negatiivisiä seurauksia, joilla voidaan puolestaan perustella tarvetta toteuttaa ohjelmia tietoturvatietoisuuden parantamiseksi yrityksessä. Mutta mitä menetelmiä yrityksen tulisi käyttää parantaakseen työntekijöiden tietoisuutta tietoturvariskeistä? Mitkä näistä menetelmistä ovat tehokkaita?

Teoreettiset ratkaisut tietoturvallisuustietoisuuden parantamiseksi yrityksissä arvioidaan ja analysoidaan jotta voidaan määrittää miten teoreettiset ratkaisut voidaan toteuttaa käytännössä vähentääkseen todennäköisyyttä että yrityksen aineeton omaisuus vaarantuu.

Nokia Oyj oli kohteena tapaustutkimukselle jossa neljää johtajaa haastateltiin ja järjestettiin 25 satunnaisesti valitulle yksilölle kysely tietoturvallisuudesta. Kohderyhmä kyselyä varten valittiin Nokia Oyj:n pääkonttorista Karaporttissa. Kyselyn ja haastatteluiden tulokset verrattiin toisiinsa selvittääkseen mitä odotuksia on Nokian työntekijöiden taitoon käsitellä tietoa päivittäisessä työssä jotta voitaisiin tehdä johtopäätöksiä ja ehdottaa ratkaisuja tutkimusta varten esitettyihin kysymyksiin, ja selvittääkseen miten työntekijöitten nykyinen tietoisuus tietoturvariskeistä korreloi johdon odotuksiin nähden.

Opinnäytetyön tulokset viittaavat siihen, että vaikka Nokia Oyj:llä on selkeät turvatoimet yrityksen tiedon suojaamiseksi ja suoriutuu hyvin verratessa toisiin yhtiöiden nähden sertifioinnin kautta niin yksittäisten työntekijöiden tietoturvallisuuden liittyvien haasteiden havaitseminen yrityksessä on edelleen haaste. Siksi tutkimuksessa ehdotetaan erilaisia ratkaisuja miten nykyistä tietoturvallisuustietoisuuden tasoa voidaan parantaa tulevaisuutta nähden.

Avainsanat: Tietovuoto, tietoturvallisuus, tietoisuus tietoturvariskeistä, käyttäytymispsykologia, sosiaalipsykologia, yrityksen tieto ja aineeton omaisuus

Table of contents

1 Introduction

In today's day and age, cyber threats are becoming more prevalent, and are more dangerous to organizations than they ever have before. As countermeasures, technical safeguards such as encryption technology are utilized and people's awareness of cyber security threats is raised through education. But the question is, is the education effective? Is an adequate level of awareness among all the employees and potential contractors achieved as it is within the organization in order to prevent data leaks? And is this awareness of potential risks enough? A common saying in security management is that you can use the best available technical safeguards in the market, but they are worthless unless your employees don't understand how to use them to achieve the desired level of security.

The data leak is a feared consequence of information security being neglected or compromised within companies, as it may have evolved as a result from a smaller information security risk and it is often associated with further consequences such as loss of financially valuable information, damage to the reputation or the trust reputation between either business partners, or customer companies in business-to-business or retail and end-user customers depending on the business model of a company. Data leaks may occur as a result of the efforts of cyber criminals or inside attackers within a company, but they may also occur if employees make errors when handling a company's information.

To study the phenomenon of data leaks being caused as a result of a human error, Nokia Corporation was used as the company for a case study to in order to ascertain the methods by which a company seeks to protect its critical information from data leaks, and how the employees of Nokia are trained in order to ensure that they meet, by the very least, the minimum criteria expectations on information security awareness. By studying Nokia's methods for promoting information security within the company's the workplace culture and the employees' mindset, one can get a better understanding of how well the company is proactively engaged in preventing information security related risks such as data leaks.

Nokia is one of the largest international companies in the world which operates in the industry of communications. The company mainly conducts business to business sales, as some of its most important customers are for example mobile operators. Regarding information security, Nokia has published in their "Nokia Government Relations policy paper" that the company believes that cyber security is not only an asset which improves trust and thereby strengthens the foundations for conducting business in a secure cyber environment, but is a mandatory prerequisite for conducting business as well. (Nokia Corporation 2016)

In order to understand the expectations of Nokia Corporation on the employees' knowledge of information security, the critical information protection "CIP" program leader, the head of information security and the chief security officer were interviewed in semi-structured inter-

views. These expectations were compared to the results of a qualitative survey which helped to determine the current attitude towards information security in Nokia, and assess the success of the programmes that have been implemented in Nokia to establish an appropriate level of information security knowledge.

2 Research design, methodology and research questions

In this section of the thesis, the approach and the methodology which were used to studying the phenomena of data leaks being caused by employee errors are explained. The way the methods and research design were applied in this study and the choices of specific research methods are justified, as well.

2.1 Explorative research design

Research design is defined by John Dudovskiy, the author of "The Ultimate Guide to Writing a Dissertation", as a plan for how research questions are intended to be answered, as well as well as describing the research methods and how they are used to answer those questions, and finally how the data that has been gathered as a result of the research is to be analyzed and the way the research questions that have been asked are to be answered using the collected data. (Dudovskiy 2016) Research design exists in two forms, either in conclusive or exploratory research. In the case of this thesis, the research design model which was deemed most appropriate was the exploratory research design. Exploratory research is defined as an approach to the research questions that is conducted in order "to have a better understanding of the problem", (Dudovskiy 2016) rather than approaching the subject matter in a conclusive manner, which is an approach that attempts to deduce a concrete solution to a hypothesis with the intention to solve the research problem once and for all. (Dudovskiy 2016)

One motive for choosing the exploratory research design to approach the research questions of this thesis is due to the nature of the subject matter, as the development of safeguards against information security threats and data leaks should be considered to be a process, because the existence of a potential final solution to the issue is highly improbable. Another motive for choosing the exploratory approach is that the common research methods which are characteristic of the exploratory research design are more applicable for researching the phenomenon of data leaks being caused by employee error. Exploratory research is also useful as an approach for the subject because it can lay the foundation for future research into specific research questions which can be researched in a more conclusive manner. (Dudovskiy 2016)

2.2 Research methodology

Commonly, the research methods that are used in exploratory research are qualitative rather than quantitative. A qualitative research method is defined as a research method that aims to get a nuanced perspective of the issue which is studied rather than to establish statistical data. (Dudovskiy 2016) In the process of examining different options for conducting qualitative research to gain results to the research questions that were posed, different types of methods were evaluated to ascertain which of them would be appropriate. Conducting a qualitative survey was chosen as one method for getting information from a portion of Nokia's employees, as using this method allowed for analyzing the connections between the different data that was collected from the survey, and gave the focus group opportunity to give more nuanced answers to the questions that were asked. Another reason for conducting a qualitative rather than a quantitative survey is the amount of Nokia's employees, because the available resources for this thesis were not sufficient for conducting a quantitative survey on the subject, as it would require a large enough portion of the company's employees in order for it to establish any accurate statistical data.

The results of the semi-structured interviews with information security management and the chief security officer serve as representation of the management's opinion on the expectations on the employees, and are used as a contrast to the results of the qualitative survey. A semi-structured interview is a research method where, when interviewing several people on an issue, the answers to the questions that were asked by all interviewees can be compared in order to establish more reliable data. The interviews also contained one or more questions which weren't prepared prior to the interview, either to adapt the interview to different areas of expertise among the interviewees, or to understand the opinions of the interviewees better through asking follow-up questions based on their answers. (Dudovskiy 2016)

2.3 Research questions

The most important research questions to be answered in the thesis related to the employee awareness of a company's information security principles, as in how the compliance of employees to the information security guidelines can be ensured through implementing information security awareness programmes in order to deter information security risks such as data leaks, and how the solutions to promoting information security awareness can be implemented at Nokia. Additional questions which are related to this issue are concerned with the relevance of social and behavioral factors on an employees' behavior regarding information security compliance, the probability of data leaks being caused by employee error in organizations and risks associated with the phenomenon, and finally the best courses of action in preventing data leaks proactively in a company.

3 Handling information within a company

When considering the subject of preventing data leaks that could be caused by employee errors, the issue is divided in to two components: errors that can occur when handling information, and the risks that are actualized when an error has occured. Handling information responsibly is a crucial component of ensuring information security in the company to reduce the likelihood of errors occurring in the first place.

In this section, issues relevant to handling information within a company are further elaborated upon. Firstly, the significance of information to a company in the form of information assets is discussed. General principles of information security, national and international legislation that sets requirements on handling information and the hierarchy of documents within a company that dictate how information security is to be implemented within a company are also relevant themes which are covered as well. The purpose of this section is to clarify the reasons for a company to handle its information assets responsibly.

3.1 Information assets

To understand the reasons for making the prevention of data leaks a priority, and the process of handling information within a company, one must first consider information as an asset to a company. But what are information assets? As defined by the Cambridge dictionary, information assets are pieces of information that has either financial value or are of other importance to the company. (Cambridge Dictionary 2016) Common examples of information assets could be financial reports, business plans, patents, non-disclosure agreements, client or employee information, or product and pricing information.

