Jaakko Jalkanen

IS HUMAN THE WEAKEST LINK IN INFORMATION SECURITY?

SYSTEMATIC LITERATURE REVIEW

UNIVERSITY OF JYVÄSKYLÄ
FACULTY OF INFORMATION TECHNOLOGY
2019

TIIVISTELMÄ

Jalkanen, Jaakko
Is Human The Weakest Link In Information Security: A Systematic Literature Review
Jyväskylä: Jyväskylän yliopisto, 2019, 61 s.
Tietojärjestelmätiede, pro gradu -tutkielma
Ohjaaja: Siponen, Mikko

Tämä pro gradu -tutkielma tutkii ihmisen roolia tietoturvassa sekä esittää tunnetuimpia tietoturvaheikkouksia. Tutkielma on toteutettu systemaattisen kirjallisuuskatsauksen keinoin ja siinä etsitään vastausta tutkimuskysymykseen ”onko ihminen tietoturvan heikoin lenkki”. Tutkielma koostuu 31 pääartikkelin, sekä niiden lähteiden analyysistä, joiden pohjalta on tutkittu väitettä tai oletusta, jonka mukaan ”ihminen on tietoturvan heikoin lenkki”. Tutkimuksen johtopäätöksissä todetaan, että kyseistä väitettä, sekä sen eri versioita on käytetty hyvin laajamittaisesti tietoturvakirjallisuudessa, vaikka tieteellistä näyttöä ihmisen roolista heikoimpana lenkkinä ei tutkimuksessa löydetty tai edes pyritty löytämään. Tämän tiedon avulla organisaatiot pystyvät yhä paremmin näkemään, missä organisaatioiden ”heikoin lenkki” mahdollisesti sijaitsee, sekä myös suhtautumaan tietoturvakirjallisuuden yleistyksiin pienellä varauksella. Tässä tutkielmassa esitellään myös esimerkki tietomurtoja, sekä analysoidaan niiden kompleksisuutta.

Avainsanat: tietoturva, ihminen tietoturvakontekstissa, heikoin lenkki, tietoturvauhka, systemaattinen kirjallisuuskatsaus

ABSTRACT

Jalkanen, Jaakko
Is Human The Weakest Link In Information Security: Systematic Literature Review
Jyväskylä: University of Jyväskylä, 2019, 61 p.
Information Systems, Master's Thesis
Supervisor: Siponen, Mikko

This master's thesis examines the role of human in the information security and presents the most known information security threats. Based on a systematic literature review, this thesis tries to find an answer to the research question: "is human the weakest link in information security". The thesis consists of an analysis of 31 main articles and their sources on the basis of which the claim or assumption "human is the weakest link in information security" has been studied. The study concludes that this phrase, as well as its various versions, has been used extensively in security literature, although scientific evidence on the role of human as the weakest link was not found in the research. With this information, organizations are increasingly more capable to see where the organizations' weakest link might actually be located, and also to take a general view of the generalization of information security literature. This thesis also introduces an example of data breaches, and analyzes their complexity.

Keywords: information security, humans in information security, weakest link, information security threat, systematic literature review

FIGURES

TABLES

CONTENTS

1 INTRODUCTION

Data has become the crown jewelry of companies and is also claimed to be the most important part of business (Redman, 2008). In data-based business, information security is playing a very important role since information security incidents have grown year by year due to criminals trying to get access to their data. It is becoming increasingly difficult for companies protect themselves against the information security threats. The information security literature in management systems literature often suggests or generalizes the users as the greatest threat, or "the weakest link" in information security without any proof. In chapter three, we can see that there are numerous articles which write about human being the weakest link, even if the studies of information security incident causes are telling a different story.

The aim of the thesis is to provide new insight into the question: "**Is human the weakest link information security?**", based on the systematic literature review. In order to find the answer to this question, the literature related to the subject and the research question must be carefully and systematically reviewed. By answering this research question, companies can get valuable information on how they should be prepared for security attacks and which parts of information security they should invest in. The results will help organizations determine if they are trusting the wrong assumptions in order to manage their information security as well. This literature review also provides a critical view of the current literature and challenges the generalizations made therein. To address these problems in a systematic way, the study has been conducted in the form of a systematic literature review.

This thesis consists of six chapters: 1. Introduction 2. Background of the research 3. Methodology and the research process 4. Literature review 5. Discussion 6. Conclusion. In this chapter the area and need of the research has been described. The second chapter presents the background of the study and introduces important terms for the research. In the third chapter the research methodology and the research process is explained and the different stages of the research are presented in more detail. The fourth chapter consists of the actual literature and its analysis and in the fifth chapter the results of the literature

review are discussed. The sixth and the final chapter summarizes the results of the study, discusses different limitations and proposes future research topics.

2 BACKROUND OF THE RESEARCH

Security is one of the basic needs in human nature (Mitzen, 2006), but what does it mean in the internet era? Bosworth and Kabay (2002 p. 4) defined security as follows: "The state of being free from danger and not exposed to damage from accidents or attack, or it can be defined as the process for achieving that desirable state.". To achieve that desirable state humans have produced different solutions to keep them safe as long as they have been on the planet. The only difference is that the threats to security are changing and we have to adapt to them. Only a couple hundred years ago, people were dying of plague because we did not have advanced medicine. Now we are facing huge amount of threats from the internet and we must find ways to protect ourselves from them to be, or at least feel, secure. In this chapter, the concept of information security is explained along with other important terms for this study.

2.1 Information security

Information security can be defined in many ways. Von Solms (1998 p. 224) defined information security thusly: "The aim of information security is to ensure business continuity and minimize business damage by preventing and minimizing the impact of security incidents". Chellappa & Pavlou (2002 p. 359) defined information security as "…the subjective probability with which consumers believe that their personal information will not be viewed, stored or manipulated during transit or storage by inappropriate parties, in a manner consistent with their confident expectations". Moon, Choi & Armstrong (2018) defines information security as a practice of defending information from unauthorized access, use, disclosure, disruption, or destruction. Although all of these definitions are a bit different, they all have the same goal, which Gulappagol & ShivaKumar (2017 p. 253) summarized: "Information security is to protect the confidentiality, integrity and availability of information assets that use, store or transmit information from risk". Confidentiality, integrity and availability are the most common way to define information security and also

the worldwide standard ISO/IEC 27002 defines information security by those three elements (Sahibudin, Sharifi & Ayat, 2008; Von Solms & Van Niekerk, 2013; Disterer, 2013). When defining information security, it is sometimes confused with information system security, which is not the same thing. Information system security has the same main elements as information security (confidentiality, integrity and availability) but it includes also non-repudiation, accountability, authenticity and reliability (Von Solms & Van Niekerk, 2013). In this chapter we will be focusing on the information security instead of information system security.

Confidentiality, integrity and availability, better known as the CIA triad, is a model, which is commonly used in an information security context (Ning, Liu & Jan, 2013; Agarwal & Agarwal, 2011; Cherdantseva & Hilton, 2013). Already in 1975, Saltzer and Schroeder presented the concept of CIA, but it was more for computer security and the terms were unauthorized information release, unauthorized information modification and unauthorized denial of use (Saltzer & Schroeder, 1975). The CIA triad term in itself was presented in late eighties by NASA (Cherdantseva & Hilton, 2013). Since then, these requirements have become widely used to describe the fundamental goals of information security and the meanings for confidentiality, integrity and availability have changed only slightly. Confidentiality determines that information cannot be accidentally or purposefully encountered to people who should not have access to it. Integrity ensures that the information is not changed during any form or at any time when it is not meant to be changed and it stays the same. Availability permits access to information when needed. (Ning et al., 2013; Agarwal & Agarwal, 2011)

Risks and threats are always the other side of all security. Each of us determines the risk ourselves, because experiencing risk is very personal but there are still key elements which affect the definition of risk. Bosworth & Kabay (2002 p. 4) defines risks as "the chance of injury, damage, or loss. Thus, risk has two elements: (1) chance—an element of uncertainty, and (2) loss or damage". Another definition is "risk is a measure of the inability to achieve overall program objectives within defined cost, schedule, and technical constraints and has two components: (1) the probability of failing to achieve a particular outcome and (2) the consequences of failing to achieve that outcome." (Simpleman, McMahon, Bahnmaier, Evans & Lloyd, 1998). Both of these definitions rely on two things: uncertainty and loss or damage, and together these create risks that have different probability and impact.

2.2 Information security threats

In information security it is very important to identify and prepare for the risks because the "other side" will always find a way into the attack. The information security risks also differ from the "traditional" risks since they are possible to do online and physical contact is not needed. Information security threats can

be classified in different ways. A common classification is to divide them to outside threats and inside threats, and from there on into smaller pieces. (Armbrust, Fox, Griffith, Joseph, Katz, Konwinski, Lee, Patterson, Rabkin & Stoica, 2010; Jouini, Rabai & Aissa, 2014; Loch, Carr & Warkentin, 1992). Jouini et al. (2014) and Loch et al. (1992) both have quite similar classifications. As we can see from Figure 1 and Figure 2, both Jouini et al. (2014) and Loch et al. (1992) have divided all threats to internal and external threats. After that, Jouini et al. (2014) classification becomes a bit more specific since both internal and external threats are divided to human, environmental and technological threats. In turn, Loch et al. (1992) divide them only as human and non-human threats. Human threats are classified by Jouini et al. (2014), which are divided into malicious and non-malicious threats, and then both of these are divided to accidental and intentional threats. The accidental and intentional threats are divided to seven different types of threat impacts, which are: destruction of information; corruption of information; theft, loss of information; illegal use; disclosure of information; denial of use and elevation of privilege. (Jouini et al., 2014) Environmental and technological threats are both non-malicious and accidental but both can also be divided further into the same seven threat impacts as previous threats, which were destruction of information; corruption of information; theft, loss of information; illegal use; disclosure of information; denial of use and elevation of privilege. In Loch et al.'s (1992) classification the consequences or, as Jouini et al. (2014) calls them, "threat impacts", are divided to only four types: disclosure, modification, destruction and denial of use. Both of these classifications have many similarities and the basic idea how information security threats are divided to internal and external threats is identical. Loch et al. (1992) have created the basis of which Jouini et al. (2014) has continued and divided the elements more specifically.

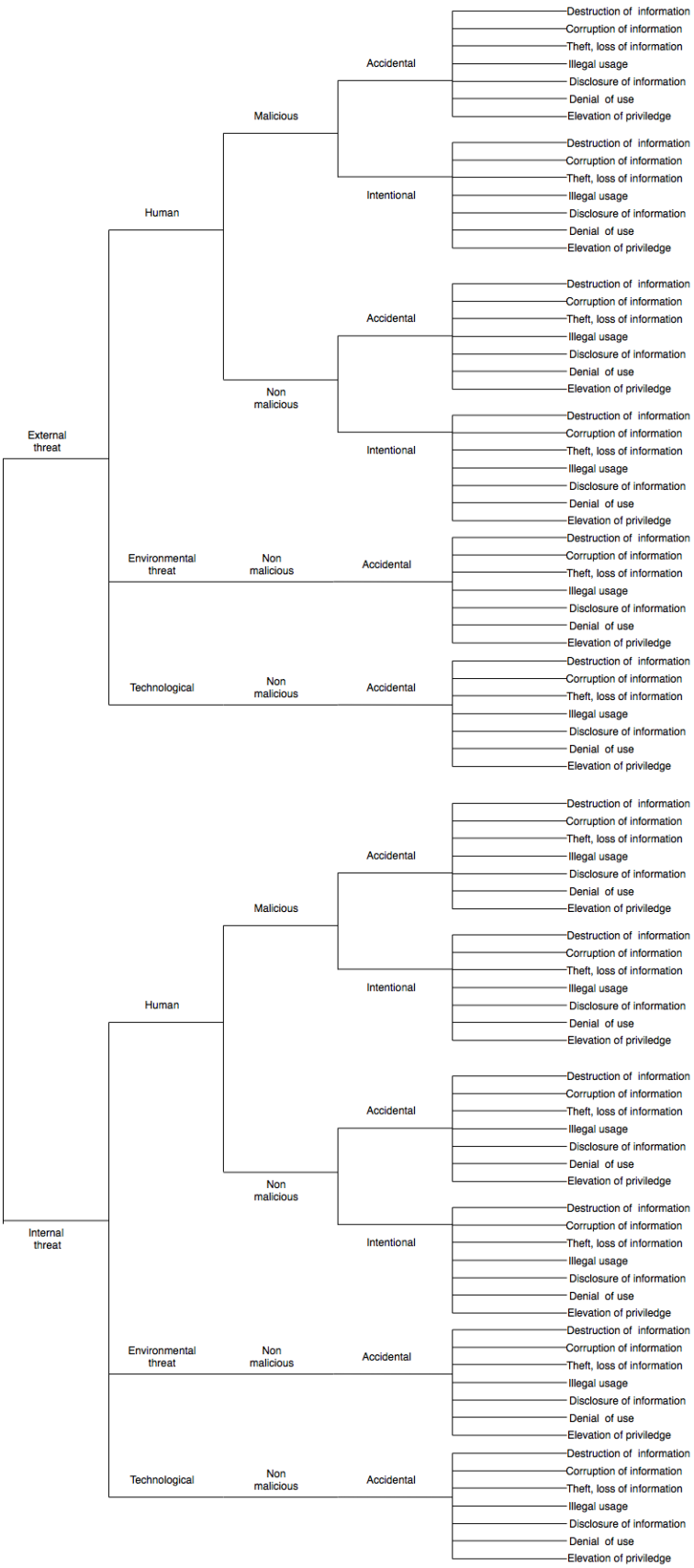

FIGURE 1 Information Security threats classification. Modified from Jouini, Rabai & Aissa, 2014

