LUISS

Department of Business and Management
Degree Program in Management and Computer Science

Course of Digital Business and Workplace Technology

Cybersecurity and Human Behavior: Are Humans the Weakest Link?

Prof. Paolo Spagnoletti

SUPERVISOR

Shefik Memedi 286861

CANDIDATE

Academic Year 2024/2025

Acknowledgments

I would like to express my heartfelt gratitude to Professor Paolo Spagnoletti for his invaluable guidance and expertise in finishing this thesis.

This thesis is dedicated to my mother, father, sister, and entire family for their unwavering trust in my abilities. Their encouragement has been a constant source of motivation throughout my academic journey.

Contents

Abstract

In this conceptual work, an attempt is made to demonstrate the theoretical misunderstandings in explaining the role of human behavior in the field of cybersecurity. In demonstrating these theoretical misunderstandings, we will mainly refer to the application of psychological theories in understanding and explaining the human behavior in the context of cybersecurity. In doing this, we will rely mainly on a literature review on studies conducted in the last two decades in explaining the human nature and behavior when dealing with the issue of multiple breaches in the field of cybersecurity. It is our belief that the hypothesis of human behavior being the weakest link in the context of cybersecurity should be taken with reservations, hence, we need a new paradigm shift in explaining cybersecurity breaches. We agree that the human element cannot be overlooked, but we do maintain that we are in a dire need of a balanced approach between hardening the technical systems and incentivizing secure human behavior. An in depth understanding of cybersecurity behavior is vital to identifying anomalies and preventing cyberattacks.

Keywords: Information security, cybersecurity, hacking, human behavior, weakest link, literature review.

Chapter I

Introduction

The world we live in today, without any doubt, cannot function without the use of computers, cellphones, and internet. All over the world, impacts of information technology have been felt regardless of the location. Using information technology is a way of life and connects people to what's new and popular. Without any doubt, people have gained benefits from information technology and cyber advances that held in the growth of the production industry such as energy, retail, transportation, technology, healthcare, banking, governmental institutions, education, and many other fields. Information technology, therefore, is valuable and critical to the modern society. Looking at it from this perspective then, information technology is meant to progress the world around us and give benefits to society in numerous ways.

However, this huge surge in interest and acceptance of information technology did not happen without leaving huge gaps in using or misusing this great advancement of the technology, because, as already witnessed on many occasions throughout human history, human beings have a great capacity to use, as well as misuse, the advancement of human knowledge, with special focus on the advancement of information technology. This is evident due to the large numbers of significant security incidents and data breaches that are being publicized on a regular basis. As a result of the continuing publication of high-profile security breaches, organizations are increasing attention and looking for ways to improve their assurance in order to protect their brand and reputation, as well as to prevent or reduce the associated financial implications.

As a consequence of this, although this was not the case at the beginnings of cybersecurity research, in the last two decades we are faced with an explosion of research by cybersecurity scholars who have started observing that the human element cannot be overlooked when dealing with numerous breaches in the field of cyber security. According to them, not only is human behavior one of the biggest risks to a secure network, but understanding typical behavior is vital to identifying anomalies and preventing cyber-attacks. Therefore, many scholars in the field of cyber security, intentionally or unintentionally, started blaming the human behavior whenever faced with situations of explaining numerous attempts of cybersecurity breaches. In other words, various scholars of information technology started hypothesizing, and today making it an all

accepted norm, that the "human behavior is the weakest link."

For the sake of the argument, we can say that most of these studies and reports about the "weakest link" narrative are coming due to the increasing number of cyber incidents, hence it is assumed that "human error" is to be blamed for this unstopping phenomenon. According to these studies and reports conducted in the last two decades, humans are considered the greatest vulnerability to security Schneier [2004]; Furnell and Clarke [2012] . One report, for example, estimated that 95% of cyber and network attacks are due to human errors Nobles [2018]. According to the IBM [2015] Cyber Security Intelligence Index, human error was responsible for 9 out of every 10 information security incidents that year IBM [2015]. A follow-up study by IBM Security [2019] examined the top three root causes (malicious or criminal attack, system glitch, and human error), which shows that human error accounted for 24% of them IBM Security [2019]. Another report coming from Verizon's 2023 Data Breach Investigations Report Verizon [2023], an astounding 74% of all data breaches involve the human element. Even more astonishingly, email serves as the attack route in 98% of all social engineering incidents, which include widespread phishing campaigns. Evans et al. [2016], for example, found that in 2014, approximately 50% of the world's worst data breaches resulted from unsuspecting human error. This work by Evans et al. [2016] showed that half of the significant security incidents result from specific elements, including users and unintentional errors. In short, it is worth noting that almost all of these studies and reports into the role of humans in cybersecurity see human as the problem rather than the solution Triplett [2022].

In this context, therefore, most research on this area focused on errors done by computer system users (King et al. [2018]; Andrade and Yoo [2019]). In other words, according to the majority of these studies and reports, company employees are treated as the "weakest link" in ensuring system security (for more see, to Ifinedo [2014]; Sasse et al. [2004]; Vroom and Von Solms [2004]; Stanton et al. [2005]; Guo et al. [2011]. These alarming numbers, maintain proponents of this approach, underline the exploitation of human psychology by threat actors to devise precise and sophisticated attacks. Through creative techniques, maintain these researchers, these actors manipulate individuals into compromising security by either disclosing confidential information or engaging with malicious content. Because of these astounding numbers in the breaches in the cybersecurity, proponents of this approach started to hypothesize and coined the term "human beings are the weakest link" in information security. In fact, the viewpoint that the "human is the weakest link" today continues to be arguably the most prominent view within industry and research (Goo et al. [2014]; Hughes-Lartey et al. [2021]; Lowry and Moody [2015]; Sabillon [2022]).

However, we maintain that this narrative that has grown and become a norm today, is still in its infancy stage and requires further investigation. We think that the simplification and the easiness in which the human behavior has been, and continues to be blamed as the "weakest link" in the context of cybersecurity, solely on the basis of numerous breaches in the cybersecurity is scientifically incorrect, and does not offer any practical usefulness to the breaches in cybersecurity. In this regard, today we have a plethora of research that attempt to demonstrate that "human as the weakest link" discourse is not only unhelpful but largely invalid (Beautement and Sasse [2009]; Inglesant and Sasse [2010]; Nurse et al. [2011]; Weirich and Sasse [2001]). The research, therefore, reflects a need for more 'positive' security research and dialogue, both within academia and industry Zimmermann and Renaud [2019]. In this regard then, understanding human behavior's role in cybersecurity is of paramount importance in recognizing common threats that might often originate from simple mistakes or misunderstandings; rather than just blaming everything on the human being as the "weakest link."

Having said this, it is our impression that these existing studies on the "weakest link" phenomenon have made profound impacts that lead scholars thinking about a paradigm shift Kuhn [1996] in cybersecurity behavior research, by shifting research attention from the technological or organizational capacity to the human ability, in order to aim for protection and effectively and efficiently defend the use of cyberspace from cyberattacks. This change in emphasis from technology and organization to human behavior, therefore, shifted furthermore research attention from cybersecurity professionals to ordinary cyber users. In doing so, this shifted research attention from building the strongest system, to tackling the weakest link in order to improve cybersecurity effectiveness. However, as it is going to be demonstrated in this conceptual study, this is both dangerous and incorrect, and therefore we need a new paradigm shift of returning to the original work on building strong platforms and protocols to having a secured information technology, organizational network, and at the same time, using the "strongest link" in human behavior in building a technology that is not only secure, but at the same time beneficial for the development of human knowledge.

In this conceptual work, therefore, an attempt will be made to demonstrate that the narrative of "human behavior being the weakest link" is grounded on an inadequate explanation of the cybersecurity behavior, and that this premise has produced an incorrect direction for many cybersecurity scholars in explaining and concluding about the "nature" of human behavior when dealing with numerous breaches in cyber security. It is our belief that this explanation of the human behavior as the "weakest link" should have produced by now a practical solution to the ever increasing cyber breaches, but this is not the case. Having in mind the everyday facts that information security management

did not offer any recipe to cybersecurity because of the continuous increase in the gaps and weaknesses within industry and practice Evans et al. [2016], we are obliged to see what went wrong, and hopefully offer functional solutions to the ever increasing incidents in the field of cybersecurity. Of course, we do agree and believe that expertise in the behavioral analysis should be increased and become an important aspect of cybersecurity education programs, but what we noticed in the cybersecurity research of the last two decades is the inadequate explanation of the human behavior as the "weakest link," and the fact that this approach has not produced any practical solutions to the increasing numbers of breaches in the field of cyber security.

In demonstrating this inadequate and incorrect explanation of the human behavior as the "weakest link", we are going to tackle the thesis through two responses that we believe are of crucial importance in understanding rightly the nature of human behavior when attempting to offer solutions to cybersecurity breaches. Firstly, while conducting a literature review on cybersecurity and human behavior, we have observed that the premise of the "weakest link" narrative is not supported by empirical studies. In other words, the continuous repetition of this narrative that has grown into a norm today, is being defended solely by certain surveys and general assumptions conducted by certain organizations and companies that human behavior is the "weakest link" since cybersecurity breaches continue to happen at an alarming rate. As it is going to be demonstrated in the following chapters, beyond some surveys and reports, there is hardly any real-scientific study that would take into consideration all possible factors that might influence data breaches and incidents, like technology, organizations, governments, policies, environment, and many other possible factors. We maintain that all these factors must be studied accordingly in relation to breaches in cybersecurity if we want to build a strong causal relationship between all these elements and breaches in cybersecurity. Without this real-based research, we claim that this explanation is not adequate and sufficient, hence the "weakest link" narrative needs to be detached from the cybersecurity research, if we really want to find solutions to the numerous breaches and incidents in the field of cybersecurity.