A company can lose its competitive edge against other companies in the market if for example specific information on a new product release were to be leaked. This means that information assets all have a form of value. But how is the value of information measured? Information as an asset can be difficult to appraise as it can either be measured in financial or non-financial contexts. However, several factors contribute to information being valuable to a company. One way to determine the value of information is to consider the estimated profit that could be gained to the company through the appropriate usage of it, or the cost of having it misused or lost. Information can be also be appraised based on its merits, for example the reference or source where the information had been gathered from, or how comprehensive or descriptive it might be. An information asset's value can also be measured in impact on the competitiveness of the company from a business perspective, either in the value of the company's ability to perform its business tasks effectively, or the impact on the company's reputation if the information's confidentiality is compromised. The value of information can also be measured by how much time is consumed in order to produce it, as an employee or

several would have to be compensated for the time spent producing the information regardless whether or not the information is kept safe in the company or lost, which creates a risk for additional company costs. (Laskowski 2014)

Figure 1: Information Lifecycle management

Another important factor to consider when measuring the value of information assets is the information handling lifecycle. Above is a figure that illustrates the lifecycle of handling information that has been made by Spirion LLC. (Spirion LLC 2016) Information that a company uses has its own lifecycle, which begins with the data first being collected in order to create information which is stored to be available for usage. Information in this stage, where it's still being processed and used for business purposes by a company, can be argued to be most valuable to the company for a number of reasons. Firstly, losing data at this stage could result in a loss of company productivity, as employee work hours likely have been used to produce the information. Secondly, if the information leaks to another company while it is still in this stage, it may have the most value to a competitor in the market. (Haeusser et al. 2007)

On the other hand, the stages of the information lifecycle that follow determine whether or not the information retains a value that necessitates continued protection. Information such as an annual review of the company's business may have very high confidentiality and protection priority while it is being produced or while the information contained within it could benefit the competition and affect the company adversely as a result. However, once the report is published according to an expected schedule, the information becomes public. While the report as information generates value to the company. When the report is published, the previously present risk of the information being exploited by other parties is eliminated, and the potential losses as a result of that risk being actualized is eliminated as well.

This is not the case for all information, as some information within the company retains its value to the company or is either personal information or otherwise has priority for being protected. This information, depending on the nature of it, has to be contained and stored within the company for a certain amount of time until it no longer can be seen as having value to a competitor or causing problems for the company if it would be leaked. This can be compared to storing radioactive waste, as the same principle of storing it until it no longer causes a hazard applies. Information can also have aspects to it that makes it necessary for the information to be destroyed in a secure manner, as it could even after having been stored for a longer period of time cause a data leak. (Haeusser et al. 2007) For this information, a secure disposal of confidential waste process is necessary. A common saying is that with great knowledge comes great responsibility, and this saying can be applied to a company's responsibility to handle their information assets.

3.2 Handling information assets responsibly

Handling a company's vital, mission-critical and even customer data correctly can be seen as a business principle by which a company can maintain high standards of business ethics. When a company conducts business with another company, they have to agree upon mutual standards for information security and methods for handling information.

To live up to this principle, a company has to collect, store, process and dispose data in a responsible manner. From a business model perspective, the prospect of losing the ability to compete with competitors in the market should be incentive enough for companies to make preventing data leaks from happening a priority, as it endangers the trust relationship between stakeholders. However, to actualize this principle, the handling of information in a company should be conducted according to information security principles.

3.2.1 Information security principles

There are information security principles that are widely accepted as the cornerstones of information handling that should be considered when handling information that is of importance. The most commonly used principles regarding information security are the principles of the confidentiality, integrity and availability of information. Confidentiality is the principle of preventing the unauthorized access of data, which could cause financial loss or other risks to the profitability of the organization when the confidential information is accessed by unauthorized users. An organization may be exposed to significant risks when an unauthorized user gains access to and modifies the valuable data of the company. Therefore, the integrity of information is a principle which companies may shape their information secu-

rity policy around. Finally, the information of the company should be kept accessible for the people who are authorized to view and make use of the information, even when measures are taken to safeguard the confidentiality of the information, which is why the availability of information has to be considered. (Vacca 2010, 49)

3.2.2 Legislation related to handling information

When a company uses or stores information, that information has to be handled within the company in a manner that satisfies the criteria that are created by contractual or legal obligations. This is especially true for personal data. Information which belongs to Nokia's customers may be handled in the company's business operations, and this information may include personal data. In the context of legislation, personal data is defined as information which can be used to identify a natural person. (Office of the Data Protection Comissioner 2016)

As Nokia's business operations are worldwide, the company is required to adhere to legislation regarding handling personal data both nationally and internationally. There are a number of regulatory requirements which are relevant in different parts of the world. In Finland, where Nokia has been founded as a company and has its headquarters, there is the Personal Data Act (523/1999) which contains all clauses which have been specified in the In the Data Protection Directive (95/46/EC) by the European Council. (Finlex 1999) Within the European Union, whenever there are updates to legislation, they have a different process of implementation depending on the type of legal act that is concerned. According to the EU legislative procedures, regulations are distinguished from directives, whereas the regulations are directly applied as law throughout the European Union, while directives are applicable by different means in each member country of the EU, as long as all clauses of the directive are met in the national legislation. Neglecting the legal obligation that a company has with regards to handling personal information may result in sanctions. (European Union 2016)

Additionally, the Information Society Code (as unofficially translated from the Finnish law "Tietoyhteiskuntakaari 917/2014") is very relevant for Nokia as legislation, as the Information Society Code includes several requirements pertaining to information security within communications. (Finlex 2014) This legislation has increased the authority as well as the responsibility of operators since it had been introduced, and this in turn affects Nokia as requirements on the protection of personal data have to be adhered to according to this legislation when Nokia handles personal data which belongs to one of its customers. (Teleforum Ry 2014) The Information Society Code also includes the legislation previously known as Lex Nokia (125/2009) which gives a company the right to monitor the email and internet activity of their employees for the purpose of proactively preventing threats to the information security

of a company and to protect the trade secrets. (Finlex 2009) (Tietosuojavaltuutettu 2015) (Korhonen 2014)

Similar legislation exists in other parts of the world where the company conducts business, such as the United States of America, where the National Security Agreement has specific requirements associated with data protection. There have also been updates in legislation in other areas as for example Russia, where the companies are now required to store personal information of customers and employees locally. (Gallia et al. 2015)

Additionally, further obligations can be dictated by customers of the Nokia Corporation by contract. Often, the customer contracts tend to contain more stringent limitations on how data should be processed. These customers, or some governments, may conduct audits during which the company's information handling and the success of the implementation of an information security training programme may be evaluated. A company such as Nokia could be adversely affected and face sanctions if for example an audit revealed non-compliance with data privacy legislation. (Päivänsalo 2016. Pers. com.)

As Nokia has very few private customers of its own, the largest responsibility associated with handling personal data is through the information which belongs to the customers of Nokia's customers. Therefore, the requirements that are imposed on Nokia through its customers are of very high importance when personal data protection is concerned. (Mölkänen 2016. Pers. com.)

3.3 Classification of information

In order to protect information assets in a company, the classification of information is a necessary task that has to be performed. When information assets are classified, they are given a level of classification based on the value of the asset. By establishing a system of classifying information assets according to their value, a company's most critical information can be identified and prioritized when either designing or applying existing safeguards against risks that can affect it.

Nokia has an extensive information breach management process blueprint that defines the different levels of information classification that is used within the company as follows: public information, Nokia internal use, confidential and secret information. (Nokia Corporation 2015) These levels of classification are intended to be used according to the best applicable category when considering which of the levels is to be used for a particular document. The approach of Nokia to using information classification is that the information which is classified as secret or confidential should be isolated as much as possible from information of lower levels of classification in order to facilitate the process of identifying

and securing the most critical information of the company. (Päivänsalo 2016. Pers. com.) (Rantanen 2016. Pers. com.)

The process of classifying information is a method for verifying that the balance between the confidentiality and the availability of information is maintained. Information should be readily available for anyone that requires it and kept away from those who shouldn't have access to it. Balancing these two principles of information security guarantees a good foundation which can help in preventing data leaks from occurring. Access to data which is classified should be restricted by default to designated personnel, who only should have access to as much data as necessary to complete their task. (Vacca 2010, 49)

Protecting sensitive data is a growing concern and an area of focus for Nokia. It is also an area of concern for their customers who are contractually obligating Nokia to ensure that they handle, protect, and manage appropriate access control to data. The importance of the process of identifying and securing the most critical information in Nokia has been recognized and is performed as a high priority function within the information security department. However, the responsibility does not lie solely with a centralized unit, but rather the company as a whole. As an example of this, it has been recognized that while the management of Nokia has a responsibility of making sure that employees are aware of information security instructions and guidelines and receiving the appropriate training that is necessary to carry out their work-related tasks securely and successfully, all its employees should realise their role in enforcing a workplace culture that supports the company's principles of information security. (Päivänsalo 2016. Pers. com.) (Vacca 2010, 49-50)

3.4 The hierarchy of principles, policies, standards, procedures and guidelines

With the principles of information security in mind, how does a company then proceed to plan its solutions to achieve these principles? The answer to this question is through policies. A policy is defined as a document which defines a plan by which the management achieves the company's principles. (Cambridge Dictionary 2016) In the case of an information security policy, the goal is to implement principles such as confidentiality, integrity and availability to the company. This hierarchy defines the levels on which a policy, which is at the highest position of this hierarchy, is employed to the workplace culture of the company by the company's management. Definitions of each level have to be made in order to distinct the tiers of this hierarchy more clearly.