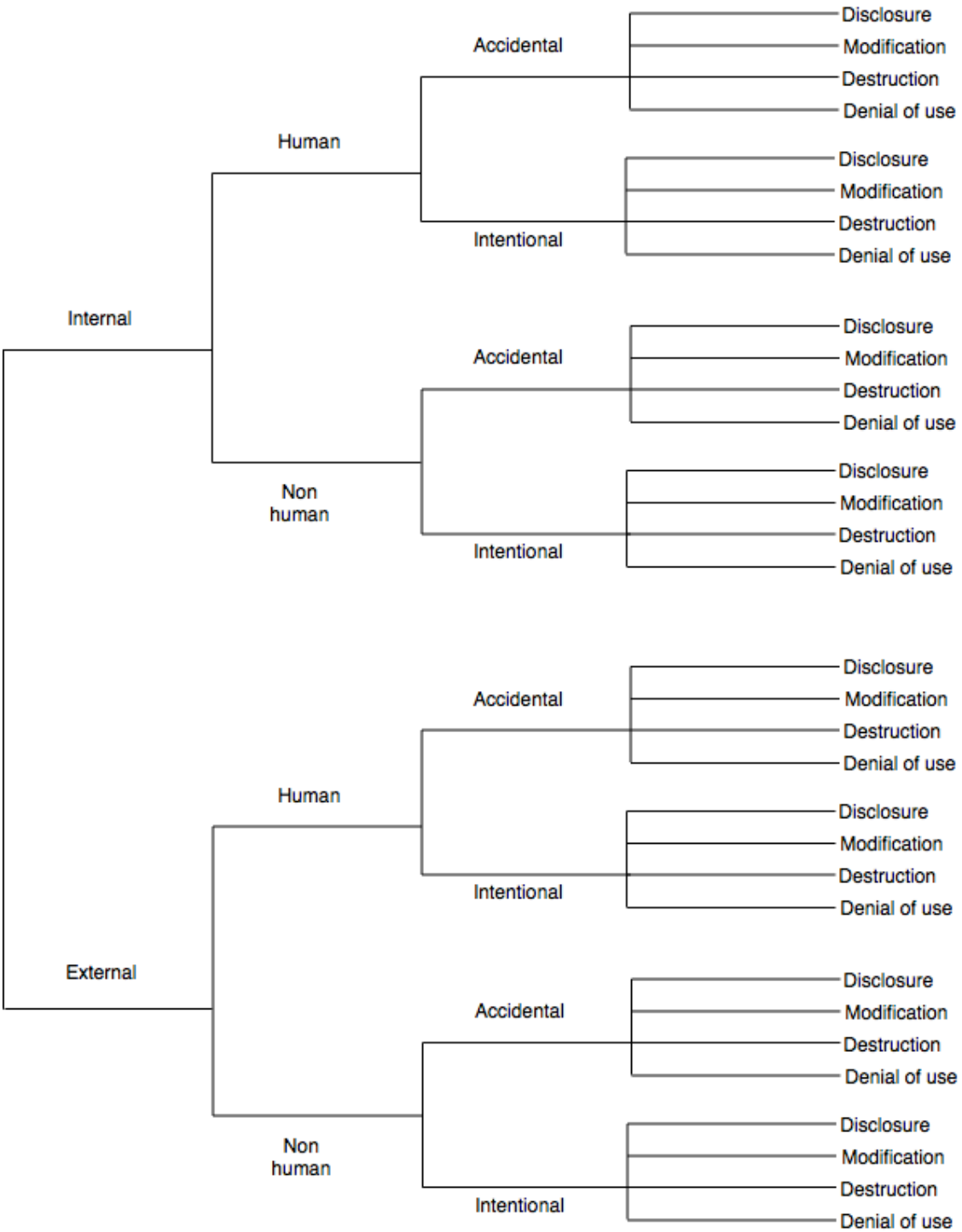

FIGURE 2 Information Security threats classification. Modified from Loch, Carr & Warkentin, 1992)

As we can see from the threat classification lists of Jouini et al. (2014) and Loch et al. (1992), there are many different threats to information security and human-related threats are only a part of them. Also, the causality of human related threats can be very complex, and the main reason could be something else than human. Consider, as an example, a situation where the user finds an

USB stick from the street, installs it into a computer, and infects the computer with a malware after the USB stick installation. In this case, is the real reason behind the malware infection 1) the malicious actor that has set the infected USB stick; 2) the computer which starts to auto read the USB stick; 3) the person who installed the unknown USB stick to computer?

2.3 Human terms in information security

The human terms related to information security are not used consistently. There are many definitions for the same term and different studies might use the same term for different purposes. In addition to this problem, in information security literature there can often be seen many different terms to describe internal or external threats.

One of the most common terms in information security human threats is "insider" and like Coles-Kemp & Theoharidou (2010 p. 47) said, "The broad range of interpretations of the insiderness concept is reflected in the various definitions that are used in information security literature". The problem of various definitions also applies to another common term "hacker", which is problematic. Crossler, Johnston, Lowry, Hu, Warkentin & Baskerville (2013 p. 92) opened in their article as follows: "The study of computer hackers is made even more difficult with the various definitions of hackers that exist". As we can see from both of these statements, there are many different definitions and because of that I argue in this thesis that these terms are not used consistently across different scholars and often they mean different things in different studies. In the following chapter the different definitions of these terms are presented.

2.3.1 Insider and internal threat

Neumann (1999 p. 160) presents a definition for an insider as follows: "An insider is someone who has been (explicitly or implicitly) granted privileges authorizing use of a particular system or facility.". Anderson, Bozek, Longstaff, Meitzler & Skroch (2000 p. 21) had a similar definition for insider but they assumed that an insider is always malicious: "Any authorized user who performs unauthorized actions". The problem with these definitions is that there could be an insider in the organization who could but does not do any malicious acts. The second problem is that someone might be an insider without knowing it, for example in situations where someone has been fooled to perform such actions that might put the organization at risk, but the person does not realize it. To address these problems in the definitions, I would define insider as a malicious or non-malicious person who has access to the organization's system or perimeter and is authorized but is not necessarily the organization's employee. (Neumann, 1999; Anderson et al., 2000)

I also present definitions for the term "internal threat" to avoid confusion with the terms "insider" and "internal threat". Anderson et al. (2000 p. 21) defined the term internal threat as "any authorized user who performs unauthorized actions that result in loss of control of computational assets". This definition differs from an insider because according to Anderson et al. (2001) internal threats are always malicious and performing some malicious acts. A threat is usually something that has not happened yet and as Deutsch & Krauss (1960 p. 182) define it: "threat is defined as the expression of an intention to do something detrimental to the interests of another". So, based on these definitions I would argue that an internal threat has not necessarily performed any malicious actions but is capable of doing so. Another definition for internal threat is defined by Jouini et al. (2014 p. 494): "A threat can be internal to the organization as the result of employee action or failure of an organization process". In this definition the problem is that it only counts employees as internal threats, even if internal threat can be also someone else who has been granted access to the organization.

To see the difference between these two terms it can be said, based on the previous definitions, that an insider is not necessarily malicious before unauthorized actions are performed. Thus, an insider can be both malicious and non-malicious. However, at the point when insider turns malicious, it also changes to an internal threat because a malicious insider has the opportunity to do actions that may threaten the organization. When a malicious insider performs these actions, the internal threat is being realized.

2.3.2 Employee

The employees are part of human threats and the threat that they pose can be malicious or non-malicious, as we could see from the threat categorization list by Jouini et al. (2014) Malicious employees are current employees who are intentionally misusing their authorized access to the system or information, but often in information security literature, malicious employees are seen as malicious insiders (Cappelli, Moore, Trzeciak & Shimeall, 2009; Colwill, 2009; Sarkar, 2010; Kandias, Virvilis & Gritzalis, 2011). Cappelli et al. (2009 p. 5) define a malicious insider as someone who "has or had authorized access to an organization's network, system, or data and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems". Sarkar (2010 p. 124) wrote "Every employee in an organization may be a potential threat agent if they possess the motivation to take advantage of their capabilities and the opportunities they have while working for the organization. The malicious insider's motivation may come from personal gain, revenge, competitive advantage, ideology or could be a combination of them". Gandias et al. (2011 p. 4) also saw malicious employees as insiders: "Insider threat in the cloud provider: Where the insider is a malicious employee working for the cloud provider". Alberts & Dorofee (2002 p. 254) defined malicious/disgruntled

employees as "people within the organization who deliberately abuse or misuse computer systems and their information.".

Non-malicious employees mean persons who accidentally or unintentionally cause security threats, which Colwill's (2009 p. 194) example explained well: "non-malicious behaviour should also be targeted, for example, those who attempt to cut security corners to meet business deadlines", so people could try to save time by turning the antivirus software off but they do not realize or even think that it could compromise the whole computer and the company for threats. Alberts & Dorofee (2002 p. 254) define non-malicious employees as people "people within the organization who accidentally abuse or misuse computer systems and their information".

2.3.3 Hacker

While the term hacker has been used for a long time and it is in common use, the scientific literature provides different definitions or characterizations for the term hacker (Silic & Back, 2013). According to Silic & Back (2013), one of the reasons why a hacker is difficult to define is because there are many different types of hackers. For example, there are "bad" hackers, which are people who commit cybercrime and other illegal activities (Silic & Back, 2013). In turn, there are "good" hackers who try to prevent these illegal activities and help people to improve their information security by searching security holes and providing this info for them. (Silic & Back, 2013) Still, there is one problem with "good" hackers, and the problem is it is illegal to hack into company systems even if it is done with good intentions. Because of this phenomena, many big software companies such as Google and Microsoft have designed "bug bounty programs" where hackers are allowed to hack into their systems and if they find major issues they are rewarded (Chatfield & Reddick, 2017). Of course, these two definitions do not define all possible hacker types and it is hard to categorize all hackers to only "good" or "bad" hackers. This is because there are many ethical issues since legislation is always coming "behind" and some activities might be legal even if they are ethically wrong (Smith & Rupp, 2002).

2.4 Causality

The concept of causality is hard to define since it is a very philosophical issue and there are at least a dozen different theories and definitions of causality (Cartwright, 2006). Causality has also changed over time as Illari, Russo & Williamson (2011, p. 4) write, "The concept of cause is changing, and the sciences are forefront of these changes. In Aristotle's time causality was understood as explanation in general: the search for causes was search for "first principles", which were meant to be explanatory. However, now causal explanation is usually thought of as just one kind of explanation. In the modern era, causality be-

came tied up with the notion of determinism, the prevailing scientific view of world in Newtonian times".

Cox (1992 p. 292) presented a simple but not very complete definition: "One definition of causality used in the philosophical literature requires that, if C is to be the cause of an effect E, then C must happen if E is to be observed. This is clearly inappropriate in, for example, most epidemiological contexts, settings where some probabilistic notion seems essential, involving usually also some idea of multiple causes. Thus, smoking is neither a necessary nor a sufficient condition for lung cancer". As the author said, that definition has some problems, but it still explains causality in a simple way. Cartwright (2006, p. 57) summed up the problem of finding the perfect definition for causality:

> The variety of theories of causal law on offer provides one of the major reasons in favor of this plurality view. Each seems to be a good treatment of the paradigms that are used to illustrate it, but each has counter- examples and problems. Generally the counterexamples are provided by paradigms from some one or another of the other theories of causality. Usually in these cases we can see roughly why the one treatment is good for the one kind of example but not for the other, and the reverse. (Cartwright, 2006, p. 57)

From these findings I argue that causality cannot be defined perfectly but to understand the concept we have to understand that the basic idea of causal laws is that something will have an effect on something else, like in Cox's (1992) definition where C must happen for E to happen.

In information security, there are tens of different factors which might affect the result, which might be for example a data breach from the organization. In one example the data breach has been done from an employee's computer, which was forgotten in a restaurant. It would be easy to say that the employee (A) who forgot the computer to the restaurant is the reason for this data breach. But we have to take all the other factors into account as well; the intruder (B), computer (C), restaurant (D), organization's policies (E) and organization's database (F). Of course, A is one of the biggest reasons why this breach has happened, but it is not the only reason. If the intruder (B) would not have stolen and accessed the computer, the breach would not have happened; if computer (C) would have been secured properly it could not have been accessed; if the restaurant (D) would have noticed the forgotten laptop and they would have picked it up it would not have been possible for the intruder (B) to get it; if organization (E) would have had better security policies, employee (A) would not have had the computer at restaurant in a condition that it can be accessed and if organization's database (F) would have had better restrictions, the intruder (B) might not have been able to get into it or at least import all the data from there. All of these are factors that have to be taken into account while evaluating the complexity of similar situations as this. In this thesis, causality is used to explain similar situations, where the situation is very complex and it cannot be said for sure what is the "right" answer.

3 METHODOLOGY AND THE RESEARCH PROCESS

In this chapter, I will present the rationale for systematic literature review as the research method and the reasons why, from all the different types of literature review, I chose systematic literature review. Also, the study process is presented, and the related steps are explained in more detail.

3.1 Why literature review

Literature review can be defined in many ways and many researchers see the definition differently depending on the desired way of research. (Salminen, 2011) Miller & Yang (2007, p. 62) defined literature review as follows: "The literature review is a comprehensive survey of previous inquiries related to a research question. Although it can often be wide in scope, covering decades, perhaps even centuries of material, it should also be narrowly tailored, addressing only the scholarship that is directly related to the research question. ". Baumeister & Leary (1997) found similar reasons for literature review and listed the five goals for literature review. The first goal is to develop a new theory based on existing literature. The second goal is to evaluate a theory based on existing literature. Third is to review the knowledge of particular topic based on existing literature. Fourth goal is problem identification and more specifically, finding problems or weaknesses from the existing literature. The fifth is providing history of theory development and more specifically how that theory has been developed in the past. (Baumeister & Leary, 1997) Miller & Yang (2007, p. 62) also noticed that "the literature review also provides clarity on a given subject by revealing long-standing conflicts and debates, reveals the interdisciplinary nature of research on a subject, and places the work in a historical context.".

The goal to this study is to find weaknesses and problems of the particular area of humans in information security, which perfectly fits the fourth goal of Baumeister & Leary (1997, p. 312): "A fourth category of literature review has problem identification as its goal. The purpose is to reveal problems, weaknesses, contradictions, or controversies in a particular area of investigation". Based

on these definitions and goals, I can say that literature review is the best possible research method to find an answer for the research question. The research question "Is human the weakest link in information security?" is a very complex question which includes a lot of causalities due to many different factors. In a literature review, it is possible to get a good understanding of the information security landscape in academic literature and see if the "general" opinion that humans are the weakest link supported by any evidence. Literature review also gives the "freedom" to follow article chains if needed and go "off-track" if it helps to understand the bigger picture better.