Secondly, from the systematic literature review that will be demonstrated in the following chapter, it may be easily deduced that the proponents of the "weakest link" narrative have already accepted this narrative as an accepted norm, therefore many scholars of the field rushed in using and implementing many psychological theories in order to understand and improve human behavior. As it is going to be demonstrated in the following chapters, in the last two decades, we have an explosion of studies where scholars of information systems research are using many psychological theories, in particular behavioral theories, in order to understand and improve human behavior in the context of

cybersecurity. We believe that there is nothing wrong in using behavioral theories in explaining the human behavior in the context of cybersecurity because of the interdisciplinary nature of the field in question. However, we maintain that this can be done only after you demonstrate the real causal relationship between "human behavior" and the "weakest cybersecurity link" which in our case here is definitely lacking. As a result of this, we believe that the research studies conducted in the last two decades have done a great job in understanding better the human behavior in the context of cybersecurity, but practically speaking these research studies are of no help in dealing with the "weakest link" narrative, hence having a more secured cyber space. We maintain that the uses of these psychological theories in understanding better the human behavior is offering a weak solution to the "weakest link" narrative.

Moreover, having in mind that we believe that the "weakest link" narrative is not offering any solution to the increasing problem of cybersecurity breaches and incidents, in the third part, therefore, we offer a balanced view to the ever-increasing number of data breaches. In other words, in order to have a more secured cyber space, we propose a balanced approach of treating and considering with full care and attention all the factors that play an important role in the field of cyber security. We propose to replace the linear narrative of the "weakest link" as a solution to the already existing problem of data breaches, therefore, we propose that scholars of the field need to move away from blaming the human behavior for all the ills that are happening with regard to the cybersecurity incidents and breaches, and focus more on conducting studies in understanding and improving the cyber space, by concentrating on all the possible factors that play a role in the organizational context. In taking this balanced and non-linear approach, of course, we rely firstly on the ground breaking theory of organizational behavior by March and Simon [1958], which emphasizes the role of organizational structure, processes, and social influences in shaping individual behavior and decision-making. As a result of this complexity, therefore, we can say here that the uses of psychological theories and methods to understand and explain human behavior in cybersecurity, is not adequate in explaining and offering solutions to the ever-increasing phenomenon of cybersecurity breaches. This is so because todays organizations requires considering the interplay between technology and society as crucial pillars in understanding better the field of cyber space, and hopefully offer better solutions to the ever-increasing phenomenon of cybersecurity breaches. At the same time, in proposing such a balanced approach, we rely also on the theoretical contributions made by Hanseth and Ciborra [2007], which provide a lens for analyzing the dynamic, shared, and often unpredictable nature of the technological underpinnings of modern life, highlighting the crucial interplay between technology, people, and organizations in their evolution and use. By grounding our ar-

gument in these two theories, therefore, we hope to offer a better answer to our research question of the "human behavior being the weakest link," and hopefully provide a better solution to the ever-increasing data breaches and incidents in cybersecurity.

Certainly, the field of psychology has plenty of theories and empirical data to explain differently the human nature, and move away from this deterministic and pessimistic view of human behavior in various organizational settings, but at the same time, there is a need for having a more balanced approach with regard to other important factors, like technology, policies, governments, organizations. All these factors must be treated accordingly by the scholars of the field, if we want to have a more robust and secured cyber space. The actual approach of the "weakest link" narrative does not offer a positive picture in this regard. In this work, therefore, through systematic literature review, an attempt will be made to recognize and understand these gaps and weaknesses within the research offered on cybersecurity and human behavior, having in mind the continuous significant security incidents and data breaches that are being publicized on a daily basis, without a clear solution yet to be offered. This will be done after problematizing the "weakest link" hypothesis, as the only solution to the existing problem of cybersecurity breaches.

1.1 The research aim of this work

The aim of the current research is to provide insights about the current direction taken by many scholars of information systems and cybersecurity when attempting to explain the nature of the human behavior being the "weakest link" in the context of cybersecurity breaches. Through this research aim, an attempt will be made to demonstrate that the hypothesis of the "weakest link" remains just a general assumption and a claim without a scientific-based research. The numerous studies in the last two decades in using and applying psychological theories and methods in order to understand and hence improve human behavior do not relate to the "weakest link" phenomenon. In achieving this aim, therefore, we hope to demonstrate the fact that this kind of approach proposed by many scholars of the field in question, has not offered any solution to the increasing number of breaches in cyber security. We continue to be faced with thousands of data breaches every single day. In reaching this research aim, therefore, we are going to rely mainly on a systematic literature review of numerous studies conducted in the last two decades in the field of cybersecurity and human behavior.

In this regard, the aim of this conceptual work is to provide new insights into the question: "Is human behavior the weakest link in information security?" In answering this question, we will rely on a systematic literature review. By answering this research

question, organizations 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, we hope, will help organizations determine if they are trusting the wrong assumptions in order to manage their information security. In order to find the answer to this question, therefore, the literature related to the subject and the research question must be carefully reviewed. To address these problems in an organized way, the study will rely solely on a systematic literature review. In this way, we hope that this literature review will also provide a critical view of the current literature and challenges the generalizations made within.

In this work, therefore, we argue that while many of the articles stress that "human is the weakest link in information security", for example, Schneier [2000]; Mitnick and Simon [2002]; Vroom and Von Solms [2004]; Bulgurcu et al. [2010], Chen et al. [2008], they have not justified this claim with any direct scientific evidence. In the following chapter, therefore, we are going to examine some of these articles and see how they have used generalizations in their text but have not justified their arguments in any way possible. As it is going to be demonstrated, most of these articles deal with changes and possibly improvement of the human behavior, without bothering much to defend the causal relationship between the "weakest link" narrative and the breaches in cybersecurity. In this work, therefore, an attempt will be made to demonstrate how causality is used by these researchers to explain these complex situations, whereas in fact there are many factors that can affect the situation and other factors, but that all of these factors have been ignored by various scholars of the field.

Therefore, the research aim of this theoretical work is to present the state of the art of the research conducted in the last two decades in the context of cybersecurity and human behavior. This state of the art is going to be represented through systematic literature review research. By using the method of literature review, an attempt will be made to contribute to the existing theoretical research on cybersecurity and human behavior, with special focus on finding better solution to the numerous breaches on cybersecurity. In other words, the aim of this theoretical research is a modest contribution in seeing whether the thesis of the "human behavior being the weakest link" is being defended without reasonable doubt, and hopefully to initiate a new paradigm shift with regard to finding solutions to cybersecurity breaches. It is further argued that when security measures and policies have failed previously, it is because they were not usable or workable, not because the human is an inherent 'weakness' in cyber-security processes.

In achieving these aims, we organize this work in different chapters, in order to have a clear picture of all these undertakings. In this sense therefore, in Chapter 2, we present the most up-to-date literature review of the theoretical work done in studying cyberse-

curity and human behavior. In Chapter 3, we discuss the ways in moving forward from the current state of the art in the topic of the "weakest link" phenomenon in the context of the cybersecurity and human behavior. Here, an attempt will be made to offer a different perspective and solution with regard to breaches in cybersecurity. Finally, in Chapter 4, we will try to provide certain concluding remarks with regard to future research on cybersecurity and human behavior, with special attention on the "weakest link" phenomenon.

Chapter II

Literature Review on the "Weakest Link" Narrative

In this chapter, we will present the literature review on the "weakest link" narrative by focusing exclusively on the systematic literature review. Before dealing with this topic, however, we will explain methodology and the research process of this study, in order to have a full picture of the rationale for opting for this research method and the related steps.

2.1 Systematic literature review

We have to make it clear at the outset that the research method used in this particular study is the literature review, with special emphasis on systematic literature review. According to Baumeister and Leary [1997], one of the goals of literature review is problem identification and more specifically, finding problems or weaknesses from the existing literature. A systematic literature review is a structured, methodical, and comprehensive way of collecting, evaluating, and synthesizing research on a specific topic or research question. In other words, this kind of literature review, unlike other traditional literature reviews, follows a clear, predefined protocol to minimize bias and ensure replicability of the study. The goal of this particular literature review is to summarize existing evidence on a particular topic. In doing this, a researcher aims to identify possible research gaps of this particular evidence, and possibly propose a new framework, or keep a balance between the two. In this way, there is a hope that the researcher supports decision-making in policy or practice, and possibly provide a base for future research.

The goal of this this study, therefore, is to find weaknesses and problems of the particular area of humans in information security, with special focus on the "weakest link" hypothesis, and hopefully provide a new conceptual framework of dealing better with overall breaches in cyber security. Based on these identified goals, therefore, we 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 causal relationships due to many different factors that might influence the topic in question. Through systematic literature review, therefore, we hope to get a good understanding of the cybersecurity

and human behavior landscape in academic literature and observe if the general narrative that humans are the "weakest link" is supported by scientific evidence.

The aim of this systematic literature review is to have an overview of scholarly work conducted in the context of cybersecurity and human behavior in order to understand the ways how the scholars of the field treated the complexity of human behavior in the field of cybersecurity. In this way, this literature review narrows its focus by drawing on theory and research grounded in psychology, when attempting to understand and explain numerous breaches in the field of cyber security. By drawing on such cyber-security fields, the current literature review looks at how previous research on cybersecurity and human behavior has influenced the study of human factors being the "weakest link" with regard to breaches in cybersecurity. In doing so, as explained briefly in the previous chapter, we hope to identify gaps in the research studies, and recognize the incorrect direction taken in proposing solutions to numerous cybersecurity breaches that continue to happen on a daily basis, regardless that these solutions have been identified over two decades now. Much of this literature, of course, comes from the broader umbrella field of studies in cybersecurity and human behavior.