In order to connect the employees of a company with an information security policy, lower-tier documents are required for specifying more concrete methods by which the employees should achieve the expectations that are set by the management through the principles of information security. To make an information security policy more accessible for a company's employees, specific procedures are constructed for achieving the plans which are made in the

policy. A procedure is by definition the instructions by which a task is to be completed to achieve a goal. (Cambridge Dictionary 2016) In the corporate world, documents specifying these types of instructions are called standard operating procedures "SOP"s. (Cambridge Dictionary 2016)

Instructions in a company's SOPs are often based upon standards. A standard is that is used is often defined as a widely-accepted minimum level of quality, (Cambridge Dictionary 2016) and in the case of information security, standards lay the foundation for the best information security practices which a company compares its procedures to. The ISO 27000 series of standards is a common reference which companies strive to live up to in their information handling processes. The motive for using these international standards as a reference point is to ensure that the information security policy and the procedures that made for employees based on it are compliant with internationally identified best practices. An international standard is however, in my opinion, not a level of document which is directly implementable as a procedure to dictate employees' behaviour directly for mainly two reasons. Firstly, I would argue based on the hierarchy that the international standards state identified best practices on a general level and aren't necessarily applicable to every detail and have to be specified further through guidelines and instructions. Secondly, it became apparent when interviewing Nokia's head of information security Antero Päivänsalo that in international corporations such as Nokia, differences in information security requirements can exist in different countries due to the difference in the nature of information security risks that are present in different environments. This variety of information security requirements necessitates a form of customization which can be provided through adapting the information security requirements and procedures in different areas that the company operates in. (Päivänsalo 2016. Pers. com.)

The last level of this hierarchy are guidelines. Guidelines, in the context of information security, are ideas which support the ideal methods of protecting information and give direction on how to implement information security. The ideals, however, are not written rules or procedures that an employee must follow, but rather given as recommendations for how a procedure (either related to information security or not) can be fulfilled more effectively or in a more secure or safe manner. (Cambridge Dictionary 2016) However, an employee makes a choice whether or not they want to perform tasks according to specific guidelines.

Below is a figure which has been made as based on the hierarchy of principles, policies, standards, procedures and guidelines by Walter Beddoe. (Beddoe 2015)

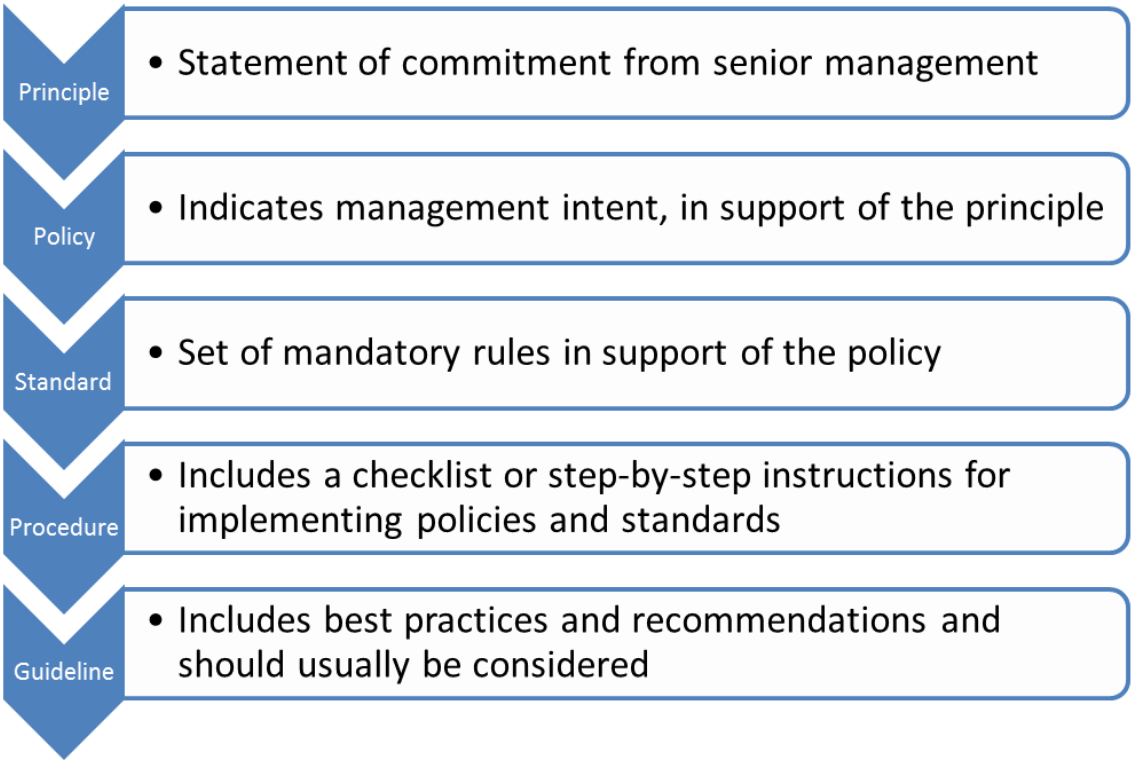

Figure 2: Hierarchy of principles, policies, standards, procedures and guidelines

4 Literature review: Employees' compliance, behaviour and the effects of the workplace environment

This section of the thesis is dedicated to further analyzing the factors that affect implementing information security awareness within a company by reviewing existing theories which are applicable for the subject matter by conducting literature review. The impact that different psychological and socio-psychological factors have on an employee's attitude towards complying with information security guidelines are analyzed by exploring the existing research in those areas. Lastly, theoretically established solutions to increasing information security awareness among employees will be considered in order to determine what a company can do to improve the workplace culture's inherent defence against data leaks.

To understand the behaviour of employees when they encounter information security related issues in their work, one has to consider decision-making and assessment of consequences from a psychological standpoint.

4.1 An individual's attitude towards compliance

Prevailing theories of behavioral psychology are relevant in the process of predicting the behaviour of individual employees, which can help in reducing information security risk likelihood if the theories are considered when creating procedures which are used to guide the

behaviour of employees. One such theory is the theory of planned behaviour. If the theory of planned behaviour were to be considered in the context of information security, one has to compare the information security instructions that are given to an employee versus the tasks which they perform on a daily basis and if the instructions can cause possible interference with those tasks. When an employee considers the consequences of their actions, there are three distinct categories which affect their decision-making process and their attitude towards complying with an information security procedure. These categories are the benefit of compliance, the cost of compliance and cost of noncompliance. (Bulgurcu et al. 2010)

When evaluating whether or not there is a benefit in complying with information security guidelines, an employee may consider the recognition they may receive from complying with the guidelines, or potential benefits which may facilitate their work, hence being intrinsically beneficial to being complied to. The cost of noncompliance is also a factor that increases the likelihood of an employee deciding to comply with a guideline due to the negative consequences of neglecting to comply with it, or simply the fear of those negative consequences. (Bulgurcu et al. 2010) The consequences which an employee may be afraid of facing could be the damage that could be caused to the reputation of Nokia or the trust relationships between customer companies of Nokia.

On the other hand, an employee may assess a certain aspect of an information security policy to be encumbering in their work and in turn will induce a cost of compliance. If the cost of complying with information security guidelines overrides the benefits of compliance and the costs of noncompliance, an employee's attitude towards complying with information security guidelines may be reduced, and they will in turn be more likely to attempt to find shortcuts or ways to reduce the costs of compliance in order to facilitate their work by making a decision not to comply with the encumbering guideline. (Bulgurcu et al. 2010)

4.2 Social factors and the workplace culture

As established previously, an individual makes their own evaluations in their work when they are faced with situations where complying with information security procedures which could be an encumbrance on their work. However, in modern companies, especially large companies where most business processes are maintained in social contexts, such as project work and teamwork, one individual's own evaluation of the necessity to perform tasks according to specific instructions to the letter, or attitude towards perform tasks according to guidelines, is not the only psychological factor to consider.

Work conditions and workplace culture is also a major factor that affects the implementation of information security controls and safeguards. An individual employee's personal experiences of and understanding of information security affects the company's information security,

and employees have varying levels of information security awareness and face information security risks to a varying degree depending on the information that they handle in their work. Even so, they all are equally required to understand the responsibilities they have with regards to information security while doing their part at the workplace. (Vacca 2010, 37) This is why theories about individual's behaviour in social contexts and interactions have to be examined as well in order to determine the impact of a company's workplace culture on the actions of an employee. A relevant concept within social psychology is the concept of face-work, which was coined by Erwing Goffman, is a factor which contributes to an individual's behaviour.