3.2 Systematic literature review

Systematic Literature Review (SLR) is a literature review method which uses systematic techniques to search and present existing literature to answer the research question. Previously, the type of research has been held as "traditional" and related to healthcare but lately it has also received support from other areas of science (Salminen, 2011; Okoli & Schabram, 2010). There are many different definitions for SLR but they all differ depending on the area of research. Petticrew (2001 p. 98) defines SLR as "a method of locating, appraising, and synthesizing evidence". Another definition for SLR by Kallio (2006, p. 26) is "a societal approach based on the ideology of the systematic review of source material, aiming at generic visibility of a problem, topic, or discourse". Both of these definitions describe the main features of SLR and it can be seen that SLR is a good method to investigate the inadequacy of previous studies and to evaluate the reliability of the claims they contain. All in all, according to Salminen (2011, p. 9) SLR "is an effective way to test hypotheses, present research results in a close form, and evaluate their consistency".

Okoli & Schabram (2010 p. 5) have expanded these definitions to address SLR better in regards to information systems research by thinking the "systematic" term more as a qualitative adjective that "describes the nature of a thing in a way that can be qualified by greater or less; that is, we can speak of a review as being more systematic or less systematic, or very systematic". Even if SLR is conducted in a very systematic way it is helpful to see the base of the study more as a mountain that can be approached from many different directions rather than just one.

Baumeister & Leary (1997) have presented nine points where the researcher can make mistakes in SLR. These nine points are:

1. Inadequate Introduction
2. Inadequate Coverage of Evidence
3. Lack of integration
4. Lack of critical appraisal
5. Failure to Adjust Conclusions
6. Blurring Assertion and Proof
7. Selective Review of Evidence

8. Focusing on the Researchers Rather Than the Research
9. Stopping at the present

To avoid these nine mistakes, I have taken actions such as research protocol and accurate process, which helps to keep on track and thus avoid mistakes. Other limitations and concerns of the study are discussed further in the discussion part.

3.3 Research process

I have chosen to follow Okoli & Schabram's (2010) SLR research process, which is designed more to information system research and because of that it fits better to an information security related study as well. Okoli & Schabram's (2010) process consist of eight steps:

1. Purpose of the literature review:
2. Protocol and training
3. Searching for the literature
4. Practical screen
5. Quality appraisal
6. Data extraction
7. Synthesis of studies
8. Writing the review

In the first step researcher clearly identifies the purpose of the literature review. When researcher have clear purpose, it is usually easier to communicate to the reader as well (Okoli & Schabram, 2010). In the second step, a detailed protocol is made to ensure clear process tracking and if there is more than one writer it is also adhered to by all participants. In the third step literature is searched and the channels and the literature are justified (why that material has been taken into study). The fourth step is the step where literature is pre-screened and the material that does not fit the purpose is left out. In the fifth step all the material that has passed the pre-screening will be evaluated and the literature used in the actual review is chosen. In sixth step all the studies that have passed quality appraisal are reviewed and the necessary information is extracted. In the seventh step, also known as analysis, the synthesis is written based on the information, which was found in data extraction. In the final step all the analysis and findings from step seven is reported. (Okoli & Schabram, 2010)

3.3.1 Inclusion and exclusion criteria

In Okoli & Schabram's (2010) second step "protocol and training" I have decided following criteria to as my protocol:

Included:

1. Papers have to be published earliest 2000
2. Papers are from academic sources
3. Paper is related to information security
4. Paper is at least doctoral thesis level
5. Paper is published in English
6. Paper discusses humans or human factors in information security
7. Paper is free of charge
8. Reference articles can be used outside these criteria

Excluded:

1. Paper is published earlier than 2000
2. Paper is from non-academic sources
3. Paper is not related to information security
4. Paper is not from academic sources
5. Paper is not published in English
6. Paper do not discuss humans or human factors in information security
7. Paper is not free of charge

I have chosen to accept papers from 2000 onwards because the research question is so broad that it needs longer-term information to support it. The year of publishing has been limited to 2000, because I argue that older publications are not relevant anymore, since the information security landscape has changed rapidly and the research in publications before that day might not be relevant anymore. In addition, almost 20 years is enough to find out whether the claim is rooted in a long period of time or whether it has become common only in recent years. In order to improve the reliability of the research, I will only accept publications that are from academic sources. However, if the paper from the original selection refers to a non-academic source, this publication may be included in the research based on criteria eight. All the papers that are used in the research have to be related to information security because the research question pertains only to information security. To improve the reliability of the research even further I will only accept academic papers that are at least at a doctoral thesis level. In order to find the answer for the research question, all the papers must discuss the role of humans or human factors in information security, because otherwise they are not relevant to the study. This research does not have funding or other sponsors, so literature that is not free of charge will not be used. In order for the research to be carried out, it has to be possible to follow the references from the original article. This is important for assessing the reliability of the source of the statement.

3.3.2 Research material gathering and critical assessment of search

In order to follow Okoli & Schabram's (2010) process and step three "Searching for the literature", I have chosen to use Google Scholar as the main search engine with the following keywords, presented in table 1. To choose the right keywords some preliminary searches were made to ensure that there was enough material. The starting point was to find the background material and the general terminology of the research area; the broad keywords "information security" and "information security threat" were chosen. Next the research needed literature where authors have written about human's role in information security and also about being the weakest link. For this reason the keywords "biggest information security threat", "is human the weakest link", "humans as the weakest link", "human factor information security", "humans in information security" and "weakest link in information security" were chosen. To show all the different threat sources and to find the "real" threat sources keywords "vulnerabilities in information security" and "information security threat classification" was chosen. For the last keywords, I wanted to present some example cases of data breaches and their complexity. For this reason the keywords "data breach + human" and "information security accidents" were chosen.

Biggest information security threat	Data breach + human	Information security accidents
Information security	Information security threat	Information security threat classification
Is human the weakest link	Humans as the weakest link	Human factor information security
Humans in information security	Vulnerabilities in information security	Weakest link in information security

TABLE 1 Keywords used in research

The following table 2 shows how many papers were found for each keyword from Google Scholar before matching them to the criteria. Due to the Google Scholar search system, only the first criteria could be set before doing the searches.

Keyword	**Google Scholar**
Biggest information security threat	2
Data breach	2
Information security accidents	88
Information security incidents cause	2
Information security human factor	30
Information security threat assessment	26
Information security threat categories	4

Humans as the weakest link	35
Human factor information security	29
Humans in information security	22
Vulnerabilities in information security	66
Weakest link in information security	286
Total	592
Total relevant	96
Total selected	31

TABLE 2 Search results per keyword

From these 592 papers, I started the Okoli & Schabram's (2010) fourth step "Practical screen", where the papers where pre-screened towards the including and excluding criteria. In the pre-screening I found 96 relevant papers, which pre-matched the criteria based on the info and title. With 96 papers I continued to Okoli & Schabram's (2010) step five "Quality appraisal" where I skimmed the articles through and matched the actual content towards the matching criteria. From this step the 31 papers + the references from these studies were selected to the actual study. The reason for the over 300% exclusion rate was mostly due to the wrong context; articles which did not fit the criteria and there were also a few that were not academic papers. The results of Okoli & Schabram's (2010) steps six and seven are presented in the "Literature review" chapter.

4 LITERATURE REVIEW

Information technology is one of the fastest growing areas in our society (Acemoglu, 2012). Information has become one of the most important things to our life and also to organizations. In recent years most of the software organizations are transferring from products to services and many traditional companies have changed their business model from "traditional products" to internet and technology based business (Cusumano, 2008). This change has emphasized the importance of information and data. Zins (2007 p. 480) defined data and information as follow:

> In computational systems data are the coded invariances. In human discourse data are that which is stated, for instance, by informants in an empirical study. Information is related to meaning or human intention. In computational systems information is the contents of databases, the web, etc. In human discourse systems information is the meaning of statements as they are intended by the speaker/writer and understood/misunderstood by the listener/reader. (Zins, 2007 p. 480)

While the amount and need of data to organizations rises all the time, it is becoming a more and more valuable asset to organizations and as the European Consumer Commissioner, Meglena Kuneva (2009), said, "Personal data is the new oil of the internet and the new currency of the digital world". When the value of data increases, it has also increases the number of threats to it significantly (Johnston & Warkentin, 2010; Yeh & Chang, 2007), which means that organizations have to pay more attention to their information security to keep their data and information safe (Moon, Choi & Armstrong, 2018). Only in the 2000s have organizations began to understand how significant impact security breaches could have to their business and economy.

Already in 2006, the companies that reported vulnerability breaches lost an average 0,6% of stock market price, which is 860 million dollars on average (Telang & Wattal, 2007), and that is only the daily stock loss. In addition to stock loss organizations can face governmental sanctions, litigation and lose their competitive edge (Goel & Shawky, 2009). A 2014 study predicted that cyber security issues would cost 445 billion dollars annually (Janakiraman, Lim & Rishika, 2018), which could even grow more in the future because data is be-

coming more valuable in our society. The economical effect is so significant that companies must improve their information security and to do that they need toboth recognize the possible threats and try to prevent them. Organizations often struggle with managing information security (Dhillon, 2001), which might lead to a situation where organizations try to find answers from existing information security literature. In this scenario, it is crucial that organizations can understand the actual study results and do not act based on "generalizations" where people just believe that something is true if enough people have said it.

In this thesis, the role of human will be about the end user. Of course, one could say that human has built all the systems, which are used by humans and even the criminals are, at least for the time being, still human. But, as we can see from the literature the authors do not mean this by saying, "human is the weakest link". The reference is always towards end users, the ones who are actually using the system or working at the organization and for this reason I will only deal with the subject from the perspective of end users.

4.1 Humans as the weakest link in literature

I argue in this thesis that while many of the articles stress that "human is the weakest link in information security", for example, Vroom & Solms (2004); Bulgurcu, Cavusoglu & Benbasat (2010), Chen, Medlin & Shaw (2008), they have not justified that claim with any evidence. In the following subchapter, I am going to examine these articles and see how they have used generalizations in their text but have not justified their arguments in any way. In this thesis, causality is used to explain these complex situations where there are many factors that can affect the situation and other factors.

Workman, Bommer & Straub (2008) discusses the topic of "knowing-doing" gap and they create a threat control model to explain and understand the gap better. A Knowing-doing gap means a situation where people know how they should act in any situation but still they do not behave the way they know would be for the best. (Workman et al., 2008) One can imagine this phenomenon in the case of information security compliance. For example, an organization's employee knows that they are not allowed to download third party applications from the internet but because the employee needs the application to work, he/she does it anyway. While explaining this problem Workman et al. (2008, p. 2800) writes, "The IS community has proposed to circumvent the 'weakest link' and thereby avoiding the knowing-doing gap by using automated and mandatory security measures". With this claim Workman et al. (2008) suggest or assume that the humans in general or employees in particular are the weakest link in information security. However, they haven't justified this assumption that humans are the weakest link. The authors say that "IS community has proposed to circumvent the weakest link" (Workman et al. 2008, p. 2800). Despite that the reference to "IS community" implies rather wide generalizations, Workman et al. (2008) do not provide any references while making this claim. I argue that by making this claim Workman et al. (2008) are

implicitly committed to this claim, because they only talk about human mistakes and how they cause problems to organizations. The reader is left with the idea that humans are the weakest link.

Vroom and Solms (2004) discuss the problematic of information security auditing and how human behavior and the "human factors" can affect the auditing and also how to take these problematic parts into account. Vroom and Solms (2004) note that previously human factors have not been taken into account and the information security audits have been focusing only on the technical side. When Vroom & Solms (2004, p. 193) start the section of human factors they say "The role of the employees is vital to the success of any company, yet unfortunately they are also the weakest link when it comes to information security. Security incidents regarding insiders of the organization exceed the amount of security breaches with outsiders, which demonstrates the fact that the actual employees are an enormous threat to the well being of the company". The research that Vroom & Solms (2004) refer is an Information security industry survey (Briney, 2001), which has been published in an online magazine. In the research Briney (2001, p. 34) writes that "Overall, 'insider' security incidents occur far more frequently than 'external' incidents. Nevertheless, the number one priority of security professionals is securing the network perimeter against external attack.". Vroom and Solms (2004) base their claim that employees (insiders) are the weakest link because insiders create more security threats than outsiders. However, Briney (2001), the source to which Vroom and Solms (2004) cite and base their claim, suggests that the number one priority is securing the network perimeter against external attack. If we know that employees are the weakest link, then why we should focus our resources to defend against external threats? A badly secured network could lead to the situations where employees can do something that would cause a security threat or give external threats access the organization more easily. But, in both of these situations, the cause seems not to be human. The cause seems to be the badly secured network and for that reason, we cannot say that in this case human would be the weakest link in information security. The claim of human being the weakest link in information security is a very complex claim and for example in Vroom & Solm's (2004) article the threat would also have to be a "bad hacker" so that the risk would realize. This causes complex phenomena because there is a causal relation between the bad hacker, the employee and the network design. For example if the network is not designed well enough to be secure it would still need the hacker to attack for risk to realize, so there has to be cause C that E happens. Same kind of situation is if employees' actions would leave the network unsecured, but it would still need one of the following things to happen: network settings (A) have to allow the employee (B) to do these actions. So, if B would not make it possible for A to change settings the risk would never realize.