For this work at hand, therefore, we have decided to select for analysis and evaluation papers from year 2000 onwards, having in mind that the research question is so broad that it needs more space to support it, which we do not have it for this undergraduate thesis. The year of publishing has been limited from 2000 and onwards, having in mind that in this period of time of just over two decades we have an explosion of research studies in cybersecurity and human behavior. In addition, almost 20 years is enough to find out whether the "weakest link" narrative is rooted in the past or whether it has become common only in recent years. Moreover, in order to improve the reliability of the research, we will only accept publications that are mainly from academic sources, with occasional reference from non-academic source, whenever needed to support our conceptual framework. All the papers that are used in the research have to be related to information security because the research question pertains only to cyber security. In order to find the answer for the research question, all the papers must discuss the role of humans or human factors in cybersecurity, because otherwise they are not relevant to the study.

In this regard, we decided to use Scopus which is a huge multidisciplinary database with citations and abstracts from peer-reviewed journal literature, trade journals, books, patent records, and conference publications, with the following keywords, "weakest link in cybersecurity", "humans as the weakest link", "human error cybersecurity", "psychological theories in cybersecurity", and organizational factors to cybersecurity breaches. With regard to the first keyword of "weakest link in cybersecurity", we got in

total 183 results, of which 46 were academic articles, all published from year 2000 and onwards. The second keyword of "humans as the weakest link" resulted in 545 findings, of which 342 academic articles. The third keyword being "human error cybersecurity" resulted in total of 380 findings, of which 124 were academic articles. "Psychological theories in cybersecurity" resulted with 68 findings, of which 32 were scientific articles. The final keyword of "organizational factors in cybersecurity breaches" provided 45 results, of which 23 were academic articles. We have to mention here, however, that due to the limited space allocated for this undergraduate thesis, it is not possible to include all these findings and academic articles as part of this literature review. In this systematic literature review, therefore, we are going to review only certain articles pertaining directly to the research question of the "weakest link", which is around 30 books and articles, with the hope that these scientific articles are representative for all other remaining articles dealing with the narrative of the "weakest link."

In the table below we present the search results per keyword in order to have a better picture of the entire material collected from the Scopus multidisciplinary database:

Keyword on Scopus	**Total results**	**Academic articles**
Weakest link in cybersecurity	183	46
Humans as the weakest link	545	342
Human error cybersecurity	380	124
Psychological theories in cybersecurity	68	32
Organizational factors in cybersecurity breaches	45	23
Total	**1221**	**567**
Total selected	**163**	**30**

Table 2.1: Search results per keyword

We have to mention here that the rationale behind this kind of selection of the academic articles to be incorporated in the literature review for in depth analysis, stems from our research question dealing exclusively and directly with the phenomenon of the "weakest cybersecurity link," which is just over 100 academic articles. We hope that this selection of 30 articles is a good representation of all the remaining articles not being covered here in this undergraduate thesis. The reason for the exclusion of other articles, in total 567 articles, was mostly due to the wrong context; articles which did not fit the criteria of practicality and quality appraisal, and there were also a few that were not academic papers.

2.2 The origins of "weakest link" narrative

Before we start reviewing the literature on the "weakest link" narrative, that Sasse et al. [2001] has defined it as a phenomenon that ordinary users rather than cybersecurity technologies is the ultimate source of most cybersecurity breaches and thus they are the weakest link in the cybersecurity chain, it would be important to see the background and the origins of this premise, in order to have a full picture of the topic in question. Although tracing the origin of this narrative is not our primary target here in this work, still we hope that this background information will help to have a better grasp and understanding of the analysis and evaluation of the literature review on the topic later in this chapter. In fact, we hope that by tracing the potential origins that give rise and dominance to this narrative, will help us to better understand the implications that this premise has on viewing the presence of human behavior in the cybersecurity circle. Although it is difficult, if not impossible, to find the exact origins of the notion that "human is the weakest link" Soliman and Järveläinen [2024], still we can say that this term was coined by people who saw in humans problems in the production line and are often the first to blame in the breaches in cybersecurity. In this line of reasoning then, there is a clear indication that roots of this narrative could be rooted in writings that are influenced by Taylor's scientific management Braverman [1998].

Another possibility of tracing the origins of this narrative might be coming from Schein [1996], who coined the term "engineering culture." According to Schein [1996], who has worked extensively on culture, when he talks about "engineering culture" he refers to the "designers of the technology underlying the work," and this kind of education "reinforces the view that problems have abstract solutions and that those solutions can, in principle, be implemented in the real world with products and systems free of human foibles and errors" (p. 14). Similar view in the cybersecurity discourse was noticed by Ebert et al. [2023] when they claimed that during scientific management of Taylorism, "human operators were framed as a problem to be controlled by enforcing compliance with rules and penalizing violations" (p. 2). This kind of thinking, of course, today has led many other authors to remove human element from the equation altogether because the human error is the biggest threat, accounting for over 80% of incidents and cybersecurity breaches Chamorro-Premuzic [2023]. It is our belief that by tracing back the origins of the "weakest link" narrative to this line of reasoning, these researchers opened a new way of thinking with regard to bringing into equation the artificial intelligence to be the tool that helps businesses keep human negligence in check by relying on machine intelligence to de-risk human behavior Chamorro-Premuzic [2023]. Since this is totally a new topic that requires special attention and treatment, we are

mentioning here superficially only to demonstrate the link between the "weakest link" narrative and its trace in the "engineering culture" mentioned above.

Since the primary aim of this work is not tracing the roots of this narrative, however, we can skip this and other related background information, and jump directly to when this premise got firstly coined as the "weakest link" in the field of cybersecurity. In this regard, the "weakest link" phenomenon was firstly coined in the field of cybersecurity by Schneier [2000], when he said that "People often represent the weakest link in the security chain and are chronically responsible for the failure of security systems" (Schneier [2000], p. 149). According to Mc Mahon [2020], Schneier is considered as an influential cybersecurity expert who has published several books on the topic and regularly writes blogs on cybersecurity issues. Although it is unlikely that the origins of this narrative are coming directly from Schneier, still we can claim that he has influenced a wide distribution of the "human as the weakest link" narrative. Around the same time period, Mitnick and Simon [2002] maintained a similar point by comparing cybersecurity to home security, and how people install locks in order to feel safe, and no matter what is put in place, the home remains essentially vulnerable, because "the human factor is truly security's weakest link." The proponents of this premise on many occasions even refer to Kevin Mitnick, one of the most famous computer hackers, which offered an insider's view when he testified before the Congress after spending five years in prison, stating: "The human side of computer security is easily exploited and constantly overlooked. Companies spend millions of dollars on firewalls, encryption and secure access devices, and its money wasted, because none of these measures address the weakest link in the security chain" Poulsen [2000].

In short, the idea that "humans are the weakest link" has dominated academic and industrial space of security information systems for over two decades. While its philosophical origins predate the industry by several decades, for our present purposes we need to go back no further than the beginning of this millennium. The influences of these scholars are such that this phrase developed significant prevalence in information security circles, though it was likely an already common trope in physical security discourse. However, from what has been presented in these studies and reports, it is our belief that there is no scientific justification of the assumption that humans are the "weakest link." The authors generalize that human behavior is "the weakest link", but there is no scientific reference in making such a claim. We argue that by making this claim, authors are obliged to offer scientific proof and evidence, but we only see implicit claims that human beings make mistakes and that these mistakes cause problems to organizations. The reader is left with the idea that humans are the "weakest link," solely on the basis that security breaches are happening. Therefore, it is of paramount

importance to review the existing literature on the "weakest link" narrative in order to have a full picture of the topic at issue.

2.3 Human behavior as the "weakest link" in the literature

In the field of cybersecurity, human behavior was mainly viewed through lenses and theories borrowed from disciplines such as criminology, D'Arcy and Greene [2009], Straub [1990], psychology Moody et al. [2018], Herath and Rao [2009], health psychology Boss [2015], Johnston et al. [2015], Liang and Xue [2010], Jiang et al. [2016], Verkijika [2018], and moral philosophy Siponen [2001], just to mention a few. The application of these theories from other disciplines has raised questions regarding their applicability in behavioral cybersecurity Crossler et al. [2013], Truex [2006], and we are going to discuss these implications in the following sections accordingly. For now, it is sufficient to say that several frameworks or theories have been applied to research human behavior in the field of cybersecurity. Of course, these and many other studies are just a few examples of over 500 empirical articles on cybersecurity behavior published in a wide variety of general interdisciplinary journals, such as Nature, Science, and New England Journal of Medicine; cyber behavior research journals, like Behavior & Information Technology, Cyber-psychology, Behavior, and Social Networking, Computers & Education; and cybersecurity technology journals, like Computers and Security, Computer Fraud and Security, Journal of Information Security and Application; Journal of Cybersecurity, International Journal of Information Security, MIS Quarterly, Journal Information Systems Research, and Network Security.

Of these over 500 empirical articles, approximately over 100 journal articles have been published, explicitly specifying the phenomenon of the "weakest link" Hinde [2001] Sasse et al. [2001]. In fact, the recognition and the treatment of the "weakest link" phenomenon today is one of the most important scientific contributions in cybersecurity behavior D'Arcy and Greene [2009], Sasse et al. [2001], Schneier [2000] Stanton et al. [2005] Crossler et al. [2013]. These articles have made various empirical, theoretical, methodological, and practical contributions to the area of cybersecurity behavior, conveying a highly encouraging and valuable research direction that has not only scientific importance but also broad societal impacts, and helped the research community and the general public to better understand the complexity of cybersecurity in general and cybersecurity behavior in particular Yan et al. [2018]. It remains to be seen whether this enormous amount of research studies in the field of cybersecurity and hu-

man behavior is able to explain the hypothesis of the "weakest link" phenomenon in relation to the enormous breaches in cybersecurity.

