Measuring the Effectiveness of Information-Security Education, Training, and Awareness

Rickhard Alén

Department of Computer and Systems Sciences

Degree project 30 HE credits
Computer and Systems Sciences
Degree project at the master level
Spring term 2019
Supervisor: Afzal Siddiqui
Reviewer: Janis Stirna
Swedish title: Mätning av effektivitet av informationsskydd, utbildining och medvetenhet

Stockholm University

Abstract

Data breaches are becoming more frequent year by year, and the threat caused by the phenomenon to businesses and societies increases along with the number of attacks. So-called “human factors,” i.e., errors by individuals, tendency to be trustful or helpful, or negligence, seem to be one major cause of the incidents in the information security field. The “human factor” can be mitigated through technical solutions and processes to support the user; however, this alone might not be enough. Ways of affecting human behaviour, knowledge, and understanding of the risks as well as the security culture within organisations can be advantageous or even necessary. Administrative solutions to mitigate threats caused by human factors can be as diverse as information-security education, training, awareness, or a combination of the aforementioned.

Information-security education, training, and awareness are claimed to be useful methods of mitigating security threats in organisations. However, the effectiveness of the aforementioned seem to be rarely measured, and no common ground concerning the measuring and metrics exists. This study aims to answer how the effectiveness of information-security education, training, and awareness can be measured and what variables affect the effectiveness of the aforementioned.

The choice of the research strategy is grounded theory, which enables the development of strategies based on collected data and are suitable for qualitative and exploratory research. Data-collection methods used in this study are documents and interviews. Documents are selected as a primary method of data collection to create a foundation for the theory, which can be challenged or complemented through the use of interviews. The data-analysis method is based on the grounded theory, i.e., open coding of the identified data from which categories, themes, and, finally, a theory are formed.

The research concludes that methods of measuring the effectiveness of a program based on information-security education, training, and awareness exist. This study finds out that financial measuring, such as cost-benefit analysis, is lacking as of now due to the state of statistics concerning the threats and because too many assumptions have to be made that cannot be justified, e.g., attacker motivation, capability, or similar. However, methods for measuring the effectiveness of an information-security education, training, and awareness program in a specific area, e.g., password strength or social engineering threats, exist and are applicable. The study also found that variables that affect the effectiveness can be such as motivation of the participant, method of delivery, or how the organisation is performing. Future research concerning the variables could be beneficial as the statistics related to the subjects of this study are likely not to change in the near future.
Keywords: Information-security education, training, and awareness (SETA), effectiveness, data breach, human factor, threat, risk, measurement, metric, and uncertainty.

Synopsis

Background	Data breaches are becoming more frequent year by year, and threats caused by the phenomenon to businesses and societies have increased along with the number of attacks. So-called "human factors" i.e., errors by individuals, tendency to be trustful or helpful, or negligence seem to be one major cause for incidents in the information-security field. The "human factor" can be mitigated through technical solutions and processes to support the user; however, this alone might not be enough. Ways of affecting human behaviour, knowledge and understanding of the risks, and security culture within organisations can be advantageous or even necessary.
Problem	Information-security education, training, and awareness are claimed to be a useful methods of mitigating the security threats in the organisations. However, the usefulness of effectiveness of the aforementioned is rarely measured, and no common ground concerning the metrics exists.
Research Question	The main research question of this study is: "How to measure the effectiveness of information-security education, training, and awareness?" To support the main research question following sub-questions are studied as well: "Which variables related to the participant affect the effectiveness of information-security education, training, and awareness?" and "Which other variables affect the effectiveness of information-security education, training, and awareness?"
Method	The research strategy chosen is grounded theory, which enables strategies to develop based on the collected data and is suitable for qualitative and exploratory research. The data-collection methods are documents and interviews. The methods are selected due to that they support each other; a foundation is created through documents, which can be challenged and complemented through interviews. The data-analysis method is coding based on grounded theory, i.e., open coding of the identified data from which categories, themes, and finally a theory are formed.
Result	The results of this study theorise that measuring the effectiveness of an information-security education, training, and awareness program from a financial point of view is not feasible currently. The reasoning behind this theory is that statistics concerning data breaches and other cyber threats are lacking, and the threats themselves are hard to measure due to numerous variables from the attacker to the target that are unknown or have to be assumed. However, organisations can measure how an information-security education, training, and awareness program performs in a certain area, and this can be used as a metric of effectiveness.
Discussion	While it is possible to calculate the costs of the administrative solutions, possible estimations of the benefits from the aforementioned are too vague as of now. Still, organisations can use metrics related to a specific subject to see how the program (or a part of it) performs. The research conducted in this study indicates that organisations, in general, do not measure the effectiveness of a solution they buy, and the motivation for the solutions bought tends to be a necessity.

Acknowledgements

I want to thank Stockholm University's professors at the Department of Computer and Systems Sciences for the support and teaching during past years.

Specifically, I would also like to thank:

- **Participants of the research** for their time and opportunity to learn from them,
- **Anssi Porttikivi, Afzal Siddiqui, Karri Tomula, and Janis Stirna** for their feedback and assistance during the thesis process,
- **My wife, relatives, and friends** for their assistance which made it possible to do this all during my parental leave,
- **And last but not least, my son** for those days when you napped more than an hour.

Table of Contents

List of Figures

List of Tables

List of Abbreviations

- CAQDAS – Computer-aided Qualitative Data-Analysis Software
- CIA – Confidentiality, integrity, and availability
- GDPR – General Data Protection Regulation
- KPI – Key Performance Indicator
- ROI – Return-On-Investment
- SETA – Security education, training, and awareness
- QDA – Qualitative Data-Analysis

1 Introduction

1.1 Background

During the past years, data breaches have become a more frequent and severe threat to organisations, and findings suggest that the potential costs are increasing yearly, e.g., from the year 2013 to 2015, costs increased by 23% (Algarni and Malaiya, 2016, pp. 1 & 13). Reports by Data Breach Index show that in the year 2013, at least 575,486,661 data records were lost or stolen (Gemalto, 2013), and in the first half of 2018, this number was 3,353,172,708 (Gemalto, 2018).

Year after year, we are undergoing "the worst year ever" concerning data breaches and other cyber incidents. While the number of incidents varies based on the report, the common trend is that the number of attacks is increasing exponentially, along with the financial losses (OTA, 2018). Moreover, the losses due to the data breaches are not only financial; according to the HIPAA, as many as 2,100 deaths might have occurred due to the data breaches in the healthcare industry in the United States alone. Indeed, the research used in the article shows that there was a 0.23% increase in the mortality rate one year following a data breach and a 0.36% increase two years after the breach (HIPAA-Journal, 2018). In the Ashley Madison breach, the data breach resulted in several suicides (the total number is uncertain, but some are rather confidently linked to the breach) or loss of personal trust or other non-financial damage (Lamontm, 2016).

The prevalence of human factors varies based on the study, e.g., Ponemon (2018) had "human factor" as a root cause in only 27% of data breaches. In a report concerning insider threats, the percentage was 63% when counting employee or contractor negligence of the internal incidents (Ponemon, 2018). According to the statistics available, one of the easiest ways for the organisations to mitigate losses due to data breaches could be to focus on the adequate training of their employees.

Information security is commonly linked with three principles: confidentiality, integrity, and availability, which are also known as the CIA triad. C, confidentiality, refers to the ability to protect data from those who are not authorised to view it. I, integrity, refers to the ability to prevent the data from being altered without authorisation in any form. A, availability, refers to the ability to access the data when needed. The former can be extended to "Parkerian Hexad," which adds possession, authenticity, and utility. The possession or control refers to the physical disposition of the media on which the data are stored. Authenticity refers to the ability to question the owner or creator of the data in question. And, utility refers to the usefulness of data (Andress, 2011, pp. 4-8).

It is not uncommon that an organisation might be deploying the majority of its information security budget on technical solutions, such as firewalls, antivirus software, intrusion detection systems, etc., which are also known as logical controls as their aim is to prevent unauthorised activities within the systems, networks, and environments where the organisation handles its data (Andress, 2011, p. 11). Such investment in technical solutions tends to come at the expense of administrative solutions such as procedures, policies, and training offered to employees (Pompon, 2016, p. 72). The claim is supported by a survey that found that 45% of the information security budget is spent on hardware and software (Sen and Borle, 2015, p. 333). Another point of

view concerning the human factor is that all technical solutions are directed at controlling human access to the system. Therefore, what we process within the information-security field is for the people, and output is used by the people; hence policies, standards, procedures, and other administrative solutions are needed to support the technical solutions (Desman, 2003, p. 40). It has been found that there is a correlation between information-security awareness and the overall information security level within organisations; therefore, it can be assumed that the human factor should not be ignored and that technical solutions alone are not enough (Šolić et al., 2012, p. 50).

Recent studies have found out that human error (Hofmann et al., 2018, pp. 14-15), human behaviour and lack of positive security culture, i.e., a culture of security within organisations where employees understand that information-security starts with them, they are not punished for reporting the incidents, but encouraged to do it, and the commitment towards this change is supported by the management (Wittkop, 2016, pp. 88-89; Metalidou et al., 2014, p. 427), lack of logic (Won, 2013, p. 229), or combination of the aforementioned factors (Verizon, 2015, pp. 8-29) are major causes for data breaches.

1.2 Research Problem

The claim concerning usefulness of security education, training, and awareness is a common one nowadays (Herrmann, 2007, pp. 665-668; Colwill, 2009, p. 195; Whitman and Mattord, 2018, p. 268; Watson, Mason and Ackroyd, 2014, pp. 340-341; Schroeder, 2017, pp. 1-3; Pompon, 2016). The usefulness can be financial (Gardner and Thomas, 2014, p. 5), cultural (Peltier, 2005, p. 49), or something else such as reputation and public image (Mann, 2008, pp. 610-611). However, knowledge gap in respect of the measuring within organisations indicates that the usefulness or effectiveness of information-security education, training, or awareness are rarely documented or measured, and what does not get measured is difficult to quantify.

Information-security education, training, and awareness, or information security, in general, can be seen as only an obligation due to legal requirements, business partner, e.g., a governmental organisation requires that certain standard is fulfilled before they can buy a service, or have an organisation as 3rd party in a project, or some other reason instead of an opportunity (Whitman and Mattord, 2018, pp. 276-278). This might lead to a situation where information-security awareness training is inadequate and aims just to fulfil requirements that can be vague such as “appropriate” or “reasonable” since no real measure is given, and the motivation for the measurement is lacking, along with the efficiency of the training (Sloan and Warner, 2017, p. 3). Efficiency from now on within this study will refer to the outcome that can be measured as financial profit, an increase in a certain area of measurement, e.g., the outcome of a simulated social engineering attack, or combination of them.

One of the problems that this thesis address is the lack of standards concerning the measurement of the effectiveness of information-security education, training, and awareness. This should be answered to give decision makers within organisations the opportunity to understand the possible value of successfully implemented information-security education, training, and awareness. The problem is related to all industries instead of some specific organisations due to the commonality and growth of information infrastructure across all sectors (Sloan and Werner, 2017, pp. 11-12).

The research conducted in this thesis aims to contribute to Cyber Security and Risk and Decision Analysis which both are disciplines within Computer and Systems science. The problems that the research

studies, i.e., data breaches and other cyber threats, are directly connected to the discipline of the Cyber Security- However, the methods this thesis offers to solve or mitigate the aforementioned problems are linked to the risk analysis and decision support, hence, they are directly connected to the discipline of Risk and Decision Analysis.

1.3 Research Questions, Aims, and Objectives

As previously mentioned the research problem is related to all industries instead of some specific organisations due to the commonality and growth of information infrastructure across all sectors (Sloan and Werner, 2017, pp. 11-12). The threats caused by cyber incidents are not limited just to the businesses but can impact societies as well. We have entered an age where an attack on a power grid, for example, is a reality, and the consequences can affect everyone within society; hence methods of mitigating or eliminating these threats when possible are crucial for both businesses and governing bodies. When a safeguard is selected, it should serve the needs of the client, and be as effective as possible. What makes the research problem particularly interesting is that administrative solutions are rarely measured, if at all. Therefore the research questions of this thesis are the following:

The main research question of this thesis is:

- How to measure the effectiveness of information-security education, training, and awareness?

Beyond this, the following sub-questions are studied to support the main research question:

- Which variables related to the participants affect the effectiveness of information-security education, training, and awareness?
- Which other variables affect the effectiveness of information-security education, training, and awareness?

The aim of this study and research questions above is to offer methods of how to measure the effectiveness of information-security education, training, and awareness. The primary objective is to give a method or a model on how to measure the aforementioned financially, but the study also aims to examine methods beyond the financial point of view. Therefore, the reason behind leaving the term “measure” open in terms of research questions is deliberate as measuring was not to be limited to financial outcome, or similar, but would explore methods of measuring without restrictions.

Beyond this secondary objective is to research variables related to the effectiveness of information-security education, training, and awareness, the variables will not be limited to the participants of a training program for example but try to take organisational variables in the account as well. While the study conducted focuses on the measuring of the effectiveness of information-security education, training, and awareness, it is crucial to know from which the effectiveness is constituted. Without an understanding of what can make information-security education, training, and awareness effective measuring of aforementioned is difficult, and the assumptions related to the measurements might be misled.

2 Scientific base

The research conducted in this study is directly connected to Cyber Security and Risk and Decision Analysis which both are disciplines within Computer and Systems Science. The problem, e.g., data breaches and other cyber threats are directly connected to the discipline of Cyber Security. While the research will be focusing primarily on the data breaches due to the availability of statistics and reports, the assumptions and possible solutions apply to the other cyber threats that can be mitigated through administrative safeguards. The solutions that this thesis aims to offer are directly connected to the discipline of Risk and Decision Analysis, e.g., a model for analysing a dilemma or similar methods to help the decision-making process.

2.1 Overview of Data Breaches

Definition of what is a data breach varies slightly among sources, and the following definitions have been used concerning the phenomenon:

> *"A data breach incident involves unauthorized access to sensitive, protected, or confidential data resulting in the compromise or potential compromise of confidentiality, integrity, and availability of the affected data. Sensitive, protected, or confidential data may include personal health information, personal identifiable information, trade secrets or intellectual property, and/or personal financial data." (Sen and Borle, 2015, p. 315)*

> *"A data breach is a "compromise of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to protected data transmitted, stored or otherwise processed." (Lending et al., 2018, p. 414).*

While the definitions are not limited to those above, a conclusion can be made from the two that were selected. A data breach is an event in which confidentiality, integrity, or availability of the information is compromised by unauthorised action, external attacker, human error, or negligence, i.e., the CIA triad is violated (Andress, 2011, pp. 4-8). To protect against a threat, it is necessary to identify who are the perceived perpetrators and how the threats emerge. The perpetrators can be split into two sources, internal and external, insider and outsider threats. Between these two sources, internal threats are often more severe in terms of economic cost (Lv et al., 2018, p. 333), and the amount of time to fix a breach takes about 50 days in internal cases, while by contrast, an external attack is contained within 2 to 5 days in most of the cases (Lv et al., p. 334). In the case of external threats, the motivation can vary from money, industrial espionage/trade secrets, hacktivism, and cyberwar to bragging rights (Gardner and Thomas, 2014, pp. 9-12).

Regardless of whether the threat is internal or external, the main vulnerability seems to be coming from the human factor. Since outsider attackers know that the weakest link of the defence tends to be human, social engineering is an attractive method of attack (Sloan, and Warner, 2017, p. 8). This vulnerability might be because we are taught to treat others the way we want them to treat us (Gardner and Thomas, 2014, p. 46).

Organisations should not ignore that there are threats caused by insiders. These risks can be mitigated through an appropriate risk assessment that takes motivation, opportunity, and capability into account. Even with proper risk assessment, it should be accepted that individuals in a trusted position can abuse that trust and that accidental data breaches due to human error (or successful social engineering) are more likely than

malicious insider attacks. Thus, the human factor is something that should be assessed and managed even if it cannot be truly eliminated (Colwill, 2009, pp. 194-195).

2.2 Overview of Information-Security Education, Training, and Awareness

> *"The single most effective mechanism to limit risky behaviour and prevent unauthorized activity is to raise the awareness of all individuals, thereby limiting the liability of the organisation and changing the culture of the company. The higher the level of risk that individuals manage, the higher the level of security awareness and training they must be provided"* (Vacca, 2017, p. 415).

Awareness can be defined as having or showing realisation, perception, or knowledge of a subject. In the case of information-security awareness, this can mean being aware of social engineering, the perception of potential phishing attempts, or understanding that opening attachments from an unknown source could lead to virus infection. Individuals within an organisation need to realise that their actions can and will prevent damages and other undesirable outcomes (Gattiker, 2004, pp. 30-31). As a by-product, they need to realise that education provided by information-security awareness training is to protect the organisation and, by extension, their livelihood (Information-Security, 2008, p. 5).

Information-security education, training, and awareness often are labelled in a way that might not represent the actual focus, purpose, and method of delivery concerning the offered service. For example, information security education (ISE) focuses on insights and understanding with the purpose of equipping the employees with the know-how and expertise to ensure confidentiality, integrity, and availability of the organisation's information. The education is offered with theoretical instructional methods such as seminars, classroom discussions, and research. Information-security training (IST) focuses on information-security skills and information-security knowledge, and the purpose of the IST is to equip employees with information-security skills and information-security knowledge specific to their roles and responsibilities. The method of delivery is more practical for information-security training, i.e., methods such as seminars and workshops are common. Information-security awareness (ISA) focuses on attention directing and reminders, and its purpose is to ensure that all employees within the organisation realise their roles and responsibilities concerning the organisation's intellectual property. Common methods of delivery are printed and electronic media such as videos, flyers, and posters (Amankwae et al, 2014., p. 251). Education deals with "why" questions and offers an understanding with the aim of mitigating long-term impacts. Training deals with "how" questions and offers skills and expertise and impacts within the intermediate timeframe. Awareness deals with "what" and offers information to recognise and to repel threats and impacts should be seen in short term (Wilson et al., 1998, p. 18). A combination of the aforementioned is also known as information-security education, training, and awareness i.e., SETA (Whitman and Mattord, 2018, p. 267), and this term is used from here on when discussing information-security education, training, and awareness excluding situations where a specific part is addressed.

2.3 Evaluation of the Effectiveness of Training

While there exist multiple frameworks of evaluation effectiveness of training one of the most well-known and used is the Kirkpatrick four-level model. It has been in use since the late 1950s, and it has motivated multiple different models, e.g., a model released by NIST evaluation (Wilson et al., 1998).

> "*All meaningless training is expensive, even where the direct cost outlay, or cost-per-student, maybe low. Because agencies cannot afford to waste limited resources on ineffective training, evaluation of training effectiveness should become an integral component of an agency's IT security training program. A robust training evaluation effort may be the second most effective vehicle for garnering management support for IT security—the first being the occurrence of a serious security incident."* (Wilson et al., 1998, p. 157).

The four levels of evaluation by NIST SP800-16 are described in Table 2 (Wilson et al., 1998, pp. 161-163).

Table 1 Four levels of NIST SP800-16 (Wilson et al., 1998, pp. 161-163)

Level	**Description**
Level 1, End-of-Course Evaluations (Student Satisfaction)	Participants' satisfaction to the training facility, instructor, manner of presentation and objectives, for example, can be measured.
Level 2, Behaviour Objective Testing (Learning Effectiveness, Teaching Effectiveness)	The level 2 includes measurement of learnt knowledge/skills and changes in behaviour. NIST emphasises on that the participants' knowledge/skills should be evaluated with pre/post testing, i.e., both before and after the training.
Level 3, Job Transfer Skills (Performance Effectiveness)	According to NIST level 3 should take place 30 to 60 days after the training activity, level 3 measures how the students' performance has changed after the training.
Level 4, Organisational Benefit (Training Program Effectiveness)	Level 4 organisational benefit tries to quantify what the training conducted brings to the organisation. Here the metrics are recommended to measure a change in activity related to training to support the claim that training is beneficial to the organisation.

The above framework offers are four level evaluation process; however, the process itself while worthwhile is a generalised method and the measurements or questions related to the process do not apply to the research problem in this study. The process highlights that there is multiple points of views when trying to measure the effectiveness of training, and this study will focus on levels 2, 3, and 4. While level 1 will have an effect on how the participants might learn from the training it is not directly connected with how to estimate the effectiveness of the SETA program.

2.4 Metrics

To evaluate the effectiveness of the SETA program, one needs to consider what to measure and what the appropriate metrics are. Subjects of measuring can be the training itself, e.g., how the participants felt about the training, was the instructor to their liking, etc., how the employees perceived the training, were they

satisfied, and similar metrics. However, if the measuring the effectiveness of the SETA program is limited only to that (and understanding of terminology), then there is no clear indicator that the behaviour of the employees changed and the SETA program had effects desired (Tsohou et al., 2012, p. 345). If the measurement process is lacking, then the organisation is not measuring and controlling information security (Hayden, 2010, p. 21).

Definitions related to the terms “metric” and “measurement” have some variation, but common characteristics exist. A metric/measure is a measurement standard that facilitates decision making by quantifying relevant data, and measurement is the process by which quantifying relevant data (metric/measure) are obtained (Barabanov et al., 2011, p. 5). A simple way to rephrase the aforementioned definitions is that metrics are a result and measurement is an activity (Hayden, 2010, p. 27).