In basic terms, Goffman's theory is that individuals have a social identity which is the so called "face" which is shaped by the individual according to how the person wants to viewed by others in social circumstances. A person who is afraid of losing face in for example teamwork situations, someone may feel that they should avoid speaking their mind on a certain topic in the fear of losing face. This may also contribute to a person's fear of admitting that they have made a mistake in fear of losing face. Especially, if a person has specific expertise in a subject such as information security, it may be difficult for an expert to admit to making a mistake. An employee may also face a situation where they feel that they have a good understanding of information security risks related to a situation, but end up in a disagreement with a superior or a co-worker in the matter and choose not to speak their mind if there is a risk of impacting the relationship with a co-worker or superior, or a fear of losing face. (Goffman 1967, 5-9)

In their paper, Bulgurcu et al. argue that all these factors that affect the behaviour of employees, their intention of complying and their evaluation of consequences determine whether or not an employee is likely to be motivated to act according to a company's information security policy. This, in my opinion, is true only when the information security policy is used as a reference to how they should act in situations. However, while the information security policy is the ideal by which the employees should act, I would argue it is unlikely that an employee would change their behaviour or approach to information security simply through the awareness of a company's information security policy. The motive for the argument that knowledge of the company's ISP doesn't in itself motivate an employee to act according to it is further down in the hierarchy of principles, policies, standards, procedures and guidelines. As following information security guidelines is often recommended, but not necessarily mandatory to complete tasks, the compliance with information security guidelines needs to be incentivised through other means. (Pahnila et al. 2007)

The negative consequences for information security risks are also very strongly visible in the media, while positive images of information security are few in comparison. (Rantanen 2016.

Pers. com.) This can affect the way people perceive information security, and make them afraid of making a potential mistake when facing the possibility of being responsible for causing a loss of information.

4.3 Solutions for creating information security awareness among employees

In his Ph.D. titled "A design theory for employee information security awareness", Petri Puhakainen has conducted a comprehensive study of the current research that attempts to suggest solutions to increasing employees' awareness of information security risks in different ways, and that have identified the different factors that improve employees' attitude towards awareness of information security. Puhakainen criticized the majority of existing research that has attempted to suggest solutions to improve employees' compliance with organizations' guidelines for information security through awareness trainings and campaigns and other methods, as he deemed that most solutions which have been suggested haven't had a scientific basis for why the solutions were proposed. He had also concluded that the guarantees for the majority of suggested method of improving employee compliance through promoting awareness were lacking as there had been a lack of research on the effectiveness of the methods which would indicate that the method actually provided any benefit that could be established empirically.

Therefore, Puhakainen also conceived of three design theories for implementing information security awareness in a company. Puhakainen's three design theories consist of a framework for implementing information security awareness training, a framework for creating an information security awareness campaign, and finally a system by which rewarding and punishing employees with the intention of encouraging good behavior and deterring bad behavior to improve employees' compliance with a company's information security principles.
(Puhakainen 2006)

4.3.1 Designing a successful information security awareness training

Puhakainen established that in order for awareness training to be effective, there are conditions which are to be considered. As employees of different education and background have different levels of awareness, the potentially large differences in knowledge of information security should be considered. The applicability of the training that is implemented for employees should also be considered as the conditions where the employees get an opportunity to learn may differ greatly from the conditions that they may face in their work. Therefore, while implementing a training program, the conditions which the training takes place should also be explained to a participant in the training program while instructing them on the task itself. Lastly, the training which is to be implemented should not only make it possible for

employees to handle information in a secure manner, but also instill motivation in the employees which makes them willing to handle information correctly. To guarantee that the training is successful, the participants should also be tested to measure the success of the training.

As the types of training scenarios that can be arranged vary on the objectives of the training, the objectives of the training programme should be clearly defined. Depending on the type of issue that a practicioner wants to increase awareness on, it needs to be determined whether or not a training environment or task can be implemented at all, as there might be scenarios that can not be practiced, or tests can be conducted where one may not be able to measure the success of the training. (Puhakainen 2006, 70-76)

4.3.2 Creating a successful information security awareness campaign

A campaign within a corporation is a type of project which includes several activities that are performed in order to bring attention to a particular subject or achieve a specific result that benefits the company (Cambridge dictionary 2016) In his design theory, Puhakainen has applied the framework for creating a successful marketing campaign by Philip Kotler in the context of information security awareness.

According to the design theory of creating a successful information security awareness campaign, conducting a successful campaign rests on a foundation of successful communication between all the parties involved within it. If all communicating parties aren't participating in achieving the goals of the campaign, or are involved on different terms (meaning that some may have limited opportunity to express their opinion or to contribute to the campaign), or relevant information is excluded from some of the parties involved in the campaign, the campaign can not be successful in producing results that benefit the company as a whole.

The process of designing a campaign for improving information security awareness involves the following steps. Firstly, all stakeholders of the campaign and those who may be affected by it should be identified. This is essential for formulating the message that is to be broadcasted in the campaign. Similar to implementing training programs, campaigns should also have defined goals, as the type of message that the campaign is to have and the channels which are used to broadcast the message of the campaign depend greatly on the objectives of the campaign. A campaign cannot either be considered complete without using more methods than broadcasting a message through message channels, and so the additional methods which are to be used to bring the campaign into the company's attention and the available resources for conducting the campaign and enabling the practicioners of the campaign to make

use of the methods involved need to be determined both in material costs and immaterial costs.

The success of the campaign should, according to Puhakainen, be established in the same manner as when evaluating the success of a training program in that the effects of the campaign on the employees' information security awareness should be assessed to see if an improvement in the attitude or knowledge about risks and threats can be demonstrated.

Puhakainen articulated that campaigns may often be viewed as a process of handing down information from for example the management to the employees, and thus not creating a necessary communicating relationship between the parties involved in the campaign. The campaign can also not be successful if there is a perception that in order to achieve the results of the campaign, the responsibility lies with a specific section of the participants of the campaign, as the nature of a campaign is intended as a project that seeks to achieve an improvement throughout the whole organization. (Puhakainen 2006, 77-82)

4.3.3 Rewards and punishments

The implementation of a system where employees are awarded for behavior which is compliant with a company's information security principles and reprehends the non-compliant behavior of employees is the third design theory which Puhakainen suggests as a solution for improving information security awareness. The basis of this design theory is the assumption that employees will refrain from repeating behavior that causes negative consequences to them and that positive encouragement or rewards in other forms are likely to increase an employee's interest to become aware of information security procedures and guidelines. However, these rewards and punishments may be effective or ineffective depending on the employee's view of them. Observations which Puhakainen had made by assessing several studies that he referenced was that a financial reward in some cases is ineffective as a method for rewarding positive behavior, as it may only enforce behaviors rather than both behavior and attitudes, and that punishments may produce different forms of undesired side-effects that could impact the behavior of individual employees further even if the harmful behavior that negatively impacts the company's information security is prevented. An organization that intends to implement a reward and punishment system has to communicate it well to the employees in order for the system to be effective, and the specific behaviours which are rewarded and punished.

Among the design theories, the success of implementing rewards and punishments to improve information security awareness in companies is by far the one with the most contradictions in the results of research between individual theories. Therefore, it is vital that if a system of

rewarding and punishing employee behaviors were to be implemented in a company, the effectiveness and consequences of having rewarded or punished employees should be monitored to establish whether or not the methods which are used in the company are effective and promote the goal to improve information security compliance and awareness of the company's information security principles. (Puhakainen 2006, 82-87)

5 Case study: The "human error"-factor's impact on Nokia

The focus of this section is on establishing where the specific potential problem in enforcing employee information security awareness in Nokia, what the impact of the phenomenon of data leaks happening as a consequence of an employee's error could be on a company such as Nokia, what the associated risks are as based on the previous section and the results of the qualitative research that was conducted, and which of the risks specifically cause the largest threats within Nokia.

A SWOT analysis was also conducted to provide further data to analyze in the process of conducting risk assessment. The abbreviation SWOT stands for strengths, weaknesses, opportunities and threats, and this form of business analysis helps to distinguish the good and worse qualities of a company, and it also helps to identify which development areas a company can improve on to increase its profitability. (Dudovskiy 2016) The SWOT analysis that was conducted had a specific focus on information security aspects of the company and other aspects of Nokia as a corporation which are relevant to the subject.

5.1 SWOT analysis with a focus on information security

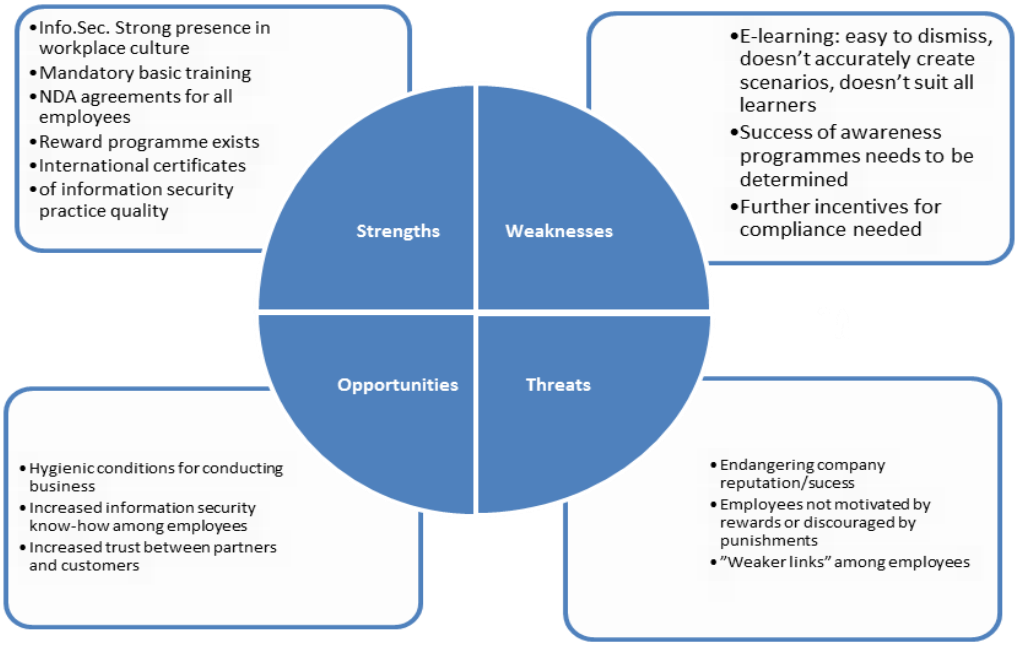

Figure 3: SWOT analysis

With regards to information security, there is qualitative data that implies that Nokia has many strengths in the subject. In Nokia, information security is present in daily work in services. As stated by the Nokia information security managers in Nokia, these are considered prerequisites rather than responsibilities for Nokia to conduct its business. The fact that information security is a strong component of the company's workplace culture is a factor that increases the general awareness among the employees about the subject.