Of course, in recent years the science of cyber behavior is witnessing an unprecedented surge in this specific research area, cybersecurity behavior research, which examines cognition, emotion, and behavior of human beings in cybersecurity and cyber privacy Aiken [2016], Hadlington [2017], Suler [2015], Yan et al. [2012], but relating these research studies in the context of "weakest link" narrative and breaches in cybersecurity, is nowhere to be found. For example, only in the Journal Computers in Human Behavior, more than ten empirical studies have already been published just in the year 2017. The studies have examined various aspects in cybersecurity behavior, such as data hacking anxiety Elhai et al. [2017], cybersecurity hazards perceptions (Van Schaik [2017], internet scam victimization Chen et al. [2017], and social engineering attack interventions Junger et al. [2017], but we continue to wait for a direct response to our question, but without any success. In fact, we are even surprised at the speed in which this "weakest link" hypothesis is accepted by a huge number of scholars without a concrete base in the scientific principles, in relation to the breaches in cybersecurity.

In fact, today cybersecurity is completely immersed in this idea that has become like a cliché. It features significantly in security awareness blogs Spitzner [2019], information technology industry publications Rossi et al. [2015], Wright [2016], media outlets Vishwanath [2016], and even Oxford University Press monographs Singer and Friedman [2014]. As such, this negative characterization of human nature shows no sign of disappearing; on the contrary, it gains an overall presence and acceptance on a daily basis. A vast amount of literature explicitly advocated for it: in the context of airport Schwaninger [2006] and mobile security Lau et al. [2017]; systematic reviews Mahfuth et al. [2017], cyber-psychology Wiederhold [2014], social networking Lehrman [2010] - and many more, and these are only those who just openly mention the idea of "weakest link." No matter how advanced our technological defenses become, maintain scholar of this approach, the human element is likely to remain the weakest link in the cyber security chain. However, we continue to search for cause-effect relationship in this regard, but such a relationship is lacking in these studies. In fact, we want to understand how these scholars reached these conclusions because by understanding psychological principles as applied to cyber security, we will be able to craft security strategies that resonate with employees and encourage proactive and security-conscious behaviors Von Oertzen [2025], but we see no such justifications.

In other words, whether we are talking about studies that developed theoretical models of the weakest link phenomenon Grossklags and Johnson [2009], Pieters [2013], research that examine a wide variety of specific factors that are associated with cyber-

security breaches, such as gender Anwar et al. [2017], attitude Bulgurcu et al. [2010], organization culture Hu et al. [2012], motivations Guo et al. [2011], self-efficacy and perceived vulnerability Ifinedo [2012], perceived severity and locus of control Workman et al. [2008], social pressure Dang-Pham and Pittayachawan [2017], personal responsibility, intervention strategy, and prior knowledge Shillair et al. [2015], and personality (Shropshire et al. [2015], the situation remains the same with regard to providing a direct causal relationship between all these factors being studied, and the phenomenon of the "weakest link." Certainly, all these factors play an important role in changing and improving human behavior in the context of cybersecurity, but this particular attempt to change human behavior needs to be applied only after has been established beyond any reasonable doubt the causal relationship between "human behavior" and breaches in cybersecurity. To conclude that there is a causal relationship between all these factors and the "weakest link" hypothesis, solely on the interaction between a computer system and the human user is scientifically unacceptable. The idea that in order for computer system to do anything useful, in one way or another it is going to have to interact with users in some way, and this interaction is the biggest security risk of them all, leaves the readers with so many gaps since there is no single causal relationship between all these factors and the "weakest link" phenomenon.

2.3.1 Psychological approaches and empirical limitations in answering the "weakest link" narrative

This literature review, of course, cannot deal with all the research studies in this field, due to the space allocated for this undergraduate thesis, and therefore will deal only with some of the most prominent psychological theories used in cybersecurity and human behavior research. Such research studies belong to the general group of theories related to General Deterrence Theory Beccaria [1986] and Bentham [2000], Neutralization theory Sykes and Matza [1957], behavioral theories like, Protection Motivation Theory Prentice-Dunn and Rogers [1986] , and the Theory of Planned Behavior Ajzen [1985], just to mention some of the main theories used to explain human behavior in the field of cybersecurity. In general, such theories have been applied to cyber security to aid understanding of why individuals may behave in what security professionals see as a non-compliant manner. In this way, this review will look at the practical ways researchers have previously used these theories in cyber security in order to change perceptions and behavior of human beings when faced in cyber security processes, with the intention to solve the problem of human behavior being the "weakest link." Within each relevant section, therefore, this review will summarize research that has applied

social psychological theories to the field of cyber security, as well as highlight gaps in the current research in the field in question.

Viewed from a superficial level, we can say that these psychological theories mentioned above not only that they do not provide an answer to the "weakest link" hypothesis, but at the same time, they pose problems with far bigger consequences for both humans and organizations by relying solely on inducing fear-behavioral corrections. According to Soliman and Järveläinen [2024], the most popular theories in behavioral cybersecurity research, such as Deterrence Theory (DT) and Protection Motivation Theory (PMT), attempt to provide solution to the "weakest link" problem through fear-induced behavioral correction. On one hand, these particular theories like Deterrence Theory, for example, emphasizes the fear of severe, certain, and swift punishment as a mechanism to deter bad behaviors by humans that result in numerous breaches of cybersecurity. On the other hand, the Protection Motivation Theory emphasizes fear appeals, like awareness messages, as a mechanism to steer people away from unhealthy behaviors, borrowed extensively from health sciences. We suspect that these ideas not only that they have become so prevalent in the cybersecurity, but at the same time have caused many ethical problems by relying exclusively on fear and punishment, without any concrete results in reducing or stopping breaches in cybersecurity.

For example, propagating the narrative that "humans are the weakest link" can be damaging to problem formulation and the solution search possibilities. By stressing and accepting all the time this narrative unquestionably, could clearly limit researchers and practitioners in cybersecurity to focus on the strengths that humans can offer to having a more secured cyber space. The same was maintained by Soliman and Järveläinen [2024], when they said that adopting a criminological lens, such as Deterrence Theory, might lead us to treat employees who do not comply with security policy as "criminals." In this way, by looking at this problem from the lenses of Deterrence Theory, we are actually approaching the cybersecurity problems through sanctions and punishments. By using sanctions as a preferred solution, we might be opting for a punishment as a solution that might be doing more harm than good. This is especially the case, for example, when punishing employees for falling victims to a phishing attack Kim et al. [2020]. As a result of this, therefore, we challenge categorically this common assumption associated with employing fear appeals and sanctions to regulate cybersecurity behavior, not only because it does not lead to any real positive effect of securing cyber space, but also because of the fact that it has no direct causal relationship in supporting the "weakest link" narrative.

Moreover, the use of psychology in this area has often been to help increase compliance and help change behavior without looking at the problems and experiences of

employees. Such studies have predominantly been survey- or questionnaire-based, testing the concepts and their relative impact on the intention of employees to inform behaviors Iuga et al. [2016]; Flores et al. [2014]; Kirlappos and Sasse [2012]; Renaud and Simpson [2011]; Sheng et al. [2010]; Vance et al. [2012]. In order to have a full picture, researchers have called for more qualitative research, as well as research where academia and industry work together Uchendu [2021]. At the same time, in addition to personal factors, there is no doubt that other environmental variables can influence an individual to engage in harmful behavior, but this has not been considered by scholars of cybersecurity. Several factors such as culture Chang and Lin [2007], policies, participation in the security education, training, and awareness program Han et al. [2017], organizational structure Hong and Furnell [2019], managerial participation, and leadership Guhr et al. [2018] have been examined as environmental influences, but have been excluded by many scholars of cybersecurity when explaining the overall engagement in harmful behavior in breaching cyber security. This can result in individuals focusing on the wrong threats or failing to prepare for potential attacks adequately. In short, the information security deterrence literature has produced some discrepant findings, suggesting an uneven and often contradictory understanding of the influence of sanctions D'Arcy and Herath [2011]. As a result of this, employees may continue to violate security policies despite being aware of possible sanctions they may incur, but this has been ignored by many scholars of the field. One explanation for this behavior is the use of neutralization techniques, i.e., justifying poor behavior, that only recently has been introduced in the cybersecurity research Siponen and Vance [2010].

In typical cases examined in the cybersecurity literature the importance of guilt and shame as a motivator of Neutralization theory seems quite debatable. Users may be motivated by other factors in neutralizing the behavior that could be causally relevant in predicting noncompliance behavior. According to Siponen et al. [2025], the guilt and shame experience is assumed (theoretically) but not tested empirically. This is primarily because behavioral cybersecurity studies have typically applied previously validated instruments Straub [1990] and neutralization techniques measures from research conducted in criminology. However, the argument advanced in neutralization theory is that an individual is often able to avoid self-censure by cognitively redefining situations in a way that minimizes culpability in their own eyes Silic et al. [2016], but that this explanation has been widely ignored by scholars of the "weakest link" paradigm.

The same thing, more or less, might be said about the Theory of planned behavior, which despite being one of the most-researched theories in the behavioral sciences, yet it has not been widely proposed or used as a basis for ideas on how security behavior should be influenced or controlled. According to Sommestad and Hallberg [2013], a lot

of the studies conducted in the field of information security did not follow the guidelines, caveats, and recommendations regarding how this theory should be applied and tested. In this regard, even the founders of this theory, Fishbein and Ajzen [2010] maintain that their theory has not been used correctly, “even though virtually hundreds of studies have tested variations of our theory, we were able to find only relatively few that contained all the elements required for a complete and valid test”. This is especially the case in the application of the studies that apply the Theory of planned behavior to information security policy compliance and violation. The implication of these two factors, incomplete models and incompliance with guidelines, maintain Sommestad and Hallberg [2013], is that the results should be interpreted cautiously because the regression coefficients can be influenced dramatically.