Safa, Solms & Futcher (2016) studied human aspects of information security in organizations and in the beginning of their article they discuss humans' different roles in information security. In this context Safa et al. (2016 p. 15) say: "several studies have implicated people as a weak link in the information security chain", while referring to two articles, which are Safa,

Sookhak, Solms, Furnell, Ghani and Herawan (2015) and Safa, Solms & Furnell (2016). However, neither of these articles have said that human is or could be the weakest link. Safa et al. (2015) studied information security conscious care behavior formation in organizations and how it affects the overall security. In the article Safa et al. (2015) explained different behavioral models and how they affect information security, where they come to the conclusion that security awareness and policies are the most important things regarding information security. In their conclusions, Safa et al. (2015, p. 76) state "information security conscious care behavior decreases the risk of information breaches when the area of weakness is human behavior.". However, I do not find them saying in their article that human is the weakest link. The other reference was Safa et al. (2016) where they studied information security policy compliance in organizations and built a model to explain and visualize this issue. In the beginning of the article, Safa et al. (2016) wrote how human aspects of information security should take into account along with the technical aspects, and they saw these two factors as different parts that, at best, create a more secure environment. Safa et al. (2016 p. 70-71) wrote "acceptable information security behaviour should ideally be combined with technological aspects" and they referred to Furnell & Clarke (2012 p. 983), where they wrote "however, it is increasingly recognized that technology alone cannot deliver a complete solution, and there is also a tangible need to address human aspects". Although the article is written from a human point of view and tries to find a means to increase and improve information security policy compliance among employees, the authors never say that human would be the weakest link in information security.

Bulgurcu et al. (2010) studied rationality-based beliefs and information security awareness in the information security policy compliance. Bulgurcu et al. (2010, p. 523) began their article by saying "many organizations recognize that their employees, who are often considered the weakest link in information security, can also be great assets in the effort to reduce risk related to information security." However, later in the introduction Bulgurcu et al. (2010, p. 524) note that the focus of information security is shifting more and more to information security policies because of employees: "As the focus on information security shifts toward individual and organizational perspectives, employees' compliance with information security policies (hereafter ISPs) has emerged as a key socio-organizational resource because employees are often the weakest link in information security". In this claim "employees are often the weakest link in information security", Bulgurcu et al. (2010) referred to two articles. The first reference is Mitnick's and Simon's (2002), which discuss the human element of information security and how vulnerable humans are in that sense. The book is completely based on Mitnick's experiences and it does not have any references. In the book, Mitnick tells about his crimes and how he was able to perform them. Mitnick and Simon (2002) say "the human factor is truly security's weakest link." but they have not provided any justification or explanation for this claim. Mitnick and Simon (2002) note also in the book that:

> Despite the efforts of security professionals, information everywhere remains vulnerable and will continue to be seen as a ripe target by attackers with social engineering skills, until the weakest link in the security chain, the human link, has been strengthened. (Mitnick and Simon, 2002)

> Individuals may follow every best-security practice recommended by the experts, slavishly install every recommended security product, and be thoroughly vigilant about proper system configuration and applying security patches. Those individuals are still completely vulnerable. (Mitnick and Simon, 2002)

Again, they do not provide any justifications or explanations for this claim. It seems to me that these claims on the weakest link are in these examples are Mitnick's opinions, which unfortunately lack any evidence that humans are the weakest links.]

The other reference, namely Warkentin and Willison (2009), discusses behavioral and policy issues in information security and what is the threat of insider. In the article Warkentin and Willison (2009) talk about endpoint security problem, which refers to the employee who is the endpoint of information systems. The endpoint security problem consists of the employee's activities that may increase the risk of creating an information system security threat (Warkentin & Willison, 2009). After introducing the endpoint security problem, Warkentin and Willison (2009 p. 102) explain the problem by saying "It is sometimes said that the greatest network security problem – the weakest link – is between the keyboard and the chair.". By using the phrase "it is sometimes said" Warketin and Willision (2009) are correct, because it is often said, that human is the weakest link in information security. But the problem is in what comes after that, and by not providing any alternative views to this claim "the weakest link – is between the keyboard and the chair" (Warkentin & Willison, 2009 p. 102), it gives reader the image that it this assertation is truth. I argue that while Warkentin and Willision (2009) do not explicitly endorse the claim that humans would be the weakest link, readers can get the impression that they are implicitly committed to the claim. When Bulgurcu et al. (2010, p. 523) made the claim "employees are often the weakest link in information security" they referred to this article and as we can see, Warkentin and Willison (2009) do not confirm this on a reliable basis.

Chen et al. (2008) wrote an article of information security awareness programs. Chen et al. (2008) studied how security awareness can affect organizational security. While they discussed situational learning to improve security awareness they said: "The 'human' factor is the weakest link in information security and the cause of many security threats, according to NIST-SP-800-50" (Chen et al., 2008, p. 362). NIST-SP-800-50 by Wilson and Hash (2003) is the US National Institute of Standard and Technology's special publication that focuses on building information technology security awareness and training programs. In the publication cited by Chen et al. (2008), Wilson & Hash (2003, p. 1) wrote:

> As cited in audit reports, periodicals, and conference presentations, it is generally understood by the IT security professional community that people are one of the

> weakest links in attempts to secure systems and networks. (Wilson & Hash, 2003, p. 1)

But again, we face the question: does "generally understood" make the claim true? For example, in 1912 it was generally understood that Titanic "could not sink", which even lead to the situation where many people refused to board the lifeboats because they believed that Titanic was non-sinkable (Landesberg, 2001). The whole program is made on the basis that human is one the weakest links and it should be strengthened. But as we saw in the sad Titanic case, "generally understood" does not make it the truth and that's why organizations should never base their actions to factors that are "generally understood".

Luo, Brody, Seazzu and Burd (2011) wrote an article about social engineering and how neglected the human factor is in information security management. In the article, Luo et al. (2011) studies the social engineering and how vulnerable people are in the eyes of social engineering. The biggest reason why social engineering is so dangerous is the trust that people have for each other; in another words, people want to trust each other, and do not want to assume that people would want to trick or harm them (Luo et al., 2011). In the article Luo et al. (2011, p. 2) notes: " SE [social engineering] is undoubtedly one of the weakest links in the domain of IS security management, because it is beyond technological control and subject to human nature." So, Luo et al. (2011) did not directly say that human is the weakest link, but instead that humans can be used as the weakest link. Krombholz, Hobel, Huber & Weippl (2015) say: "Social engineering is the art of getting users to compromise information systems. Instead of technical attacks on systems, social engineers target humans with access to information, manipulating them into divulging confidential information or even into carrying out their malicious attacks through influence and persuasion". From this definition we can see that there is no social engineering without humans, so if social engineering is one of the weakest links, then I would argue that by saying social engineering is the weakest link, they mean humans are the weakest link. Although the claim by Luo et al. (2011) might be true, there is no evidence to confirm this. To understand the complexity of blaming only humans in social engineering we can think of a social engineering example where some people are able to access some other people's accounts by basic information they have been able to gather. In this case we could argue that the system authentication is insufficient if it only requires information that someone else can easily get. In cases like this, one of the weakest links could be the system rather than human - of course the system is designed by humans, but that is a whole other discussion.

Martins and Elofe (2002) wrote an article about information security culture. According to Martins and Elofe (2002), the information security culture consists of three different levels, which are organizational, group and individual. While presenting this idea, Martins and Elofe (2002, p. 203-204) presented two different claims: "The procedures that employees use in their daily work could represent the weakest link in the information security chain" and "At any given point users interact with computer assets in some way and for some reason. This interaction represents the weakest link in information

security", in which they refer to Schneier (2000). In the first reference Martins and Elofe (2002, p. 203-204) used the term "could represent", which could be true since humans are certainly one reason for information security incidents. However, in the second quote they said, "interaction represents the weakest link in information security", which sounds very unconditional and, as argued earlier, it isn't necessarily true. Later Martins and Elofe (2002) present the model of information security culture, which consist of inputs, different levels, and outputs. The interesting part is that in change inputs, human is only one of the six different inputs and as Martins and Elofe (2002, p. 207) say, "All processes and structures start at organizational level". Thus, if we say that human is one of the six possible inputs to build information security culture and from which the organization is responsible, can we say that a "normal" employee is the weakest link if there are five other things that affect the information security culture?

The Schneier's (2000) book that Martin and Elofe (2002) refer to discusses the phenomena of digital society and its information security problems. Schneier (2000) recognizes humans as one of the reasons for security threats but does not say that humans would be the weakest link. In the book Schneier (2000) refers many times to "weakest link" or "security chain" but does not claim that humans would be that weakest link. In the beginning of the book Schneier (2000) writes: "Throughout this book, I argue that security is a chain, and a system is only as secure as the weakest link. Vulnerabilities are these weak links." so as we can see from here it is "the vulnerabilities". Later Schneier (2000) writes: "The security of the system may not be better than it's weakest link, but that generally refers to the individual systems. In a smart system, these technologies can be layered in depth, and the overall security is the sum of the links". So Schneier (2000) believed more in overall security and the security of all links rather than blaming humans as the weakest or the most common weak link.

West, Mayhorn, Hardee & Mendel (2009) wrote an article that discusses why users make poor security decisions from a psychological perspective. In the article, West et al. (2009) did a case study where they analyzed the cases on a system model approach, which consisted of three parts: user, the technology and the environment. In the article West et al. (2009) found that all of these three elements can increase the risk of security accidents, but still they are the elements that can strengthen the information security if they are being taken care of. In the conclusion West et al. (2009 p. 15) said: "Users are generally considered to be the weakest link when it comes to computer security", while they explain the phenomena of human factors in information security. This claim is quite generic and as I have argued before, "generally considered" is not a reliable starting point for making assumptions. Even if West et al. (2009) do not claim that this is necessarily true, they give such an idea to the reader. The only time when West et al. (2009 p. 16) refer to a "weakest link" is while talking of human factors and later in the conclusion they say "by conceptualizing the system as an inter-related mechanism that relies on the interactions between human, technology, and environmental factors, security professionals might be able to develop interventions that work to strengthen the weak links". By

reading this, it is easy to understand that humans would be the weakest link and that link has to be strengthened, even if the authors do not necessarily claim that.

Grossklags and Johnson's (2009) article studied the impact of bounded rationality and limited information on user payoffs and strategies. The main goal was to investigate the weakest link security problem from an economical perspective (Grossklags & Johnson, 2009). In the article Grossklags & Johnson (2009) discuss the human role in information security from multiple perspectives. In the beginning of the article, Grossklags & Johnson (2009) note: "On the one hand, technology and code quality are often the culprits of (un)predictable weaknesses in the chain of defense", but later on the same page they note that "on the other hand, many observers argue that the 'human factor is truly security's weakest link'". Even if the authors did not necessarily make the claim that humans would be the weakest link, they created the impression and like Grossklags and Johnson (2009) continue, "an abundance of incidents involving lost and stolen property (e.g., laptops and storage devices), as well as individuals' susceptibility to deception and social engineering are evidence of breaches characterizing weakest-link vulnerabilities". In the first statement by Grossklags & Johnson (2009) the authors also notice that technology can be one of the weakest links. The technology is a huge part of information security and of course when there is that much technology, there might be some problems and threats. One problem with technology is that because "everything" is coded, we actually do not always know what is happening inside the system. As Grossklags & Johnson (2009) said, it is often unpredictable weakness. The other statement that Grossklags & Johnson (2009) made is about human factors being the weakest link. They referred to Mitnick & Simon's (2002) book, which has been already evaluated earlier and it leaves us with many questions about the reliability of their claims. Also, in the third quote Grossklags and Johnson (2009) say "characterizing weakest-link vulnerabilities", which seems to be based on the previous quote about human being the weakest link. Based on these evaluations of the quotes I argue that the whole article is based on assumptions, that even if Grossklags & Johnson (2009) do not say that those are absolute truth they give the reader a strong impression of it.

Gupta (2008) wrote a book about social and human elements of information security. The main idea of the book was to find out emerging trends and countermeasures on information security issues. In the book, Gupta (2008 p. xvii) attributed many of these problems to human problems and like they say in the beginning of the book: "More often than not, it is becoming increasingly evident that the weakest links in an information-security chain are the people because human nature and social interactions are much easier to manipulate than targeting the complex technological protections of information systems". Gupta (2008) did not justify this claim with any references or studies and that is why we cannot say for sure that humans are much more easier to manipulate humans than information systems. Gupta (2008) also used many times the phrase about humans/employees being the weakest link without evidence. For example Gupta (2008 p. xvi ; xxii) wrote: "The human element can become the leaky faucet that spills sensitive information, as employees are often

the weakest link when it comes to information security“ and “In many cases, people, not technology, form the weakest link in the security of an information system”. Neither of these claims has any evidence behind them and later in the book when Gupta (2008, p. 16) explained why human is the weakest link, he writes: “While this information has not been judged against academic standards, it is still relevant, because it is the information attackers will try to use for their attacks and therefore important to know“. Gupta (2008) admitted that there is no evidence to these claims and it only represents the author's own opinion. The whole book is based on the idea that humans would be the weakest link and, perhaps worryingly, Gupta (2008) also gives recommendations on how to be secure from attacks to information security solely based on the idea that humans would be the weakest links. Gupta (2008, p. 25) actually writes in the chapter “why humans are the weakest link” in the following way: “The goal has been to give concrete examples of well-established techniques and methods, together with practical uses.”. But all these recommendations are based on a “fact”, which is actually more the author's own opinion and less a fact.

Gonzalez & Sawicka (2002) introduced a framework for human factors in information security, which allows better understanding of people security problem in designing robust security policies. In the beginning of the article Gonzalez & Sawicka (2002) say: “Technological advances make the armory more and more impressive, but it is becoming increasingly evident that the human factor is the Achilles heel of information security”. The “Achilles heel” is from a very well-known story of Achilles being dipped into the river Styx after he was born, ensuring he was safe from attacks on all parts that the river covered, which was his whole body except his one heel from which he was held. His heel being the only vulnerable part on his body, it was targeted by his foes and led to his death. Today, Achilles heel is usually used to describe the weakest spot (Partridge, 2003), which would be the human factor in this metaphor. Gonzalez & Sawicka (2002) did not provide any evidence to support this claim about human or human factors being the weakest spot/link. However, if we address this metaphor, the information security would be the armor to protect the valuable information and as that armor becomes more and more impressive, one small problem could lead to complete destruction. In other words, it does not matter how good the security system is if there is a back door or some other weakness that could bypass the whole system.