A concrete example of Nokia's preparedness against information security threats is that in order to increase awareness of information security risks among employees, there are a number of security and privacy trainings, such as the "Data Storage Protection" training. (Rantanen 2016. Pers. com.) Providing trainings like this to employees who are deemed to need it in order to perform their work-related tasks may increase the risk resilience of the company as a whole, and the goal is to integrate the new and existing policies, guidelines and instructions to the workplace culture.

As a method of there are different categories of E-learning trainings which have been directed to certain employees who have a specific need for additional awareness of information security because of the work they are performing and the information they handle for those tasks. Attendance and participation by employees to any training programs which are created in order to increase awareness and knowledge about information security threats and best information handling practices is the key to make sure that the employees of the company live up to the expectations and requirements that are set by the management.

When considering the strength of a company's performance in information security, an important method for evaluating it is conducting benchmarking. International standards of information security management are not only effective for being used as a comparison for generating best practices of information security in a company and shaping a company's information security policy around, but are also useful for benchmarking, as a company can be certified in having implemented a specific standard throughout the company. When a company has this certification, it is easier to determine the level of quality of the information security that the company has achieved.

Weaknesses, or areas to be developed upon, were recognized by the information security management as well. One aspect that comes with the large size of the company is the monitoring the effectiveness of implementing information security training to newly recruited employees. The responsibility of making sure that a new employee receives information security training is largely left with the line managers of the new employees, and the newer employees of Nokia may face risks related to information security before they receive any form of information about the company's guidelines for employees. In the recruitment process of Nokia, it is mandatory for the new employee to sign a nondisclosure agreement (NDA), which a method to instill responsibility in the hope of preventing information from leaking outside of the organization. The process of making all employees sign an NDA is a method which a common understanding at the workplace is established about sharing classified information that they may have access to, and a method that makes the employees responsible for their actions and enables for them to be held legally accountable for those actions as well.

Nokia also has a specific policy in place which defines methods by which disciplinary action is implemented when violating information security procedures in the company, such as installing unlicensed software on a machine or sending spam emails from a Nokia email account. Concerning this topic, I would argue based on the previously mentioned theory of planned behaviour that while an information security and IT violation disciplinary action policy exists and employees are required to sign an NDA (which are both factors that contribute to the perceived cost of non-compliance), an employee may still not actively consider the positive outcomes of well-implemented information security without being further incentivized to follow guidelines to generate perceived benefits of compliance. However, it must be mentioned that within the human resource department of Nokia, there is a function by which the management can reward good employee behaviour, not only regarding information security but in general. (Mölkänen 2016. Pers. com.)

As confirmed by chief security officer Petteri Rantanen of Nokia Corporation, Nokia has mostly focused on implementing their information security awareness training in the form of E-learning. (Rantanen 2016. Pers. com.) While there are benefits to e-learning which include the constant availability of a training program that can be accessed and completed by employees of Nokia, there are also some issues with E-learning that have to be considered. If not

considered mandatory by an employee, they may dismiss an E-learning course easily due to the fact that it is always available. They may also dismiss the program out of a lack of time beside their other work. It is also relevant that different people prefer different methods of learning (Figure 7), and simply focusing on improving awareness among employees through one method isn't enough. Therefore, there is a need for creating further possibilities and programs which may be more effective to improve the awareness among employees that would normally dismiss E-learning courses.

It was also recognized, based on the interviews that were conducted, that confirming the effectiveness of implemented information security awareness programs is difficult as well, not only due to the amount of people employed by Nokia but also due to the fact that the employees generally are trusted to handle information correctly. (Leiviskä 2016. Pers. com.) While a strong presence of information security within a company's workplace culture is the ideal which all companies strive for, there is also potential for a false sense of security. In order to avoid a false sense of security, verification processes are required to verify that the trust isn't misplaced.

What threats exist in the realm of information security? The current expectations on the professionalism of employees are fairly high, and this includes the ability to handle information correctly and responsibility according to a company's information security principles. The section of Nokia's management that were interviewed unanimously agreed that there always is a priority to proactively prevent data from leaking on a workplace culture level, and a strong awareness of the potential risks which are relevant to one's own tasks helps to reduce the likelihood of mistakes in handling information from occurring.

While several threats exist in the information security field, it also creates opportunities for a company like Nokia. Benefits of creating a secure environment is that it creates hygienic conditions for conducting business. This is especially beneficial as the trust relationship between service providers and customers is vital for conducting business. (Leiviskä 2016. Pers. com.)

5.2 Risk assessment and analysis

At this point, it is relevant to make distinctions and definitions clearer to establish what the specific research question really is asking. How does one approach the subject of data leaks as a risk? Whereas an information asset in a company may be exposed to risks, it is important to recognize that this does not automatically lead to a data leak. Therefore, incidents have to be distinguished from data breaches. An information security incident occurs when an information asset has been compromised, but a breach on the other hand occurs when a company can identify that information has been leaked. This is a difference which is important to recognize, as information security incidents are what lead to breaches occurring. (Verizon 2016. 5)

There are several factors that contribute to the likelihood of a human error occurring when handling information in a company. But, what are the specific risks associated with the specific consequence of a data leak happening as a result of an information security incident that was caused by an employee's error within an organization? Data leaks can be varied in the source and the nature of the leak. They can be either caused by hackers or other attackers from outside a company, deliberate negligence or insider threat by an employee, or by unintentional negligence or human error within a company. (Verizon 2016) However, only the risks which create a larger likelihood for a human error to occur in Nokia or increase the potential damage that a data leak could cause will be considered relevant to the risk assessment that is conducted in this thesis.

To further investigate these risks, the Fine-Kinney method of risk assessment was used to assess the individual risks. The Fine-Kinney method consists of evaluating the exposure to a risk, the likelihood of a risk occurring and the consequences of the risk if it were to be actualized. (Top 2012)

Firstly, let us take a look at malware as an information security risk. Malware is a category of software below which many different types of specialized malware can be classified (eg spyware, adware, etc.) and those more specific terms can be applied to describe several different types of technology themselves. The general characteristic of malware is that these pieces of software are intended to cause harm or to be used for nefarious purposes. (Cambridge Dictionary 2016) Among other methods, cyber criminals use so-called phishing attacks to distribute malware to varied recipients. These phishing attacks can be classified as a form of social engineering as the manufacturer of phishing emails attempt to mask their false emails to look like legitimate email requests. Usually, the emails encourage a victim to open a link to a malicious website or some form of malware included within the email.

In an environment such as Nokia, spam messages with malware and social engineering attempts are very common ways which cyber criminals attempt to introduce their malware. An employee may mistake a received message as legitimate and thus cause a malware infection to their computer and thereby cause a security incident that has the potential to cause a data leak if the malware is able to gain access to a computer that has confidential information. However, phishing attacks are very commonplace and a basic knowledge of the nature of phishing attacks is likely to be enough for an employee to identify phishing attempts. This type of attack is also dependant on the actions of the recipient, which means that the probability of a phishing attack being successful is rather low. According to Verizon's data breach investigations report, 13% of people who receive them get fooled by phishing emails (Verizon 2016. 17).

In what ways can careless information handling cause security incidents? Common risks which can be associated with this category of data leaks are any situations where employees are ignorant of guidelines on information handling and processing or carelessness, such as incorrect disposal of information, unintentional sharing of information with the wrong parties, incorrect classification of information, lost or misplaced hard copies of information ending up in the possession of unauthorized people, and allowing malware to enter a system via social engineering or other sources. (Verizon 2016)

A company should destroy its confidential waste using proper methods which are applicable to the medium which the information is stored in. For example, digitally stored data can require using a method such as crypto-shredding to destroy the information completely, while paper shredders and confidential waste bins with locks are appropriate for getting rid of physical copies of the information. However, a company can further reduce the risk of a security incident occuring by avoiding to use hard copies of information in the first place.