Meanwhile, cautious positions have been presented with regard to Protection Motivation Theory as well. This theory, in fact, has been criticized for failing to explain and account for why people reject risk communication messages Witte [1995], despite the fact that such messages have been considered quite useful in health sciences. It has been argued that threats to data and systems do not carry the same relevance as threats related to healthcare (which was what this model was originally designed for) that directly affect the self Warkentin and Siponen [2015]. However, with the increasing number of cyber-attacks relating to private information and data and with companies increasingly placing penalties on employees who break compliance or even make mistakes Herath and Rao [2009], cyber security and cyber threats arguably do have individual consequences to employees. At the same time, some of this research has been criticized by other psychological researchers in the area and by another fraction of cyber-security research, namely usable security, for certain methods, such as the use of fear appeals and other persuasion techniques shown to be unsuitable Bada et al. [2019]. These criticisms question the ethics of scaring individuals into ‘behaving’ as well as query the efficaciousness of fear appeals Bada et al. [2019].

2.3.2 The rise and critiques of the "weakest link narrative"

In line with the same kind of reasoning, we are faced with numerous other articles that conceptually and empirically discuss and examine the weakest link phenomenon Böhme and Moore [2009], Crossler et al. [2013], Van Schaik [2017], Vroom and Von Solms [2004]; Warkentin and Willison [2009], Wiederhold [2014], but unfortunately do not provide a causal relationship between “human behavior” and breaches in cybersecurity. Vroom and Von Solms [2004], for instance, attempted to audit human behavior in the same way that someone would audit the performance of a technol-

ogy, but was left without a solution because human behavior cannot be audited. When Vroom and Von Solms [2004] 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" (p. 193). In order to support their thesis, Vroom and Von Solms [2004] actually rely on an information security industry survey, which has been published in an online magazine by Briney [2001], implying that security breaches are far more frequently occurring by "insiders" than "outsiders." Vroom and Von Solms [2004] base their claim that employees (insiders) are the weakest link because insiders create more security threats than outsiders, although even Briney [2001] maintains that number one priority in securing the network perimeter should be from external attacks. If we know for sure that employees or insiders are the weakest link; a reasonable question to ask, then why we should focus our resources to defend against external threats? Therefore, since there is no clear causal relationship between security breaches and its cause, we cannot say that in this case the human would be the weakest link in information security.

In another research study, Bulgurcu et al. [2010] investigated rationality-based beliefs and information security awareness in the information security compliance. Among other things, Bulgurcu et al. [2010] 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 has emerged as a key socio-organizational resource because employees are often the weakest link in information security". In supporting this claim, Bulgurcu et al. [2010] make a reference to the book by Mitnick and Simon [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 which Mitnick tells about his crimes and how he was able to perform them. Mitnick and Simon [2002], as mentioned earlier, say "the human factor is truly security's weakest link," but they have not provided any single justification for this claim. It seems that these claims are Mitnick's opinions, which unfortunately lack any evidence that humans are the weakest links.

The research conducted by Warkentin and Willison [2009] is another research that is frequently being presented as an illustration that the human behavior is the "weakest link" in the information security chain. In their research, these two scholars discuss about behavioral and policy issues in information security and talk about endpoint security problem. The endpoint security problem consists of the employee's activities that may increase the risk of creating an information system security threat Warkentin and Willison [2009]. In their article, 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," without making any effort to provide any scientific proof in supporting this premise. In fact, in supporting their claim, these two researchers refer to a global survey of nearly 1400 companies in 50 countries, conducted by Ernst & Young, in which researchers found that awareness and personnel issues remain the 'most significant challenge to delivering successful information security initiatives' Ernst & Young [2008]. However, by not providing any alternative views to the claim "the weakest link - is between the keyboard and the chair," these two authors give the reader the image that this assertion is the truth without a need to support such a claim with clear empirical facts that would demonstrate the direct causal relationship between the human behavior being the "weakest link" and security breaches.

Same goes for many other researchers like Chen et al. [2008] who studied how security awareness can affect organizational security, by analyzing a case study of American and Taiwanese users' responses, and concluded that the 'human' factor is the weakest link in information security and the cause of many security threats, because this was demonstrated in a case study of students in USA and Taiwan. The findings that confirm that American users who received the situational learning training programs outperformed those users who received the traditional face-to-face instruction in comparison to Taiwanese users, does not demonstrate any causal relationship between the human factor being the "weakest link" and security awareness learning programs of American and Taiwanese users. This study, certainly might demonstrate that there are cultural differences with regard to security awareness training programs impacts on organizational security, but does not say anything how this is related to human behavior being the "weakest link." The whole idea behind this whole program is made on the basis that humans are the "weakest link" and it should be strengthened, solely on the claim that is "commonly understood" that humans are the "weakest link."

Other researchers like Luo et al. [2011], maintain the same thing when they studied the social engineering and how vulnerable people are in the eyes of social engineering. According to Luo et al. [2011], "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" (p.2). To understand, and then simplify the complexity of blaming only humans in social engineering, without having into the consideration the system itself, is scientifically incorrect. In fact, accusing the human behavior as the "weakest link," and then continue proposing instead a multi-dimensional approach including technology, policies, procedures, standards, employee training and awareness programs, that should be employed to more effectively and efficiently cope

with the ever-present threat to the IS security management, is insufficient at the least to demonstrate the causal relationship between the human factor and security breaches. To understand the complex nature of social engineering solely of blaming only humans, we can think of a social engineering examples where some people are able to access some other people's accounts by basic information they have been able to gather. In this case, for example, 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 easily be the system rather than human factor.

Another research study selected to be reviewed in this work is the West et al. [2009], who wrote an article that discusses why users make poor security decisions from a psychological perspective. In this article, West et al. [2009] conducted a case study analysis 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 breaches, but still conclude that only human behavior is the "weakest link" when they said that: "Users are generally considered to be the weakest link when it comes to computer security." By conceptualizing the system as an inter-related mechanism that relies on the interactions between human, technology, and environmental factors, and then concluding that security professionals should develop interventions that work to strengthen the "weakest link," is quite incorrect and strange, to say the least. In this regard, we can say that maintaining this claim is quite generic, and as a result of this it is not a reliable starting point for making general assumptions. By reading this article, it is easy for the readers to see the conclusions by the authors that humans would be the weakest link, although at the same time it is maintained that information security depends on more than just one factor.

We are faced with a similar situation with the research conducted by Kraemer and Carayon [2005]. These two authors wrote a publication about computer and information security culture. In the article Kraemer and Carayon [2005] 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" (p. 1483). When they make this claim, the authors are in fact referring to Sasse et al. [2001], but these authors do not support such a reasoning. In fact, Sasse et al. [2001] actually noted that: "The security research community has recently recognized that user behavior 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" (p. 122). As we can see, Sasse et al. [2001] notice 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. Hence, yet again there is no scientific justification for making such a claim about human nature when dealing with human role in the breaches in cybersecurity. These studies do not show that human behavior is the "weakest link" in the security system.

Another article reviewed in this work is the study conducted by Grossklags and Johnson [2009] that studied the weakest link security problem from an economical perspective. In the article Grossklags and Johnson [2009] discuss the human role in information security from multiple perspectives. In the beginning of the article, Grossklags and 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 this impression when they continued to say that, "an abundance of incidents involving lost and stolen property, like laptops and storage devices, as well as individuals' susceptibility to deception and social engineering are evidence of breaches characterizing weakest-link vulnerabilities." In supporting this claim, the authors refer to Mitnick and Simon [2002] book, which has been already evaluated earlier and it leaves us with many questions about the reliability of their claims. Based on these evaluations of the assumptions made by these researchers, we may argue that the whole article is based on assumptions that give the reader a strong impression that the human behavior is the "weakest link" although there is no proof for such conclusions.

The same line of reasoning goes for Gupta [2008] who 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 when he claimed that: "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". However, Gupta [2008] did not justify this claim at all with any references or studies and that is why from a scientific point of view we cannot say for sure that humans are much easier to manipulate than information systems. In fact, even Gupta [2008] admitted that there is no evidence to these claims when he said that: "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 "(p.16). Hence, since there is no scientific evidence beside a personal opinion of an author, it becomes strange to accept such a claim as a scientific

truth.

In conclusion, from all of these studies, just to mention a few, we can see that there is no evidence to support the claim that humans would be the weakest link in information security. After evaluating all of the references, we may rightly argue that none of these articles confirm the hypothesis of the "weakest link" phenomenon. Because of this, 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, but as shown above, we are far away from having a clear scientific justification in accepting the truth of this statement. In fact, the previous articles and publications reinforce the perception of creating a chain reaction that brings us to a general idea as if "everyone agrees with it", but this idea cannot be accepted by principles of scientific research without justification or any evidence. None of the previous articles have actually studied the phenomena or presented evidence that makes humans the "weakest link" and because of that we cannot say for sure that human really is the weakest link in information security.

2.4 Other sources of the weakest link

There is no doubt that psychology can provide numerous theories and methods suitable to describe, explain, predict and change human behavior Coon and Mitterer [2012]. However, from the literature review conducted in the previous section it is absolutely unclear to what extend psychological topics or psychologists have a foothold in cybersecurity research, and if psychological research practices can be found in cybersecurity in the first place. Situations where human behavior affects the security of digital systems can clearly be seen as a part of cybersecurity, hence psychological theories and concepts are important in explaining and changing cybersecurity-related behavior Coon and Mitterer [2012]. However, ensuring holistic cybersecurity, therefore, requires precision in describing, understanding, predicting and changing human behavior as it relates to cybersecurity. In this regard, whether research conducted in the last two decades has adequately addressed the need for incorporating psychology into cybersecurity and how is overall psychology positioned in this field, become important questions that require adequate answers by scholars of the field.