Huang, Rau & Salvendy (2007) did a survey of factors that influence people's perception of information security. In the survey Huang et al. (2007) wanted to investigate factors that can influence people's perception of threats in information security. In the beginning of the article Huang et al. (2007 p. 906) cited Gonzalez & Sawicka (2002): “Information security involves both technology and people, and it is becoming increasingly evident that 'the human factor is the Achilles heel of information security'”. As it was seen earlier, Achilles heel is used to describe the weakest point of something and, along with Gonzalez and Sawicka (2002), Huang et al. (2007) used this metaphor to describe the weakness of human factors in information security. Still, they did not continue this claim with any evidence even if they used terms like

"becoming increasingly evident", which could mislead the reader in the same way as previous articles.

Parsons, McCormac, Butavicius and Ferguson (2010) wrote about human factors and information security and how they appear in individual, cultural, and security environments. In this publication Parsons et al. (2010) provided recommendations on how to influence cultural and human factors and, through those factors, make the information security environment more secure. In the introduction Parsons et al. (2010 p. 1) writes: "Humans are consistently referred to as the weakest link in security" and refers to Schneier (2000) and Huang et al. (2007). I have earlier discussed both of these articles and neither of these articles does not offer any evidence to these claims and as I have discussed before this is a good example of how things can get adapted. In the article Parsons et al. (2010) say, "consistently referred" and as the articles also show in this thesis, that even if "consistently referred" is true, it does not make the claim true, like it is used in this case. Even if Parsons et al. (2010) do not say that they agree with this they neither say that they disagree with the claim, which leaves the reader with the idea that it is true.

Kraemer and Carayon (2005) wrote a publication about computer and information security culture. In the article Kraemer & Carayon (2005 p. 1483) wrote "CIS [Computer and Information Security] culture is considered to be closely related to user behavior and user behavior may be considered the 'weakest link' of the CIS system" and referred to Sasse, Brostoff & Weirich (2001) and Schneier (2000). Kraemer & Carayon (2005) said that humans "may" be the weakest link and by saying this, they agreed to it since they continued the article of how to influence these "weak" human factors. The references that Karaemer & Carayon (2005) used also do not support the argument, which the authors used the references for. Sasse et al. (2001) do not say that humans would be or would be considered as the weakest link. Sasse et al. (2001 p. 122) actually notes "The security research community has recently recognized that user behaviour plays a part in many security failures, and it has become common to refer to users as the 'weakest link in the security chain'. We argue that simply blaming users will not lead to more effective security systems". As we can see, Sasse et al. (2001) notices that this kind of claim has been made earlier and users might be one reason for security incidents, but they do not agree with this claim. Schneir's (2000) book has already been evaluated before and as I argued, Schneier (2000) never said that humans should be considered as the weakest link.

Ifinedo (2013) wrote an article about information system security policy compliance and effects of socialization, influence and cognition. Ifinedo stated that while organizations are making huge investments in information security, the security incidents and data breaches are still an increasing problem. The only explanation which Ifinedo (2013, p. 69) named was "One of the reasons why IS security incidents and abuses continue to plague organizations is that organizational employees are the weakest link in ensuring IS security". While presenting this claim Ifinedo (2013) referred to four different articles: Guo, Yuan, Archer & Connely (2011); Sasse et al. (2001); Stanton, Stam, Mastrangelo & Jolton (2005) and Vroom & Solms (2004). Stanton et al. (2011) writes about end

user security behavior but they do not say that humans/employees would be the weakest link and they only studied the behavior with passwords. As I have argued earlier, Sasse et al. (2001) do not actually claim that employees would be the weakest link. In addition to that Sasse et al. (2001) have not made such a claim; they also write about users and not especially about employees. The last reference has also been evaluated earlier and while Vroom & Solms (2004) make this claim they refer to Briney (2001) and as I have argued previously, the author does not agree with this claim. The study shows that users are not the weakest link of security.

Öğütçü, Testik & Chouseinoglou (2016) has written about information security behaviour and awareness. In the article Öğütçü et al. (2016 p. 84) references Abawajy (2014) while saying "no matter how many and how strong the layers of technological defenses in an organization, the information security is only as strong as its weakest link, and different tools, such as social engineering, can been used to target individuals, who can be considered to be the weakest link of the security chain" and referred also to: Arce (2003); Jansson & Von Solms (2013); Shultz, Proctor, Lien & Salvendy (2001) and Zhang, Reithel & Li (2009). In his own article Abawajy (2014 p. 240) studied security awareness but never said that humans would be the weakest link, only that humans are one link in the security chain: "Social engineering is an important problem to address, because it specifically targets the 'people link' that information security officers are trying to strengthen.". So, as we can see, Abawajy (2014) does not say that humans would be the weakest link, but merely that humans are one of the links, and that link is the one which social engineers try to target.

The first reference that Öğütçü et al. (2016) used was Arce (2003), which can be considered a bit odd since Arce (2003) actually defended humans and, as a support to these claims, Arce (2003) compared penetration studies and IBM's Resource Access Control Facility system, where Acre noticed that the most weakest security point was actually the internal operating system security and not a human. Arce (2003 p. 72) also stated on the basis of the results in article: "The weakest link could be defined as flaws in an operating system's security controls or as procedural weaknesses in its development and deployment process". Thus, I would argue that Acre (2003) defended humans rather than blaming them as the weakest link, like Öğütçü et al. (2016) imply.

The second reference that Öğütçü et al. (2016) used was Jansson & Solms (2013). Jansson & Solms (2013) studied phishing and made phishing activities to gather data of users' actions. In the discussion Jansson & Solms (2013 p. 591) write: "From the data and findings discussed above, it may reasonably be concluded that users can learn and positively adapt their e-mail behaviour – as a result of simulated phishing exercises – together with embedded training. Therefore, it may be deduced that simulating phishing attacks together with embedded training can, indeed, contribute towards cultivating users' resistance to phishing attacks". Jansson & Solms (2013) did not say at any point that humans would be the weakest link or even that they operated poorly in the exercise. As we can see from the citation, Jansson & Solms (2013) actually found that users can operate well, learn, and adapt to new situations.

The third reference Öğütçü et al. (2016) used was Schultz, Proctor, Lien & Salvendy (2001), who studied usability issues in information security methods. While writing about human factors, Schultz et al. (2001 p. 621) wrote: "Users have long been regarded as the weak link in information security", but like many other articles they did not offer any evidence to this. Schultz et al. (2001) claim might be true since they say only "as the weak link" rather than "the weakest link". It can be agreed that every time human is related to information security it plays a role in that chain and is somehow involved if there is an incident. So when Öğütçü et al. (2016) referred to Shultz et al. (2001) the meaning of the reference changed since there is a big difference between "weak link" and "the weakest link".

Zhang et al. (2009 p. 330) have also said that humans are the weakest link in information security: "While organizations have applied many security technologies, e.g. anti-virus software, firewalls, access control, intrusion detection techniques, encrypted login, biometrics techniques, etc. to protect their critical information, humans remain the weakest link in the information security environment and associated security processes", but they haven't justified this claim with any evidence. Later in the article, Zhang et al. (2009, p. 331) refer to a Deloitte (2009) security survey while saying, "According to a recent security survey, 71 percent of surveyed companies provide security training to employees. However, 86 percent still acknowledge human errors as the greatest weakness". From Deloitte's (2009) survey we can see that actually 86% of respondents found the human errors as a root cause of information system failure. The report has not specified if these failures lead to security incident or if they were only misuses of system that caused an error, but had nothing to do with the security incident. In Deloitte's (2009) survey, respondents were asked about internal breaches and the biggest reason were viruses / worms, which were also the biggest threat in external breaches. Even if the employees or other internal party have enabled the worm to enter the system, we can argue that is human really the weakest link, or is it just a factor that may have increased the risk of a security incident? Why did the antivirus software let the worm through, or why were there no measures that would have noticed the worm before it got into the system? The other interesting fact is that viruses are listed as both internal and external threats because only internal viruses are usually the fault of employees, and the category employee misconducts is listed separately. Another problem with the Deloitte (2009) survey is that all of the participants consisted from financial sector and cannot be used to describe the state of information security in all sectors.

From all of these articles we can see that there is no evidence to Öğütçü et al. (2016) claim that humans would be the weakest link in information security. Even though Öğütçü et al. (2016) wrote that humans are considered to be the weakest link, I would argue that by this claim and with that many references it seems, to the reader, to be true. But after evaluating all of the references I argue that not one of these articles confirm this. Because of that, it can be held as misleading for the reader since it seems very much as though the subject is actually studied and the references seem as solid evidence, even if they have used the word "considered".

Talib, Clarke & Furnell (2010) wrote an analysis of information security awareness within home and work environments. In the introduction Talib et al. (2010 p. 196) wrote: "Unfortunately, it is also a well recognized fact that security is only as strong as the weakest link; and the weakest link is frequently the end-user" and while saying this they referred to Schneier (2000). As we have seen earlier, Schneier (2000) has not made such claim or said, "the weakest link is frequently the end-user". Talib et al. (2010) used the word "frequently", which does not mean they say that it is the truth, but it is misleading for the reader. It is easy for the reader to get the assumption that it would be the truth, or that there is some study which shows that end-users are the weakest link frequently.

He (2012) wrote a review of social media security risks and mitigation techniques. In the article He (2012 p. 175) noticed: "Studies show that the weakest link in security is the human link" and referred to Curry (2011) and Vroom & Solms (2004). For the reader it is quite convincing if the author uses studies as evidence to the claim and, like He (2012), make the claim that humans are the weakest link and say that studies have shown it. The only problem with this is that neither of these articles used as reference do not present any evidence to support this claim. Curry (2011) noticed only in the internet article that humans are the weakest link but did not provide any evidence to this: "So we come back again, to the weakest link: The Human link. The best constructs and systems that we build are actually most effective and focused when the Human beings around it are focused and coordinated." Unlike He (2012) said, there was no study behind this claim or even behind the text; in actuality there were no references used and the text was presented as Curry's own opinion. The other reference that He (2012) used was Vroom & Solms (2004) which has been evaluated before, but all in all it was based on Briney's (2001) study that did not say that humans would be the weakest link in information security.

The previous articles and publications reinforce the perception of how such phrases can change little by little into a general understanding. Many times someone has made an claim without justification or any evidence and later someone else uses this claim in his text, which has resulted in a chain reaction that ends to an general idea of that "everyone agrees with this". None of the previous articles have actually studied the phenomena or presented evidence that is human really the weakest link and because of that we cannot say for sure that human really is the weakest link in information security.

4.2 The actual threats

Many scholars indicate that the biggest reasons for security incidents in organizations are due to something else than humans. For example, Bulgurcu et al. (2010) see that employees can safeguard information and technology resources by their own actions. Sasse et al. (2001) also agree that simply by blaming users we will get nowhere; instead we must learn from them and hand over these findings to security system designers. Sasse et al. (2001 p. 122) also

notice "labeling users as the 'weakest link' implies that they are to blame. In our view, this is a repeat of the 'human error' mindset that blighted the development of safety-critical systems until the late eighties", so there is no point to simply blame and label humans without thinking how we could avoid problems with humans and how to decrease the possibility of human becoming the threat to information security. Arce (2003) also argued that humans are not the weakest link and also found studies, such as penetration to evidence that support the claim. Arce (2003 p. 72;74) also said that: "Security solutions should account for our IT infrastructure's technological challenges and the particular aspects of human and organizational behavior. It is in this context that we can identify our current weakest link: the workstation", and "the primary security concern was internal operating system security. Therefore, the weakest link could be de- fined as flaws in an operating system's security controls or as procedural weaknesses in its development and deployment process".

From these articles we get the other side, compared to the others claiming human is the weakest link. There are also many studies of the most common information security incidents, which indicate that human errors are not the biggest incident group. Earlier we saw Jouini et al. (2014) and Loch et al. (1992) divide different types of threat groups, but to find the real problems we need to divide the groups even more specifically. Whitman (2003) made a study of threats to information security and created a threat category with a weighted ranking. The categories were weighted based on respondents' evaluation of each one, where they could rank the threats from "very significant" to "not significant" and then identify the five most important threats to their organization (Whitman, 2003). From Whitman's (2003) category we can see that the deliberate software attack is the number one threat, and those attacks are targeted directly to software and its flaws. The second most important threat is technical software failures, or errors that also do not fall on humans. Only the third one, "act of human error or failure" is related to the human context. So, on the basis of Whitman's (2003) categorization, human is not the weakest link, the software is. Sumner (2009) also referred to Whitman's (2003) study when talking about five biggest threats in information security, which were the five most weighted from Whitman's threat categories. Whitman (2003, p. 93) calculated the threat weight in the following way: "The ranking is a calculation based on a combination of the respondents evaluating each category on a scale of 'very significant' to 'not significant' and then identifying the top five threats to their organization.". Slay & Miller (2007 p. 75) also found similar findings: "Infections due to viruses, worms and Trojans were most common, accounting for 45% of total losses in 2004. Other prevalent forms of electronic crime were fraud, followed by abuse and misuse of computer network access or resources".

Threat Category	**Weighted Ranking**
Deliberate software attacks	2178
Technical software failures or errors	1130
Act of human error or failure	1101

Deliberate acts of espionage or trespass	1044
Deliberate acts of sabotage or vandalism	963
Technical hardware failures or errors	942
Deliberate acts of theft	695
Forces of nature	611
Compromises to intellectual property	495
QoS deviations from service providers	434
Technological obsolescence	428
Deliberate acts of information extortion	225

TABLE 3 Information security threat categories (Whitman, 2003)

In many of the articles that have claimed humans are the weakest link, the authors have referred to the problems with insiders, e.g. Warkentin & Willision (2009). In these articles two points should be considered: insiders are not the only human threats that organizations have, and many studies also show that insiders are actually not the biggest threat to all organizations (Whitman, 2003; Whitman, 2004; Sumner, 2009; Subashini & Kavitha 2011).