One additional factor that can contribute to information security not being achieved could be the complexity of solutions integrated in a company's information system. An information system in a company is defined by the Business Dictionary as "a combination of hardware, software, infrastructure and trained personnel organized to facilitate planning, control, coordination, and decision making in an organization". (Business Dictionary 2016) The risk of information security measures within an information system not being adequate to protect the company's information can be dependant on factors related to every aspect of that combination. The software or hardware solutions for securing information can be too simplistic and do not secure the information completely in their simplicity, due to the fact that the threats in the realm of cyber security are sophisticated and adapt to change, which increases the requirement to implement more complex solutions. However, it has to be understood that when more complex solutions are implemented to achieve improved security, personnel are required to have further expertise for the safeguards to be used properly. (Paganini 2015) (Leiviskä 2016. Pers. com.)

The solutions to secure information, can also be too complex as they may not be understood by employees. Therefore, a balance is ideally achieved in securing a company's information system by providing adequate training for the employees, as well as keeping them informed on changes in procedures. (Leiviskä 2016. Pers. com.)

The most important information that is handled within Nokia can be centered to a few key areas. Firstly, the highest level of management within the company, and the next tier of management that reports to the highest management. Other critical information is contained

within the product and research & development departments, and some areas such as the sales department may have access to information such as the true costs of the products that are supplied to the customers of Nokia. These are areas where information security is most important to implement. (Päivänsalo 2016. Pers. com.)

5.3 Qualitative survey results and analysis of results

In order to assess the current state of Nokia's preparedness against the risk of a data leak occurring through an employee's error, a focus group of 25 of the company's employees were surveyed about their knowledge of the company's information security policy, instructions and guidelines, their confidence in their personal knowledge of information security, a well as the importance and relevance of information security to their work, and if they had faced situations where they felt they couldn't assess potential information security risks on their own. The group was also asked about how long they had been in the company, information security training they have received, as well as discussing the challenges that cause the most concern to the employees regarding information security.

All members of the focus group were given an ID number from 1 to 25 in order to separate analyze the correlation between specific data that was collected for individual members of the focus group. It is also worth mentioning that the focus group was heterogeneous, including individual of different nationality, gender, age and time as a Nokia employee. The time range of the durations of the employees' careers at Nokia varied between having been at Nokia for four months to 31 years, and the calculated average for all survey participants was 12,8. Nokia staff within information security management or in direct contact to them were not included in the focus group to get more accurate statistics on the information security knowledge of employees not directly involved with the subject.

There were some general observations to be made based on the answers of the focus group. There was a general consensus within the focus group that the importance of information security cannot be denied. On a scale from one to five, the average value on perceived importance / relevance of information security in the respondent's work was 4.52. (Figure 4)

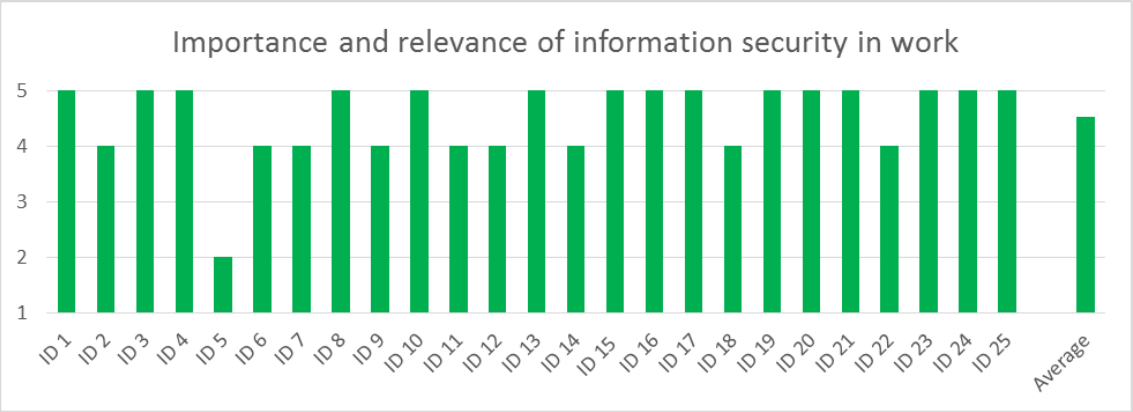

Figure 4: Perception of importance and relevance of information and security in work

This number shows that the subject is taken very seriously in the company, and the employees recognize that they have a responsibility in protecting the company's information. However, among the answers to the open ended question about the opinion on information security, some respondents highlighted that they felt that information security can difficult in its technical aspects. Some also recognized that information security can be a "hurdle" or an obstacle that potentially could interfere with their work.

Average values were also calculated for some questions. On a scale from one to five, the average knowledge of Nokia's information security policy and related procedures and guidelines was estimated at 3.48 (Figure 5), while the personal confidence in their general knowledge of information security is generally higher, at an average value of 3.88 (Figure 6). However, in determining the significance of these average values that were calculated, they were calculated simply on an observational basis rather than to attempt to create a statistical representation of Nokia employees' information security awareness in general.

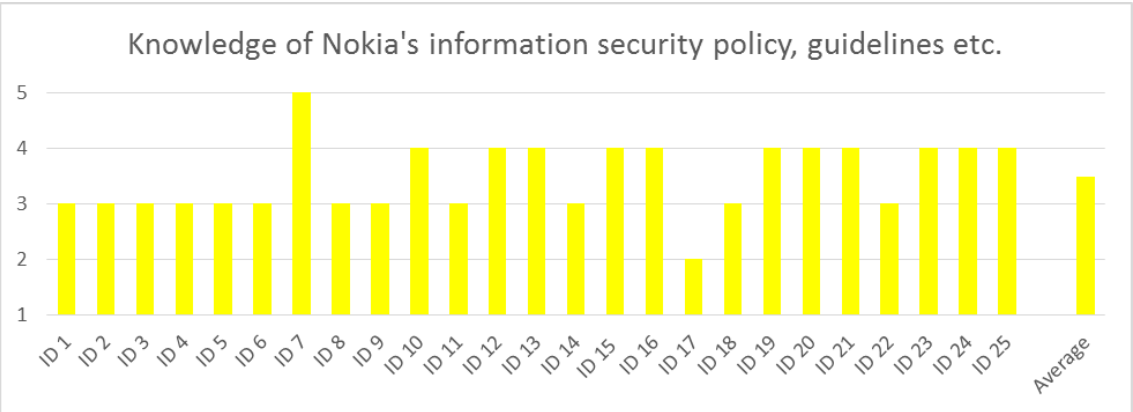

Figure 5: Employee knowledge of information security policy, guidelines etc.

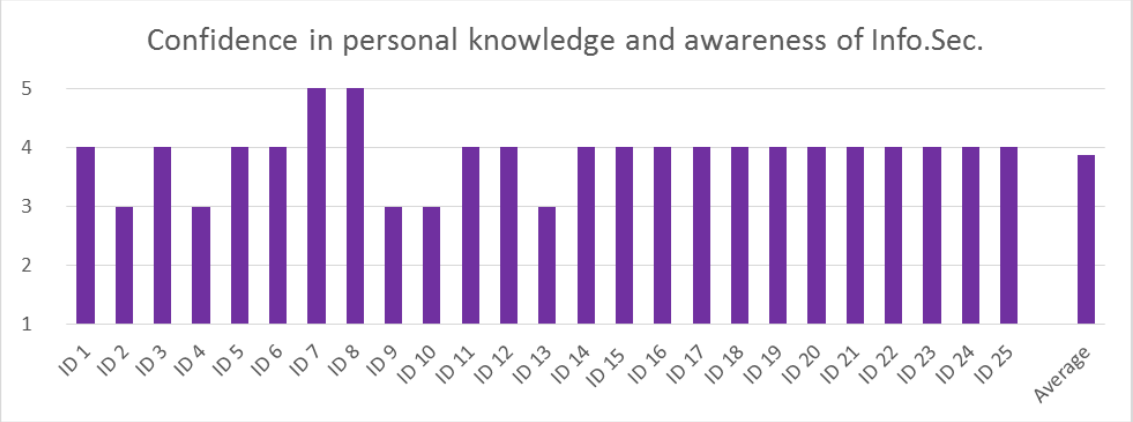

Figure 6: Employee confidence in personal knowledge and awareness of Info.Sec.

The likely explanation for the difference in these numbers is that reading the guidelines and other documents to have a is merely recommended and not mandatory, because there isn't a specific need for such a practice. According to chief security officer Petteri Rantanen, it is not important for employees to be familiar with the information security policy or any explicit documents, as long as they have the knowledge and awareness of best information security practices and are able to integrate that into their own work and deter information security risks through that. (Rantanen 2016. Pers. Com.)

However, when comparing the general knowledge of information security with the perceived importance and relevance to their work, the need for making these values align can be deemed to exist, which articulates the need for implementing information security related campaigns and training programmes to accomplish them.

All survey participants who have been at Nokia more than one year have attended the mandatory basic information security training, one of test group who has been in Nokia less than a year has not attended. The likely explanation for this is that the training is arranged once every two years and they have not yet had an opportunity attended. Additionally, 14 of 25 have attended one or more additional information security trainings during their time at Nokia. However, 17 out of 25 employees were interested in receiving additional opportunities to learn about information security.

The survey participants expressed several concern areas which they felt that were challenging regarding information security when handling information. For example, issues such as handling large amounts of communication could lead to sending the wrong information to the wrong recipient, thus creating the potential for sharing the wrong information with the wrong parties. Knowing when it is allowed to share information that is requested by different parties was also considered risk situation which could create a challenge. The survey participant with ID number 7, who had expressed a high confidence in their own personal information security

knowledge and high knowledge of Nokia's information security guidelines expressed that they felt it is difficult to trust other people's awareness of information security, as they suspected that differences in the level of information security awareness could lead to weaker links among the employees and thus creating a weaker link in the information security of the company.