We do maintain that the scholars of information technology should not ignore a plethora of research where it suggested unequivocally that policies and technology are often to blame for human error rather than the human. A multitude of studies since then have shown that, far from being the "weakest link," the insecure actions of employees are often due to the lack of user-centered security in technology and policy rather than out of inattentiveness or ill will Beautement et al. [2008]; D'Arcy et al. [2014];

Inglesant and Sasse [2010]; Renaud and Simpson [2011]. Usable security researchers, for example, have also put forward a more direct discourse to support the move away from the idea of the human as the enemy Parkin et al. [2010]; Sasse et al. [2001]. In their paper 'Transforming the 'weakest link'—a human/computer interaction approach to usable and effective security', Sasse et al. [2001] argued that simply blaming the user would not lead to more effective security systems and outlined a vision of a holistic design approach for effective security.

In this sense, in order to have a full picture of the "weakest link" phenomenon, we have to look at other possible problems when dealing with breaches in cybersecurity. In fact, many scholars indicate that the biggest reasons for security incidents in organizations are due to something else other than humans. For example, Bulgurcu et al. [2010] see that employees are in fact a strong link that can safeguard information and technology resources by their own actions. At the same time, as mentioned previously, Sasse et al. [2001] also agree that simply by blaming users will get us nowhere; instead we must learn from them and hand over these findings to the professionals of security system. In fact, we believe that by repeating the premise of the "human error," this ruined the development of safety-critical systems in the field of cyber security. Hence, there is no point to simply blame the humans without thinking how we could avoid problems with humans and how to decrease the possibility of human becoming the threat to information security.

In fact, there are also many other studies which indicate that human errors are not the biggest incident group. Whitman [2003], for example, made a study of threats to information security and created a threat category with a weighted ranking in which the human is not the weakest link, but in fact the software is. According to Whitman [2003] category, the deliberate software attack is the number one threat, followed by the threat in technical software failures, and only the third one is related to the human context. Slay and Miller [2007] also found similar findings by saying that: "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"(p. 75).

Moreover, Subashini and Kavitha [2011] found that external criminals pose the greatest threat (73%), in comparison to internal threats that pose the least threat of only (18%). From this we can see that external threats pose the greatest problems, but scholars continue blaming human behavior as the weakest link. Breidenbach [2000a] shared the same idea by quoting Schultz when said that numerically, more attacks come from the outside, but that 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 and Miller [2007] also studied the origin of attacks and found that 88% of attacks are sourced externally. Despite these results, however, people continue blaming on the insider because it looks much easier to be attacked, hence less costly to be fired if needed so, or much harder to attack the technology because of huge costs that might involve such a blame.

Moreover, the 2005 CSI/FBI computer crime and security survey conducted by Gordon et al. [2005] showed that, top three types of attack were virus, unauthorized access and theft of patented information. According to this study, these three attack types accounted for 80% of financial losses to organizations. The virus penetration, of course, 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 breaches, but we cannot say that humans are the weakest link. Gordon et al. [2005] had, more or less, similar findings when they found that the most common attack type were viruses, worms or Trojans, which caused 45% of all financial losses. According to Im and Baskerville [2005], intentional security threats such as hacking, computer viruses, and computer theft are becoming a more severe problem in relation to other security vulnerabilities (p. 65).

In other words, although it was suggested that human behavior is to blame since technology may not make mistakes, but it seems that this idea has created reservations even for well-known technologist and writer Quinn Norton. In her article "Everything is broken," writes Norton, "It's hard to explain to regular people how much technology barely works, how much the infrastructure of our lives is held together by the IT equivalent of baling wire. Computers, and computing, are broken" Norton [2014]. To back Norton's argument, Mc Mahon [2020], offers Apple's mobile operating software as an example: "Between 1 January and 31 December 2019, Apple released "20 security updates to its most recent versions (i.e., 12 and 13) of its mobile operating system, IOS" Mc Mahon [2020]. Mc Mahon expresses wonder at why we tolerate flawed software, "In any other sphere of consumer activity, this level of patching would not be tolerated" Mc Mahon [2020].

As a result of this, we are far away from pinpointing the finger to the human factor for all the negative things that are happening to the cybersecurity on a daily basis. We are resolute in removing the finger-pointing because technology is far away from being perfect, and the same thing might be said about other factors like organizational ones for example. In fact, in order for the technology and the organization to be exonerated from this link, scholars of the field must answer all possible questions, but as already explained in this and in the previous chapters, they are far away from this. In other

words, in order for scholars to conclude without reasonable doubt that human beings are the "weakest link," they need to answer following questions: Are there other links in the chain, or only humans? If humans are not alone, what are the other links in this chain, and how secured are they? Has the human been programmed out of the system in question? Only after we include or exclude all possible factors in studying a particular phenomenon, we are allowed to conclude whose chain is the strongest or the weakest.

Finally, if we want to move one step further and introduce here in this work the proposal of the latest advancements of AI as a possible solution to the "weakest link" narrative, hence removing the human factor from this equation altogether, as has been done by Chamorro-Premuzic [2023], we will be faced again with problems caused by other factors beyond human element. In fact, Chamorro-Premuzic [2023] maintained that supervised machine-learning algorithms, for example, can classify malignant email attacks with 98% accuracy, spotting "look-alike" features based on human classification or encoding, while deep learning recognition of network intrusion has achieved 99.9% accuracy. There appears to be a general tendency where advances in AI are more than welcomed in cybersecurity as an excuse for our own intellectual stagnation and careless or reckless behavior, maintains Chamorro-Premuzic [2023]. However, although they do not treat directly the problem of the "weakest link," two scholars like Spagnoletti and Baskerville [2025] present caution in using AI advances in the cybersecurity. According to these two scholars, the transformative impact of digitalization on organizations has amplified the responsibility of organizations to ensure the safety of their digital products and services, as unsafe information can cause harm to society or the environment. In this situation, maintain these two scholars, organizations need new forms of risk management that provide provenance for their digital informational products and services. According to these two scholars, the design and implementation of advanced data governance models, for example, might become a potential risk management tool for embedding safety in organizational information generated for public use. For Spagnoletti and Baskerville [2025], this requires the implementation of advanced risk management strategies, including data validation pipelines, the use of trusted and verified sources, and robust processing and oversight mechanisms. This in fact is just one small example that demonstrates and illustrates clearly once more that blaming and removing from the equation of the cybersecurity space the human factor will not eradicate the problem with breaches in the cybersecurity, therefore, this issue can be tackled when treated as whole, including the human factor as an important element to securing the information technology.

In conclusion, from the research we have observed in the previous sections, therefore, there is no indication whatsoever that human behavior is the "weakest link," and

that the technology or organization are infallible. On the contrary, human beings, instead of being the weakest links, may be the most vital link when it comes to attacks that are always mutating, in particular those aimed directly at humans. In short, we all have to agree that apart from the human behavior, the chain comprises policies, technical, physical, or similar synthetic links, and because of this fact, we must have sufficient scientific support that human behavior is the weakest link, something that we do not have it. If we humans are the weakest link, that means the other links in the chain - hardware and software, are more robust and more secure, which is absolutely not true. 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.

Chapter III

The weakest link paradigm: where do we go from here?

3.1 Discussion

Historically, and still, to this day, human factors and the user in cyber security have been treated as the "weak link," meaning that employees within organizations are generally mistrusted Goo et al. [2014]; Hughes [2021]; Boss [2015]; Sabillon [2022]. As mentioned in the previous chapters, this premise has produced over 100 articles that directly mentions the paradigm of the "weakest link," and at the same time, it is important to note that there is still ongoing research, perhaps a majority of research, which takes the perspective of the human as the problem or "weak link" in cyber security Goo et al. [2014]; Hughes [2021]; Boss [2015]; Sabillon [2022]. Proponents of this premise maintain that people are inherently prone to errors. In fact, for years we've heard the line "people are the weakest link" over and over again to such an extent, that such a premise started to give us a complex that "we the people" are the reason for data failures.

In the field of cybersecurity, as observed in the previous chapters, many scholars from the information technology maintain that the human factor continues to be a constant that remains the most significant vulnerability. According to them, understanding human psychology is crucial for effective cybersecurity because attackers exploit human vulnerabilities through social engineering, relying on techniques like phishing to bypass technical defenses. For these scholars, the human behavior remains a pivotal element in determining the success or failure of cybersecurity measures. A great number of these scholars have gone beyond this premise by proposing a new paradigm in the field of cybersecurity; a paradigm of blaming the human behavior as the "weakest link". In fact, the recognition and the treatment of the "weakest link" phenomenon today, maintain scholars of this premise, is one of the most important scientific contributions in cybersecurity behavior (for instance, D'Arcy and Greene [2009], Schneier [2000 and 2011], Stanton et al. [2005], Crossler et al. [2013].

In fact, as mentioned in the previous chapter, the idea that humans are the "weakest link" in computer security is very prevalent among computer scientists and people who work on the technical elements of cybersecurity. After all, maintain proponents of this thesis, if our job is to secure computer systems, it's satisfying to feel that the problems

lie not in the computers but in everyone else. Of course, based on the literature review observed in the previous chapter, we agree that humans do make errors that lead to possible incidents in information security, however, this does not mean that they are caused only by humans, and that most cases are too complex to blame only on humans. It's completely true that many computer security incidents involve human users making bad decisions, like opening emails or downloading files despite warning signs, but that's no reason for technologists to feel complacent about their accomplishments. On the contrary: these sorts of mistakes are evidence that the technology is failing its human users, not the other way around.