It has been stated that it is better to make a good security decision based on less-precise estimates of value and risk than to make poor security decisions supported by precise, though inaccurate, metrics. Estimating value loss and uncertainty should have greater importance that less meaningful metrics that are readily measured. Still, it should be noted that estimating intangible variables such as loss and uncertainty is challenging (Axelrod, 2008, p. 1; Riek, 1986, p. 59; Chapman and Ward, 2011, p. 47).

2.5 Overview of Cost-Benefit Analysis under Uncertainty and Monte Carlo Analysis

2.5.1 Cost-Benefit Analysis under Uncertainty

Even in the simplest project, there exist multiple predictions and assumptions. These are not often taken into account within cost-benefit analysis while the analysis itself has already two sets of predictions. Predictions of the future where an organisation does not undertake the project and predictions where the organisation does conduct the project (Ward, 2015, pp. 1-2). Traditionally, it is assumed that the organisation undertaking the cost-benefit analysis knows all the probability distributions of all potential outcomes. In practice, however, this is impossible as the probability of outcomes is unknown and, thus, uncertainty exists (Andersen, 2014, p. 57). Uncertainty can arise from multiple sources, such as problems with data, problems with models, or other sources such as human behaviour or climate change (Firoozye and Ariff, 2016, pp. 110-111). Table 2 (Sanderson, 2012, p. 437) offers a view on how the future can be perceived, where risks exist when the potential event or outcome can be reasonably identified and estimated with a certain degree of confidence, e.g., annual rainfall, wind intensity, or likelihood of West Bromwich Albion’s winning the Premier League. Uncertainty exists when the potential event or outcome cannot be reasonably identified, or the probability of an event’s happening is unknown, e.g., change in taxation or technological improvement (Salci and Jenkins, 2016, p. 6). The same problems related to uncertainty exist within other methods of risk assessment beyond the cost-benefit analysis.

Table 2 Risks and uncertainties (Sanderson, 2012, p. 437)

Risk Category 1: A priori probability	The decision maker's view is s/he faces are able to assign objective probabilities to a known range of future events on the basis of mathematically "known chances"', e.g., the probability of throwing a certain number with a die.
Risk Category 2: Statistical Probability	The decision maker's view is s/he faces are able to assign objective probabilities to a known range of future events on the basis of empirical/statistical data about such events in the past, e.g., the probability of being hit by a car.
Uncertainty Category 1: Subjective probability	The decision maker's view is that s/he faces a known range of possible future events, but lack the data necessary to assign objective probabilities to each. Instead, they use expectations grounded in historical practice to estimate the subjective probability of future events, akin to scenario planning, e.g., how much will a SETA program reduce incidents related to human behaviour?
Uncertainty Category 2: Socialized	The decision maker's view is that s/he faces a situation in which the nature and range of future events are unknown, not simply hard to understand because of the lack of relevant data. The future is inherently unknowable because it is socially constructed and may bear little or no relation to the past or the present, e.g., how will driverless automobiles change the nature of the transportation system?

2.5.2 Monte Carlo Analysis

Simulation-based risk analysis, known as Monte Carlo analysis, is a form of sensitivity analysis in which outcomes are calculated using input values based on probability-weighted distributions. Monte Carlo analysis is often used to estimate cost, impact, or such and to assist in decision-making. The method simulates a large number of draws decided by the analyst, and the input of these draws can be used to establish a distribution of outcomes. The accuracy of Monte Carlo simulation is based on how accurate and realistic the assumptions and data underpinning the analysis are. The accuracy of the model depends wholly on the accuracy of the probability distribution of risk variables (Salci and Jenkins, 2016, p. 9). While Monte Carlo simulation requires extensive input, the output is extensive and informative as well. The main disadvantage of the Monte Carlo method is that it is time and resource heavy, and the complexity of a model can be a downside as well as a more complex program is harder to check if it has been written correctly and can produce trustworthy results (Aven, 2008, pp. 83-84).

3 Methodology

3.1 Choice of Method

3.1.1 Research Strategy

The research strategy can be defined as a plan of action designed to achieve a specific goal (Denscombe, 2014, p. 3). According to Denscombe (2014), there exist nine different research strategies: surveys and sampling, case studies, experiments, ethnography, phenomenology, grounded theory, action research, systematic reviews, and mixed methods. When selecting the research strategy, it is important to think about how appropriate and useful the strategy is related to the research conducted. Denscombe offers a checklist of the choice of the research strategy consisting of factors: suitability, feasibility, and ethics (Denscombe, 2014, p. 6).

The choice of the research strategy was between the systemic review and grounded theory. As the research deals with the effectiveness of a phenomenon, it could fit nicely with the systemic review as systemic reviews tend to be associated with the evidence-based practice. The strategy is a review of the research literature that aims to conclude the state of the knowledge on a topic. It consists of searching for relevant literature, review of the findings, and conclusions based on an objective analysis of the data found (Denscombe, 2014, pp. 132-133). However, due to the phenomenon studied, systemic review as a choice of strategy does not fit after all as quantitative research concerning the research topics of this study is lacking, and applicability to qualitative research lacks in case of systemic review (Denscombe, 2014, p. 143).

The research strategy chosen for this research is grounded theory. The purpose of grounded theory can vary from clarifying concepts, producing new theories to exploring a new topic, and providing new insights (Denscombe, 2014, p. 4). As the main research question “How to measure the effectiveness of information-security education, training and awareness?” and the sub-questions “What variables related to the participant affect the effectiveness of information-security education, training and awareness?”, and “Which other variables affect the effectiveness of information-security education, training, and awareness?” are all exploratory questions, the research is exploratory itself, and this is where grounded theory tends to be useful (Denscombe, 2014, p. 109). The main point of grounded theory is eventually reaching an adequate theory for its eventual use (Roman et al., 2017, p. 987), generating of theory needs that concepts appear in the data, such as documents, as well in empirical research, e.g., interviews (Roman et al., 2017, pp. 987-988). This research deals with “positivist theory” as it deals with a general phenomenon, i.e., it seeks causes, favours deterministic explanations, and emphasises generality and universality (Charmaz, 2006, pp. 125-126). Also, the grounded theory allows the researcher to study the phenomena holistically (Cho and Lee, 2014, p. 16). The process of grounded theory is described in Figure 1 (Roman et al., 2017, p. 994) modified to suit this study. The parts of the process are described in their sub-sections.

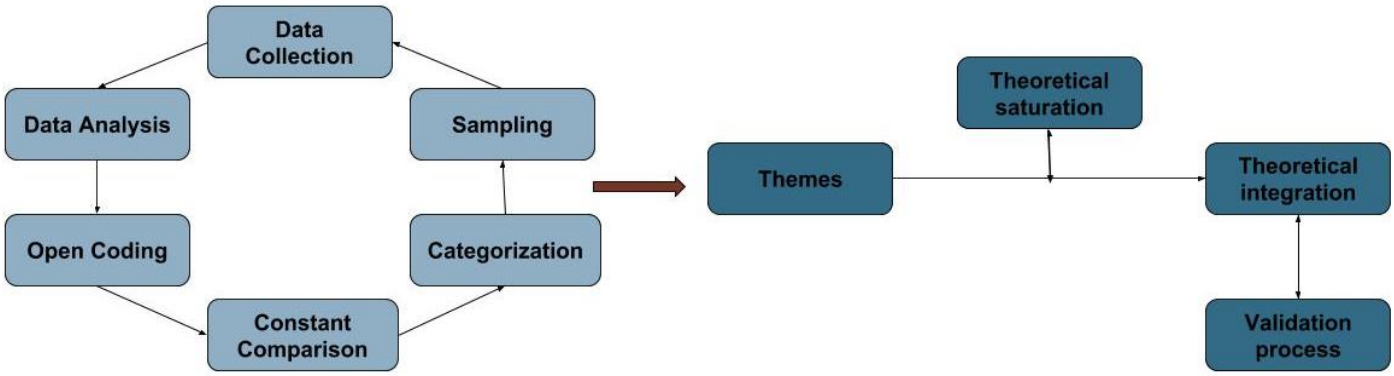

Figure 1 Grounded theory procedure adapted from Roman et al., 2017 (p. 994)

While the grounded theory was deemed as the most suitable strategy for this study, it is not without limitations. The strategy makes precise planning difficult due to the theoretical saturation, i.e., it is impossible to predict when data collection through interviews, for example, can be stopped. Contextual factors have a role for every phenomenon, and there is a danger that theory generated will ignore the influence of social, economic, and political factors (Denscombe, 2014, p. 119). Grounded theory can be a time-consuming and complex strategy that deals with vast volumes of data, however; the latter "weakness" is an advantage as well when trying to generalise findings, even if they are only theoretical generalisations (Denscombe, 2014, pp. 119-120). Beyond these, while grounded theory offers procedural rules concerning the data-collection and analysis it does not provide a predefined sampling process; therefore, achieving theoretical saturation in sampling needs rigorous theoretical sensitivity within the data-analysis process (Cho and Lee, 2014, p. 17).

Theoretical saturation, which has been mentioned twice, is achieved by joint collection and analysis of data. The point of saturation is reached once no more properties, i.e., codes can be developed for categories. Saturation can never be achieved by studying one incident in one group; hence, a sample consisting of different individuals and use of ample data is necessary (Glaser and Strauss, 1967, pp. 61-62).

3.1.2 Data Collection

Denscombe outlines four different methods for data collection, i.e., questionnaires, interviews, observation, and documents. The decision of choosing which data-collection method is used is based on how the method suits the task at hand. While some methods are often linked to specific research strategies, e.g., questionnaires are often linked with surveys, this, however, does not mean that data-collection methods are mutually exclusive. The aforementioned in practice means that if the use of multiple methods is beneficial to research, then it is better to do so (Denscombe, 2014, pp. 163-164).

Methods used in this research are interviews and documents. An interview is a method that relies on what people tell to the researcher, what people say they do, what they say they believe, or what opinions they say they have (Denscombe, 2014, p. 184). When considering the feasibility of interviews one should consider the possibility of gaining access to potential interviewees, costs (travel and such), and type of the data required for the research. If one needs to gather quantitative data, then the use of questionnaires instead of interviews

should be a more cost-effective method. However, if rich data concerning a subject are required, then the use of interviews as a data-collection method can be justified (Denscombe, 2014, pp. 185-186).

Documents is a data-collection method that deals with written texts, digital communication, and visual sources. Documents tend to be a cost-effective approach but face certain potential disadvantages such as credibility of the source (or data) or access to the data (Denscombe, 2014, p. 225). Document review as a data-collection method can be justified to gather background information and understanding of a phenomenon, for example, or to collect enough information to formulate a questionnaire, interview, or an observation guide.

3.1.2.1 Choice and Justification of Methods

Table 3 below shows the choice and implementation of the data-collection methods in this study with justifications based on the reasoning of Denscombe (2014).

Table 3 Method choice and justification (Denscombe, 2014, pp. 112, 118, & 186)

Method:	
Documents	Document review is used to study the underlying assumptions concerning three main areas of the research, to gain an overview of the themes and to formulate latter methods in a form suitable for this research. The three areas of the research are data breaches, information-security awareness, education, and training and ways of evaluation effectiveness of the aforementioned (Denscombe, 2014, p. 118).
Interviews	Some interviews from experts from the field were deemed necessary to achieve theoretical saturation on a level adequate for this study. As the goal of the interviews was to gather thoughts, opinions, and experiences concerning the areas of research, it was decided that interviews would be held as semi-structured. Semi-structured interview in practice means that interviewer has a clear list of issues to be addressed and questions to be answered, but the structure is not restrictive, e.g., the order of questions can change (Denscombe, 2014, p. 186). While the grounded theory favours unstructured interviews it was deemed that some sort of structure would not limit the generation of data, especially as the questions selected did not try to confirm existing theories or assumptions, but to explore (Denscombe, 2014, p. 112). It was decided that interviews would not be limited to just one-to-one interviews as an interview can gain from the interaction between multiple interviewees, especially when the form is not overly structured.

3.1.3 Sampling Strategy

The goal of the sampling strategy is to help to produce reasonably accurate findings without the need for collecting data from every member of a research population. The exploratory sample is connected to small-scale research and qualitative data (Denscombe, 2014, p. 32). As the point of the interviews conducted for this research is to gather insight and information related to the main research areas, the use of the exploratory sample is self-evident.

When creating a sample, the selection of the informants is done by probability or without it. Non-probability sampling means that the researcher selects informants knowingly for a variety of reasons, e.g., because sufficient experience or knowledge of the subject might not occur in the general population

(Denscombe, 2014, pp. 33-34). In the case of this study, probability sampling is used for the interviews since random sampling would not necessarily provide adequate insight concerning the main research areas.

Non-probability sampling techniques used for this study were purposive sampling and snowball sampling. Purposive sampling means that individuals are hand-picked basis on their relevance and knowledge so they might provide valuable data related to the subjects of the research (Denscombe, 2014, p. 41). Snowball sampling means that the next individual to interview emerges through a reference from one person to another, and, as in this study purposive sampling was used as the main sampling technique, it is highly likely that results from the snowball sampling would fit the criteria concerning the subjects as well (Denscombe, 2014, pp. 42-43).

Methods for calculating sample size are split among statistical, pragmatic, and cumulative (Denscombe, 2014, p. 44). Cumulative sizing is often connected with qualitative studies of a smaller scale. In this method, the sample is increased until the researcher feels that sufficient information has been gathered and the increase in the sample size would not provide more relevant information (Denscombe, 2014, p. 51). In case of this research cumulative sizing is used for the interviews as the sample size is relatively small, yet the final size of the sample was unknown at the start of the research. Once an adequate amount of information was gathered, the interviewing could be stopped, in terms of the research strategy, this is where theoretical saturation happens. The research based on grounded theory continues until new data seems only to confirm the analysis instead of adding anything new to it (Denscombe, 2014, p. 112).

3.1.3.1 Sample-Related Biases

It must be acknowledged that the main sources of the interviews are from within the information security industry, and, therefore, there exists the likelihood that bias concerning the main research areas and their importance occurs. Thoughtful selection of questions and use of supplemental questions when necessary to ensure that the questions were answered and understood were used to limit possible biases, i.e., if something was given more, or less, importance compared to the literature review or previous interviews it was examined why this happened.

3.1.4 Data Analysis

Three forms of data analysis exist, i.e., description, explanation, and interpretation. The description can be identified as a method of gaining a clear vision of what a phenomenon entails, i.e., measurements, components, dates, frequency, etc., before trying to give an explanation or interpretation of how it works. The description can be used as either a stand-alone method or a prelude for further investigation. What something looks like, when something happened, who was involved, or how often something happens are under description as analysis method (Denscombe, 2014, p. 243). Explanation aims to find how things work through how things are connected, why things happen, or when things happen (Denscombe, 2014, p. 244). Interpretation focuses on how and why things happen, who undertook the research, when and where the study took place, and what alternative explanations exist (Denscombe, 2014, p. 244).

As the research strategy chosen is grounded theory, the data-analysis method is already chosen, i.e., qualitative analysis (Glaser and Strauss, 1967, p. 101), which is described in data-analysis procedure sub-section 3.2.2.

3.2 Application of Method

3.2.1 Literature Review and Document Search

The literature review is used to provide context for the study and is used later on for the implementation of metrics and such. The procedure related to the literature review and document search in terms of this study is described in Table 4. Besides the procedure described in Table 4, the timeframe of the sources was considered, as the information security field is fast evolving in terms of science and transition. Therefore more recent publications were mainly selected when possible. The publications that were used in the study varied, scientific journals, prior studies, and books related to the topics are just examples of these publications.

Table 4 Literature review and document search procedure for this thesis

Step	**Description**
Definition of the topics	In the first step of literature review and document search, main research areas were used as topics for the document search, those being: information-security awareness, information-security awareness training, data breaches, metrics related to aforementioned and methods of training evaluation.
Definition of the key words	From the topics key words were derived, terms such as “uncertainty,” “effects,” “results,” and such were used jointly with their corresponding topics to make results of the search more suitable for this research. Key words were used later on for both search of the information and browsing of the information. The key words were selected on how they served the research questions of this study, for example, “results” and “effects” both gave useful findings when combined with a topic such as information-security awareness.
Sources of the information	Here sources for the document search were identified, namely the Stockholm University Library (https://www.su.se/english/library/), as the library uses multiple databases for journals, books, and articles it was deemed to be enough as a stand-alone source of the information. Beyond the use of the library some resources were preferred directly by the informants of the interviews.
The search of the information	The search was performed in the Stockholm University Library by the topics and key words.
Browsing of the information	Here the key words were used to find if the resources found contained information relevant to this research if so the resource was kept and catalogued, if not it was discarded.
A thorough study of the relevant information	Relevant sources were read thoroughly, and notes were made from the sources.
Use of the information	Relevant sources were cited or summarised within the thesis.

3.2.2 Interviews

As mentioned before, the interviews conducted in this research were semi-structured. The first interview that was held for this study did not follow any structure as it was used more as open discussion concerning the research areas and research questions of this study. Interviews conducted later on were based on the questions shown in Appendix B, the flow of the interview dictated when each of the topics was discussed as no strict structure was followed.

As mentioned previously, the individuals who were interviewed were professionals from the field. In practice, this meant that every individual that were interviewed were working in a role where they had been responsible for implementing any part of information-security education, training, or awareness. Beyond this, it was seen as a positive upside if the individuals had hands-on experience with customers during the project so that they had experience and knowledge related to that how the customers viewed the process and what are their opinions related to the SETA.

3.2.3 Data-Analysis Procedure

The data-analysis procedure starts with selecting the units of analysis, which was done during the literature review and interview process. Coding in grounded theory is the process of analysing the data. While the foundation of grounded theory was created by Glaser and Strauss, the process of analysing the data differs with the authors, and the method has evolved since its creation. The main difference seems to be that Glaser emphasises openness and imagination when it comes to the interpretation of data, and Strauss emphasises precise and rigid routines in data-analysis (Walker and Myrick, 2006, pp. 557-558).

This research follows the process of grounded theory analysis described by Harry et al. (2005, pp. 5-12), which is the method inspired mainly by Strauss. The process is described in Table 5 below with slight modifications to the data-analysis process described by Harry et al. (2005).

Table 5 Data-Analysis Procedure adapted from Harry et al. (2005, pp. 5-12)

Phase 1: Open coding	The units of data analysis, e.g., results of the literature review and the interviews are analysed. Codes, e.g., financial, human, and lack of understanding, are identified from the material.
Phase 2: Categories	Results of phase 1 are assigned into categories, e.g., risk, human factor, and variable.
Phase 3: Themes	Categories are formed into themes, e.g., threat, data breach, and SETA.
Phase 4: Testing the themes	All the themes were compared with the units of data-analysis and following questions were explored. Are identified themes observed within data in a remarkable extent, and what additional themes/categories/codes emerge from data before the theoretical saturation is reached.

Phase 5: Interrelating the themes	Connections between themes given above are discovered, if existing, and elaborated.
Phase 6: Theory	A theory is formed from the themes.

3.3 Research Ethics

When research conducted involves data collection from or about living people it requires ethical scrutiny. Most of the time, these data-collection methods include questionnaires, interviews and observation (Denscombe, 2014, p. 307). There exist four key principles of research ethics: participants' interests should be protected, participation should be voluntary and based on informed consent, researchers should operate openly and honestly concerning the investigation, and research should comply with the laws of the land (Denscombe, 2014, pp. 309-315).

In terms of this thesis, the following steps were taken to ensure ethically palatable research. When interviews were held, informants were asked to provide consent beforehand, and the interview was recorded to ensure that information would not be altered due to scripture mistake, and the permission to use generic information related to the informants was asked. Interviews (and the transcripts made from the recordings) are excluded from the study to ensure the anonymity of the informants; however, if requested, then access to the interviews could be provided if consent is obtained from the informants. Third and fourth key principles related to open and honest research and to comply with legislation respectively were respected as breaching these principles would not give any benefits to the research but would challenge the credibility of the results.

3.4 Quality Criteria

The credibility of qualitative research is sometimes harder to judge when compared to quantitative research, while it might be an adequate solution to repeat the research in case of quantitative research it is not applicable for qualitative research. The social setting is rarely the same even if multiple steps are undertaken to mimic the situation; time changes things both concerning phenomena and the individuals in a way that even if the setting could be replicated perfectly, the participants will differ. Credibility is judged by concepts such as validity, reliability, generalizability, and objectivity (Denscombe, 2014, p. 297).

Validity also known as credibility refers to how accurate and appropriate data used within research is. In terms of this research as with any qualitative research, it is impossible to prove that data is right. Hence, the term credibility is often used instead of validity. Steps such as respondent validation, grounded data, and triangulation can be used to address this issue (Denscombe, 2014, pp. 297-298).

Dependability, also known as reliability, refers to the neutrality of researcher and methods used. This can be ensured by an account of research procedures, methods, and decision making. If the account of aforementioned exists in an adequate way, then it is possible to understand how research's findings were reached (Denscombe, 2014, p. 298).