Other challenges were expressed regarding the ever-developing and altering nature of information security. Some expressed that new tools with new features could have information security aspects that should be considered which weren't immediately clear, while others mentioned staying "on board" with the changing requirements with regards to information security. Knowing the differences between information security requirements and legislation in a global company was also expressed as a concerning issue for some of the respondents.

When asked about the method by which the focus group would consider most effective for learning about information security, the respondents' answers varied to a large extent. In the following chart, the percentage of group participants preferring a certain method for learning about information security is represented. Category 1 (yellow) represents participants who prefer training events such as meetings or other face-to-face activities, category 2 (purple) represents the participants preferring E-learning opportunities such as online courses and online seminars. Category 3 (green) felt that they might learn most effectively by receiving bulletins or through other methods with a short amount of information to take in on a regular basis. Lastly, category 4 (red) said that they didn't feel strongly about any certain method, and category 5 (blue) did not provide an answer to the particular question.

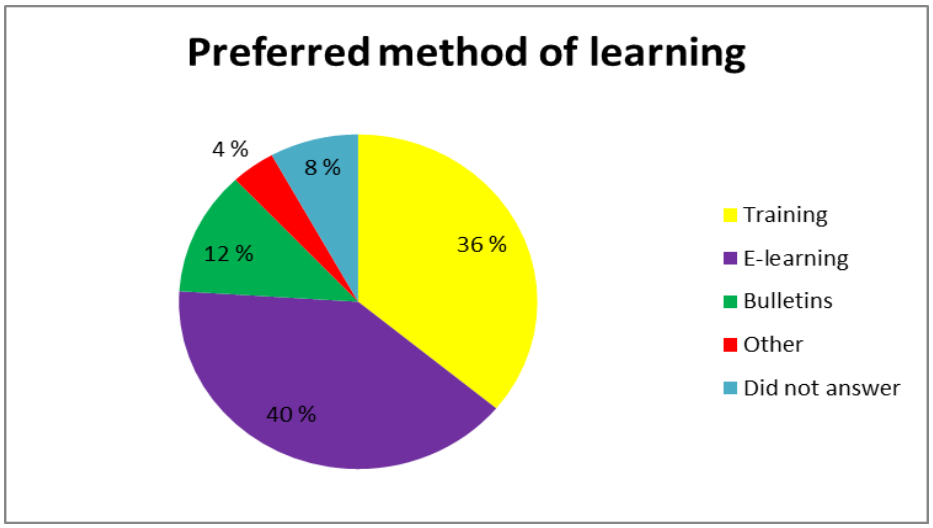

Figure 7: Preferred method of learning about information security

6 Adapting solutions for increasing information security awareness among employees of Nokia

This section of the thesis is dedicated for discussing the practical implementation of a information security awareness program in the case of Nokia, and considering any additional factors that might affect implementing solutions.

How can the solutions proposed for improving information security awareness be applied to improve awareness among the employees of Nokia? According to CSO Petteri Rantanen, the training and education material which is provided for Nokia employees is mainly implemented through E-learning courses, but the aims are to increase the variety of training programmes available to suit the different types of employees own preferred learning style. As almost 50% of the respondents to the survey felt preference towards other methods, it highlights that there is a need for providing training in other forms than simply through E-learning. (Figure 7)

Considering the nature of data leaks and preparation against them, creating one training programme can be difficult if the objective were to comprehensively prepare the participants for preventing every risk scenario that could potentially cause data leaks, but a potential method to approach this problem could be to arrange a series of information security awareness trainings which gave participants an opportunity to face individual information security risks which can result in data leaks in as accurately built scenarios as possible with an evaluation of the individual employees' performance after each training has been completed. This series of training programmes, combined with a reward system that could award the participants with diplomas or another form of rewards which potentially could even be listed on a curriculum vitae as a sign of competence in responsible information handling, could have the potential of improving employees' information security awareness. In some areas of Nokia, such as the financial or legal departments, or other departments where responsible handling of information is a vital principle, this type of opportunity for an employee to develop themselves and strengthen their personal portfolio is something which a large number of employees within the company could consider as a benefit, given that it were possible for Nokia to arrange such training programmes.

Where future developments in information security related legislation are considered, there are large changes in the near future which require the attention of companies such as Nokia. The European General Data Protection Regulation (GDPR 2016/679) is an update to the current legislation on processing personal data which will be introduced the 24th of May 2018, which will replace the Data Protection Directive (95/46/EC), and the Directive of the European Parliament and of the Council (2016/680) which was introduced in May 2016 has to be implemented to the legislation of every EU member state by the 25th of May 2018. (European

Commission 2016) The GDPR and other updates to legislation on personal data will likely make companies further responsible for protecting personal data and show evidence for doing so. Nokia also has to follow potential changes in regulation in the United States after having merged with Alcatel Lucent. (Rantanen 2016. Pers. com.)

At Nokia, future legislation regarding information security requirements that concern data protection is prepared for by conducting risk assessment and management within the company as well as reviewing the consequences of the updated legislation and potential necessary changes to business procedures with the company's customers. (Mölkänen 2016. Pers. com.)

7 Conclusions

Awareness of information security threats is crucial for preventing security incidents that could result in data leaks in organizations. While Nokia employees are expected to know how to handle the information that they gain access to while working at Nokia on a workplace culture level, there are challenges and threats related to information security that are always present regardless whether or not the risks are mitigated, which requires that the employees have a responsibility to consider information security practices while they handle the company's information.

However, the management of the company also has a responsibility to monitor the success of information security awareness programs that they may implement to improve the awareness of the employees. There are great opportunities to improve information handling practices within Nokia and the presence of information security in the workplace culture by implementing information security campaigns and training programs. Not only may the information security practices in Nokia improve, but positive outcomes can also manifest as potential benefits for specific employees that not only can improve the employees' confidence in their personal knowledge about information security, but can also increase their motivation to perform their normal work duties better from an information security point-of-view. To tap in to those opportunities, information security awareness training programs have to be developed to be motivational and relevant for the work of the employees.

Developing information security awareness trainings, campaigns and reward systems may require constant attention from those that design them, but the quality of those programs has potential to be perpetually increased in the process.

8 Refutability of the research in the thesis and potential for further research

What potential issues could affect the credibility of the research that was conducted? A number of problems regarding the falsifiability of the research that was conducted for this thesis can be determined as based on the methodology that was used. For example, qualitative research methods are deemed problematic in the sense that the data which was produced for this case study may not be reproduced if the research were carried out again by another researcher, especially if a similar qualitative were survey conducted with another focus group, the results may vary greatly from the results that were produced in this study. Other problems that apply to the qualitative methods that were used in the thesis are that the interpretations of data that was collected through the research methods such as the semi-structured interviews and the survey are subject to bias, and since the information security knowledge between different employees of Nokia varies greatly, (Leiviskä 2016. Pers. com.) the research results which were produced with the focus group are not likely to represent the information security knowledge of Nokia's employees as a statistical average. (Dudovskiy 2016)

The focus group was randomly chosen within the company but also excluded any information security specialists. The likelihood of bias towards the subject matter is therefore determined to be low. However, some survey participants left some questions unanswered, and might therefore have chosen to withhold their opinions. Also, it unclear whether or not some survey participants may try to appear more knowledgeable than they are, which affects the credibility of the gathered results.

Studying the implementation and effectiveness of a potential training programmes that would be focused in the subject of preventing a specific type of risk that could cause a data leak, or the effectiveness and success of information security awareness campaigns in further detail are subjects which have room for further research. Also, conducting further research in the success of methods which Nokia uses to incentivize employees to increase their information security awareness could reveal to be fruitful for the company.

References

Beddoe, W. 2015. Understanding the hierarchy of principles, policies, standards, procedures and guidelines. Accessed 11 November 2016. https://www.linkedin.com/pulse/understanding-hierarchy-principles-policies-standards-wally-beddoe

Bulgurcu, B., Cavusoglu, H. & Benbasat, I. 2010. Information Security Policy Compliance: An empirical study of rationality-based beliefs and information security awareness. MIS Quaterly. Accessed 6 November 2016. http://aisel.aisnet.org/cgi/viewcontent.cgi?article=2919&context=misq

Business Dictionary. 2016. Information system meaning and definition. Accessed 7 November 2016. www.businessdictionary.com/definition/information-system.html

Cambridge dictionary. 2016. Meaning of "campaign" in the English dictionary. Accessed 7 November 2016. http://dictionary.cambridge.org/dictionary/english/campaign

Cambridge Dictionary. 2016. Meaning of "guideline" in the English dictionary. Accessed 7 November 2016. dictionary.cambridge.org/dictionary/english/guideline

Cambridge Dictionary. 2016. Meaning of "information asset" in the English Dictionary. Accessed 7 November 2016. dictionary.cambridge.org/dictionary/english/information-asset

Cambridge Dictionary. 2016. Meaning of "policy" in the English dictionary. Accessed 7 November 2016. dictionary.cambridge.org/dictionary/english/