As we saw from the literature review in the previous chapter, it can be said that the hypothesis "human is the weakest link" is used as a general narrative without scientific evidence. Many of the articles use this premise with some generalizations such as "commonly acknowledged" Thomson and Nierkerk [2012], when in fact has no scientific base. As time passes, the trope of the "weakest link" moves to a situation in which implies that it has been proven to be that way, but we are far away from such a conclusion. From what we reviewed and observed in the previous chapter, we would expect real empirical study in support of the claim human beings being the "weakest link." In fact, what we observed and reviewed were numerous empirical studies using psychological theories to attempt to change human behavior in order to improve human behavior move away from the "weakest link" implications. But what we were missing to find was the causal relationship between the "weakest link" paradigm and the breaches in cybersecurity. Only after this link has been established beyond reasonable doubt we are allowed to move forward with providing steps to improve human behavior to overcome the gaps. As we saw in the previous chapter, 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. By claiming humans as the "weakest link" 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. 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 holistic picture, and not focus simply on blaming the one link that seems to be the obvious choice.

Moreover, despite the theoretical arguments and existing research illustrating the effects of psychological variables on cybersecurity-relevant behavior, the extent to which psychological research is integrated into cybersecurity research has not been adequately assessed neither quantitatively nor qualitatively. From a psychological perspective, defining psychology in cybersecurity based on the concepts and theories used is prob-

lematic, as the potential list of concepts and theories used to explain human behavior in the field of cybersecurity would be somewhat arbitrary. Therefore, not only that there is a need for a measurable, well-defined representation that represents psychology in cybersecurity, but at the same time, it must be demonstrated empirically that there is a causal relationship between the "weakest link" and breaches in cybersecurity. Only after this connection has been made, we can proceed to use psychological and behavioral theories to change and improve human behavior in order to solve the problem of the "weakest link" in human behavior. In this regard, it can be assumed that there is a strong theoretical need of psychology on cybersecurity, and not just an arbitrary use of certain theories and methods as introduced in totally other fields than in the field of cybersecurity. Certainly, the human security knowledge domain does provide a defined list of sub-topics prevalent in cybersecurity that are closely related to psychology, but this requires a well-defined theory, in order not to conclude hastily that "human behavior is the weakest link", just because breaches to cybersecurity continue to happen at an alarming pace.

In other words, how are we going to know for certainty that the increase in cybersecurity incidents is happening because of the human behavior being the "weakest link", and not because of policies, technology, organizations, that are often to be blamed? From a scientific point of view, we can say that first we have to demonstrate the causal links between all these factors, and only after these links have been established beyond reasonable doubt we are allowed to move forward offering possible solutions, in our case using psychological theories to change and improve human behavior in securing cyber space. In fact, researchers in the field suggest that we are far away from shifting focus from technical aspects of cyber security to "human behavior" due to a lack of consolidation of the attributes pertaining to human factors, the application of theoretical frameworks, and a lack of in-depth qualitative studies Jeong et al. [2019]. Therefore, staying up-to-date with emerging threats is essential for maintaining robust cybersecurity measures. Without doubt, understanding the technical ins-and-outs of network security is important to having a successful information technology that is both powerful and more importantly secure.

As already demonstrated in the previous chapters when discussing the state of the art of cybersecurity and human behavior, the research conducted in this field does not give us the right to blame everything on the human behavior as the "weakest link." In fact, in a seminal paper 'Users are not the Enemy' Adams and Sasse [1999], it was demonstrated that such behavior was often caused by the way in which security mechanisms were implemented and users' lack of knowledge. According to these findings, it was suggested that security-focused departments within organizations need to com-

municate more with users and adopt a user-centered design approach Adams and Sasse [1999], and not blame everything on the human behavior. In other words, this paper demonstrated a shift away from the previous narrative maintained by cyber-security research, which had predominantly focused on the human as the problem Goo et al. [2014]; Hughes [2021]; Boss [2015]; Sabillon [2022]; attempting to remove the human from the process, or at least control the human element with strict compliance policies.

Furthermore, since there is no evidence that current blame on the human behavior as the weakest link is causing breaches in the cybersecurity, then all the uses of psychological theories to remedy these "weaknesses" in human behavior will not lead to any positive effect. On the contrary, we agree fully with a small number of scholars who argue that calling people the "weak link" implicitly blames individuals for not being able to comply with policies Sasse and Rashid [2021], when, as this literature review has demonstrated, this is not always the case and is often counterproductive, especially within an organizational context where this weak link viewpoint could lead employees to believe that they are not capable and reduce self-efficacy, with far more consequences for having a secured cyber space. Hypothesizing that the human behavior is the "weakest link" without having a clear support from research studies that would support such a premise, is not only scientifically wrong, but more importantly dangerous for the practical implications that lead to. Therefore, we believe that we should aim to shift the dialogue from demonizing the human as the "weak link" to viewing the human more positively Sasse and Rashid [2021], because this demonization of the human nature has not offered any single solution to the problem at issue.

Blaming everything on the human behavior has not yielded to any concrete solution to the increasing problems in breaches in cyber security. The numbers are increasing on a daily basis, despite the incorrect recognition that human behavior is the "weakest link". In this regard, designers of security mechanisms must realize that they are the key to successful security system, as maintained by Adams and Sasse [1999], and not just blame human behavior that there is something innate in their nature to be the weakest link. According to Adams and Sasse [1999], unless security departments understand how the mechanisms they design are used in practice, there will remain the danger that mechanisms that look secure on paper will fail in practice, as has been demonstrated up to now with explosion of breaches in the field of cybersecurity.

On the contrary, we have no problem in believing that the public as well as private entities throughout the world, invest a huge amount of money in protecting their own institutions from possible cyber-attacks by different individual as well as organized foreign entities. In fact, most of the research on cybersecurity has rightly focused on improving computer network systems Nobles [2018], as many believe that information

technology advances and software development is the main way to increase information security Sadkhan [2019]. By implementing these strategies consistently over time, therefore, organizations can significantly improve their overall cybersecurity posture because we do believe also that technical and data-driven solutions are foundations of cybersecurity. We maintain that organizations should regularly review their systems' vulnerabilities and invest in advanced technologies such as firewalls, antivirus software, encryption tools, etc., that protect against evolving cyber threats. However, this cannot be done at the expense of the human factor, just because of the general thought that human behavior is the "weakest link", without having research based studies that would confirm this hypothesis D'Amico et al. [2005]; Barford et al. [2010]; Dutt et al. [2013]; Knott et al. [2013]; Mancuso et al. [2014].

In fact, Zimmermann and Renaud [2019] provide clear examples of where employees have been blamed for cyber-attacks despite employee behavior not triggering the given breaches. Because of this, Zimmermann and Renaud [2019] argue that there needs to be a complete paradigm shift that recognizes the employee as a contributor to success within wider socio-technical systems. This is so because if underlying assumptions of employees are unfounded or wrong, then the solutions developed will also be ineffective or mismatched. According to these scholars, the assumption that the human constitutes a problem to control has been demonstrated to be totally wrong by the research conducted, therefore, it is up to the organizations, governments, policies, leaders, to work effortlessly to engage employees to be involved in trainings, understand the technology better, and when needed exclude, constrain, and control to comply with security policies Zimmermann and Renaud [2019]; Weirich and Sasse [2001].

3.2 Bridging the gap between technology, organization, and human behavior

The often-repeated statement that humans are the "weakest link" in the security supply chain must be questioned. We maintain that instead of blaming human behavior as the "weakest link," it would be much productive for various scholars of information technology to strengthen cyber technology, and work together with users of technology and organizations to protect itself from possible cyber-attacks. Research is yet to look at how this dialogue of the human as the weakest link manifests itself in practice in the organizational context and whether this dialogue is changing. Research needs to understand whether and why employees might see themselves as the weakest link and whether this relates to perceptions of the human factor more generally, or if this is a

mindset that security professionals influence or put forward.

In proposing a shift from blaming the human element as the "weakest link", to bridging the gap by having a balanced view between technology, organization, and the human element, as mentioned albeit briefly in the first Chapter, we ground our argument exclusively on the theory of organizational behavior by March and Simon [1958], and the Information Infrastructure Theory by Hanseth [2002] and Hanseth and Ciborra [2007]. In fact, we believe that proponents of the "weakest link" narrative ignore the contributions of these two theories when attempting to understand and provide solutions to the ever-existing problem of data breaches in the field of cybersecurity. In other words, if we take into consideration how organizational structures, processes, and social dynamics shape individual behavior and decisions, how human decisions are made in complex settings, then certainly we would need more space to explore the cognitive and social factors in influencing organizational behavior. The main thesis is that understanding organizational behavior requires moving beyond purely rational models of decision-making and incorporating the cognitive and social limitations of individuals within the organizational context. Instead of viewing organizations as composed of perfectly rational actors striving for optimal solutions, March and Simon [1958] argue that individuals operate under bounded rationality. Having this groundbreaking contribution in mind, therefore, it is a bit strange to continue thinking in a linear-simplistic way about the human behavior being the "weakest link," when such an explanation has been refuted as being too simplistic, overly rational, and that this needs to be replaced with a more empirically grounded understanding of how decisions are actually made in organizational settings.