Subashini and Kavitha (2011 p. 7) found that "external criminals pose the greatest threat (73%), but achieve the least impact (30,000 compromised records), resulting in a Pseudo Risk Score of 67,500. Insiders pose the least threat (18%) and achieve the greatest impact (375,000 compromised records), resulting in a Pseudo Risk Score of 67,500". From this we can see that external threats pose the greatest threats but their actual impact ranks the lowest, while insiders pose the least threat but their impact is greatest. Breidenbach (2000) shared the same idea and quoted Schultz, saying "Numerically, more attacks come from the outside now, but one insider with the right skills can ruin your company". From these articles we can see that outside threats are numerically higher, but threats from inside are more dangerous to organization. Slay & Miller (2007) also studied the origin of attacks and found that 88% of attacks are sourced externally. Colwill (2009 p. 187) summarizes the problem with insider well: "A malicious insider has the potential to cause more damage to the organization and has many advantages over an outside attacker: they have legitimate and often privileged access to facilities and information, have knowledge of the organization and its processes and know the location of critical or valuable assets. Insiders will know how, when and where to attack and how to cover their tracks".

Often, when referring to human weakness, authors use third party surveys as a reference. Many big consulting companies do their own studies on the state of information security in the world. The most used surveys in information security literature are from Deloitte, PwC, and Ernst & Young. Deloitte's (2009) survey has been used, for example, in Metalidou, Marinagi, Trivellas, Eberhagen, Skourlas and Giannakopoulos' (2014 p. 425) article in an

information security threat context: "According to Deloitte (2009), human error is overwhelmingly stated as the greatest security weakness in 2009 (86%), followed by technology (a distant 63%)". Deloitte's (2009) survey has already been discussed earlier and as I have argued, it contains many problems.

Ernst & Young's global information security survey (2008) has been referred to by Warkentin & Willision (2009 p. 102): "In a global survey of nearly 1400 companies in 50 countries, researchers found that awareness and personnel issues remain the 'most significant challenge to delivering successful information security initiatives'", and Hu, Dinev, Hart & Cooke (2012 p. 616): "A recent survey of IT managers of global companies indicates that people remain the weakest link for information security in organizations". In this Ernst & Young (2008) survey the questions are not available, and they do not actually tell what they have asked from the participants. They also do not provide graphs from all of the questions and the section that Hu et al. (2012) cite has not been validated with any evidence. The only part that Ernst & Young (2008 p. 16) has told is "Organizational awareness was cited by 50% of respondents to be the most significant challenge to delivering successful information security initiatives - more significant than the availability of resources (48%), adequate budget (33%) and addressing new threats and vulnerabilities (33%)". This summary does not give us enough information to blame it only on people, since organizational awareness could mean many things beyond simply preventing human errors.

From PwC, the most used survey was the information security breaches survey (2006), which has been made in association with Microsoft, Clearswift, Entrust and Symantec. Like the two other surveys, this one has a few problems. The participants for the survey were all from UK, so this survey cannot be generalized to the whole world. Also, it has been made in cooperation with companies which offer information security services and might not want to release information that is not beneficial to them. Despite that, the survey had more interesting points compared to the other two. In this survey, it was determined that only 2% of system failures or data corruption were because of human errors. Later in the survey, participants were asked about the most significant incidents to their business, and system failure was the most significant with 17% of participants answering, "very major". So only two percent of the most significant incidents have been caused by human errors.

The 2005 CSI/FBI computer crime and security survey by Gordon, Loeb, Lucyshyn and Richardson (2005) showed that top three types of attack were virus, unauthorized access and theft of proprietary info. These three of thirteen attack types accounted for 80% of financial losses to organizations. As we can see, the top reason for financial losses have been viruses. The virus may have been able to enter the company's systems because of human error, but that is simply one explanation. There could be many other explanations as to how the virus entered the system. Based on this survey we could say that human errors can increase the risk of information security incidents, but we cannot say that humans are the weakest link or the biggest reason for incidents. Australian Computer Crime and Security Survey 2004 (AusCERT, 2004) had similar findings as Gordon et al. (2005) when they found that the most common attack

type were viruses, worms or trojans, which caused 45% of all financial losses. Im & Baskerville (2005) analyzed several reports including Gordon et al. (2005) and the 2003 AusCert survey to find different threat categories of information security. After Im & Baskerville (2005 p. 69) had analyzed the studies, they noted that "these reports suggest that intentional security threats such as hacking, computer viruses, and computer theft are becoming a more severe problem in relation to other security vulnerabilities".

4.3 Case examples of data breaches

Data breaches are part of information security incidents. Sen & Borle (2015 p. 315) defines data breaches as follow: "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". So, the definition is mostly the same as information security, but usually when people discuss data breaches they mean it in the sense that personal data has been breached from the company. In the following chapter, I will show some examples of data breaches and discuss their root causes. These cases are presented to show the problematically behind finding the "root cause". As we have seen before in many times human are blamed as "the weakest link" without any evidence. These cases are good examples of how the situation could appear to be a human fault, but in reality, there are many causalities behind these cases. Many newspapers blamed human and human factors in all of these cases as the one and only cause. Of course, humans have been part of these incidents, but we must understand the other factors. So, the key takeaway from these cases should be the fact that in information security incidents it is incredibly difficult to determine the "root cause" and these causalities should be taken into account when reading about these types of incidents.

4.3.1 Case TJX

TJX is one of the biggest textile retailers in the US and their data breach in 2006 was one of the biggest breaches of that time. In the breach the attackers were able to get the credit card information of more than 45 million individuals (Xu, Grant, Nguyen & Dai, 2008; Fisher, 2012). The attack started in 2005 when attackers were able to capture wireless transactions from the store with an external antenna. The store's wireless network used WEP security standard, which was the earlier version of WPA, which is the current wireless networks security standard (Xu et al., 2008). By monitoring the traffic in the wireless network, the intruders were able to crack the security code of the network. With that information intruders were free to gather the information of 45 million different credit cards during May to December in 2006 (Xu et al., 2008). So the intruders were able to track credit card payments for half a year without anyone noticing

their presence, and in total they were in the system for 18 months (Fisher, 2012). In December TJX had some problems with credit card payments, so they hired a company to investigate the problem. It was then that they found out that they had been breached. Still, it took quite some time to discover how the breach was executed and what information they had lost (Xu et al., 2008).

Whose fault was this data breach? Like we have seen from the information security literature, in many cases companies prefer to blame insiders. However, as we have also seen they are not the reason in most cases and the same goes for this. TJX confirmed that there were no internal employees involved with this incident (XU et al., 2008). So, the two big questions are 1) why no one noticed that intruders were in their network for 18 months, and 2) why it only took couple of days for intruders to crack the security key for the wireless network. According to Xu et al. (2008), a big information security company had offered TJX an antivirus software that could detect incidents like this, but they decided that they would not need it. If they would have taken the offer and implemented the software, could it have prevented the whole data breach? That is a question we do not know the straight answer for because the software may not have noticed the intruders or maybe someone would have closed the warning. Finding the root cause for this kind of breach is very complex because almost every player in the event has some kind of causality. Is it the managers' fault because they did not purchase and implement the software, or is it the wireless network router's fault because intruders were able to access the network so easily? The other question is also hard to answer because we do not know how the security key was discovered. It sounds like the security key may have been quite poor if intruders were able to crack in couple of days, because the password cracking systems were not that developed in 2005 and, still today, a 16 characters randomized password with upper and lower case letters combined with special marks and numbers would be impossible to crack (it would take thousands of years to try every combination). So, one might think that this is the fault of whoever set up the (presumably) poor password, but there is always the other side. Why is it possible to set a weak security key for a wireless network? Why is it not mandatory to set strong, 16-character keys that could not be cracked in a mere two days? The question is whether it is the fault of the person or the software.

4.3.2 Case Target

In 2013 Target revealed that they had a massive data breach which consisted of credit card information combined with personal information (Manworren, Letwat & Daily, 2016). Target is one of the biggest retailers in United States and a Fortune 500 company. What is the interesting part of this case is that Target had just bought the best malware and virus detection tools available at the time, but they still lost tens of millions of credit card numbers because of a "simple" malware (Manworren et al., 2016). The actual attack was done by stealing the credentials to Targets systems from a third-party contractor that ran Target's climate systems. With access to Target's main system, the attackers were able to

install malware, which stole the credit card information from the payment point (Manworren et al., 2016). After that, the attackers could collect credit card information freely, and no one within Target was aware of the breach for a long time.

Also, with this breach there are two big questions, 1) why did the third party contractor have access to the entire Target system, and 2) why the state-of-art malware detection tool not detect this malware? The first question is fully Target's fault since they had not complied with least access model, which means that each employee can only access the systems that he/she would need complete their job. Target should have limited the access of third party contractors and also set some measures to know if a third party is using them wrong. In this case, a climate system contractor should never have access to payment systems. The second question is a bit more complicated, since their new system had a function that would automatically detect and delete malwares. However, according to Manworren et al. (2016), Target's security team disabled that function. The reason for disabling the function was that it was too sensitive, as it marked many emails and good software as malware too (Manworren et al., 2016). So again, one might say that is was the security team's fault, because they did not restrict the access of third-party contractors and they disabled the malware function. But we could also argue that is the system truly functional if it marks everything as malware? How would the company employees be able to work if all their emails are marked as malware? Was there any other option than to disable that function, save removing the system completely? Here we can see another causality factor, which is that malware software has to be designed for real use, because otherwise it does not matter how good it is if it cannot be used in the situation it has been created and bought for.

If we compare this to the information security literature this goes within the results found. This is mostly a software bug that allows an attacker to get the payment data. Of course, employees are playing a big role in this incident and we can see that they impacted this incident, but they are not only reason. They might have increased the risk by disabling the malware function, but the software should still have detected the malware. So, employees were merely one part that increased the risk but the main reason is still the software, since employees are not able to detect this kind of incidents without software.

4.3.3 Case Yahoo

In September of 2016 Yahoo announced that it had been breached in 2014 and information on 500 million accounts had been stolen. Then, later in December they released that in 2013 they had lost over billion accounts, making these two breaches the world's biggest data breaches (Trautman & Ormerod, 2016). According to the US government and Yahoo the breach was done by the Russian government by exploiting vulnerabilities in Yahoo's security systems (Trautman & Ormerod, 2016). There is not much technical information of what were the vulnerabilities, but there are many reasons as to how this incident might have been prevented.

Trautman and Ormerod (2016) presented a few reasons on how Yahoo's data breach was possible and why there were such vulnerabilities. The first reason was that Yahoo did not establish a reward program for hackers until 2013. In 2010 Google and Yahoo were both compromised by Chinese hackers and Google immediately took very serious actions after the incident, the reward program being one of those (Trautman & Ormerod, 2016). The second way where Yahoo went wrong according to Trautman and Ormerod (2016) was that Yahoo hired a new Chief Information Security Officer (CISO) but then denied requested resources from him. For example, the new CISO insisted that Yahoo should start using end-to-end encryption, but the senior management did not agree with this. Secondly, the CEO refused to invest in information security and even turned off the some of the security systems. The same CEO also rejected the idea of an automatic password change after the breach, which could have initially saved tens of millions of accounts from being breached (Trautman & Ormerod, 2016). The third reason why the incident happened was bad monitoring and reporting. In 2014 Yahoo's monitoring team brought up to the directors that they might have been breached by hackers using cookies to steal account credentials. The directors closed the investigation, claiming that it is not possible to steal Yahoo's account credentials through cookies (Trautman & Ormerod, 2016).

From here we can see that there were many different reasons that might have led to the world biggest data breach. It is hard to name one root cause for this breach, even if it eventually was the software where the vulnerability was. Many employees made wrong choices or were forced to step down with their good ideas. What if Yahoo had established a hacker reward program and someone found the vulnerability before the big breaches, or what if there would have been end-to-end encryption, which would have prevented the hackers from getting the credentials? These are all questions that we cannot know the answer for sure. Only thing that we know is that just like the previous cases, these incidents are mix of humans, software and luck. So, we should find the real causes and try to think ways to prevent them in the future rather than just blaming the users or some other element, simply because it's the easiest way.

4.3.4 Other possible case

Let's think about one hypothetical case, which might well be true. A big corporation has identified the need for new information security system that covers all the information security areas of their company. The system's requirements have been well-thought and after that the system has been built based on them. After the system has been built and tested in the vendor environment and found safe, it is implemented into the customer's network and systems.

Some time after the system has been taken to use, the company notices that they have had a data breach. After the company has investigated the issue, they notice that there is a backdoor that has been activated by one of their employees. When they question the employee, they discover that the system has asked the employee if he wants to disable one feature of the system. The em-

ployee disables that feature, thinking it is useless, but by disabling that one feature, the poor employee has unwittingly opened the access to the backdoor to the whole internet. Not long after that, a "bad" hacker finds this backdoor and uses it access the company's internal network and steals their valuable data.

Now, when the company investigates this issue they want to find out and determine who is responsible for all this. Is it the employee who has disabled the function and enabled the hacker to break into their network? Is it the system vendor's fault that they designed it in such a way that it was possible to disable such a function? Is it the testers' fault who did not find such a vulnerability from the system? Is it the hackers' fault that they took advantage of the vulnerability and committed a crime? All of the answers for the questions could be the right answers and this is why these cases are so complex. For example, one would think that it is the employee's fault that the company had data breach, but what if the hacker would not have exploited the backdoor? So we can see the causality between all of these actors; for example if the tester or the vendor would have found this error in the system, the employee would not have been able to disable the function, and the hacker would not have been able to break into the system. In another scenario, if the employee hadn't disabled that function the hacker would not have been able to get into the system, at least from that backdoor. Then if the hacker had not been a "bad hacker" and would not have taken advantage of this situation, there would not have been a data breach and, in the best scenario, the hacker would have informed the company of such a vulnerability.

5 DISCUSSION

As we can see from the analysis, it can be said that the phrase "human is the weakest link in information security" or varieties of it are used without evidence that would show this to be true. Many of the articles use the phrase with some generalizations such as "generally considered". By using the phrase "human is the weakest link in information security" and not criticizing it any way, or at least not withdrawing themselves from such a claim, it can be argued that the authors are committed to the claim (or at least the reader can believe or assume so). A good example of this is Thomson & Nierkerk (2012, p. 39) who has written: "It is commonly acknowledged that employees are often the weakest link when it comes to protecting information assets". So as time passes the phrase moves to a situation where it is referred to as "commonly acknowledged", which implies that it has been proved to be that way. It is a short way from "commonly acknowledged" to be a fact and Flores and Eksted (2016 p. 26-27) actually wrote: "It's a well-known fact that employees are the weakest link in an organization's defense against external information security threats". While saying this, Flores & Eksted (2016) did not present any evidence or references to show this true. So all the discussion around this topic have changed the "generalization" to "well-known fact" but I argue that it cannot be fact if there is no evidence to support this claim.