Transferability, also known as generalisability, refers to how representative the research conducted is in similar cases. As qualitative research tends to deal with smaller studies, the generalisability is called transferability. In practice, this means that instead of asking "to what extent are the findings likely to exist in

other instances," it should be asked "to what extent could findings be transferred to other instances," the aforementioned is also known as analytical generalisation instead of statistical (Denscombe, 2014, p. 299).

Conformability, also known as objectivity, refers to the degree of influence of the researcher in the research. As qualitative data are a product of the process of interpretation possible biases from the researcher might end in the research. There are two options to handle this; one, the researcher can admit that his/hers identity, values, and beliefs play a role in the production and analysis and the researcher should distance themselves from his/hers normal beliefs and such related to the phenomenon. The second option is to admit that the research agenda is shaped by the aforementioned. The truth is that while either of the options "should be selected" in reality the situation tends to be between both options. No matter which approaches the researcher selects or strives to respect an open mind concerning the research is necessary, neglecting data that do not fit the analysis should not be ignored, and rival explanations should be explored. Beyond this, a reflexive account of the researcher can be used to describe possible influencing factors to the reader of research (Denscombe, 2014, pp. 300-302).

4 Results

4.1 Data Analysis

The coding process was done with the use of a CAQDAS known as the QDA Miner. The data analysis based on the interviews and literature resulted in 218 codes that were designated into 27 categories and 5 themes. Codes were derived from short sentences, longer paragraphs, or anything in between. Statistics concerning code categories are found in Table 9 in Appendix B. An example of code retrieval is shown in Figure 9 in Appendix C.

Coding concerning the interviews is not shown as the transcripts made from the interviews are excluded from this study as elaborated under the research ethics. However, the observed key findings of the interviews and basic generic information about the participants can be found in Appendix D. The organisations that were surveyed vary from small-sized local actors to large well-known global actors. Some of the organisations are focused on information security, and the larger ones are more extensive with their services; however, all of the participants that were interviewed are working specifically in the information security field. The themes and their categories are shown in Table 6 below.

Table 6 Themes and categories

Theme	**Category**
Threat	Human Factor
	Risk
	Insider
	Outsider
	Variable
Data Breach	Causes
	Costs
	Consequences
	Bad Statistics
	Lack of statistics
	Increasing
	Need for data breach notification
	Technical safeguards
	Need for counter-measures
SETA	Motivation for SETA
	Method important
	“Carrot”
	Too general
	How often
	Lack of responsibility
	”Stick”
	Lack of motivation
Risk Assessment	Uncertainty assessment
	Need for a model/assessment
Metric/Training Evaluation	Need for measuring
	Attributes
	Cost efficiency

While a profound analysis of each category was conducted, the following sub-sections will be focusing on the research questions of this study and how the themes are connected. However, analyses of each category conducted can be found in the appendices E, F, G, H, and I for those readers interested.

4.1.1 Theme - Threat

Figure 2 Analysis of Threat

The theme threat is formed from categories insider, outsider, risk, human factor, variable, and uncertainty. A profound analysis of the categories not deemed indispensable can be found in Appendix E. In terms of this study's research questions only indispensable categories are uncertainty and risk.

Uncertainty creates an environment where estimating consequences and occurrence of the threats is difficult. Uncertainty related to the threats arises from the lack of information and the lack of guidance. Lack of information creates a situation in which the scale and impact of the threat are either unknown or wrongly assumed. And lack of guidance leads to that appropriate safeguards or actions are not exercised. (Sloan and Warner, 2017, pp. 11-12). It is known that there is a need to deal with the threats, and there will be consequences if we fail to do so. However, the choice of how to deal with the threats is affected negatively by uncertainty existing concerning the phenomenon. If the threats, vulnerabilities, consequences, and the likelihood are not measured, then it is unlikely that the decision concerning how to deal with the threats is optimal. The

aforementioned deficiency can be mitigated by metrics and measurements (Brotby and Hinson, 2013, p. 19). If the "unknown" (i.e., rare events), for example, risks with severe consequences and low likelihood are ignored, then the analysis might not be meaningful (Riek, 1986, p. 109).

The risk is affected by uncertainty in a negative way. Lack of understanding about data breaches tends to increase the likelihood of being a victim of an attack (Casey, 2011, p. 1). Lack of relevant data (Sloan and Warner, 2017, pp. 11-12) and sufficient information related to the probabilities and costs (Sloan and Warner, 2017, pp. 16-17) create an environment where the decision-making related to the safeguards concerning information security is lacking. If the organisations lack understanding and the data associated with the threats, then it is difficult to justify or to decide upon an action. Without proper guidance and understanding, the relevant countermeasures are either not used when required or might not be the most beneficial options. If the risk is realised, then the consequences can be plentiful; however, the financial and reputational consequences tend to be ones that are most often mentioned in the literature analysed, e.g., prior studies and publications related to the problem.

4.1.2 Theme – Data Breach

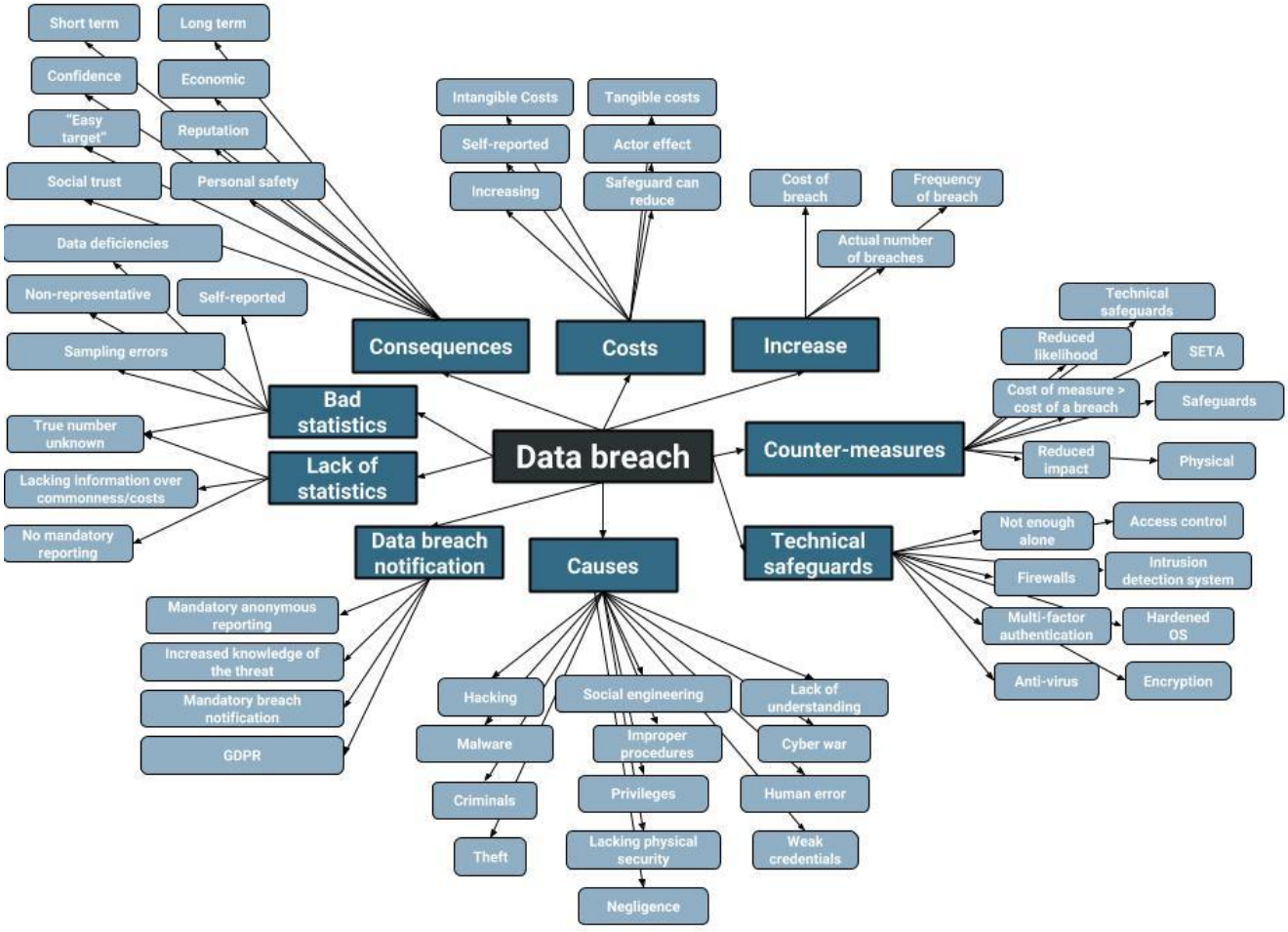

Figure 3 Analysis of Data Breach

The theme data breach is formed from categories consequences, costs, increase, countermeasures, technical safeguards, causes, data breach notification, lack of statistics, and bad statistics. Again, full analysis of the categories can be found in Appendix F. For this study, the relevant categories are bad statistics, lack of

statistics, data breach notification, costs, and consequences,

Data deficiencies related to the data breaches affect the decision making related to information security in a negative way (Makridis and Dean, 2018, p. 81). These deficiencies manifest themselves due to a number of reasons. Since organisations do not publish details concerning the costs (Algarni and Malaiya, 2016, p. 12), and statistics concerning the data breaches tend to be self-reported, which means they might not be representative at all. And the sampling methods used in the two of most noteworthy reports, i.e., Ponemon and Verizon, are not scientific, hence, sampling error is highly likely (Ponemon, 2018, p. 22).

Breaches that occur are either not detected, detected, or detected and reported. While recent legislations such as GDPR are steps in the right direction concerning the notification, results of the aforementioned will need time to be realised in terms of statistics. Even if GDPR increases the number of detected and reported breaches, those that are not detected are still a problem when analysing the threat. Participants 1 and 6 highlighted that GDPR has increased discussion about the threats, even if the improvements related to the statistics have yet to manifest.

Even if the legislation enforces notification within a given timeframe, it does not help statistics concerning the breaches that are undetected as previously mentioned. If an organisation has not observed any data breaches during the past two years, then, in reality, it might not indicate that no breaches happened but that they were just not detected (Makridis and Dean, 2018, p. 80). As of now, only the tip of the iceberg is visible, and estimation of the actual number of breaches and incidents is speculation. In fact, there is speculation that the actual number of incidents could be easily over two times the number that is reported (OTA, 2018, p. 4). One could also argue that anonymous reporting could be beneficial as it can be assumed that some of the organisations might avoid notification to their best ability as the knowledge of that organisation has been a victim of a data breach can have adverse effects; hence, anonymous reporting could help statistics concerning data breaches (Sloan and Warner, 2017, pp. 20-22).

However, this theory was challenged during the interviews as the consequences of hiding the breach could be more severe compared to admitting what happened and handing it adequately. Some of the literature supports this opinion, if an organisation is breached and the breach is handled adequately, i.e., customers are notified, and consequences are "accepted," then organisations can mitigate the potential reputational risks such as trust between partners, customer trust, or public image in general (Bisogni et al., 2017, p. 11).

Participant 2 highlights that "random statistics" make it hard to measure or estimate anything related to the data breaches, and information security incidents in general. Participant 4 mentions that beyond the number of incidents, it would be beneficial to study the so-called lifecycle of attacks as well for not only more significant successful incidents, but also smaller attacks.

The costs related to breaches that are published often do not correlate with the real numbers. Still, some information related to the costs provides an estimate of the financial costs related to the data breaches (Algarni and Malaiya, 2016, p. 13). No matter the source, the trend is that the cost of a data breach keeps increasing per year, e.g., according to Ponemon (2018, p. 9), the average total cost of a data breach increased by a 6.4% and the per capita cost increased by a 4.8% last year. The costs vary based on the country where the breach happens, industry affected, how fast the breach is identified and contained, and the malicious or criminal nature of the attack (Ponemon, 2018, pp. 9-10). However, a global average based on Ponemon's (2018, p. 15) statistics was $3.86 million per breach. Estimating a cost of a breach is a difficult task, but even an inaccurate estimation

based on biased statistics is something that can be used to estimate potential costs of data breaches (Sloan and Warner, 2017, pp. 1-2). While prior breaches and statistics related might not always be able to indicate the consequences, participant 1 made an estimation that just a single proper breach can deprive half of the organisation's business. The extent of what the business meant was not specifically confirmed during the interview but based on the prior discussion it is assumed that business revenue is the measure in this claim.

4.1.3 Theme - SETA

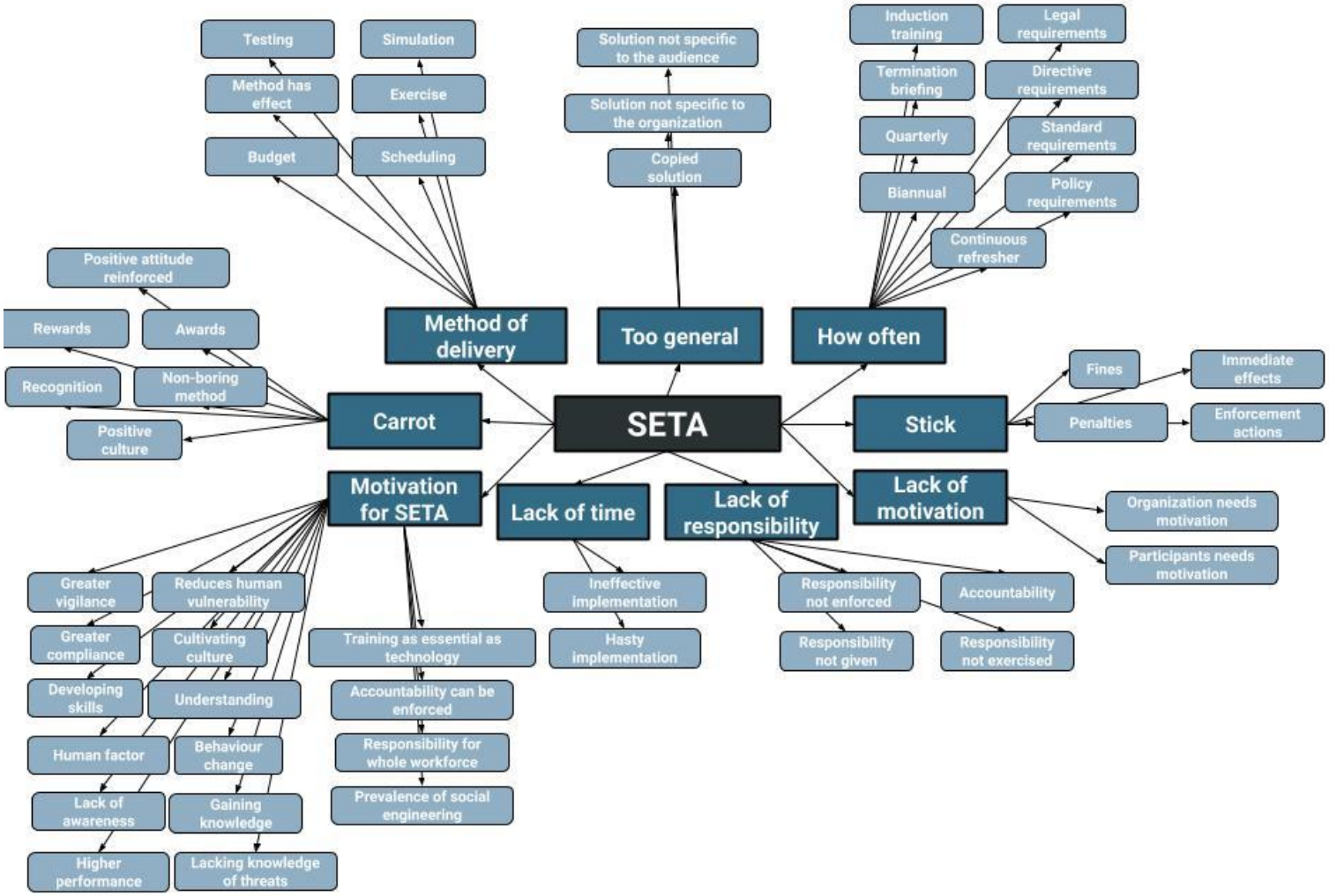

Figure 4 Analysis of SETA

The theme SETA is formed from categories stick, carrot, lack of motivation, lack of responsibility, lack of time, motivation for SETA, method of delivery, too general, and how often. The full analysis of the categories can be found in Appendix G. The relevant categories that can affect the effectiveness of a SETA program are a method of delivery, too general, how often, carrot, and stick. The trio "lack of …" might affect the effectiveness of a SETA program in certain situations; hence, the trio is covered to a degree here, but the full analysis can be found in Appendix G.

The most appropriate method of delivery is a compromise amongst the budget, schedule, and other needs or restrictions of the organisation (Whitman and Mattord, 2018, p. 274). Table 12 (Whitman and

Mattord, 2018, p. 274-275; Saleem and Hammoudeh, 2018, p. 614-616; Herold, 2005, p. 4; Wilson et al., 1998, p. 157) consisting some of the most common delivery methods, their advantages and disadvantages, and when they can be applied can be found in Appendix G.

Beyond the method of delivery how of often, a part of SETA is conducted to gain most benefits is an important question. While quarterly training might be beneficial as new threats, arise constantly, and trends change. As antivirus and similar safeguards need to be up-to-date the same principle applies to people. If the organisation is unwilling for a reason or another to conduct the training quarterly, then the minimum amount the organisation should invest in the information-security awareness training is biannual. If the training is conducted only biannually, then the focus should be on the critical topics such as how to identify phishing and how to report those attempts, how to handle sensitive information, how to prevent tailgating, and laptop (and other equipment) safety. The aforementioned topics should be included in the quarterly training as well, but they could be focused less on those topics as they are addressed more often (Gardner and Thomas, 2014, p. 90). While general training to the whole workforce can be a useful way to handle some part of a SETA program, it is important that when an employee is hired, s/he should be made aware of the organisation policies and procedures, what s/he is responsible for in his/her role, and this should be acknowledged by a signed document. Here, an opportunity to ask questions related to information security and the responsibilities should be offered as well to ensure that the new employee understood the document they signed and accountability that comes with it (Hanley and Tiller p. 158). If the contract of an employee is terminated, then a briefing related to the intellectual property and what information ex-employee is forbidden to spread should be given (Vacca, 2017, p. 501).

While multiple organisations tend to base how often they offer SETA on legal, policy, standard, or directive requirements, this should be only the minimum frequency, and it is highly likely that this will not often be enough (Peltier, 2005, p. 49; Wilson et al., 1998, p. 50). It should be remembered that awareness does not arise from a short program once a year. Instead, it develops due to cultural changes within the organisation, so less information given often works better when compared to too much information given rarely (Hadgany, 2010, p. 340). The program should be customised to the needs of the organisation and the target audience, and a copied or pre-made solution rarely fits those requirements. Spending time and resources on training that does not meet the requirements of the organisation and the audience might create an illusion that the threat is handled. Likewise, when it is realised that the product did not achieve its goals, it might create a feeling within the decision makers of an organisation that security is either waste of money or a bottleneck of productivity (Herold, 2005, p. 56; Wilson et al., 1998, p. 157). Most of the participants highlight that it is better to offer less often and more rarely (see Section 5.2).

Users can be split into groups based on their “riskiness” so that the higher the level of risk, the better the education, training, and awareness should be (Vacca, 2017, p. 415). The high-risk category can include employees who have direct access to critical information or systems. The medium-risk category can include individuals who have potential access to critical information or systems, and the low-risk category can consist of individuals who do not have access to aforementioned (Mann, 2008, p. 202). Another way is to split the audience based on their background or role within an organisation (Colwill, 2009, pp. 272-273). With a targeted approach, the effectiveness of a SETA program can be assumed to be superior to a non-targeted approach. The implementation of targeted approaches aforementioned could in practice mean that all of the risk categories

have their training separately instead of a solution that is offered to the whole workforce. Beyond separating the groups, the high-risk category could receive extra hours of training compared to those below and so on.

The motivation of participants tends to affect how well they learn, remember, and behave. It has been found that employees want both security and flexibility, and reaching a balance between these variables is a challenge in itself. Too intrusive solutions might affect the motivation or efficiency of the workforce negatively, and too weak solutions can expose the organisation to threats. A culture where positive security behaviour is valued is essential, and it needs to be communicated that each employee is responsible for the security within his/her infrastructure, businesses and their services (Metalidou et al., 2014, p. 427). However, it has been shown that reminding users that they will be caught, and will be punished in case of information system misuse is beneficial as well (Tsohou et al., 2012, p. 345). Part of the SETA program should be informing the users that they will face monetary or other sanctions in case of non-compliance with information-security policies. Emphasis should be on the immediate effect of the sanctions as individuals tend to attribute greater value to short-term gains over the long-term costs (Tsohou et al., 2012, p. 138). The consequences of breaking the rules should be relative to the offence and when this is understood by the employees, it will eventually change user behaviour and might decrease incidents caused by insiders (Veseli, 2011, p. 63).

Employees should be encouraged to report any suspicious activities, such as potential pretexting or phishing incidents, and in some cases, rewarding such actions can be beneficial (John, 2017, p. 101). Workshops and other "hands-on" methods tend to increase employees motivation and interest in the subject (Albrechtsen and Hovden, 2010, p. 444), and it is one of the most effective methods of delivery (Albrechtsen and Hovden, 2010, p. 443). The method of delivery in itself can be seen as "rewarding," yet beneficial to the organisation's end goal as well. Sometimes the process behind the method matters more than its contents and subjects.