Cambridge Dictionary. 2016. Meaning of "procedure" in the English dictionary. Accessed 7 November 2016. dictionary.cambridge.org/dictionary/english/procedure

Cambridge Dictionary. 2016. Meaning of "standard operating procedure" in the English dictionary. Accessed 7 November 2016. dictionary.cambridge.org/dictionary/english/standard-operating-procedure

Cambridge Dictionary. 2016. Meaning of "standard" in the English dictionary. Accessed 7 November 2016. dictionary.cambridge.org/dictionary/english/standard

Dudovskiy, J. 2016. Conclusive research. Accessed 4 November 2016. http://research-methodology.net/research-methodology/research-design/conclusive-research/
Dudovskiy, J. 2016. Exploratory Research. Accessed 4 November 2016. http://research-methodology.net/research-methodology/research-design/exploratory-research/

Dudovskiy, J. 2016. Interviews. Accessed 4 November 2016. http://research-methodology.net/research-methods/qualitative-research/interviews/

Dudovskiy, J. 2016. Qualitative Research. Accessed 4 November 2016. http://research-methodology.net/research-methods/qualitative-research/

Dudovskiy, J. 2016. Research Design. Accessed 7 November 2016. http://research-methodology.net/research-methodology/research-design

Dudovskiy, J. 2016. SWOT Analysis. Accessed 6 November 2016. http://research-methodology.net/theory/strategy/swot-analysis/

European Commission. 2016. Reform of EU data protection rules. Accessed 6 November 2016. http://ec.europa.eu/justice/data-protection/reform/index_en.htm

European Union. 2016. Regulations, Directives and other acts. Accessed 6 November 2016. https://europa.eu/european-union/law/legal-acts_en

Finlex. 1999. Henkilötietolaki. Accessed 11 November 2016. http://www.finlex.fi/fi/laki/ajantasa/1999/19990523?search%5Btype%5D=pika&search%5Bpika%5D=tietosuoja

Finlex. 2009. Laki sähköisen viestinnän tietosuojalain muuttamisesta. Accessed 11 November 2016. http://www.finlex.fi/fi/laki/alkup/2009/20090125#Pidp1025392

Finlex. 2014. Tietoyhteiskuntakaari. Accessed 11 November 2016. www.finlex.fi/fi/laki/ajantasa/2014/20140917

Gallia, A.L., McLoughlin, L.P., Khaskelis, A.S. & Voltchenko, M.A. 2015. Russian Federation: Russia's Personal Data Localization Law goes into effect. Accessed 6 November 2016. http://www.mondaq.com/russianfederation/x/435890/Data+Protection+Privacy/Russias+Personal+Data+Localization+Law+Goes+Into+Effect

Goffman, E. 1967. Interaction Ritual: Essays on Face-to-Face behaviour. Penguin Books.
Haeusser, B. et al. 2007. ILM Library: Information Lifecycle Management Best Practices Guide. IBM Redbooks Web site. IBM Redbooks Accessed 4 November 2016. http://www.redbooks.ibm.com/redbooks/pdfs/sg247251.pdf

Korhonen, S. 2014. Lex Nokia ei katoa mutta siirtyy. Accessed 6 November 2016. http://www.tivi.fi/Uutiset/2014-01-30/Lex-Nokia-ei-katoa-mutta-siirtyy-3207516.html

Laskowski, N. 2014. Six ways to measure the value of your information assets. Accessed 4 November 2016. http://searchcio.techtarget.com/feature/Six-ways-to-measure-the-value-of-your-information-assets

Nokia Corporation. 2015. Information Breach Management Global Process Blueprint. Classified source: Nokia Internal Use

Nokia Corporation. 2014. Information Security and IT Violation Disciplinary Action Policy.

Nokia Corporation. 2016. Nokia government relations policy paper on cybersecurity in the programmable world. Nokia Corporation Web Site. Accessed 24 October 2016. http://company.nokia.com/sites/default/files/download/nokia_government_relations_policy_paper_on_cybersecurity_in_the_programmable_world.pdf

Office of the Data Protection Comissioner. 2016. EU Directive 95/46/EC - The Data Protection Directive. Accessed 4 November 2016. https://www.dataprotection.ie/docs/EU-Directive-95-46-EC-Chapter-1/92.htm

Paganini, P. 2015. What causes an information security program to fail? Accessed 6 November 2016. https://www.veracode.com/blog/2015/12/what-causes-information-security-program-fail

Pahnila, S., Siponen, M. & Mahmood, A. 2007. Employees' behavior towards IS Security Policy Compliance. CiteseerX. University of Oulu, Department of Information Processing Accessed 6 November 2016. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.106.7038&rep=rep1&type=pdf

Puhakainen, P. 2006. A design theory for information security awareness. University of Oulu, Department of Information Processing Accessed 4 November 2016. http://jultika.oulu.fi/files/isbn9514281144.pdf

Spirion LLC. 2016. The phases of Data Lifecycle Management (DLM). Accessed 11 November 2016. www.spirion.com/us/solutions/data-lifecycle-management

Teleforum Ry. 2014. Tietoyhteiskuntakaari voimaan 2015 alusta. Accessed 6 November 2016. https://www.teleforum-ry.fi/uncategorized/tietoyhteiskuntakaari-voimaan-2015-alusta/

Tietosuojavaltuutettu. 2015. Tietoyhteiskuntakaari. Accessed 6 November 2016. http://www.tietosuoja.fi/fi/index/lait/sahkoisenviestinnantietosuojalaki.html

Top, W. 2012. Risk Classification. Accessed 11 November 2016. http://www.topves.nl/risk-classification.html

Vacca, J.R. 2010. Managing Information Security. Burlington: Elsevier Science.

Verizon 2016. Data Breach Investigations Report. Accessed 11 November 2016. http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/

Figures

Appendices

Appendix 1: Nokia Information Security Survey

Information Security Survey

Q: How long have you been at Nokia?

Open answer

Q: What is your opinion about information security?

Open answer

Q: How familiar are you with the information security policy and other information security related guidelines of Nokia? (Answer by circling the most appropriate alternative)

1 - 2 - 3 - 4 - 5

Q: Do you know where to look for information security guidelines if you need them? (Answer by circling the most appropriate alternative)

Yes / No

Q: How confident are you in your personal knowledge of information security? (Answer by circling the most appropriate alternative)

1 - 2 - 3 - 4 - 5

Q: How important/relevant do you consider information security to be in your work? (Answer by circling the most appropriate alternative)

1 - 2 - 3 - 4 - 5

Q: Have you attended the mandatory basic information security training which is arranged by Nokia? (Answer by circling the most appropriate alternative)

Yes / No

Q: Have you received any other information security training during your time at Nokia? (Answer by circling the most appropriate alternative)

Yes / No

Q: If you have, how many sessions have you attended?

Open answer

Q: Would you like to receive more opportunities to learn about information security? (Answer by circling the most appropriate alternative)

Yes / No

Q: What would you consider an effective way to learn about information security?

Open answer

Q: What do you personally find most challenging about information security?

Open answer

Q: How often have you during your work faced a situation or a problem where you felt you couldn't assess the potential information security risks on your own? (Answer by circling the most appropriate alternative)

Never / Seldom / Occasionally / Often

Q: If you need guidance in information security procedures and guidelines, who / what do you turn to?

Open answer

Appendix 2: Nokia employee error risk assessment

Detailed description	RISK DEGREE	Source	Type	Subtype
Detailed scenario of a risk	*R = E x P x C*	*Source type*	*Event type*	*If needed*
Malware introduced into employee computer through social engineering. An employee may mistake a received message as legitimate and thus cause a malware infection.	160	Employee error / Outside attacker	Malware infection / Social engingeering	Risk depends on employee's actions
Information sent to wrong recipient. An employee may send confidential information to an unauthorized party by mistake, or be instructed to send something by another person.	350	Employee error / incorrect instruction	Careless information handling	
Incorrect disposal of information. An employee may dispose of information in an incorrect manner (not using confidential waste bin or paper shredder) or be incorrectly instructed to do so, and the information could be accessed by an unauthorized party.	105	Employee error / incorrect instruction	Careless information handling	
Incorrect classification of information. Information may be given an incorrect classification level that does not comply with Nokia's policies by mistake.	60	Employee error / incorrect instruction	Careless information handling	
Hard copies of information compromised. A hard copy of confidential information may be lost or misplaced and be found by an unauthorized person.	14	Employee error / incorrect instruction / Outside attacker	Careless information handling	
Unauthorized person's unreasonably easy access to employee credentials. An employee may not use passwords of adequate strength and thus create opportunity for attackers.	600	Employee error / Outside attacker	Carelessness / Negligence	Risk depends on employee's negligence of information security principles

EXPOSURE	PROBABILITY	CONSEQUENCES	TYPE OF CONSEQUENCE
Estimated exposure to risk (0.5 - 10)	*Estimated probability of risk occurrence (0.1 - 10)*	*Estimated seriousness of consequences (1 - 100)*	*Type of consequence, cost/reputation/continuity/injury*
8	2	10	Reputation / Continuity (Cost)
10	5	7	Reputation / Continuity (Cost)
5	3	7	Reputation / Continuity (Cost)
2	3	10	Reputation / Continuity (Cost)
2	1	7	Reputation / Continuity (Cost)
10	4	15	Reputation / Continuity (Cost)