As we can see in the figure 3, all of the articles used in the literature review that claim human is the weakest link have used references that do not actually support this argument. It is interesting to see how many articles have made that claim and refer to another article that does not actually make that claim or does not support any evidence to this claim. Based on the figure 3 and the previous text I argue that this phrase is used without any justification. By claiming humans as the weakest links in information security, many organizations may have allocated resources to the wrong places and, in the worst case, may have left some other important links without any protection at all. Based on the literature review I also argue that humans are, without a doubt, one of the (weakest) links in information security and many information security incidents are caused directly or indirectly by humans. However, this does not mean that they are caused only by humans, and most cases are too complex to blame

only humans or some other one link. The causalities between different links are strong in most of the cases, as we can see from the example data breaches, and this is why we should always look at the "bigger picture" and not focus simply on blaming the one link that seems to be the obvious choice.

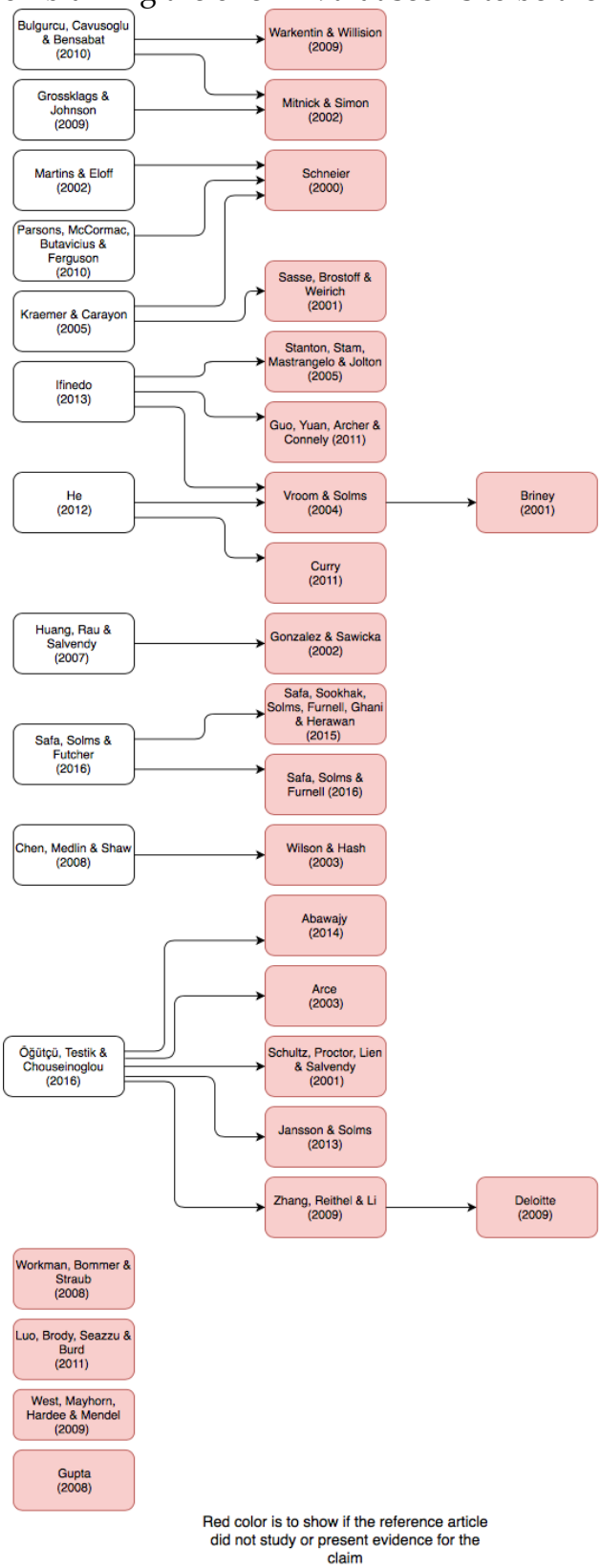

FIGURE 3 (articles links to their references)

5.1 Importance and the contribution of the study

Many of the studies (which have been referred to earlier) offer advice to organizations on how they should divide their resources in regard to the information security area, e.g. He, 2012; Whitman & Mattord, 2012; Parsons et al., 2010 & Gupta, 2008. Most of the advice and recommendations within these reports are based on the "fact" that human is the weakest link and for that reason, based on the literature, I argue that these evidence-lacking recommendations should not be agreed to action if it is not in line with the organizations own strategy. This study shows that these "generalizations" have been used in many studies and, by its mere usage, the phrase "human are the weakest link in information security" has been considered as a fact in some studies without evidence. This research also challenges the general view on whether things can be stated without evidence. On the other hand, this research also challenges the general illusion of human being the weakest link based on research data.

Many of the articles taken into this thesis blamed human as the weakest link. These results show us that it is not true, or at least not true on the basis of this literature review. Many of the studies have not studied this exact thing (are human the weakest link in information security), so this thesis finding does not make those studies invalid, but it does show their grievances. For an information security researcher, this thesis offers a critical viewpoint, and encourages challenging existing generalizations and justifying the allegations made. For a businessperson this thesis also offers the critical viewpoint and, as we have seen before, many authors have suggested actions for organizations based on this "false" information. So, with this info they can be more critical of this knowledge and look for alternative ways to guide their actions. For a "normal person" this thesis offers the humble suggestion that maybe we are not the weakest link, and by developing ourselves we can become the strongest link in the future. The positive atmosphere can make it easier for many people to rely on their own abilities compared to the accusing atmosphere.

5.2 Reliability and validity

The study has been carried out as a SLR, which means the reliability is highly dependent on the previous research. In this study, this problem has tried to be negated by following Okoli & Schabram's (2010) eight steps, which have given a good framework for the research. The most important thing for validity and reliability has been the protocol, which has determined the guidelines for searching, picking and validating the literature used in the study. Since all material that fulfills the criteria is included in the study, the result of the study should be the same if it were carried out again. The literature used in the study can be considered relevant for the study. Based on this material, it has been possible to answer the research question to the fullest extent possible. Also

guidelines such as choosing only academic literature and limiting the literature to publications from 2000 and onward have improved the validity of the study.

6 CONCLUSION

The aim of this study was to determine whether or not humans are the weakest links in information security. This study was conducted as a systematic literature review to get the broadest possible understanding of the subject. The literature review itself consists more than 40 different studies in the area of information security. The majority of these studies claimed or implied that humans were be the weakest link, although the studies that have actually studied information security threats and information security accidents did not confirm these claims.

The research topic itself proved to be very complex and no straight answer to the research question was received. It can be said that humans are irrefutably one part of the chain and, in some cases, they might even be the weakest link. However, as it can be seen from the literature, it is not easy to determine the actual reason for any information security incident. This study suggests that the phrase "human is the weakest link in information security" is used without any evidence and sometimes it is talked as though it is “fact”. This study proves that human is not necessarily the weakest link and that there are large amount of factors which could affect that.

Future research related to humans in information security should focus more on the root causes and explaining the complexity and causalities between different actors in information security incident. Future research topics could be “The causalities between different actors in information security incidents” or “The complexity behind finding the root cause in information security incidents”. More qualitative research could be conducted on the area of threat sources in information security. I also hope that, with this study, the literature will not use general beliefs to support the authors’ own argument, nor claims without any evidence.

In regards to limitations, it can be said that the result of the study did not answer the research question in a straight way and, due to the relatively small amount of literature, the results are not generalized to the entire sphere of information security research. The study method of systematic literature review also needs more use in the information security area, because many of the frameworks were designed to support different areas in science, mostly

healthcare. Regarding the study process it can be said that when you go through hundreds of articles, there is always the possibility that an important or less important article has been accidentally missed in pre-screening period. It is also worth noting that only one search engine (Google Scholar) was used for research, although it covers most of the scientific literature.

REFERENCES

Abawajy, J. (2014). User preference of cyber security awareness delivery methods. *Behaviour & Information Technology*, *33*(3), 237-248.

Acemoglu, D. (2012). Introduction to economic growth. *Journal of economic theory*, *147*(2), 545-550.

Agarwal, A., & Agarwal, A. (2011). The security risks associated with cloud computing. International Journal of Computer Applications in Engineering Sciences, 1, 257-259.

Alberts, C. J., & Dorofee, A. (2002). Managing information security risks: the OCTAVE approach. Addison-Wesley Longman Publishing Co., Inc..

Anderson, R. H., Bozek, T., Longstaff, T., Meitzler, W., & Skroch, M. (2000). *Research on mitigating the insider threat to information systems-# 2* (No. RAND-CF-163-DARPA). Rand National Defense Research Inst Santa Monica CA.

Arce, I. (2003). The weakest link revisited [information security]. IEEE Security & Privacy, 99(2), 72-76.

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., ... & Zaharia, M. (2010). A view of cloud computing. Communications of the ACM, 53(4), 50-58.

Baumeister, R. F., & Leary, M. R. (1997). Writing narrative literature reviews. *Review of general psychology*, *1*(3), 311-320.

Bosworth, S., & Kabay, M. E. (Eds.). (2002). Computer security handbook. John Wiley & Sons.

Breidenbach, S. (2000). How secure are you?. InformationWeek, (800), 71-71.

Bulgurcu, B., Cavusoglu, H. & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. MIS Quarterly, 34(3), 523-548.

Cappelli, D., Moore, A., Trzeciak, R., & Shimeall, T. J. (2009). Common sense guide to prevention and detection of insider threats 3rd edition–version 3.1. *Published by CERT, Software Engineering Institute, Carnegie Mellon University, http://www. cert. org*.

Cartwright, N. (2006). Where is the Theory in our "Theories" of Causality?. *The Journal of philosophy*, *103*(2), 55-66.

Chatfield, A. T., & Reddick, C. G. (2017, June). Cybersecurity Innovation in Government: A Case Study of US Pentagon's Vulnerability Reward Program. In *Proceedings of the 18th Annual International Conference on Digital Government Research* (pp. 64-73). ACM.

Chellappa, R. K., & Pavlou, P. A. (2002). Perceived information security, financial liability and consumer trust in electronic commerce transactions. *Logistics Information Management*, *15*(5/6), 358-368.

Chen, C. C., Dawn Medlin, B. & Shaw, R. S. (2008). A cross-cultural investigation of situational information security awareness programs. Information Management & Computer Security, 16(4), 360-376.

Cherdantseva, Y., & Hilton, J. (2013, September). A reference model of information assurance & security. In 2013 International Conference on Availability, Reliability and Security (pp. 546-555). IEEE.

Coles-Kemp, L., & Theoharidou, M. (2010). Insider threat and information security management. In Insider threats in cyber security (pp. 45-71). Springer, Boston, MA.

Colwill, C. (2009). Human factors in information security: The insider threat–Who can you trust these days?. Information security technical report, 14(4), 186-196.

Cox, D. R. (1992). Causality: some statistical aspects. Journal of the Royal Statistical Society: Series A (Statistics in Society), 155(2), 291-301.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. computers & security, 32, 90-101.

Cusumano, M. A. (2008). The changing software business: Moving from products to services. Computer, 41(1), 20-27.

Deutsch, M., & Krauss, R. M. (1960). The effect of threat upon interpersonal bargaining. *The Journal of Abnormal and Social Psychology*, *61*(2), 181.

Dhillon, G. (2001). Violation of safeguards by trusted personnel and understanding related information security concerns. *Computers & Security*, *20*(2), 165-172.

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for information security management. Journal of Information Security, 4(02), 92.

Fisher, J. A. (2012). Secure my data or pay the price: Consumer remedy for the negligent enablement of data breach. *Wm. & Mary Bus. L. Rev.*, *4*, 215.

Flores, W. R., & Ekstedt, M. (2016). Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. *computers & security*, *59*, 26-44.

Furnell, S., & Clarke, N. (2012). Power to the people? The evolving recognition of human aspects of security. *computers & security*, *31*(8), 983-988.

Goel, S., & Shawky, H. A. (2009). Estimating the market impact of security breach announcements on firm values. Information & Management, 46(7), 404-410.

Gonzalez, J. J. & Sawicka, A. (2002). A framework for human factors in information security. (s. 448-187)

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Richardson, R. (2005). 2005 CSI/FBI computer crime and security survey. Computer Security Journal, 21(3), 1.

Grossklags, J. & Johnson, B. (2009). Uncertainty in the weakest-link security game. (s. 673-682) IEEE.

Gulappagol, L., & ShivaKumar, K. B. (2017, December). Secured data transmission using knight and LSB technique. In Electrical, Electronics, Communication, Computer, and Optimization Techniques (ICEECCOT), 2017 International Conference on (pp. 253-259). IEEE.

Guo, K. H., Yuan, Y., Archer, N. P., & Connelly, C. E. (2011). Understanding nonmalicious security violations in the workplace: A composite behavior model. *Journal of management information systems*, *28*(2), 203-236.

Gupta, M. (Ed.). (2008). *Social and Human Elements of Information Security: Emerging Trends and Countermeasures: Emerging Trends and Countermeasures*. IGI Global.

He, W. (2012). A review of social media security risks and mitigation techniques. *Journal of Systems and Information Technology*, *14*(2), 171-180.

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing employee compliance with information security policies: The critical role of top management and organizational culture. *Decision Sciences*, *43*(4), 615-660.

Huang, D., Rau, P. P. & Salvendy, G. (2007). A survey of factors influencing people's perception of information security. (s. 906-915) Springer.

Illari, P. M., Russo, F., & Williamson, J. (Eds.). (2011). *Causality in the Sciences*. Oxford University Press.