If the organisation decides to reward employees, then the delivery of the "prize" should be thought out. If the prize is known "before the game starts," then the effects will be less than those from an unexpected one. If the award is announced beforehand, then the behaviour change in itself might not occur, instead, an employee might just aim for the prize, while this short-term behaviour might serve the needs of the organisation in the long term it is more beneficial that the behaviour change happens due to some other motivation than financial gain or fame (Schroeder, 2017, p. 14). An unexpected reward does not need to be money; an access to an opportunity or an experience such as a short trip to a vineyard, restaurant dinner, or a massage can have more positive effects that a monetary reward, especially when aforementioned is combined with a recognition and praise along emphasis with on what the employee did. The prize should be viewed as a treat earned, rather than as a payment (Schroeder, 2017, pp. 14-15). While the interviews highlighted that it is easier to reward than to punish, primarily due to the fact that the aim of stick or carrot system is easier to achieve through the means of carrot and no best practice seems to exist concerning the rewarding. It seems that awarding systems, if one exists, should be in line with the system that already exists in the organisations related to other areas, e.g., an employee of the month and the "cyber" employee of the month could receive the same prize, no matter what it is. It was mentioned by participant 1 that the reward could also take the form of praise or acknowledgement in general, which itself requires no financial contribution from the organisation but the effort from the management. However, participant 1 also mentioned that it is hard to succeed in either rewarding or punishment.

4.1.4 Theme - Risk Assessment

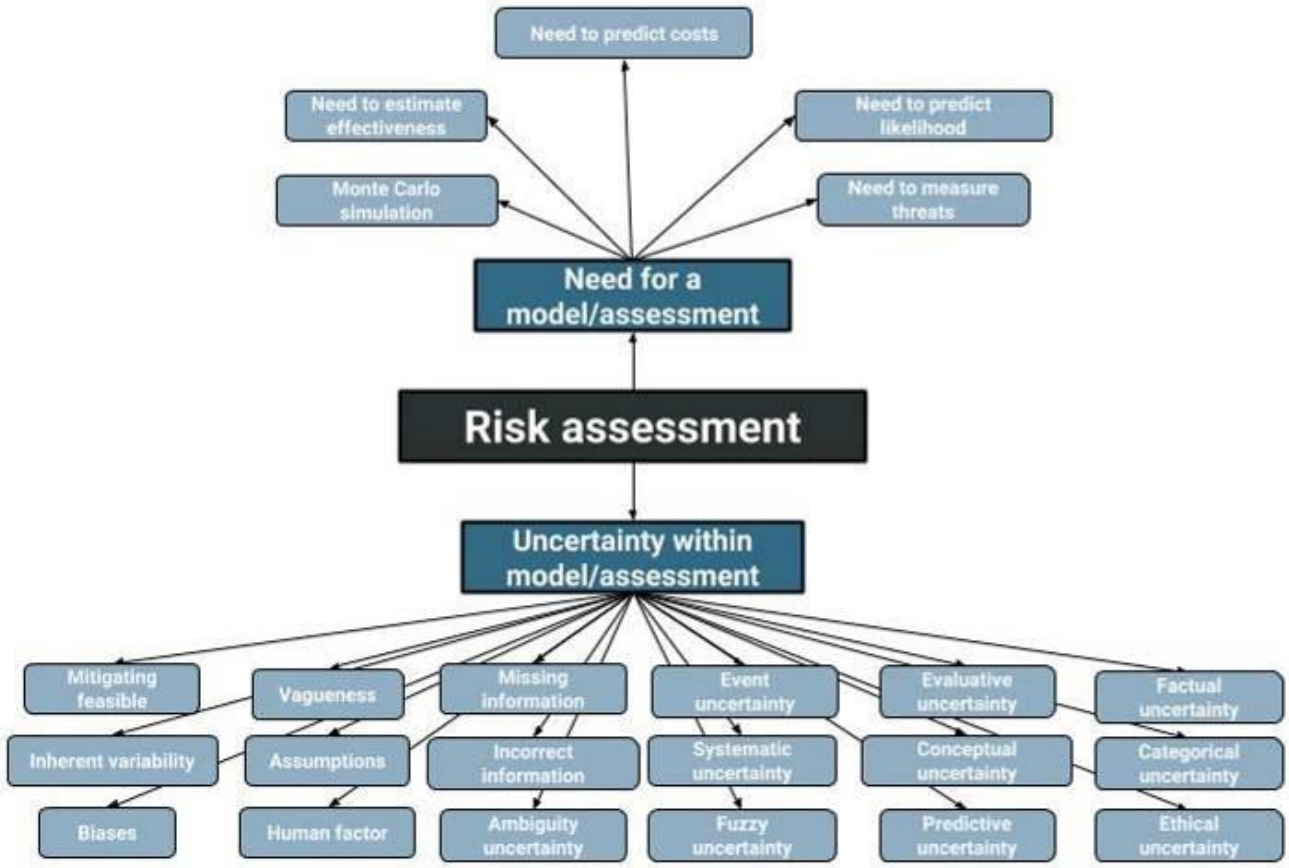

Figure 5 Analysis of risk assessment

The theme "risk assessment" is formed by categories need for a model/assessment and uncertainty within model/assessment.

Uncertainty within model/assessment, however, has an effect on how the measurement concerning the SETA can be done and how trustworthy the results are. As previously mentioned, the potential consequences and costs related to data breaches are increasing yearly as is the number of incidents and successful breaches. This alone means that there is a need for a model to calculate costs related to data breaches with predictive capabilities (Algarni and Malaiya, 2016, p. 12). In a situation where there are little relevant data available using standard mathematics or statistical techniques might not be the best solution. It has been argued that an expert opinion could be a better solution to the statistical models, while opinions are based on experience, belief, and are subject to over- or underestimating, they still can provide reasonable results with the current state of data concerning the phenomenon (Sloan and Warner, 2017, pp. 16-17). Problems with data can negatively affect the model, but so can the problems with models themselves. For example, we might have historical data and a model structure, but there is a reason to believe that parameters or model structure will change over time, or we might have the structure but unknown or erroneous values of some crucial parameters (Firoozye and Ariff, 2016, pp. 110-111).

Businesses can never eliminate risks, but they can mitigate those risks they can recognise. While some threats are unlikely, such as a highly sophisticated attack on a small- to medium-sized organisation, it is highly likely that those organisations might be a target of social engineering attacks (Watson et al., 2014, pp. 341-342).

Hence, even if the risk cannot be removed, its costs can be reduced, which is something that needs to be shown to decision makers within the organisation. It is possible to have a clear idea of the consequences, or estimation at least, even if we do not know how likely the event is. Estimating the likelihood of a major disaster, such as the earthquake, is a difficult task, but understanding the potential consequences on a vague level is not. Instead of focusing on the likelihood that is often impossible to measure on a satisfactory level one should focus on the consequences. You do not buy insurance because you expect to be hit by a car; instead you, buy it because of the consequences (Taleb, 2007, p. 211). A similar way of thought can be beneficial when trying to estimate the likelihood of an event such as data breach and if an organisation invests in information security or not. No matter what is the decision, risk events and profiles need to be identified and communicated to the organisation by those responsible for the risk management (Cambell, 2015, pp. 169-172).

Table 13 (Chapman and Ward, 2011, pp. 33-34; Riek, 1986, pp. 108-109, Dompere, 2009, pp. 6-7) consists of uncertainties related to a model or risks can be found in Appendix H. Beyond uncertainties, levels of unknowns related to the risk management are relevant as well, Table 14 (Firoozye and Ariff, 2016, pp. 117-118) consists of a view of these and can be found in Appendix H as well. Both tables demonstrate that there exist multiple uncertainties related to the risk assessment of a data breach. In practice, even with limited data on which to base estimates of probability distributions such as a phenomenon in this research, it is preferable to base the decision on even the simplest forms of probability distributions when compared to dimensional point estimates or risk assessments based on subjective ratings (Chapman and Ward, 2011, p. 47).

Depending on the level of uncertainty, or unknown, the risk management and mathematical methods vary. For example, in the case of black swans thought experiments and scenario analysis are only feasible options as they are beyond the realm of modelling (Firoozye and Ariff, 2016, pp. 188-190).

The use of Monte Carlo simulation pops up in multiple sources (Barabanov et al., 2011, p. 35; Hayden, 2010, pp. 254-259; Edwards et al., 2016, p. 10; Salci and Jenkins, 2016, p. 9; Chapman and Ward, 2011, p. 297); however, the use of Monte Carlo simulation requires parameters for the simulation that as of now can only be based on historical data that are inadequate and are most likely subject to change continuously. The aforementioned creates problems with the model that make use of Monte Carlo simulation an inappropriate option (Firoozye and Ariff, 2016, pp. 110-111). Example of a situation in which the use of Monte Carlo is feasible could be a simulation that estimates the probability of getting two pairs or any other combination from a deck of cards. You know the variables, i.e., cards; hence, calculating the outcome for any combination is possible from a deck, i.e., $C_5^{52} = \frac{52*51*50*49*48}{5*4*3*2*1} = 2,598,960$. While 100 iteration of randomly drawing a deck might not result in a probability of getting two pairs from the deck, i.e., 4.7539%, eventually when the number of iterations is high enough, e.g., 50,000, the result will be closer to the probability above.

Concerning risk assessment related to the information security, participant 2 stated that "Random statistics make it hard to measure or estimate anything," in this case term "random statistics" refers to statistics created under the influence of statistical problems that have been discussed previously, such as self-reported results, breaches that are not detected, and similar problems.

According to the participants, there exists a need to predict or estimate costs, likelihoods, and threats, but statistical problems related to information security make it difficult to do so. Moreover, even if a model is offered, it is rarely feasible in practice as the "battleground" evolves constantly, and the variables related to the

assessments are numerous and subject to change as well, e.g., a single bad apple can be enough as participant 1 pointed out, and it is impossible to predict if or when a bad apple manifests. On the other hand, an organisation can have countermeasures to decrease the possibility of such bad apples, such as profound background checks, monitoring, or other measures (Appendix E).

4.1.5 Theme - Metrics/Evaluation

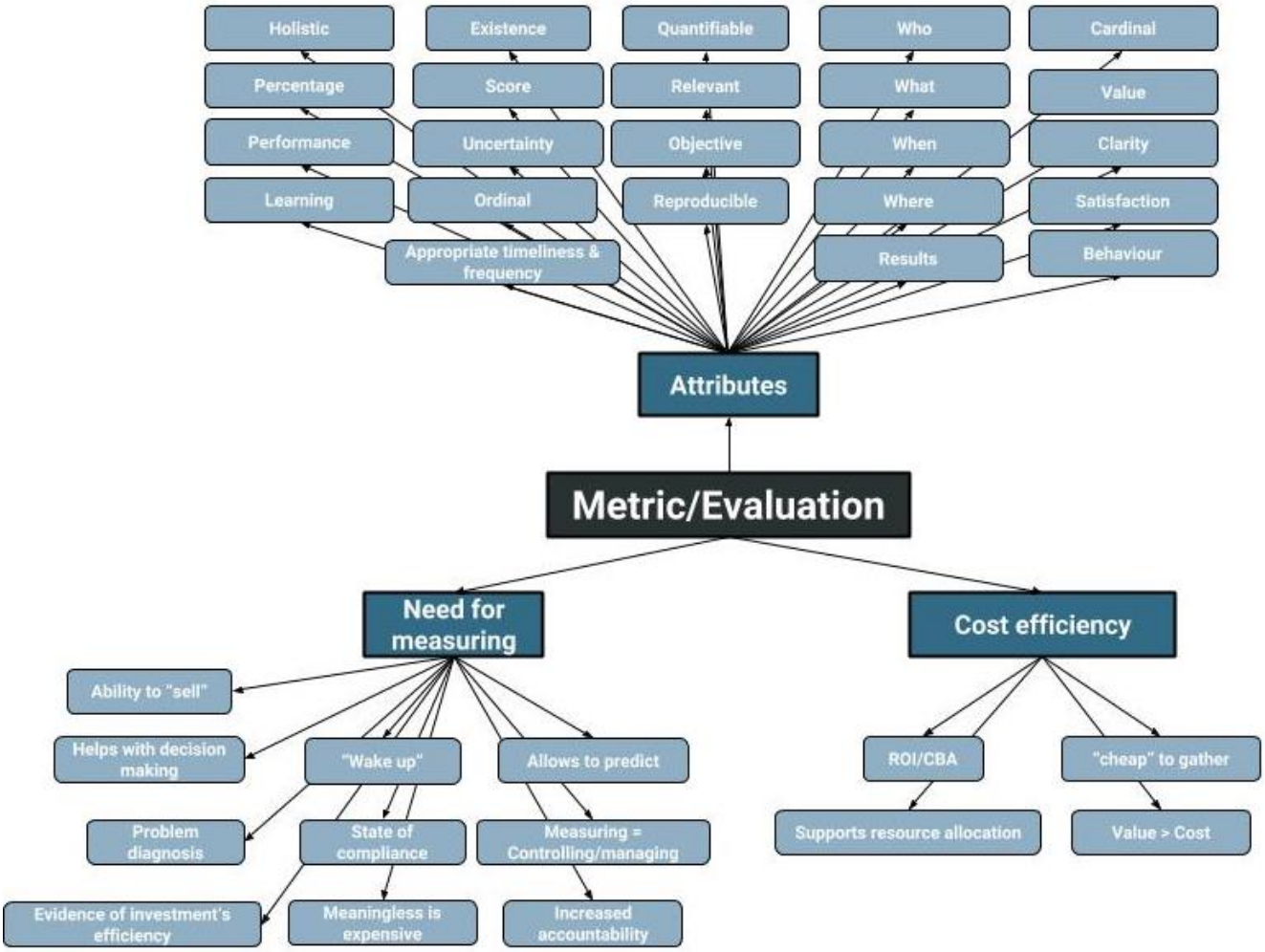

Figure 6 Analysis of metric/evaluation.

The last theme metric/evaluation is formed from categories attributes, cost efficiency, and need for measuring. The full analysis can be found in Appendix I. As all of the categories are relevant for the study, the most important parts of the analysis for each category are found here as well.

Metrics can be identified by a category where they belong, the categories of metrics, what they describe, and what they do not describe are elaborated in Table 15 (Axelrod, 2008, pp. 2-5, Firoozye and Ariff, 2016, p. 15), which can be found in Appendix I. Table 16 (Barabanov et al., 2011, pp. 6-7; Rathbun, 2009, pp. 6-8; Jaquith, 2007, pp. 26-27) found in Appendix I offers a selection of qualities concerning what makes metric a good or a bad one.

When deciding on the metric, the goal of the organisation (or a program) should be first acknowledged. After this, the key indicators related to the phenomenon measured should be identified, i.e., if a SETA program focuses on passwords, then testing what percentage of the passwords can be cracked under four hours is an example metric. If the organisation either does not offer SETA training to all of the employees or offers a

different level of training for different stakeholder groups, then these groups or employees without training should be compared to those who have undertaken the SETA program (Jaquith, 2007, pp. 114-117). The metric(s) decided should help to diagnose problems, provide support to the decision-making process, guide resource allocation, and demonstrate the state of compliance within an organisation. They can be used to benchmark the organisation within the industry or to compare if a policy change or training conducted affected the organisation in the desired way (Rathbun, 2009, pp. 3-5).

Figure 7 (Brotby and Hinson, 2013; Jaquith, 2007; Houngbo and Hounsou, 2015; Cambell, 2015) describes a limited selection of information-security controls and metrics that can be used to measure them. Note that this is a limited selection, and there exist metrics beyond the ones used for controls in the figure.

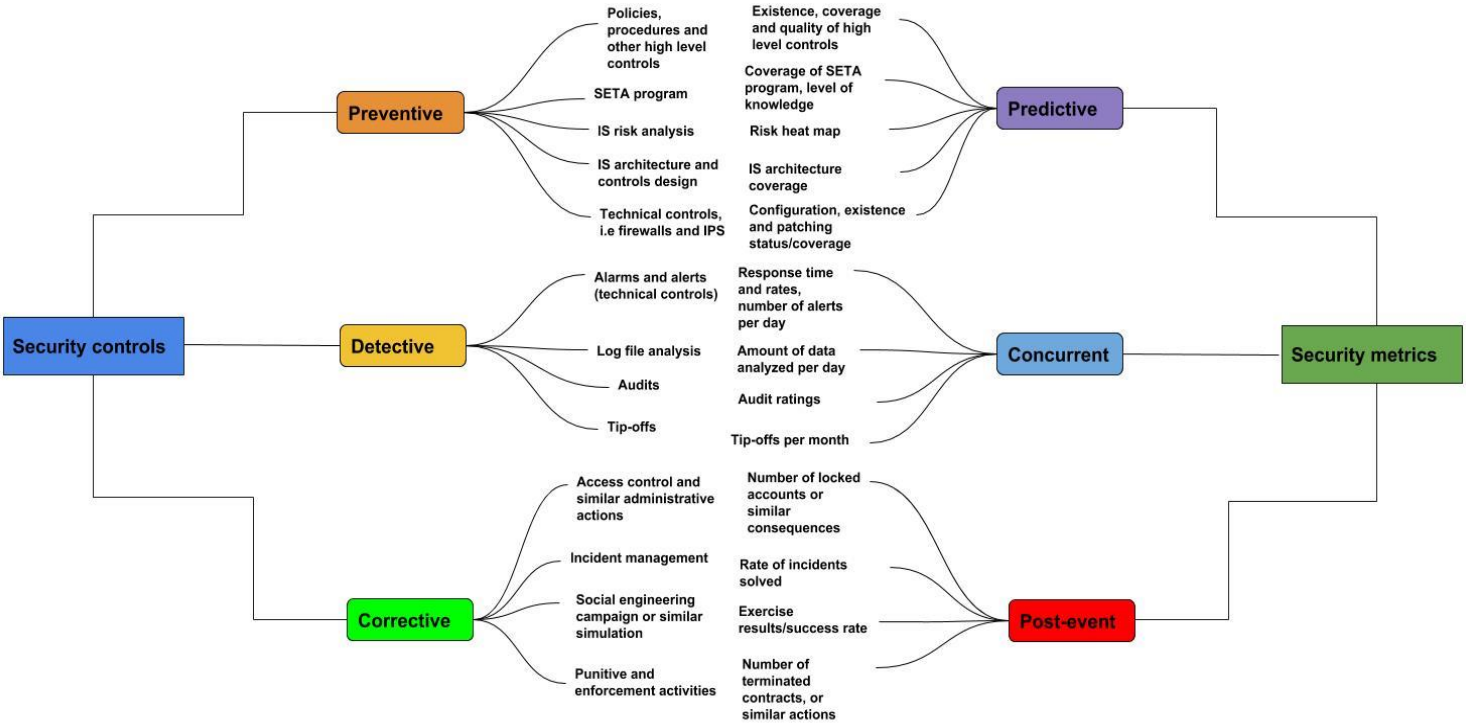

Figure 7 Information-security controls and metrics connected.

Since decision makers in organisations and policymakers in government need evidence to make well-informed decisions regarding the information-security investment (Makridis and Dean, 2018, p. 81), it is the role of the metrics, measuring, and assessment to give this evidence. Through measuring and studies related to the impacts of a breach, it is possible to enable organisations to be more proactive (Densham, 2015, p. 5). And, without consistent and objective measurements it is impossible to demonstrate the performance and effectiveness of a solution (Rathbun, 2009, p. 3). Frankly the same goes towards the learning of the employees and results of a SETA program (Cambell, 2015, p. 142).

One of the greatest challenges related to measuring security is that objectives, capabilities, and the environment changes all the time, and the countermeasures need to be adjusted appropriately with all three. And, while there exist frameworks that account for the capabilities adequately, they often do not treat the environment in a formalised or standardised way (Barabanov et al., 2011, p. 43). Another challenge is correlating any part of SETA with operational security metrics; in one source it was mentioned that only one

company in their experience did so during ten years of research. However, this was in the early 2000s (Jaquith, 2007, p. 21). While human behaviour and attitudes can be hard to measure, one method can be questionnaires, but as you answer to them yourself, it is easy to "cheat" just to give "right results" and not show what you are thinking actually. Nevertheless, password protection and management, sensitive information handling, social engineering (success rate in a simulated attack), physical/office protection, and the incident response rate are metrics that can be used to solve this challenge (Veseli, 2011, p. 63).

Metrics that the participants have used varied. Some did not measure at all, while some stated that measuring the successfulness of a SETA program or similar is rather difficult and measuring technical know-how is easier. Others did use social engineering campaigns and some sort of test to test understanding related to the content. The latter was deemed a bad way of testing actual understanding by participant 1 and 4, "Asking same questions prior the SETA and after is a bad method." and "Exams and such "mandatory" tests after the SETA are a bad way to test how the information was learnt." However, the reason why this method was viewed as a bad method was the way that the method was implemented, not the method itself.

According to most of the participants, customers rarely ask for any sort of measuring related to the SETA programs or proof that the product they bought had any effect. This might be due to the fact that most of the organisations buy administrative solutions because they are viewed as a necessary evil instead of an opportunity. The aforementioned is supported by the fact that two of the participants mentioned that if the organisation had any interest about the subject itself, e.g., information security or threats related to it, they did ask about the results and how and what was done.

4.2 Relationship of Themes and a Theory from Themes

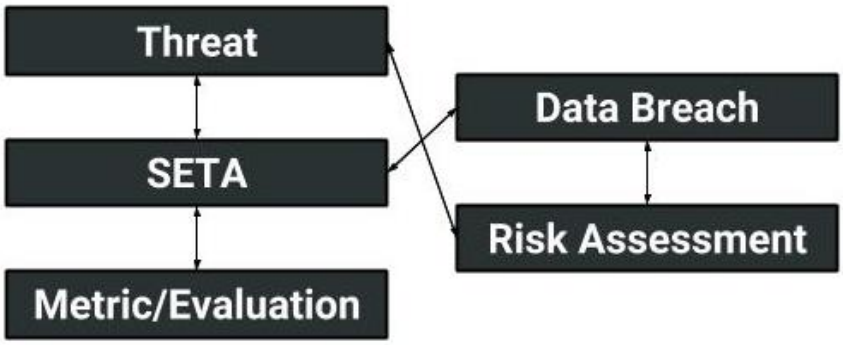

Figure 8 Relationship of themes

The connections between themes are shown in Figure 8 above. Threats in general and data breaches are risks that need a risk assessment. SETA is a safeguard that can be applied to mitigate threats, especially data breaches, and there exists a need for measuring the effectiveness of a SETA program.

It can be theorised that measuring the effectiveness of a SETA program from a financial point of view is incomplete as long the statistics and information related to the threats such as data breaches are lacking. Methods and metrics to evaluate the effectiveness of a SETA program in a certain category, e.g., social engineering or password strength, exist, but they should always be specific to the organisation's needs; hence,

no copied solution should be applied without careful evaluation of whether the metric serves the organisation or a program. The main reason why the organisations, i.e., customers, do not ask about measuring of the administrative solutions such as SETA might be that most of the organisations see these as a necessity. The view that SETA is a necessity can arise due to legal enforcement or requirement. Therefore SETA is not viewed as an opportunity to increase business revenue or to decrease the likelihood of losses due to errors or threats.

5 Discussion and Conclusion

5.1 Discussion Concerning SETA Programs and the Metrics Related to Them

The following chapter aims to answer the primary research question from the non-financial point of view by examining how the effectiveness of a SETA program can be measured through metrics in specific areas.

Based on the analysis it can be assumed that all of the education, training, and awareness can be beneficial to the organisation. All three aspects need to be implemented within the organisation, development of information security within an organisation needs the combination of training, education, and awareness to increase the understanding of information security and responsibilities each employee has towards the organisation. How the organisation conduct its SETA program and what is includes within it should be based on the organisational needs, employees (their skill level and role), and should be performed regularly. If the organisation fails to respect these three guidelines or tries to cover its SETA with a copied solution, it then can be assumed that results are lacklustre.

Metrics implemented should be based on the organisation's goals as well. Quantity does not equal quality in case of the metrics. As previously mentioned, no standard set of metrics exists, perhaps due to the fact they are always based on the organisation's goals and situational. There exist multiple sources for possible metrics, such as those by NIST (Wilson et al., 1998) who are directly connected with the United States, or by independent authors such as Brotby and Hinson (2013). The sources have more in common than differences, the metrics that are listed repeat themselves and the arguments are often lacking concerning how and why to implement the metric in question.

If an organisation aims to measure how its SETA program succeeded, the metrics described in Table 7 could be implemented. Metrics such as the percentage of personnel who have received annual/biannual/similar SETA program or existence of a SETA program are omitted as they do not measure the effectiveness of a SETA program, but its existence or coverage. The metrics offered by this study are nothing unique, and, a variation of these can be found in multiple other sources most likely, in case of these metrics the inspiration came from the interviews and my views after the qualitative analysis. However, argumentation how the metric could be implemented is offered, and, the reasoning is based on the analysis conducted for the study, e.g., trying to prove actual change or effectiveness instead of superficial metrics such as existence. Also, the interviews hinted that the metrics that prove effectiveness in practice tend to be the best, e.g., simulated attacks or situation where a participant needs to prove that they understood what they heard (i.e., open-answer instead of ticking a box).

Table 7 Example metrics for a SETA program

Metric	Category	Description
Knowledge test related to the education or training offered	Percentage & Cardinal	Percentage of the participants who pass the test should be measured, and the change that happens overtime to this baseline should be monitored. While the metric does not ensure that the

		participant will act according to their knowledge it can be used to measure the knowledge related to the subject(s), i.e., the answer should be written instead of selecting from multiple choices.
Phishing campaign	Percentage & Cardinal	Phishing campaigns can be useful metrics to measure actual understanding of social engineering and do they act according to what they should know. A percentage of successful attacks and how far victims went if the attack has "multiple phases" should be measured. Once again, after the baseline is established the change concerning the metric should be monitored. Beyond the cardinal and percentage metric one should also focus on the "who" i.e., who were the individuals who failed a the simulated attack, those individuals who failed multiple times should receive extra attention and if they fail to correct their behaviour an action should be taken to limit possible damage that their credentials can use. One participant mentioned that even more sophisticated phishing attacks, i.e., spear phishing, should be carried out if resources enable.
Quality of passwords	Percentage & Cardinal	Percentage of passwords that were cracked after under 4 hours and 24 hours could be measured, the period used can be modified according to the organisation's goals, but based on the interviews these translate to "satisfactory" and "good" passwords. Once again, after the baseline is established the change concerning the metric should be monitored. Both password related metrics are a good measurement to see how the password policy of the organisation and guidelines are understood and followed.
Physical penetration test	Cardinal	A test concerning how many of the physical penetration attempts are successful should be carried out to see if the employees understand the function behind physical safeguards and are they able to perceive suspicious actors. Note that percentage is an unnecessary category if you measure just a couple of tries per month.

How often above metrics should be carried out depends purely on the organisation and its resources: from the interviews, it was determined that few organisations carry e-mail-based phishing campaigns monthly against themselves, for example. Based on the literature and interviews, phishing campaigns and physical penetration tests should be carried more often than the metrics related to the passwords or knowledge of the subjects. A knowledge test could be carried out every time a more laborious part of the SETA is conducted, e.g., education or training. The quality of passwords, if automated, could be tested out weekly.

5.2 Estimated Effectiveness of SETA Program from a Financial Point of View

Following chapter answers the primary research questions from the financial point of view through a model that was constructed during the research process. The chapter also answers partly to the sub-questions related the variables of the participant and those which are not connected to the participant, e.g., how often training is offered and similar variables.

As the analysis points out, there exist problems concerning the statistics related to data breaches as of now. Based on the documents and interviews, a model was constructed by the researcher. The model assumes the main goal from the organisation's point of view is to reduce the likelihood of possible breaches due to human factors and to see the financial effects of a SETA program. If the situation is as aforementioned, the following model could be used:

1. The effectiveness of the SETA program per participant. Motivation, behaviour, time, i.e., how often and how long of the SETA program has been offered, and appropriateness are taken into account to calculate EP_i, which indicates the effectiveness of the SETA program per participant (cf. Equation 1).
2. The effectiveness of the SETA program per organisation. The effectiveness of the SETA program per participant is divided by the number of participants to calculate EO_i, which indicates the effectiveness of the SETA program in the organisation (cf. Equation 2).
3. Probability of a breach depending on the source:
    a. Attacker motivation, attacker capability, and the effectiveness of the seta program are taken into account to calculate PB_i, which indicates the probability of a breach (cf. Equation 3a).
    b. A priori probability of error/accident and the effectiveness of the seta program are taken into account to calculate PB_i, which indicates the probability of a breach (cf. Equation 3b).
4. Total probability of a breach. PB_i, from both sources, i.e., attack and error are used to calculate TB_i, which indicates the total probability of a breach (cf. Equation 4).
5. Cost of a record. Industry, a country where the organisation is located, detection time, post-breach management, the cause of a breach, and sensitivity of information are taken into account to calculate CR_i, which indicates the cost of a record per breach in question (cf. Equation 5).
6. The potential cost of a breach. The cost of a record and number of records breached, which indicate the potential cost of a breach PC_i (cf. Equation 6).
7. The expected cost of a breach per year. The potential cost of a breach and probability of a breach are taken into account to calculate EC_i, which indicates the expected cost of a breach per year (cf. Equation 7).

$$EP_i = \sum_{i=1}^{n} M_i + B_i + T_i + A_i \quad (1)$$

$$EO_i = \frac{EP_i}{n} \quad (2)$$

$$PB_i = (AM_i * AC_i) - EO_i \quad (3a)$$

$$PB_i = AP_i - EO_i \quad (3b)$$

$$TB_i = \sum PB_i \quad (4)$$

$$CR_i = I_i + C_i + DT_i + PBM_i + CA_i + S_i \quad (5)$$

$$PC_i = CR_i * NR_i \quad (6)$$

$$EC_i = PC_i * PB_i \quad (7)$$

Units for measures are up to the organisation's liking, but a score from 1 to 10 can be used for variables that lack actual unit of measure. The variable time should be transformed into the same scoring scale as well, e.g., 10 hours a year receives a score of 2, or whatever is the organisation's view on the subject. When estimating the probabilities organisation has to decide the impact that its SETA programs effectiveness has, e.g., an organisational score of 5.6 is transformed into a 28% decrease in the probability. Variables related to the costs should use the currency that is most relevant to the organisations.

The aforementioned model assumes that variables that affect the participants are known, variables related to the attacker(s) are known, a priori probability of a threat is known, variables related to the cost of a record are known, and the number of records that would be affected by the assumed breach is known. Based on the analysis conducted in this research as of now, no statistics exist that could give realistic information concerning the variables, and, based on the interviews and the literature available; it is highly unlikely that any organisation is collecting the aforementioned details related to itself. The cost-benefit part of the model comes from that model can be used to compare how the EC_i responds to changes in EO_i and how the expected cost compares to the costs of the SETA program during a period probability is calculated on, in this case, a year.

The number of variables in the EP_i is just an example, and, in reality, there would be more than the motivation, behaviour, time, and appropriateness. Participant 1 highlights that the efficiency of SETA is a social phenomenon that needs good culture and atmosphere within the organisation to work, and that just a couple of bad apples can ruin the results. Participant 2 states "If the organisation is doing badly, the turnover rate of the employees is high, human relations within the organisation do not work etc., it is desperate to implement a SETA program successfully. Humour and a positive atmosphere are really important," which supports the aforementioned point of view. Participant 3 has a similar opinion but adds that how much employees actually care about their job and how much they are about their organisation and work community affects as well.

The rest of the participants focus on the method of delivery, and the frequency of the training, e.g., participant 5 states that "Continuous is important, people tend to forget things they do not see as important, and my experience over 95% don't see the phenomenon as important." While participant 6 said "Continuous SETA, a robust solution at least twice a year that can be a workshop or two in a week combined with continuous information related to threats and overall "reminder" from management or such." Participants 4, 5, and 6 also mentioned that the message needs to be easy to grasp, e.g., "Message needs to such that it is easy to understand, and it feels relevant (i.e., you can show an example of an attack that happened through leaked credentials or similar that is relevant to the audience) and is interesting. The use of too technical terms and jargon makes it harder to understand the message in overall audience.", "easy to grasp message is important as most of the threats are hard to comprehend, so examples that are tangible help out a lot. And, the recommendations or guideline should be applicable to "normal life," and "Easy access, cannot be too technical, needs to be interesting."

Due to the amount of uncertainty and unknowns related to the phenomenon, it could be argued that the use of cost-benefit analysis or such is not feasible. Insurability of the cyber risks is a somewhat studied phenomenon, and results of studies show that lack of insurability exists because insurances prices cannot be calculated (Eling and Wirfs, 2018, pp. 21-22), which is due to the aforementioned problems concerning the statistics. Another study found out that randomness of loss occurrence due to the lack of data, changing nature of cyber risks, and small risk pools that cannot be diversified insurability of cyber risks is problematic (Biener et

al., 2015, p. 148). Cyber risk is a relatively new risk category; hence, the lack of data for an adequate estimation of probability, and, as previously mentioned, the dynamic nature of the risk and its proclivity to change makes use of the past statistics sub-optimal choice (Eling and Schnell, 2016, p.480). OECD (2018) highlight that quantifiability of cyber risks is challenging due to the limited availability of historical data, changing nature of cyber risks, and access to corporate security information (OECD, 2018, pp. 95-96), i.e., statistical problems are brought up once again. If insurance companies face the aforementioned problems concerning the modelling of cyber risks, such as data breaches, then it can be theorised that as of now use of a model such as that offered in this study or similar is an insufficient solution.

5.3 Conclusions

This study focused on a primary research question "How to measure the effectiveness of information-security education, training and awareness?" This study aimed to contribute with a method or a model on how to measure the aforementioned financially and to study methods beyond the financial point of view. The primary research question was answered with the above methods, the organisation can use metrics to measure the effectiveness of a program in the specific areas, or an organisation can use a model for a cost-benefit analysis to estimate the aforementioned from a financial point of view.

Both metrics and the cost-benefit analysis can be flawed methods, the latter more so. Metrics can show improvement or decrease in a certain area, but there is a possibility that the change happens due to some other reason than the SETA program whose effectiveness is measured. The cost-benefit analysis always deals with assumptions and uncertainty, especially in case of a data breaches that are identified as the premier target of mitigation by the SETA programs in this study. As long as the statistics are in a state they are now, doing any sort of analysis concerning costs and likelihood will be misleading at best. Therefore this study implicates that financial analysis related to the cyber threats such as data breaches and how they can be mitigated through information-security education, training and awareness is impossible as now if the analysis aims to offer even remotely reliable results. While the study contributed to the dilemma by making a model that (while limited) could be used to estimate the aforementioned, the model itself is not that useful as long the statistical problems exist.

Beyond the primary research question, this study aimed to answer what kind of variables can affect the effectiveness of a SETA program. The analysis conducted in this study answers the sub-questions related to the variables concerning the SETA. Variables such as morals, beliefs, an opinion of the organisation, knowledge concerning the threats, and resilience are just examples of these variables related to the individual. It was found that the method of delivery and the target audience of a SETA program are important as well, so both the organisation, e.g., instructor and management, and the audience have an effect how the SETA program performs. Social issues such as how participants see their organisations, job, and work atmosphere can affect the results as well. Therefore, this study implicates that multiple variables can affect the effectiveness of a SETA program, however, while the research conducted contributed by discovering a number of the variables that can affect this number is limited, and, therefore the variables related to the dilemma need further research.

5.4 Quality Criteria

The quality criteria are respected to the best ability of the researcher. Quality criteria, as described in Section 3.4 consist of credibility, dependability, generalisability, and objectivity in terms of this study.

Credibility is respected by data triangulation; the pieces of data in almost every scenario exist in several sources. Dependability is respected by that description of data gathering, and analysis procedures exist; hence, it is possible to find how the results were reached. Generalisability is acknowledged, but it is impossible to know that interviews by another scenario would result in similar data. However, the researcher deems this to be likely, this view is supported by the discussion related to the topic I have witnessed, and by the literature that exists, still, a differing opinion must exist.

In terms of objectivity, the researcher cannot ensure that his identity, values, and beliefs did not play a role in the production and analysis conducted. However, the researcher will admit that his views related to the phenomenon did change during this research by the literature analysed and through interviews conducted. At the start of the research, the researcher had a belief that cyber threats can be assessed by the likelihood and consequences; however, this study has demonstrated that statistical problems and the nature of the threats make this near impossible, and any analysis conducted will be far from trustworthy.

5.5 Further Limitations of this Study

The research conducted for this study could have suffered from biases by the author or by the participants. The number of the interviews was on the side of small, even if the theoretical saturation was achieved in researchers view as every interview more or less followed the earlier it is possible that the tenth or twentieth interview could have offered some new information or views that could add value to this study. However, due to the time constraints of the thesis itself and the researcher's obligations, it was not feasible to pursue further interviews as those that were conducted reached the theoretical saturation in researchers opinion.

The data related to the data breaches (and other cyber threats) is viewed as not optimal as of now, hence the study is limited by the state of the statistics and reports. This, while not fault of the researcher himself, must be acknowledged as a significant limitation.

5.6 Future Research

While the problems related to the statistics concerning the phenomenon most likely will not change in a while, it might be beneficial to study the variables concerning the effectiveness of a SETA program on more a profound level. For example, whatever or not the target audiences' education level affects the results of a SETA program, and similar variables could be studied furthermore.

To be more specific future research could deal with questions such as:

- **How does the participant's level of education affect the effectiveness of a SETA program?**
    - It would be beneficial to study how education affects the effectiveness of a SETA program or similar. The researcher assumes that individuals with a higher level of "learning", i.e.,

undergraduate degree, have an easier time absorbing and retaining new information if motivated (prior research conducted on another study showed results that hint this). Hence, if a targeted approach is the most efficient solution as argued within this study, the education could play a part in the segregation of groups of targeted approach.

- **What kind of variables (e.g., risk aversion, age, or sex) can help to identify individuals who need specific attention concerning cyber threats that are connected to the human factor?**
    - As aforementioned, the research questions such as above could help to target the group(s) that are more vulnerable to social engineering, or inclined to errors.
- **What are the organisations view related to the administrative safeguards and why they are such?**
    - While the participants of the research conducted offered some views related to how organisations view administrative safeguards and why they are such it could be beneficial to gain further insight related to the topic, for example, through qualitative research and by interviewing relevant decision-makers of the organisation. If the general view is that administrative safeguards are limiting, useless, or negative in some other way, the results of such study could help the organisations that offer those administrative solutions to make them more supporting to the needs and wants of the organisations, as long as the trade-off does not end up hindering the security.

References

Albrechtsen, E., & Hovden, J. (2010). Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study. Computers & Security, 29, pp. 432- 445.

Algarni, A. M., & Malaiya, Y. K. (2016). A consolidated Approach for Estimation of Data Security Breach Costs. Colorado State University.

Amankwa, E., Loock, M., & Kritzinger, E. (2014). A Conceptual Analysis of Information security Education, Information Security Training and Information Security Awareness Definitions. The 9th International Conference for Internet Technology and Secured Transactions, pp. 248-252.

Andersen, T. J. (2014). Contemporary Challenges in Risk Management Dealing with Risk, Uncertainty and the Unknown. Palgrave Macmillan.

Andress, J. (2011). The basics of information security, understanding the fundamentals of InfoSec in Theory and Practice. Syngress.

Awad, A. I., & Fairhurst, M. (2018). Information Security: Foundations, Technologies and Applications. Institution of Engineering and Technology.

Aven, T. (2008). Risk Analysis, Assessing Uncertainties beyond Expected Values and Probabilities. John Wiley & Sons Ltd.

Axelrod, W. (2008). Accounting for Value and Uncertainty in Security Metrics. ISACA.

Badie, N., & Lashkari, A. H. (2012). A New Evaluation Criteria for Effective Security Awareness in Computer Risk Management based on AHP. Journal of Basic and Applied Scientific Research, 2(9) pp. 9331-9347.

Barabanov, R., Kowalski, S., & Yngström, L. (2011). Information Security Metrics, State of the Art. DSV Report series No 11-007.

Biener, C., Eling, M., & Wirfs, J. H. (2015). Insurability of Cyber Risk: An Empirical Analysis. The Geneva Papers 2015, 40, pp. 131-158.

Breachlevelindex. (2019). Data Breach Statistics.

Brotby, W. K., & Hinson, G. (2013). PRAGMATIC Security Metrics. CRC Press.

Cambell, G. (2015). Measuring and communicating Security's Value, A compendium of metrics for Enterprise protection. Elsevier.

Campbell, H. & Brown, R. (2003). Benefit-Cost Analysis. Financial and economic appraisal using spreadsheets.

Casey, E. (2011). Responding to a Data Breach: A Little Knowledge is a Dangerous Thing. Digital Investigation 8, pp. 1-2.

Chapman, C., & Ward, S. (2011). How to Manage Project Opportunity and Risk, Why uncertainty management can be a much better approach than risk management. John Wiley & Sons Ltd.

Charmaz, K. (2006). Constructing Grounded Theory A Practical Guide Through Qualitative Analysis. SAGE.

Cho, J. Y., & Lee, E.-H. (2014). Reducing Confusion about Grounded Theory and Qualitative Content Analysis: Similarities and Differences. The Qualitative Report, Vol. 19, Article 64, pp. 1-20.

Colwill, C. (2009). Human factors in information security: The insider threat - Who can you trust these days? Information security technical report 14, pp. 186 - 196.

Denscombe, M. (2014). The Good Research Guide: For small-scale research project, 5th edition. Maidenhead: Open University Press.

Densham, B. (2015). Three cyber-security strategies to mitigate the impact of a data breach. Network Security.

Desman, M. B. (2003). The Ten Commandments of Information Security Awareness Training. Security Management Practices pp.39-44.

Dompere, K. K. (2009). Fuzziness and Approximate Reasoning : Epistemics on Uncertainty, Expectation and Risk in Rational Behavior. Springer.