Im, G. P., & Baskerville, R. L. (2005). A longitudinal study of information system threat categories: the enduring problem of human error. *ACM*

SIGMIS Database: the DATABASE for Advances in Information Systems, *36*(4), 68-79.

Janakiraman, R., Lim, J. H., & Rishika, R. (2018). The Effect of a Data Breach Announcement on Customer Behavior: Evidence from a Multichannel Retailer. Journal of Marketing, 82(2), 85-105.

Jansson, K., & von Solms, R. (2013). Phishing for phishing awareness. *Behaviour & information technology*, *32*(6), 584-593.

Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: an empirical study. *MIS quarterly*, 549-566.

Jouini, M., Rabai, L. B. A., & Aissa, A. B. (2014). Classification of security threats in information systems. Procedia Computer Science, 32, 489-496.

Kallio, T. J. (2006). Laadullinen review-tutkimus metodina ja yhteiskuntatieteellisenä lähestymistapana. *Hallinnon tutkimus 25 (2006): 2*.

Kandias, M., Virvilis, N., & Gritzalis, D. (2011, September). The insider threat in cloud computing. In *International Workshop on Critical Information Infrastructures Security* (pp. 93-103). Springer, Berlin, Heidelberg.

Kraemer, S., & Carayon, P. (2005, September). Computer and information security culture: findings from two studies. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* (Vol. 49, No. 16, pp. 1483-1488). Sage CA: Los Angeles, CA: SAGE Publications.

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. *Journal of Information Security and applications*, *22*, 113-122.

Landesberg, P. (2001). Back to the future--Titanic lessons in leadership. *The Journal for Quality and Participation*, *24*(4), 53.

Loch, K. D., Carr, H. H., & Warkentin, M. E. (1992). Threats to information systems: today's reality, yesterday's understanding. Mis Quarterly, 173-186.

Luo, X., Brody, R., Seazzu, A. & Burd, S. (2011). Social engineering: The neglected human factor for information security management.Information Resources Management Journal (IRMJ), 24(3), 1-8.

Manworren, N., Letwat, J., & Daily, O. (2016). Why you should care about the Target data breach. *Business Horizons*, *59*(3), 257-266.

Martins, A., & Eloff, J. (2002, July). Assessing Information Security Culture. In *ISSA* (pp. 1-14).

Metalidou, E., Marinagi, C., Trivellas, P., Eberhagen, N., Skourlas, C., & Giannakopoulos, G. (2014). The human factor of information security: Unintentional damage perspective. *Procedia-Social and Behavioral Sciences*, *147*, 424-428.

Miller, G. J., & Yang, K. (2007). *Handbook of research methods in public administration*. CRC press.

Mitnick, K. D. & Simon, W. L. (2002). The art of deception: Controlling the human element of security John Wiley & Sons.

Mitzen, J. (2006). Ontological security in world politics: State identity and the security dilemma. European Journal of international relations, 12(3), 341-370.

Moon, Y. J., Choi, M., & Armstrong, D. J. (2018). The impact of relational leadership and social alignment on information security system effectiveness in Korean governmental organizations. International Journal of Information Management, 40, 54-66.

Neumann, P. G. (1999). Risks of insiders. Communications of the ACM, 42(12), 160-160.

Ning, H., Liu, H., & Yang, L. (2013). Cyber-entity security in the Internet of things. Computer, 1.

Okoli, C., & Schabram, K. (2010). A guide to conducting a systematic literature review of information systems research.

Parsons, K., McCormac, A., Butavicius, M. & Ferguson, L. (2010). No title. Human Factors and Information Security: Individual, Culture and Security Environment.

Partridge, E. (2003). *A dictionary of Clichés*. Routledge.

Petticrew, M. (2001). Systematic reviews from astronomy to zoology: myths and misconceptions. *Bmj*, *322*(7278), 98-101.

Redman, T. C. (2008). *Data driven: profiting from your most important business asset*. Harvard Business Press.

Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A. & Herawan, T. (2015a). Information security conscious care behaviour formation in organizations. Computers & Security, 53, 65-78.

Safa, N. S., Von Solms, R. & Futcher, L. (2016). Human aspects of information security in organisations. Computer Fraud & Security, 2016(2), 15-18.

Safa, N. S., Von Solms, R. & Furnell, S. (2016). Information security policy compliance model in organizations. Computers & Security, 56, 70-82.

Sahibudin, S., Sharifi, M., & Ayat, M. (2008, May). Combining ITIL, COBIT and ISO/IEC 27002 in order to design a comprehensive IT framework in organizations. In Modeling & Simulation, 2008. AICMS 08. Second Asia International Conference on (pp. 749-753). IEEE.

Salminen, A. (2011). Mikä kirjallisuuskatsaus?: Johdatus kirjallisuuskatsauksen tyyppeihin ja hallintotieteellisiin sovelluksiin.

Saltzer, J. H., & Schroeder, M. D. (1975). The protection of information in computer systems. Proceedings of the IEEE, 63(9), 1278-1308.

Sarkar, K. R. (2010). Assessing insider threats to information security using technical, behavioural and organisational measures. *information security technical report*, *15*(3), 112-133.

Sasse, M. A., Brostoff, S. & Weirich, D. (2001). Transforming the 'weakest link'—a human/computer interaction approach to usable and effective security. BT Technology Journal, 19(3), 122-131.

Schneier, B. (2000). *Secrets and lies: digital security in a networked world*. John Wiley & Sons.

Sen, R., & Borle, S. (2015). Estimating the contextual risk of data breach: An empirical approach. *Journal of Management Information Systems*, *32*(2), 314-341.

Silic, M., & Back, A. (2013, June). Information security and open source dual use security software: trust paradox. In IFIP International Conference on Open Source Systems (pp. 194-206). Springer, Berlin, Heidelberg.

Simpleman, L., McMahon, P., Bahnmaier, B., Evans, K., & Lloyd, J. (1998). Risk management guide for DOD acquisition. DEFENSE SYSTEMS MANAGEMENT COLL FORT BELVOIR VA.

Slay, J., & Miller, M. (2007, March). Lessons learned from the maroochy water breach. In *International Conference on Critical Infrastructure Protection* (pp. 73-82). Springer, Boston, MA.

Smith, A. D., & Rupp, W. T. (2002). Issues in cybersecurity; understanding the potential risks associated with hackers/crackers. *Information Management & Computer Security*, *10*(4), 178-183.

Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. *Computers & security*, *24*(2), 124-133.

Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. Journal of network and computer applications, 34(1), 1-11.

Schultz, E. E., Proctor, R. W., Lien, M. C., & Salvendy, G. (2001). Usability and security an appraisal of usability issues in information security methods. *Computers & Security*, *20*(7), 620-634.

Sumner, M. (2009). Information security threats: a comparative analysis of impact, probability, and preparedness. *Information Systems Management*, *26*(1), 2-12.

Talib, S., Clarke, N. L., & Furnell, S. M. (2010, February). An analysis of information security awareness within home and work environments. In *2010 International Conference on Availability, Reliability and Security* (pp. 196-203). IEEE.

Telang, R., & Wattal, S. (2007). An empirical analysis of the impact of software vulnerability announcements on firm stock price. IEEE Transactions on Software Engineering, (8), 544-557.

Thomson, K., & Van Niekerk, J. (2012). Combating information security apathy by encouraging prosocial organisational behaviour. *Information Management & Computer Security*, *20*(1), 39-46.

Trautman, L. J., & Ormerod, P. C. (2016). Corporate Directors' and Officers' Cybersecurity Standard of Care: The Yahoo Data Breach. Am. UL Rev., 66, 1231.

Von Solms, R. (1998). Information security management (3): the code of practice for information security management (BS 7799). Information Management & Computer Security, 6(5), 224-225.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. computers & security, 38, 97-102.

Vroom, C. & Von Solms, R. (2004). Towards information security behavioural compliance. Computers & Security, 23(3), 191-198.

Warkentin, M., & Willison, R. (2009). Behavioral and policy issues in information systems security: the insider threat. *European Journal of Information Systems*, *18*(2), 101-105.

West, R., Mayhorn, C., Hardee, J. & Mendel, J. (2009). The weakest link: A psychological perspective on why users make poor security decisions. Social and human elements of information security: Emerging trends and countermeasures (s. 43-60) IGI Global.

Whitman, M. E. (2003). Enemy at the gate: threats to information security. *Communications of the ACM*, *46*(8), 91.

Whitman, M. E., & Mattord, H. J. (2011). Principles of information security. Cengage Learning.

Wilson, M. & Hash, J. (2003). Building an information technology security awareness and training program. NIST Special Publication, 800(50), 1-39.

Workman, M., Bommer, W. H. & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. Computers in Human Behavior, 24(6), 2799-2816.

Xu, W., Grant, G., Nguyen, H., & Dai, X. (2008). Security Breach: The Case of TJX Companies, Inc. *Communications of the Association for Information Systems*, *23*(1), 31.

Yeh, Q. J., & Chang, A. J. T. (2007). Threats and countermeasures for information system security: A cross-industry study. Information & Management, 44(5), 480-491.

Zhang, J., Reithel, B. J., & Li, H. (2009). Impact of perceived technical protection on security behaviors. *Information Management & Computer Security*, *17*(4), 330-340.

Zins, C. (2007). Conceptual approaches for defining data, information, and knowledge. *Journal of the American society for information science and technology*, *58*(4), 479-493.

Ö□ütçü, G., Testik, Ö. M., & Chouseinoglou, O. (2016). Analysis of personal information security behavior and awareness. *Computers & Security*, *56*, 83-93.

Internet sources

AusCert (2004).Australian Computer Crime and Security Survey, 2004. Accessed 29.12.2018 from **http://www.ncjrs.gov/App/publications/abstract.aspx?ID=205693**

Briney A. (2001). Information security industry survey. Accessed 13.12.2018 from **http://lfca.net/Reference%20Documents/2001%20Information%20Security%20Survey.pdf**

Curry, S. (2011), "The weakest link is the human link". Accessed 17.3.2019 from

https://www.securityweek.com/weakest-link-human-link

Deloitte (2009). Protecting what matters The 6th Annual Global Security Survey. Accessed 29.12.2018 from **https://www.iasplus.com/en/binary/dttpubs/2009securitysurvey.pdf**

Ernst & Young (2008). Moving beyond compliance, Ernst & Young's 2008 Global Information Security Survey. Accessed 29.12.2018 from http://130.18.86.27/faculty/warkentin/SecurityPapers/Merrill/2008_E&YWhitePaper_GlobalInfoSecuritySurvey.pdf

Meglena Kuneva, European Consumer Commissioner, Keynote Speech, Roundtable on Online Data Collection, Targeting and Profiling. Accessed 05.03.2019 from http://europa.eu/rapid/press-release_SPEECH-09-156_en.htm

PriceWaterhouseCoopers (2006). information security breaches survey 2006. Accessed 29.12.2018 from https://webarchive.nationalarchives.gov.uk/+/http:/www.dti.gov.uk/files/file28343.pdf

ATTACHMENT 1 LIST OF CHOSEN ARTICLES

Title	Author(s)	Year
The weakest link revisited [information security]	Arce, I.	2003
Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness	Bulgurcu, B., Cavusoglu, H., & Benbasat, I.	2010
A cross-cultural investigation of situational information security awareness programs	Chen, C. C., Dawn Medlin, B., & Shaw, R. S.	2008
A framework for human factors in information security	Gonzalez, J. J., & Sawicka, A.	2002
Uncertainty in the Weakest-Link Security Game	Grossklags, J., & Johnson, B.	2009
Social and Human Elements of Information Security: Emerging Trends and Countermeasures	Gupta, M.	2008
A review of social media security risks and mitigation techniques	He, W.	2012
A Survey of Factors Influencing People's Perception of Information Security	Huang, D. L., Rau, P. L. P., & Salvendy, G.	2007
Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition	Ifinedo, P.	2014
Human and organizational factors in computer and information security: Pathways to vulnerabilities	Kraemer, S., Carayon, P., & Clem, J.	2009
Social Engineering: The Neglected Human Factor for Information Security Management	Luo, X., Brody, R., Seazzu, A., & Burd, S.	2011
Why you should care about the Target data breach	Manworren, N., Letwat, J., & Daily, O.	2016
Information security culture	Martins, A., & Elofe, J.	2002
The art of Deception: controlling the human element of security	Mitnick, K. D., & Simon, W. L.	2002
Analysis of personal information security behavior and awareness.	Öğütçü, G., Testik, Ö. M., & Chouseinoglou, O.	2016
Human Factors and Information Security: Individual,	Parsons, K., McCormac, A., Butavicius, M., & Ferguson, L.	2007

Culture and Security Environment		
Information security policy compliance model in organizations	Safa, N. S., Von Solms, R., & Furnell, S.	2015
Human aspects of information security in organisations	Safa, N. S., Von Solms, R., & Futcher, L.	2016
Transforming the 'weakest link'—a human/computer interaction approach to usable and effective security	Sasse, M. A., Brostoff, S., & Weirich, D.	2001
Secrets and Lies: Digital Security in a Networked World	Schneier, B.	2000
Estimating the contextual risk of data breach: An empirical approach	Sen, R., & Borle, S.	2015
Lessons learned from the maroochy water breach	Slay, J., & Miller, M.	2007
A survey on security issues in service delivery models of cloud computing	Subashini, S., & Kavitha, V.	2011
Information security threats: a comparative analysis of impact, probability, and preparedness	Sumner, M.	2009
An analysis of information security awareness within home and work environments	Talib, S., Clarke, N. L., & Furnell, S. M.	2010
Towards information security behavioural compliance	Vroom, C., & Von Solms, R.	2004
The weakest link: A psychological perspective on why users make poor security decisions	West, R., Mayhorn, C., Hardee, J., & Mendel, J.	2009
Enemy at the gate: threats to information security	Whitman, M. E.	2003
Security lapses and the omission of information security measures: A threat control model and empirical test	Workman, M., Bommer, W. H., & Straub, D.	2008
Security Breach: The Case of TJX Companies, Inc	Xu, W., Grant, G., Nguyen, H., & Dai, X.	2008
Impact of perceived technical protection on security behaviors.	Zhang, J., Reithel, B. J., & Li, H.	2009