Eling, M., & Werner, S. (2016). What do we know about cyber risk and cyber risk insurance? The Journal of Risk Finance, Vol. 17 Issue: 5, pp. 474-491.

Eling, M., & Wirfs, J. (2018). What are Actual Costs of Cyber Risk Events? European Journal of Operational Research .

Fabbri, D., Frisse, M. E., & Malin, B. (2017). The Need for Better Data Breach Statistics. JAMA Internal Medicine, Volume 177, Number 11 p. 1696.

Firoozye, N. B., & Ariff, F. (2016). Managing Uncertainty, Mitigating Risk: Tackling the Unknown in Financial Risk Assessment and Decision Making. Palgrave Macmillan.

Fowler, K. (2016). Data Breach Preparation and Response. Syngress.

Gardner, B., & Thomas, V. (2014). Building an Information Security Awareness Program, Defending Against Social Engineering and Technical Threats. Elsevier.

Gattiker, U. E. (2004). THE INFORMATION SECURITY DICTIONARY Defining the Terms that Define Security for E-Business, Internet, Information and Wireless Technology. Springer.

Gemalto. (2013). Breach Level Index. Retrieved from https://breachlevelindex.com/.

Gemalto. (2018). Breach Level Index. Retrieved from https://breachlevelindex.com/.

German, P. (2016). A New Month, A New Data Breach. Network Security.

Glaser, B. G., & Strauss, A. L. (1967). The discovery of grounded theory. Aldine Publishing Company.

Greenberg, A. (2018). The Untold Story of Notpetya, The Most Devastating Cyber-attack In History.

Hadgany, C. (2010). Social Engineering, The Art Human Hacking. Wiley.

Hanley, R., & Tiller, J. S. (2007). Information Security Management Handbook 6th Edition. CRC Press.

Harry, B., Sturges, K. M., & Klingner, J. K. (2005). Mapping the Process: An Exemplar of Process and Challenge in Grounded Theory Analysis. Educational Researcher, Vol. 34, No. 2, pp. 3-13.

Hayden, L. (2010). IT Security Metrics, A Practical Framework for Measuring Security & Protecting Data. McGraw-Hill.

Herrmann, D. S. (2007). COMPLETE GUIDE TO SECURITY AND PRIVACY METRICS, Measuring Regulatory Compliance,Operational Resilience, and ROI. Taylor & Francis Group.

HIPAA-Journal. (2018). Research Suggest Healthcare Data Breaches cause 2,100 Deaths a Year.

Hofmann, A., Wheatley, S., & Sornette, D. (2018). Heavy-Tailed Data Breaches in the Nat-Cat Framework & the Challenge of Insuring Cyber Risks. Symposium on Insurance and Emerging Risks, St. John's University.

Houngbo, P. J., & Hounsou, J. T. (2015). Measuring Information Security: Understanding And Selecting Appropriate Metrics. International Journal of Computer Science and Security (IJCSS), Volume 9, Issue 2 pp. 108-120.

Information-Security. (2008). Securing Intellectual Property: Protecting Trade Secrets and Other Information Assets. Elsevier.

Jaquith, A. (2007). Security Metrics, replacing fear, uncertainty, and doubt. Addison-Wesley.

John, N. (2017). BREACH, Remarkable Stories of Espionage and Data Theft and The Fight to Keep Secrets Safe. Penguing.

Johnson, A. (2013). Politicians clash as Town Hall agrees to pay data leak victims up to £5k each in compensation.

Lamontm, T. (2016). Life after the Ashley Madison affair. .

Layon, R., & Watters, P. A. (2014). A methodology for estimating the tangible cost of data breaches. Journal of information security and applications 19, pp. 321-330.

Lending, C., Minnick, K., & Schorno, P. J. (2018). Corporate Governance, Social Responsibility, and Data Breaches. The Financial Review 53, pp. 413-455.

Liu, L., Han, M., Wang, Y., & Zhou., Y. (2018). Understanding Data Breach: A Visualization Aspect. 13th International conference WASA 2018 .

Lv, B., Wang, D., Wang, Y., Lv, Q., & Lu, D. (2018). A Hybrid Model Based on Multi-dimensional Features for Insider Threat Detection. 13th International conference WASA 2018.

Makridis, C., & Dean, B. (2018). Measuring the economic effects of data breaches on firm outcomes: Challenges and opportunities. Journal of Economic and Social Measurement 43 pp. 59-83.

Mann, I. (2008). Hacking the Human, social engineering techniques and security countermeasures. Gower.

McCormac, A., Calic, D., Parsons, K., Butavicius, M., Pattinson, M., & Lillie, M. (2018). The Effects of Resilience and Job Stress on Information Security Awareness. . Information & Computer Security, Vol. 26 Issue: 3, pp. 277-289.

McLeish, D. L. (2005). Monte Carlo simulation and finance. .

McNiff, J., & Whitehead, J. (2002). Action Research: Principles and Practice, 2nd edition. London: Routledge.

Metalidou, E., Marinagi, C., Panagiotis, T., Eberhagen, N., Skourlas, C., & Giannakopoulos, G. (2014). the Human Factor of Information Security: Unintentional Damage Perspective. Procedia - Social and Behavioural Sciences 147, pp. 424-428.

OECD. (2018). Enchaning the Role of Insurance in Cyber Risk Management. OECD Publishing.

OTA. (2018). Cyber Incident & Breach Trends Report.

Peltier, T. R. (2005). Implementing an Information Security Awareness Program. Security Management Practices, Volume 14, pp. 37-49.

Pompon, R. (2016). IT Security Risk Control Management: An Audit Preparation Plan. Apress.

Ponemon. (2017). The Impact of Data Breaches on Reputation & Share Value.

Ponemon. (2018). 2018 Cost of a Data Breach Study: Global Overview.

Ponemon. (2018). 2018 Cost of Insider Threats: Global.

Ragan, S. (2014). Code Spaces Forced to close its doors after security incident.

Rathbun, D. (2009). Gathering Security Metrics and Reaping the Rewards. SANS Institute.

Riek, C. (1986). Understanding Uncertainty in Cost-Benefit Analysis and Impact Assessment. Canadian Environmental Assessment Research Council.

Roman, D. J., Osinski, M., & Erdman, R. H. (2017). The construction process of grounded theory in administration. Contaduría y Administración 62 pp. 985–1000.

Salci, S., & Jenkins, G. P. (2016). Incorporating Risk and Uncertainty in Cost-Benefit Analysis.

Saleem, J., & Hammoudeh, M. (2018). Defense Methods Against Social Engineering Attacks in Computer and Network Security Essentials . Springer.

Sanderson, J. (2012). Risk, uncertainty and governance in megaprojects: A critical discussion of alternative explanations. International Journal of Project Management, Volume 30, Issue 4, Pages 432-443.

Schroeder, J. (2017). Advanced Persistent Training, Take Your Security Awareness Program to the Next Level. Apress.

Sen, R., & Borle, S. (2015). Estimating the Contextual Risk of Data Breach: An Empirical Approach. Journal of Management Information Systems, vol 32, No. 2, pp. 314-341.

Sloan, R. H., & Warner, R. (2017). How Much Should We Spend to Protect Privacy?. Data Breaches and the Need for Information We Do Not Have.

Šolić, K., Nenadić, K., & Galić, D. (2012). Empirical Study on the Correlaction between User Awareness and Information Security. International Journal of Electrical and Computer Engineering Systems, Volume 3, Number 2, pp. 47-51.

Tsohou, A., Karyda, M., Kokolakis, S., & Kiountouzis, E. (2012). Analyzing trajectories of information security awareness. Information Technology & People, Vol. 25 Issue: 3, pp. 327-352.

Vacca, J. R. (2017). Computer and Information Security Handbook. Elsevier.

Walker, D., & Myrick, F. (2006). Grounded Theory: An Exploration of Process and Procedure. QUALITATIVE HEALTH RESEARCH, Vol. 16 No. 4, pp. 547-559.

Ward, W. A. (2015). Assumptions versus Predictions in Cost-Benefit Analysis.

Watson, G., Mason, A., & Ackroyd, R. (2014). Social Engineering Penetration Testing: Executing Social Engineering Pen Tests, Assessments and Defense. Elsevier.

Verizon. (2015). Data Breach Digest, Scenarios from the field. Verizon.

Verizon. (2018). 2018 Data Breach Investigations Report 11th edition. .

Veseli, I. (2011). Measuring the Effectiveness of Information Security Awareness Program. Gjøvik University College.

Whitman, M. E., & Mattord, H. J. (2018). Management of Information Security, 6th edition. Cengage.

Wiles, J., Gudaitis, T., Jabbusch, J., Rogers, R., & Lowther, S. (2012). Low Tech Hacking, Street Smarts for Security Professionals. Syngress.

Wilson, M., deZafra, D. E., Pitcher, S. I., Tressler, J. D., & Ippolito, J. B. (1998). Information Technology Security Training Requirements: A Role- and Performance-Based Model. Special Publication (NIST SP) - 800-16.

Wittkop, J. (2016). Building a Comprehensive IT Security Program. Practical Guidelines and Best Practices. Apress.

Won, R. (2013). Data Security Breaches and Privacy in Europe. Springer.

Appendix A – Structure / requirements of the interviews

Table 8 Questions of the Interviews

Questions
How big is the role of "human factor", for example, errors, social engineering, and such within your work?
What do you see as a motivation for an organisation to conduct any part of information security education, training or awareness?
What variables do you think affect the success rate or the efficiency of a SETA program on an individual level?
How do you measure the success of information-security related to the "human factor", for example, number of accidental disclosures or success rate of social engineering campaign, if you do measure at all?
How often an organisation asks for some sort of measurement to prove the efficiency concerning the product they bought, for example, training?

The table 8 above shows the questions of the interviews, while the format of the question might have changed depending on the circumstance, or on the previous discussion within the interview, the requirements were the same nevertheless. Questions were selected to answer the research questions "How to measure the effectiveness of information-security education, training, and awareness" and the sub-questions related to the variables. The questions were aimed to find underlying motivations if there exist any, related to the organisation buying the product. The last question concerning how often an organisation asks for proof concerning their product was selected as the first interview held answered: "rarely, if at all".

Appendix B - Statistics of Qualitative Data Analysis

Table 9 Results of qualitative data analysis

Theme	Category	Description	Count	% Codes	Cases	% Cases
SETA	Motivation for SETA	The motivation for SETA or a part of it is brought up.	97	13,40 %	6	100,00 %
Threat	Human factor	The importance or effect that 'human factor' has is brought up.	85	11,70 %	6	100,00 %
Threat	Risk	Definition of risk, risk itself or similar is brought up.	52	7,20 %	5	83,30 %
Metric/Training evaluation	Need for measuring	The need for measuring information-security (not limited to SETA) is brought up.	50	6,90 %	6	100,00 %
Threat	Insider	The threat caused by an insider is brought up.	36	5,00 %	4	66,70 %
Data breach	Causes	A cause of a data breach is brought up.	34	4,70 %	5	83,30 %
Risk assessment	Uncertainty assessment	The need for assessment of uncertainty is brought up.	34	4,60 %	4	66,70 %
Data breach	Costs	The cost (monetary) of a data breach is brought up.	31	4,30 %	6	100,00 %
Threat	Uncertainty	Uncertainty related to the threats is brought up.	30	4,10 %	5	83,30 %
Data breach	Need for counter-measures	A need for counter-measures related to the data breaches is brought up.	27	3,70 %	3	50,00 %
Threat	Outsider	The threat caused by an outsider is brought up.	22	3,00 %	3	50,00 %
Risk assessment	Need for a model/assessment	Need for a risk assessment model, or risk assessment is brought up.	21	2,90 %	5	83,30 %
SETA	Method important	Importance of delivery method is brought up.	20	2,80 %	3	50,00 %
Data breach	Bad statistics	"Bad statistics" are brought up.	17	2,30 %	4	66,70 %
Data breach	Consequences	Consequences related to a data breach are brought up	17	2,30 %	4	66,70 %
Metric/Training evaluation	Attributes	Possible attributes related to a metric(s) are brought up.	16	2,20 %	4	66,70 %
Data breach	Technical safeguards	Mention of a technical safeguard is brought up.	15	2,10 %	4	66,70 %
SETA	"Carrot"	Reward(s) related to the SETA are brought up.	14	1,90 %	3	50,00 %
SETA	Too general	Need for individualised SETA programs for an organisation is brought up.	12	1,70 %	4	66,70 %
SETA	How often	Mention how often SETA should be taken into account is brought up.	12	1,70 %	4	66,70 %
SETA	Lack of responsibility	Responsibility (lack of it) is brought up related to the employee or organisation.	10	1,40 %	3	50,00 %
Data breach	Increasing	Increase in cost/incidents/breaches is brought up.	10	1,40 %	3	50,00 %
Data breach	Need for data breach notification laws	Need for data breach notification (laws) is brought up.	8	1,10 %	1	16,70 %
SETA	"Stick"	Punitive action is brought up.	7	1,00 %	3	50,00 %
Metric/Training evaluation	Cost efficiency	Cost efficiency of a metric is brought up.	6	0,80 %	2	33,30 %

Data breach	Lack of statistics	Lack of statistics related to the data breaches is brought up.	5	0,70 %	2	33,30 %
SETA	Lack of motivation	Lack of motivation is brought up.	4	0,60 %	2	33,30 %
Threat	Variable	Variable related to the individual is brought up.	4	0,60 %	2	33,30 %

Appendix C - Code retrieval

Whole qualitative data-analysis file is available on a request. An example of the method is shown below in figure 9 code retrieval. Note that category and code are wrongly named but are theme and category instead. Coding from categories was done after this retrieval.

Category	Code	Case	Text	Coder	Date	Words	% Words
Threat	Human factor	QDA yleinen doc	"8.2. Ensure real understanding of the reasons for security controls Security education and	Admin	27.2.2019	319	0,6%
Threat	Human factor	QDA SETA doc	"This study has proven a significant correlation between user awareness of security issues and	Admin	25.2.2019	65	0,5%
Threat	Human factor	QDA metric doc	""WHAT MAKES A BAD METRIC? Now that I have explained what makes a good metric, we should	Admin	27.2.2019	777	4,6%
Threat	Human factor	QDA yleinen doc	"creates the [employee's] sensitivity to the threats and vulnerabilities of computer systems and the	Admin	26.2.2019	86	0,1%
Threat	Human factor	QDA yleinen doc	"The title of this activity, security awareness and training, has always amused me somewhat.	Admin	27.2.2019	1417	2,5%
Threat	Human factor	QDA yleinen doc	"The single most effective mechanism to limit risky behavior and prevent unauthorized activity is to	Admin	26.2.2019	57	0,1%
Threat	Human factor	QDA data breach doc	"The role of human error is a major cause here accidental disclosures can be severe and human	Admin	24.2.2019	39	0,3%
Threat	Human factor	QDA yleinen doc	"The problem with privileges In order for the businesses to function, certain privileges must be	Admin	26.2.2019	903	1,6%
Threat	Human factor	QDA SETA doc	"The information security program has five key elements that must be presented to the audience.	Admin	26.2.2019	112	0,9%
Threat	Human factor	QDA SETA doc	"The human factor is split into two-groups management and end user. The factors belonging to the	Admin	26.2.2019	46	0,4%
Threat	Human factor	QDA SETA doc	"The effectiveness of an information security program ultimately depends upon the behavior of	Admin	25.2.2019	93	0,8%
Threat	Human factor	QDA yleinen doc	"THE HUMAN CONDITION Despite the natural urge we may have to disagree, the human being and	Admin	26.2.2019	989	1,7%
Threat	Human factor	QDA yleinen doc	"Secure Process Design In the early days of software development, until the recent past,	Admin	27.2.2019	781	1,4%
Threat	Human factor	QDA yleinen doc	"Phishing is hacker lingo for fishing, whereby a million hooks are put into the water using Spam to	Admin	26.2.2019	285	0,5%
Threat	Human factor	QDA yleinen doc	"People, Process, and Technology One of the most universally understood, yet poorly implemented	Admin	27.2.2019	828	1,4%
Threat	Human factor	QDA yleinen doc	"Once the InfoSec program's place in the organization is established, planning for security	Admin	27.2.2019	388	0,7%
Threat	Human factor	QDA data breach doc	"Leveraging human beings to gain access to information is not new; it predates binary. In our	Admin	24.2.2019	48	0,4%
Threat	Human factor	QDA yleinen doc	"Learning to Identify Social Engineering Attacks The fi rst stage in social engineering prevention	Admin	27.2.2019	589	1,0%
Threat	Human factor	QDA yleinen doc	"Key avoidable causes for incidents: • Lack of a complete risk assessment, including internal,	Admin	26.2.2019	88	0,2%
Threat	Human factor	QDA SETA doc	"It was found that participants who were more resilient had higher ISA, whereas participants who	Admin	25.2.2019	401	3,3%
Threat	Human factor	QDA SETA doc	"Information security is more than just policies, procedures, standards, and guidelines. It is more	Admin	27.2.2019	203	1,7%
Threat	Human factor	QDA yleinen doc	"In conclusion, it should be accepted that the insider threat to information security cannot be	Admin	26.2.2019	33	0,1%
Threat	Human factor	QDA yleinen doc	"I feel no curiosity That is the mantra users should have when deciding on whether they should	Admin	26.2.2019	184	0,3%
Threat	Human factor	QDA data breach doc	"Errors and Omissions As businesses explore ways to become more agile, efficient, and flexible	Admin	27.2.2019	322	2,6%
Threat	Human factor	QDA yleinen doc	"Defining social engineering Social engineering has many definitions depending on which book you	Admin	27.2.2019	156	0,3%
Threat	Human factor	QDA data breach doc	"Business and consumer information sharing can provide the data necessary to adequately	Admin	26.2.2019	114	0,9%
Threat	Human factor	QDA yleinen doc	"Being Aware of the Value of the Information You Are Being Asked For Referring to the Defcon 18	Admin	27.2.2019	1323	2,3%
Threat	Human factor	QDA yleinen doc	"Also, the security awareness portion because it needs to be general and applicable to every	Admin	26.2.2019	68	0,1%
Threat	Human factor	QDA Risk ass doc	"A cost-benefit analysis might not be meaningful because the analysis has neglected certain	Admin	27.2.2019	56	0,5%
Threat	Human factor	QDA yleinen doc	"48 percent of incidents involved a malicious or criminal attack, 27 percent were due to negligent	Admin	27.2.2019	36	0,1%
Threat	Human factor	QDA SETA doc	unfortunately, the unpredictability (or predictability) of human behavior can turn the most secure	Admin	26.2.2019	17	0,1%
Threat	Human factor	QDA data breach doc	he main human vulnerability is the human propensity to trust. Think of human vulnerabilities as an	Admin	24.2.2019	117	0,9%
Threat	Human factor	QDA SETA doc	also the enforcement of the policy, rules, and regulations should be improved (if not yet in place	Admin	26.2.2019	80	0,7%
Threat	Human factor	QDA data breach doc	While there are many tactics that can be unleashed to manipulate people, the top three, phishing	Admin	24.2.2019	34	0,3%
Threat	Human factor	QDA SETA doc	Under the influence of the availability heuristic users tend to overestimate the likelihood of vivid	Admin	25.2.2019	44	0,4%
Threat	Human factor	QDA Risk ass doc	Uncertainty due to projections of human behaviour (e.g., future consumption patterns, or	Admin	25.2.2019	29	0,3%
Threat	Human factor	QDA data breach doc	Threat actors who engage in social engineering attacks do it because they know that the human	Admin	24.2.2019	26	0,2%
Threat	Human factor	QDA yleinen doc	This means users should be an organization's number-one security concern. Phishing, by itself, is	Admin	26.2.2019	68	0,1%
Threat	Human factor	QDA data breach doc	They often take advantage of their targeted victim's sense of curiosity and psychology in order to	Admin	24.2.2019	88	0,7%
Threat	Human factor	QDA yleinen doc	The phrase "People are the weakest link in your security" is a term often used by security	Admin	26.2.2019	786	1,4%
Threat	Human factor	QDA SETA doc	The most important step in preventing social engineering attacks is teaching your workforce that	Admin	25.2.2019	120	1,0%
Threat	Human factor	QDA SETA doc	The implication of this study is that information security awareness is the key to mitigate security	Admin	26.2.2019	120	1,0%
Threat	Human factor	QDA yleinen doc	The human factors discussed in this paper provide practical levers to gain a better understanding	Admin	26.2.2019	226	0,4%
Threat	Human factor	QDA yleinen doc	The human factors discussed in this paper provide practical levers to gain a better understanding	Admin	26.2.2019	27	0,0%
Threat	Human factor	QDA training doc	The focus is beginning to change from being solely a machine view, i.e., measuring the	Admin	26.2.2019	81	0,8%
Threat	Human factor	QDA data breach doc	The biggest challenges in information security frequently involve humans more than they involve	Admin	24.2.2019	51	0,4%
Threat	Human factor	QDA yleinen doc	Technology can provide a means for controlling access to information and help the monitoring and	Admin	26.2.2019	99	0,2%
Threat	Human factor	QDA data breach doc	Social actions are typically part of a blended attack, with malware also present in 85% of data	Admin	24.2.2019	27	0,2%
Threat	Human factor	QDA yleinen doc	Since the inception of modern technology, Social Engineers and hackers have understood that the	Admin	26.2.2019	90	0,2%
Threat	Human factor	QDA metric doc	Security is the result of human activity. Effective measurement programs attempt to understand	Admin	24.2.2019	18	0,1%

Figure 9 Code retrieval

Appendix D - Participant Information and Key Findings from the Interviews

Table 10 Participant information

Participant #	**Professional age (Young > 5, Medium > 5, < 10, and Old > 10)**	**Employer**
P1	Old	A large sized global organisation
P2	Old	A large sized global organisation
P3	Medium	A large sized global organisation
P4	Young	A large sized global organisation
P5	Young	A small sized local organisation
P6	Young	A medium sized global organisation

All of the participants interviewed work within information-security spectrum, even if their organisation offers some other services as well. The education level of the participants varied, but all had at least an undergraduate or comparative degree. Beyond this the selection of participants was done respecting the criteria given in section 3.2.2.

Note that P1 & P2 were interviewed together and the interview did not follow the structure given in Appendix A. but was a more open discussion related to the data breaches, SETA, variables and such. Still the key findings from P1 & P2 distributed in a way that the rest of the key findings are done.

P1:

- Q1
    - "I have that understanding that many of the successful attacks happen due to the human factor. Technical solutions, if implemented correctly, is really hard to breach. Every human on the other hand has "weak moments", a mass phishing campaign, even if just a 1% succumbs it is a lot. Most of the hacking nowadays are through email to my understanding."
    - "Tailgating, accessing an organisation with yellow vest and ladder or just looking busy with a phone can be enough to gain physical access to the premise."

- "Just a single proper breach can deprive half of the organisations business."

- Q2
  - "Main motivation tends to be compliance which results in lacking training that is conducted quickly which cheaper solution than one thoroughly implemented. Lack of motivation exists overall. Biggest motivation tends to be "compulsion, GDPR has created discussion concerning the threats, but sanctions are still unknown".

- Q3
  - "Quality of the SETA program and targeting it to the audience to have a great effect. Examples and customs instead of threats. The culture within the organisation and atmosphere are important. Rewards and giving emphasis to positive examples is important as rewarding tends to fortify behaviour."
  - "It is hard to get reward and punishment right, but it is easier to mess up with punishments."
  - "Most of the individuals do not read the material they are given unless they are trying to get a certification or such. Web training is rarely motivating, but a good trainer can be motivating, and "rewarding" training methods such as workshops or exercises tend to excite the audience."
  - "Efficiency of the SETA is a social phenomenon as well, good culture and atmosphere can make your work easier."
  - "Just a couple of bad apples are enough to "ruin" successfulness of a SETA program, human behaviour such as attitude and motivations are important."
- Q4
  - "Asking the same questions prior to the SETA and after is a bad method."
  - "It is easier to measure know-how related to technical issues when compared to administrative."

- Q5
  - "Very rarely a customer asks for a measurement. It is really rare to test both before and after the SETA."
  - "Overall it is hard to measure."

P2:

- Q1
  - "Technical versus administrative is the wrong point of view. You cannot fix bad technical infrastructure with administrative solutions, but good technical infrastructure, but you do not have administrative solutions in best scenario its waste of money, and in a bad scenario, people trust too much on the technical solutions."

- Q2
    - “Possible sanctions is one motivation, and the fact that doing the “best practice” will be enough as that will protect your own back. Even if the industry “best practice” might be lacking it is seen as a solution that is enough and no one will judge you.”
- Q3
    - “Example by the management is important, the same goes for the work community and culture overall in the organisation related to the information security. Small amounts often are better than much rarely. “
    - “Positive culture alone is not enough to patch lacking procedures and policies, but without a positive culture and motivation procedures and policies will not work as effectively as possible. Positive culture makes effective training easier as well. Without positive culture, it can be hard to get the message across.”
    - “Right audience, right topic and right method. Once you start to fulfil these the costs arise compared to pre-made solutions.”
    - “Workshops and exercises are a good method, but tend to take resources, e.g., time and money.”
    - “If the organisation is doing badly, the turnover rate of the employees is high, human relations within the organisation do not work etc., it is desperate to implement a SETA program successfully. Humour and a positive atmosphere are really important”.
- Q4
    - “It is hard to measure the successfulness of a SETA program.”
    - “It is hard to measure ROI of information-security, it is similar as trying to measure ROI of a roof or a cleaning. Obviously, they are necessary most of the time and have an effect on productivity, but how can you measure it?”
    - “You can use KPI (key performance indicators) to measure, but they do not downright that the change happened due to SETA.”
    - “Random statistics make it hard to measure or estimate anything. Surveying different methods concerning measuring and studying them could be valuable.”
- Q5
    - -

P3:

- Q1
    - “In my own experience, very many of the attacks start from the human factor.”
    - “Human factor is acknowledged start point of the attack in multiple places (e.g., companies, organisations, etc.).”
    - “I have witnessed the prevalence of human factor multiple times as both attacker and defender.”
    - “Really big role.”

- Q2
    - "For example, I was a part of a campaign where we had only the name of the organisation and their website. The organisation asked us to demonstrate how we could attack towards them with only information we were given. After some forensic, we went to present our results to the board and they "pissed their pants". Board made a conclusion that all their employees need to step up and ordered a SETA program immediately."
    - "All the SETA activities that I have held have had a good reception. They have been called as eye-openers, and it has been said that it is good that these things are brought up. If things are not brought up and organisations are "left in the dark" they will not probably recognise the need for SETA, but all the organisation where I have had a role as a trainer or such they have recognised the need."
- Q3
    - "Information-security culture, positive opinion of information-security, overall atmosphere at the organisation, how much employees actually care about their job and how much they are about their organisation and work community."
- Q4
    - "Social engineering campaigns, hoxhunt (a phishing company), etc."
    - "If the organisation has resources and is willing to use them phishing beyond an email campaign could be used, physical penetration, social media influencing, phone calls and such give a better and broader answer concerning the effectiveness of a SETA."
    - "Exams and such "mandatory" tests after the SETA are a bad way to test how the information was learnt."
    - "Good results should receive a reward, e.g., monthly or every two months the most successful employee concerning phishing campaigns or incident reporting should receive a reward. "Reward culture" is a good thing."
    - "Password strength is dependable on the policy, it should not be an individual responsibility, but the strength should be determined from the management, and through this, the strength should be achieved."
    - "15 characters is pretty strong, almost in all of the cases."
- Q5
    - "Most of the organisations do not ask, in my previous organisation this happened more often because the customers saw that it had value and it was nice to see how the SETA actually worked".

P4:

- Q1
    - "Both customers and our organisation have the biggest errors or mistakes due to so-called the human factor. It tends to offer "the lowest hanging fruit" (i.e., easiest to abuse).

- Q2
    - "What I have noticed that customers people talk more and more about the issues, not precisely interested about possible gains, or some organisations are, but most have the motivation from that other organisations are doing things as well ."
    - "Motivation or interest can exist if you can show the changes in prior cases, e.g., statistics from some SETA activity how it succeeded. The possibility to show changes is important. Some organisations care more about that they just do not miss anything and that the individuals responsible have "done their responsibility and covered their back" concerning 3rd party risks or similar situations, but what they can achieve is not interesting."
- Q3
    - "Depends on the audience of SETA, e.g., if you are training large audience of end users with limited technical background or information in general related to the issues it is important that message is as simple as possible. Intelligibility and frequency are the most important factors."
    - "If the SETA activity is successful there is little reason to do any major changes to it, so same activities year in, year out. If an activity had good results before no reason to use a large amount of resources on it."
    - "Method of delivery is important, easy to grasp message is important as most of the threats are hard to comprehend, so examples that are tangible help out a lot. And the recommendations or guideline should be applicable to "normal life"."

- Q4
    - "Social engineering campaigns, how many responded to the phishing. A baseline before the SETA activity and a campaign after it. Random social engineering campaigns every now and then should be continued as they seem to give best results in terms of measuring and results are easy to apply, e.g., some extra training can be offered to specific users."
    - "It could be useful to measure how many incidents were due to the human factor, where the incident started from and where it ended. So-called lifecycle of attack. For smaller incidents as well, not just big successful attacks."
    - "Applications/automation works well, and sometimes not that well. Everything can be abused, and no human-constructed system is flawless."
- Q5
    - "I do not remember any situation."
    - "An awareness portal where the customer can view the results of their employees related to the questions concerning the issues exists."

P5:

- Q1
    - "Most of the time pretty small, my work is mainly on servers and technology. Sometimes I handle training and obviously there the human factor has a huge role."

- Q2
    - “Organisations want to see that issue is getting better.”
    - “In practice, organisations do not care that much how you do things, they just want to see that starting point was this and we got forward with the issues.”
- Q3
    - “Easy access, cannot be too technical, needs to be interesting, e.g., sitcoms. Ten minutes or similar length, little, but often.”
    - “Continuous SETA. Every couple of weeks to every couple of months. Continuous is important; people tend to forget things they do not see as important, and my experience over 95% don’t see the phenomenon as important.”
- Q4
    - “Three questions after the SETA period, e.g., can you fake a sender address of an email with answers ranging from no and yes to yes if the attacker is really sophisticated.”
    - “Our organisation focuses mostly on technology. Hence the password strength or such is not relevant.”
- Q5
    - “In practice always, a formal report of the process, or a meeting where the issues that were fixed etc. is always given or held.”

P6:

- Q1
    - “Really big factor, I work mainly as an instructor and auditor.”
    - “Most of the threats that customers are asking solutions are human-related. Technical solutions are pretty much in order in most of the cases.”
- Q2
    - “GDPR, overall pressure or requirements” (What kind of requirements?) “A certificate or such that is required by a future customer or change in a contract, e.g., ISO 270001.”
    - “Then there are those organisations that believe that SETA can actually have influence and offer value to the organisation.”
- Q3
    - “Continuous SETA, a robust solution at least twice a year that can be a workshop or two in a week combined with continuous information related to threats and overall “reminder” from management or such.”
    - “Message needs to such it is easy to understand, it feels relevant (i.e., you can show an example of an attack that happened through leaked credentials or similar that is relevant to the audience) and is interesting. Use of too technical terms and jargon makes it harder to understand the message in overall audience.”

- Q4
    - “Simulated attacks always give good measure.”
    - “A random test after the SETA in a week or two” (What kind of test?) “Understanding related to the content of the training held.”

- Q5
    - “Varies on the reason why the customer is buying the solution. The customer that has a motivation that is not necessity or compulsion tends to be interested in the issues, and they often ask about the results, not a measurement always, but they ask information. Organisations who buy the solution only due to the requirement such as GDPR just wanted to get over with it.”

Appendix E - Full Analysis of Theme Threat

Rest of the categories for theme threat beyond the uncertainty and risk are analysed here. The analysis starts with the actors, i.e., insider and outsider, and follows up with human factor and variables.

When insider actor is in a distinct role in a data breach that insider can be defined as a malicious insider, a misguided insider or a well-meaning insider. Incidents with internal actors come in many forms. Staff can access patient data without the genuine need for it, due to error or curiosity (Awad and Fairhurst, 2018, p. 108). While aforementioned can result in a rather small breach, it is breach nevertheless, and severity of the breach cannot only be calculated by the size of the breach as even the smallest breach can have human consequences, especially in the case of healthcare organisations.

A malicious insider is an individual who does not have the best interests of the organisation and co-workers in their mind. While malicious insiders are the smallest group of the insider actors they are most damaging, a malicious insider will intentionally target the information most beneficial to them, and this information often when breached tends to be most damaging. The motivation of malicious insider can be revenge, where the economic gain might not be a goal, but damage to the organisation or an individual within the organisation is the end goal. Malicious insiders fall into two groups, those who get employed and are eventually alienated or disgruntled for some reason or those who are malicious when employed by the organisation and have an aim to steal information from the organisation. The first group is easier to spot, especially if the organisation monitors the behaviour of the employees; the second one is much harder to detect but tends to be less common of the groups. Extensive background check and methods of gaining an understanding of the candidate can be beneficial here and increase the likelihood that possible collision of interest is detected (Wittkop, 2016, pp. 92-93).

Misguided insiders are split into two groups as well; those who believe that their actions are justified due to some reason and believe that they are entitled to steal information of the organisation.

The second group is the people who do not understand or respect the ownership of the information they use or create. Most often employees sign an agreement concerning the intellectual property they create for the employer, and this property stays with the employer even if you switch the employer. You create something on your own time (not paid), it is yours. Most of the time when you create something on your employer's time (i.e., you are paid), it is theirs. (Wittkop, 2016, pp. 93-94)

Well-meaning insiders are the majority of those who can be considered as insider actors within an organisation. These individuals do not cause a breach by purpose, but by accidents, like sending the email to the wrong recipient by mistake or through social engineering. (Wittkop, 2016, p. 93)

Methods of managing the insider threat can be such as monitoring, least privilege, strong user management, segregation of duties, knowing your users and filtering. Monitoring can include numerous controls, video surveillance in key areas, recording all entries to the systems holding confidential data or logging. Least privilege means that individuals within the organisation have access only to things they require

and no more. Strong User Management enables that organisation does not find itself in a situation where an individual is terminated, yet the account and the rights that account holds are not terminated in adequate time (instantly). While this goes beyond the termination of an employee and their user rights that situation has the potential to be harmful to the organisation if the termination of the contract was "on bad terms". Segregation of duties ensures that more than one individual is required to perform certain tasks, in practice, this is so-called "two-man rule". Segregation of duties could work in a way that developer changes the source code, but the deployment of the change has to be done by another individual, e.g., the system admin, and the system admin should be unable to change the code alone. Knowing your users refers to, knowing your users. This can be accomplished by different methods; logging of all user actions and alerting on deviation from prior behaviour is one method. However, a simpler way is to ensure that management pays attention to their employees and therefore is open to detect changes in behaviour, beyond this employees should be coached to report suspicious behaviour from their co-workers. The latter should be accomplished by an incident reporting system so that the message does get through. Filtering is a method that mitigates mistakes and some malicious actions. In practice, a tool scans for confidential data leaving the system via email for example and can prevent the message, alert about the action or encrypt the message. However DLP can easily be fooled by a skilled attacker; hence it is relevant only in some of the malicious actions, mainly in those conducted by a not-so-skilled attacker (Pompon, 2016, pp. 182-184).

The category "Outsider" is closely connected with the category "Insider" when focusing on social engineering. The "outsiders" tend to be split into following groups, but they are not limited to them, petty criminals, criminal organisations, hacktivists and nation-state sponsored criminals (e.g., cyberwar).

Petty criminals as a group (or single individuals) tend to target organisations based on the opportunity. Where hacktivist might be attacking a organisations due to their actions, or lack of them, the petty criminals tend to be financially motivated. These are the least threatening group of the outsiders as they tend to lack financial and technical resources. Hence the attacks are not that sophisticated, and even in case of a successful attack, they have a tendency for quick returns instead of getting most of their "work" (Fowler, 2016, pp. 7-8). Beyond the economic gain "bragging rights" used to exist as a motivation for hackers, reputation has value, and if one wants to join some known hacker group, it is useful to have a resume (Gardner and Thomas, 2014, p. 12).

Organised criminals tend to attack organisations for financial gain. However, they tend to have resources and often are funded by the third party. Instead of attacking only based on the opportunity these groups can carry out planned attacks on an organisation that is identified beforehand, or given to them as a target, and their attacks tend to be highly efficient (Fowler, 2016, pp. 8-9).

Hacktivists are a group of individuals; one might call them criminals and someone else might use some other term. Their attacks are carried out due to political reasons (Fowler, 2016, pp. 9-10). Nation-state sponsored criminals are hackers that are employed or contracted by nation states to launch attacks towards the target given. While some nations rely on mercenaries (organised criminals), the prevalence of cyberwar, however, has increased number of individuals contracted by nations for both defensive and offensive operations (Fowler, 2016, pp. 10-11).

No matter is the threat internal or external the main vulnerability comes from the human factor. The main cause of this vulnerability is the tendency to "trust" people. While human error causes some of the incidents that can be classified as a data breach the majority of the successful attacks happen due to phishing.

The outsider attackers know that the “weakest link” of the defence tends to be human. Hence social engineering is an attractive method of attack. (Sloan and Warner, 2017, p. 8). This vulnerability might be partly caused by that we are taught to treat others the way we want them to treat us (Gardner and Thomas, 2014, p. 46). If the employees lack the basic knowledge concerning the threats, e.g., social engineering, and how to react to in case of possible incidents this ”lack of knowledge” can be damaging to the organisation and this makes the people the “weakest link” (Awad and Fairhurst, 2018, p. 108).

An organisation should not ignore that there are threats caused by “insiders”. These risks can be mitigated through appropriate risk assessment which takes motivation, opportunity, and capability into account. Even with appropriate risk assessment, it should be accepted that individuals in a trusted position can abuse that trust, and that accidental data breaches due to human error (or successful social engineering) are more likely than malicious insider attacks. So all in all “human factor” is something that should be assessed and managed, but cannot truly be eliminated (Colwill, 2009, p. 194-195). “Morals” is one variable that is rather hard to change, if one is a “rotten tomato” and has no problem doing immoral actions it rarely changes through employer’s intervention. Behaviour, on the other hand, is variable that can be effected through penalties (Bisogni et al., 2017, p. 11), or through positive actions (Wiles et al., 2012, p. 166). “Curiosity” which is one of the variables that make social engineering easier (Verizon, 2018, p. 12) tends to be a cause of mishandling of data as well (Awad and Fairhurst, 2018, p. 108), it is not uncommon that individuals within, for example, a healthcare organisation access information that they have no need to handle.

The management has their role to play on the human factor as well, lack of awareness, “excessive workload” and “inadequate leadership” can all lead to negative consequences which might result in risky behaviour, risky beliefs, lack of motivation, or similar situation which might lead to an incident (Badie and Lashkari, 2012, p. 9335). “Excessive workload”, or “inadequate leadership” can negatively affect employees “resilience”, which refers to employees ability to cope with or adapt to stress (McGormac et al., 2018, p. 284). “Resilience” has been found to affect employees’ knowledge, attitude, and behaviour (McGormac et al., 2018, p. 285).

“Optimism bias” and “availability heuristic” refer to how the human mind functions. “Optimism bias” is that individuals underestimate the chances that threat will happen to them, and at the same time they overestimate their control over it and “availability heuristic” means that individual overestimates the likelihood of an event that is easily remembered (Tsohou et al., 2012, p. 139).

As the prevalence of the information infrastructure increases through rapidly evolving, interconnected digital ecosystems so do the scale and likelihood of a possible breach. Hence the human factor is increasing variable concerning the threat which importance is not decreasing as long as the humans play a part in the handling of data and systems (Sloan and Warner, 2017, p. 11-12). Responsibility is something that should be given and demanded from the employees concerning their role of the information-security within the organisation. It needs to be communicated that each employee is responsible for the security within their infrastructure, businesses and their services (Metalidou et al., 2014, p. 427).

Appendix F - Full Analysis of Theme Data Breach

Categories causes, counter-measures, technical safeguards, and costs to a degree from the theme data breach are not directly relevant to the research questions of this study. However, everything is connected in a way or another. Hence the categories mentioned above are analysed here.

While the increase in the costs and statistical problems related to the costs were elaborated within the study how the costs of a data breach can be split was not discussed at all. Costs of a data breach can be split into tangible costs and intangible costs/consequences. Table 11 shows some examples of these costs and consequences (Layon and Watters, 2014, p. 2).

Table 11 Costs and Consequences

Tangible cost	**Intangible cost/Consequence**
Cost of investigation and identifying the policy, application, system or network vulnerability due to which data breach occurs.	Loss of reputation.
Cost of hiring staff to plan, design, implement, operationalise and manage new safeguards to prevent future data breaches and gain an appropriate level of assurance.	The use of stolen credential for identity theft.
Costs of restoring data.	Sanctions or removal from the PCI-DSS scheme.
Legal costs to defend against litigation from customers.	Staff and customer turnover due to the breach.
Damages paid to customers due to loss, defaming or similar.	Cost of “distraction,” i.e., extra work due to the breach.
Losses due to a competitor using stolen data or intellectual property	Increased risk of future attacks, i.e., the organization is seen as an easy target.
Communication costs to notify customers.	Criminal charges being laid to against staff or office holders

It has been found that safeguards can mitigate the cost of a data breach, e.g., encryption of data, besides this faster, the breach is noticed and contained, the lower the costs (Ponemon, 2018, pp. 9-10). From insider threats, it was found out that employee or contractor negligence costs the organisations most (Ponemon, 2018, p. 3), even though the breaches caused by the human error tend to be identified and contained faster than attacks by criminals and hackers. When all the actors, insiders and outsiders are compared, it has been found out that hackers and criminal insiders are most costly and human error or negligence is the cheapest cause (Ponemon, 2018, p. 9).

The focus concerning data breaches tends to be on breaches where the size of the breach exceeds a certain threshold. Instead of focusing on the size of the breach only the severity or impact of the breach should

be viewed as a more important variable. While larger incidents tend to be more harmful in general a targeted small scale breach, especially in the healthcare industry have the potential of being more harmful than the size alone indicates (Fabbri et al., 2017, p. 1696).

One example from the past is when Islington Council paid between £1,000 and £5,000 for 14 victims of a breach, in this breach mental health problems and sexual orientation was leaked. Beyond this the council was fined for £70,000, whole economic costs were over £100,000 (Johnson, 2013). While the economic impact to the organisation responsible of a breach can be harmful enough a cynical mind might ponder what the damages might be in a country where being a member of LGBT community can be a cause of death. The aforementioned example is to demonstrate that while the costs of a breach can be "high" per record, the overall consequences can be even more severe. This example shows that when assessing a threat such as data breach one should not only focus on the costs but the non-monetary consequences as well, e.g., consumer confidence, social trust and personal safety (Liu et al., 2018, p. 884).

If an organisation is breached and the breach is handled adequately, i.e., customers are notified, and consequences are "accepted" organisations can mitigate the potential reputational risks such as trust between partners, customer trust, or public image in general (Bisogni et al., 2017, p. 11). In the end, no matter do you focus on the costs or consequences organisations should consider both short- and long-term impacts of a data breach (Lending et al., 2018, p. 451).

Methods of managing threats, i.e., counter-measures and safeguards can be split between administrative, physical, and technical. Administrative safeguards are elaborated in the analysis of SETA. Physical safeguards refer to physical access controls such as fences, gates, locks, and camera surveillance. Beyond these maintenance efforts such as heating, cooling, fire suppressions and alarms are within the scope of physical safeguards (Andress, 2011, p. 11). While one might wonder what these have to do with information security, it is important to remember that it is easy to do a lot of damage if you gain physical access to a system, be it stealing or destroying the data. Same goes for the cooling and similar operations, if your server room burns down or gets shut down due to being overheated, there might be some inconvenient consequences.

Technical or logical safeguards depending on the source refer to firewalls, antiviruses, encryption, hardened OS, encryption, and multifactor authentication. Multifactor authentication, for example, can prevent many of the threats, e.g., stolen credentials or successful phishing (Wittkop, 2016, pp. 90-91). According to the interviews organisations often see multifactor authentication as too time-consuming, or cumbersome.

No matter how successful the implementation of technical safeguards is, it is not enough alone (Šolić et al., 2012, p. 50). This statement was supported by the interviews conducted on professionals who agreed that if you have good technical solutions, but your employees "do not know what they are doing" then the money on those technical solutions is wasted. Same goes the other way, even if your employees have top-notch education, training, and awareness, but the technical solutions are lacking it is a waste of money as well. All in all successful information-security is a combination of physical, technical and administrative solutions (Sen and Borle, 2015, p. 333), the defence is as strong as the weakest link, and no matter is that link firewall, inadequate physical controls or the user (German, 2016, p. 19).

Appendix G - Full Analysis of Theme SETA

There exist multiple different methods of delivering information in the SETA programs. The most appropriate method is a compromise between budget, schedule and other needs or restrictions of the organisation. Obviously, employee satisfaction and results play a part as well, but the organisation tends to come first (Whitman and Mattord, 2018, p. 274). Table 12 offers some of the most common delivery methods, their advantages and disadvantages, and when they could be applied (Whitman and Mattord, 2018, p. 274-275; Saleem and Hammoudeh, 2018, p. 614-616; Herold, 2005, p. 4; Wilson et al., 1998, p. 157).

Table 12 Methods of training delivery

Method	Advantages	Disadvantages	Application
One-on-one: A trainer works with a trainee one-on-one on specific areas	• Informal • Personal • Customised to the needs of the trainee • Can be scheduled to fit the needs of the trainee	• Resource intensive tends to be a not cost-effective solution.	• An induction training of a new employee • Further training on a specific area in case of a change of role within the organisation, i.e., "high risk" individual.
Formal class: A single trainer works with multiple trainees in a formal setting.	• Formal training plan, efficient • Trainees able to learn from each other • Interaction possible with a trainer • Usually cost-effective approach	• Relatively inflexible • May not be sufficiently responsive to the needs of all trainees • Difficult to schedule, especially if more than one session is needed	• An entry training of multiple new employees, i.e., trainees or mass recruitment due to the expansion of the organisation.
Pre-packed Computer-based training: Pre-packed software that provides training at the trainee's workstation	• Flexible in terms of scheduling • Self-paced, individuals can work on their own • Can be very cost-effective (one license can be used for multiple trainees)	• The software can be very expensive • Content may not be customised to the needs of the organisation	• Any situation where a broad view of the areas is sufficient. Might not be the best solution in more specific scenarios due to being premade.
Customised Computer-based training: Software that is ordered or made within the organisation to meet the specific needs.	• Flexible in terms of scheduling • Self-paced, individuals can work on their own • Can be as specific as the organisation desires	• The software can be very expensive, more expensive than in the case of pre-packed software.	• Training of "high risk" individuals, i.e., those who are working in roles where responsibilities and possible damages are high.
Distance learning/web seminars: Trainees receive a seminar	• Can be live or can be viewed later on (possibility of instant	• In the case of archived seminar possibility of instant feedback, or	• Any situation where a broad view of the areas

presentation at their computers. The possibility of feedback can be provided by voice or text depending on the platform.	feedback is lost though) • Can be an inexpensive solution	feedback at all is lost; hence the learning suffers • Live versions can be difficult to schedule.	is sufficient. Can be used in more specific situations as well to a selected audience. In the case of "high risk" individuals non-live option might not be appropriate.
User support group: Support from a community of users is commonly facilitated by a particular vendor as a mechanism to augment the support for products or software.	• Allows collaborative learning • Usually conducted in an informal social setting, i.e., training might be viewed as more entertaining	• Does not often follow a formal training model • The focus is on a specific topic or product	• When new software is implemented within an organisation that deals with personal information, for example, a patient data management system a specific training on that is necessary.
Self-study: Trainees study materials on their own, usually on their own time.	• Low-cost solution to the organisation (excluding certificates) • Places materials in the hands of the trainee • Self-paced	• Shifts responsibility of training onto the trainee with little formal support	• Beyond the certificates and standards, not that appropriate solution.

Both the organisation and the participants need motivation and will for SETA to be successful, aforementioned methods can affect both from the participant's point of view, and the organisation's motivation can arise from benefits gained by SETA.

Investing in information-security often as no tangible rewards for the resources invested to it, and when an incident happens, that leads to a breach some individuals might argue that investing in the information-security would not have prevented the breach. Organisations that are more willing to invest in information-security reduce the likelihood of being a victim of a data breach (Lending et al., 2018, p. 414).

The main benefits of SETA programs can be improved employee behaviour, members of the organisation know how to report violations of policies, and they enable employee accountability. The accountability is especially important due to that it ensures that employees know that if they mess up, there might be consequences; hence they will be more observant of their actions (Whitman and Mattord, 2018, p. 268).

It has been found that the use of technical solutions can be ineffective as long as the individuals do not have responsibility, training, and time to monitor these solutions regularly (Casey, 2011, p. 1). The responsibility of incident reporting, readiness, data management, security and privacy includes all of the organisation, the board, executives, all the employees and all the departments (OTA, 2018, pp. 8-9). This fact was demonstrated in the interviews when it was mentioned multiple times that if the management does not take the policies, or procedures seriously those beneath them in the hierarchy will not respect those either. Other motivations for the organisation can that it has been found that safeguards reduce the likelihood of being a victim of a breach (Lending et al., 2018, p. 41), reduce the impact of social engineering attacks (Verizon 2015,

p. 14), and it is highly likely that the costs of a successful breach outweigh investment in safeguards (Layon and Watters, 2014, p. 2). If the organisation offers mandatory SETA and make the employees sign a form where they accept their responsibility these actions ensure that the organisation can hold employees accountable (Whitman and Mattord, 2018, p. 268; Desman, 2003, p. 43).

Appendix H - Full Analysis of Theme Risk Assessment

Following tables 13 (Chapman and Ward, 2011, p. 33-34; Riek, 1986, p. 108-109, Dompere, 2009, p .6-7) and 14 (Firoozye and Ariff, 2016, pp. 117-118) offer a broad view of uncertainty and unknowns related to the risk assessment and decision making.

Table 13 Different forms of uncertainty

Type of uncertainty	**Description**
Ambiguity uncertainty	Ambiguity uncertainty arises from lack of complete/or perfect knowledge, lack of definition of project objectives, lack of an agreed contract and the unpredictable behaviour of relevant actors. Any form of lack of ambiguity that causes uncertainty is covered by this term. Ways of reducing it can be resolving the ambiguity, or by just giving it time and expecting project management to be adequate.
Inherent variability	Inherent variability refers to events that "always happen," e.g., inflation happens, but the rate of inflation varies. Ways of mitigating the risks that arise from inherent variability are rather limited, but one possible action is to make the client responsible for inflation for example.
Event uncertainty	Event uncertainty involves events, conditions, and circumstances, pretty much anything that may or may not happen and specific responses related to the aforementioned. This can include events such as equipment failure, fire damaging the server room, and so forth. Event uncertainty is often referred as "risks", and the reason is rather obvious.
Systemic uncertainty	Systemic uncertainty refers to forms of dependence, such as general or systemic responses. For example dependence between materials and labour prices when markets strengthen can be included here. Ways of mitigating risks caused by systemic uncertainty are buying when the prices are low, or general project management to ensure that activities do not get delayed or proactive actions to ensure that the delays will not happen if it is known beforehand that delays increase the costs of the production.
Predictive uncertainty	Predictive uncertainty refers to uncertainty about project impacts.
Evaluative uncertainty	Evaluative uncertainty refers to uncertainty about the application of evaluation techniques such as discount rate and value of non-market resources.
Conceptual uncertainty	Conceptual uncertainty refers to problems related to definitions and is rather similar to ambiguity uncertainty.
Ethical uncertainty	Ethical uncertainty refers to problems with defining objectives for evaluation.
Factual uncertainty	Factual uncertainty refers to difficulties with identification of alternatives.

Categorical uncertainty	Categorical uncertainty refers to the uncertainty that arises from incomplete or lack of knowledge, or vagueness in knowledge due to a number of problems associated with cognition: biases, imprecise evidence, ill-defined explication or objectives. The uncertainty due to incomplete knowledge or lack of knowledge is known as stochastic or probabilistic uncertainty as well.
Fuzzy uncertainty	Fuzzy uncertainty refers to vagueness in the knowledge structure and explication of terms and concepts.

Table 14 Classes of the Unknown

Levels of unknown	**Definition**	**General characteristics**
Certainty	The probability of an event is known with complete certainty, i.e., 100% if true or 0% if false.	May be tautological (1+1 = 2). May be assumed true (Sun rises tomorrow). May be axiomatic (self-evident, e.g., a triangle has three sides). May still be clouded by complexity. In general, it refers to things we know we know.
Knightian Risk or Probability	The uncertainty related to the event is measurable, i.e., with possible outcomes together with their probability distributions.	Knowledge of the exact likelihood of events exist and is modelled using probability. Risk can be quantified, modelled using empirical data, and profound plan for possible events is possible. Risk-aversion can be modelled with utility theory. In general, refers to that we know that there are things we do not know.
Knightian Uncertainty or Ambiguity	The knowledge of possible outcomes exist, but no knowledge of their probability distribution exists.	We know the outcomes, but not their probabilities. Outside the realm of probability, but can be modelled by imprecise probability, second-order probability. Preferences (ambiguity aversion) can be modelled. The uncertainty here exists due to lack of knowledge and can be reduced by increasing the knowledge if information exists.
Unknown Known – Complexity or Chaos	We know things, but we are unaware of knowing or we have not realised their value.	Events are known, but complex interaction over many agents exists. Events can be fully understood, but they include complex interactions which lead to deterministic chaos or complexity.
Unknown unknowns – Black Swans	Absolute ignorance, rare, unforeseeable events of magnitude and consequence.	Probability cannot be quantified. Events that happen are unexpected and unpredicted events.

Appendix I - Full Analysis of Theme Metrics/Evaluation

Metrics can be identified by a category where they belong, the categories of metrics, what they describe, and what they do not describe are elaborated in Table 15 (Axelrod, 2008, pp. 2-5, Firoozye and Ariff, 2016, p. 15)

Table 15 Metric categories and their descriptions

Category of metric	What metric describes	What metrics does not describe
Existence	Metric existence indicates if something exists. I.e., a question "Does the organisation have a SETA program?" can be answered by yes or no, sometimes answers such as not known or not applicable are used as well.	While the metric existence defines if something is it does not define the quality or quantity in any form. I.e., even if the SETA program is said to exist within an organisation in what form it exists is not defined. Hence the metric can be rather useless as a stand-alone option.
Ordinal	Metric ordinal indicates the quantity of something in a vague form, i.e., high, moderate or low. Often used in scenarios when dealing with the likelihood of an incident for example	A major problem with the ordinal measure is that it is subjective and understanding of a term varies between individuals. Due to aforementioned the metric ordinal is a victim of subjective bias. For example, a term "likely" tends to have probability from 50% to 100% attributed to it, and it is just one example, "unlikely" has 0% to 100% and due to the results such as these use of ordinal metric is rather flawed.
Score	The score can be a scale of one to ten, or an ordinal ranking is given numerical values, i.e., one is low, two is medium, and three is high.	Suffers from the same cons as ordinal, but in case of metric score illusion of higher precision can be gained by giving numerical values to a measure that still is based on subjective bias.
Cardinal	When a number is a trend that is looked over time it is defined as cardinal, in case of this metric it can be used to imply whatever something is increasing or decreasing, i.e., a number of employees own devices within the organisation.	Example cardinal metric of employees own devices alone would not say anything without knowing how the number of employees has changed within the organisation. If the number of employees own devices is decreasing, but the number of employees is decreasing as well there might not be any "improvement" happening, this is assuming that number of own devices is viewed as a bad thing.
Percentage	The percentage indicates the proportion of something, i.e., "What percentages of employees have taken mandatory induction SETA program?"	While percentage can be rather a useful metric in some scenarios using more precise measure instead of a "common one" can be beneficial, i.e., besides the percentage example on the left a similar metric concerning "high-risk individuals" might be more

		important than the general level of employee compliance. In general, the percentage can be an accurate metric, but the level of accuracy can depend on the denominator and measurer.
Holistic	In practice, a holistic metric is one which is not restricted to any extent. I.e., if 95 per cent of systems are patched within an organisation, it could indicate that it is good, or bad. If the mean of patched systems within an industry is 60% the 95% measure is really good, however, if the industry mean is 100% the 95% measure is a poor one compared to the industry mean.	While too narrow view can be misleading it should be noted that added value from a holistic metric depends on the trustworthiness and accuracy of the source. Sometimes omitting external information if it exists might be a more beneficial option than including it, this is purely a matter of judgement.
Value	A metric that is based on an estimate of value that might be lost if an incident leads to a breach or value that can be gained by avoiding the said incident.	Value metrics tend to rather rough estimates, and they are highly subjective. While prior scenarios can be used to estimate a potential loss the situation will never be exactly the same. Hence the lost (or gained) value will always differ from the prior source used.
Uncertainty	Metric uncertainty deals with the likelihood, but in the form of probability distributions for example. It can be used to indicate the likelihood of when a threat realises itself, or what the costs might be if no strict value is feasible.	As with metrics ordinal and score, the metric uncertainty suffers from subjective bias as well. However, the probability distribution can be much more representative than a point estimate and therefore should be used instead of aforementioned, or to supplement one or both of them.

When trying to define a metric the potential qualities are more plentiful, Table 16 (Barabanov et al., 2011, pp. 6-7; Rathbun, 2009, pp. 6-8; Jaquith, 2007, pp. 26-27) offers a selection of qualities concerning what makes metric a good or a bad one.

Table 16 Qualities of good and bad metrics

Qualities of a good metric	**Qualities of a bad metric**
Consistently measured: For a metric to be a good one it is necessary that it can be compared. Hence the metric selected should be something that can be measured consistently even if the individuals responsible would change.	**Inconsistently measured:** A metric that is subjective oriented or self-reported tends to be a bad one. I.e., a questionnaire might offer some valuable information to a organisation, but rating your own knowledge about a subject is both subjective and self-reported, no one is above biases, and some people will outright lie within a questionnaire if it serves their goals.
Cheap to produce: Resources spent to gather the metric should be as minimal as possible, automated means of gathering and producing metrics is a preferable goal.	**Costly to gather:** A metric should not be too labour-intensive. If a measurement that is gathered is gathered too sparsely just due to the labour related to it, or the process related to it needs refining.

Is expressed in a quantifiable: The product of the measuring process should be expressed in a quantifiable value, such as cardinal number or percentage. Comparison of data becomes impossible in a meaningful way when ordinal values are used.	**Does not express the measurement in cardinal numbers and units:** A metric that is expressed by colours, an expression such as: low, medium, or high, or in any other nonnumeric form is a bad one. While the aforementioned scales can be used in conjunction with a good metric they should be only used to express the results instead of being the result.
Needs to satisfy specific (business) requirements: A metric gathered should add value instead of being just noise. A good question when deciding a metric is who needs to know what and when?	
Only repeatable processes or incidents should be measured: Beyond consistency related to the measuring process it is beneficial that the target of measurement is repeated.	
Contextually specific: A good metric should be a measure that matters to some stakeholder within the organisation and is clear what it indicates. If the measurement is not understood it needs to be refined or retired.	

To ensure that metric is contextually specific and yields useful data following should be thought about and considered related to the metric: Who, i.e., which users have access to sensitive information, who in organisation consistently choose weak passwords, for example. What, i.e., what ratio of the organisation's systems is not configured according to the organisation's policies. When, i.e., how often the management reviews the organisation's policies and procedures, when the security incidents occur, e.g., within the "normal hours" or outside of the normal, this might give a clue what kind of attacks are most relevant concerning the organisation. Moreover, where, i.e., which organisational units have the most security policy violations per month, what is the most common source of reconnaissance scans against the organisation's network perimeter, or similar (Hayden, 2012, p. 33-34). Timeliness and frequency of measuring also matter, as the situations tend to change and to track those changes over time is important, hence how often one should measure should also be identified when choosing a metric (Barabanov et al., 2011, p. 4). Beyond aforementioned, once the metric is decided upon one should remember clarity concerning it. Make sure that measure is easy to interpret with clearly defined semantics, e.g., measurement of the height and weight is easy to interpret, at least if you use the metric system, but measurement of an individual's attractiveness or intelligence is vague without clear definition (Lv et al., 2018, p. 49).

Appendix J - Reflection document

The goal of this thesis course is for the researcher to demonstrate his/her ability to use relevant scientific methods correctly, acquiring information related to the subject of his/her research, and analysing and summarising the aforementioned information, and hopefully contributing scientifically to development in the areas of computer and system sciences. Beyond this, the researcher should be able to critically reflect one's work and respect the ethical and societal aspects related to the research.

I feel that I have achieved the aforementioned goals. However, some of those goals needed more effort than others, i.e., selecting the appropriate scientific methods and justifying their use took more effort than I hoped. These problems might have been due to the research question, and how it was formulated, it might have been too vague, or too extensive for a master's thesis. However, I feel that all in all the research resulted in valuable information concerning the subject and the dilemmas that make the measuring of information-security education, training, and awareness a difficult objective.

While I rigorously planned a schedule for myself and followed it, I should have given more focus on the scientific methods during the start of the process; this would have conserved some time afterwards. My own deadlines, deadlines that were given by the university, and deadlines that were given by the client made it sure that I followed my plans punctually. If I do a process like this in the future, I will plan the process in a similar way, but give more emphasis on the scientific methodology until it is actually done accordingly. Due to my restrictions with time I had to use (more below) I planned the days during the past four months very precisely, which paid off.

Most of the courses I have had during the past years were all beneficial during the thesis process. Namely the courses related to the scientific research, i.e., Research Methodology For computer and Systems Sciences and Scientific Communication and Research Methodology, and courses related to the risk analysis and decision making, particularly, Decision Theory, Risk management, Risk and Decision Analysis: Special Problems, Analysis of Bases for Decision, and Business Analytics. Truthfully I could list all the courses I had excluding the Open E-Governance and E-Democracy.

The topic of this thesis lies within administrative information-security, which is the field where I hope to be employed, especially in a profession related to risk management. The research conducted offered a plentiful amount of new information related to the area of information-security and new views related to the industry, especially how the clients view the solutions and the services they are paying for.

While I might not have found the answer I wanted to find during this research, that being a method of calculating the effectiveness of information-security education, training, and awareness in a way that is even slightly trustworthy I did find out why the method is non-existent as of now. I found out during the process some of the variables that can affect the effectiveness of information-security education, training, and awareness, and therefore I feel that I gained valuable information and brought understanding related to the topic of this research. While it is not for me to make a claim that the aforementioned will have applicability in practice, I know that the information I gained during the research will be useful to me in the future if I find myself employed in the field of information security.

I am satisfied with my work and results notably due to that I were, and still am, on my parental leave and the amount of time I had daily for the research was the time my son napped, and the hours I had in the evening. Nothing is ever perfect, and I learnt a lot from the process. While I know I made some mistakes, and the thesis itself could always be better I did everything to my best ability as of now, and I view this all as a process of learning. Hence, I am not too harsh on myself on at this time due to the circumstances.