Moreover, having in mind the complexity of modern life and technological advancements, this automatically calls for a shift in perspective, moving away from simplistic notions of control towards approaches that acknowledge the inherent dynamism and unpredictability of these complex sociotechnical systems Hanseth [2002]; Hanseth and Ciborra [2007]. Since we have to move beyond viewing information systems as isolated entities to understanding them as interconnected infrastructures that shape and are shaped by their context, then employing Information Infrastructure Theory, which explores the nature, design, and evolution of shared, complex, and evolving technological and social systems that support information processing and communication within and across organizations and societies, is a necessity, if we want to find real solutions to the problems faced by breaches in cybersecurity on a daily basis. In other words, understanding the complex interplay between technology, organizations, and society, is a must for both the academic scholars and the industry if we really want a practical solution in dealing with problems in the field of cybersecurity. According to this theory,

information infrastructures are not just technical but also encompass the people, processes, organizational structures, and social norms that interact with and are shaped by the technology. As a result of all this, we are obliged not to view the phenomena in the cyber space as linear-simplistic processes, but as a dynamic, complex process that shape their development and use.

In this line of reasoning, in a study by Reinfelder et al. [2019], it was demonstrated clearly that the absence of organizational structures that include users in security development processes, security managers, intentionally or unintentionally, obtain a negative view of users, which leads to strict and rigid security measures that users cannot influence. The authors argue that to break this cycle, where it is not just the users but all humans in the process who need support, security managers need organizational structures, methods and tools that facilitate systematic feedback from users Reinfelder et al. [2019]. Similar research has argued for the application of usable security beyond end users, adding another human element for the discipline to consider Acar et al. [2016]. Research further finds that employees and managers have different attitudes toward cyber-security policy, and different factors motivate compliance between these two groups Balozian et al. [2019]. These findings demonstrate that not all individuals within organizations hold the same attitude Beris et al. [2015], suggesting that different strategies may be needed to influence their behaviors.

Because of this, we need for a more positive security narrative that should lead to more literature and more dialogue, in order for the human element to be seen as a capable and valuable part of cyber-security systems Sasse and Rashid [2021]. This means that policymakers need to trust and engage users more, rather than trying to design the human out Kirlappos and Sasse [2012], based solely on the general belief that humans are the "weakest link." Therefore, we agree with Jeong et al. [2019] when they propose that future studies should focus on, consolidating human factors, taking an interdisciplinary approach when examining cyber security, and conducting additional qualitative research whilst investigating human factors in cyber security. The perspective that more qualitative research is needed for a mixed methods understanding of cyber security is echoed by other researchers in reference to multiple aspects of cyber-security research, such as cyber-security culture Sasse and Rashid [2021]; Uchendu [2021].

Without doubt, we are in need for a more positive narrative when dealing with cybersecurity chain, because it is way too general to just identify and conclude that the ordinary users are the "weakest link," as explained in the previous chapters. We have to agree and accept that the ordinary users are an extremely complex and diverse population. In other words, if we do not have sufficient research support on the issue at matter, then we do not have clear understanding in which part of the chain there is a problem,

having in mind the complex nature of human beings, and more importantly we ignore and exclude completely from the picture the technical and organizational parts of the chain, as explained earlier in the chapter. Because of this, it needs to further identify and recognize where the specific weakest links are among these three crucial elements of cybersecurity. By categorizing them in this way then, we would be able to develop better effective interventions.

Therefore, here in this section, grounded in the works of organizational behavior theory by March and Simon [1958], and information infrastructure theory by Hanseth and Ciborra [2007], we propose a balanced approach and a dialogue in order to bridge the gap between all the camps – technology, organization, and the human element. We believe that not only these camps can coexist with each other, but rather this coexistence is a necessary prerequisite for having a more secured cyber space. What we propose here is to look at this phenomenon of the weakest link not as a "chain", but as a "net", in which all the elements are connected in a network, and that one problem in this network creates problems on the whole system. In this way, there is an interdependence between the technology, organization, and the human element, and only if treated as such we can move forward in providing a more robust system in the field of cybersecurity. In this way, we propose to move away from the linear, chain image of security information because such an assumption can easily be broken on a single point. We propose to take this road because we treat the field of cybersecurity as a complex management system containing technical and social parts, which includes organizational processes and people or actors Malatji et al. [2021]. Instead of blaming the humans, we may do a better job by addressing the challenges recognized in the cybersecurity literature, such as security environment Ebert et al. [2023]; Mc Mahon [2020], organizational processes Hagen et al. [2008], the complexity of cybersecurity policies Karlsson et al. [2017], usability of security Whitten and Tygar [1999], and many other important factors related to the information security. By oversimplifying and scapegoating one of these factors, we allow organizations and other important institutions to avoid investigating and fixing the more complex system, hence we get stuck in a situation without any concrete solution, like we are being stuck for over two decades now without any solution and with increasing number of breaches in cybersecurity.

In order for this not to happen, we propose for academics and industry practitioners to work closer together on research looking at cyber-security culture, in order to have a much needed balance and dialogue between these important elements of cybersecurity. Without integrated and interdisciplinary research within technological, organizational and human systems, it is difficult to ascertain the actual value of previous research and whether it might impact real-world cyber-security culture. If practitioners and academic

researchers co-operate, it will enable researchers to access real organizations to apply, evaluate and refine their new research. In this way, those in industry will gain access to research expertise, which is often inaccessible. After research has been widely investigated in this manner, this would ultimately lead to the design and development of a robust set of approaches suitable for particular organizations to use Uchendu [2021]. The topic of information security is of a complex nature, therefore the treatment must be adequate in order to have the best results in good cybersecurity behavior.

In this way, by understanding better the psychological aspects of human behavior, it opens the way in devising effective cybersecurity strategies. Organizations can certainly develop more effective strategies to mitigate threats and protect sensitive information by understanding how human behavior influences cybersecurity risks and vulnerabilities. From educating employees about common cyber threats to designing user-friendly security measures, incorporating insights from psychology is essential for building a resilient and security-aware organization in today's digital landscape. Of course, we do agree that humans are susceptible to cognitive biases, for example, such as the tendency to prioritize convenience over security or to underestimate risks when they perceive a task as familiar, but this should not be a sufficient condition to remove the human element from the cybersecurity equation. On the contrary, by recognizing these biases, cybersecurity professionals can tailor their approach to mitigate human error effectively. This might involve simplifying security protocols, implementing user-friendly authentication methods, or leveraging behavioral psychology principles to promote adherence to security guidelines.

In conclusion, for an information security researcher, this thesis offers a critical viewpoint, and encourages challenging existing generalizations and justifying the allegations made. For an organization, on the other hand, this work also offers the critical viewpoint by suggesting concrete actions to be taken, and to look for alternative ways to guide their actions. For "human beings", this thesis offers the humble suggestion that maybe we are not the "weakest link," and by developing ourselves we can become potentially the "strongest link" in the future.

Chapter IV

Conclusion

The aim of this study was to determine whether or not humans are "the weakest link" in information security. This study was conducted through the utilization of literature review, in order to get the broadest possible understanding of the subject. The literature review itself consisted of a review of a number of articles in the area of information security, among a plethora of research on cybersecurity and human behavior. The majority of these studies claimed or implied that humans were the "weakest link," although the studies that have actually studied information security threats and information security accidents did not confirm these claims.

The interplay between human psychology and cybersecurity is complex and multifaceted. An understanding of the human behavior and organizational dynamics is essential for strengthening the human element of cyber defense. Organizations will need to think beyond blaming the human behavior as the "weakest link," if they really want to create a robust system in the field of cybersecurity. Users must be made equal stakeholders in their own cyber safety. With technological and human defenses working together, organizations can hope to enhance their resilience significantly. The future of cybersecurity will be defined by how effectively we synthesize the teachings from psychology and behavioral sciences with rapidly advancing technology. This will require interdisciplinary collaboration and viewpoint diversity. A holistic cyber-human systems approach is needed to change the asymmetry between attackers and defenders. As people build the technology of the future, the future of security will be shaped by understanding how people interact with this technology.

While human behavior can indeed pose vulnerabilities in cybersecurity, it has to be agreed also that it presents a significant opportunity for organizations to strengthen their defenses. In today's interconnected world, where cyber threats constantly evolve in complexity and scale, the human element can serve as a challenging barrier against malicious actors. One of the key strengths of the human element lies in its intelligence and adaptability. Unlike automated security measures that may struggle to keep pace with rapidly evolving threats, human beings possess the cognitive abilities to analyze complex situations, identify patterns, and make informed decisions in real time. This human intelligence allows organizations to detect and respond to emerging threats more

effectively, complementing the capabilities of automated security systems. In the battle against cyber threats, technology alone is not enough. The human element, therefore, remains both a potential vulnerability and a potent asset in safeguarding our digital assets. By understanding the psychology of cybersecurity and fostering a security-aware culture, organizations can enhance their resilience against cyber threats and build a safer, more secure digital future.

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 certainly one part of the chain and, in some cases, they might even be the weakest link. However, as it was seen from the literature, it is not easy to determine the actual reason for any information security incident. Therefore, by understanding and influencing human behavior is a critical component of having a robust cyber security strategy. By understanding the complexities of human behavior, organizations can develop more effective strategies for mitigating risks and safeguarding digital assets. Coupled with technology solutions that support and reinforce good security practices, organizations can create a strong defense against the ever-evolving cyber threat landscape. From raising awareness and fostering a culture of security consciousness to addressing insider threats and combating social engineering tactics, integrating the human element into cybersecurity initiatives is essential for protecting against evolving threats in an increasingly digital world.

We believe that future research related to humans in information security should focus more on the root-causes and should attempt to explain the complexity and causalities between different actors in information security incident, if we want to find real solutions to the ever-increasing problem of data breaches in cybersecurity. In this regard, future research topics could be “the causalities between different factors in information security incidents” or “the complexity behind finding the root-cause in information security incidents”. With regard to limitations, it can be said that the results of the study did not answer the research question in a straight way and, due to the relatively small amount of literature, the results cannot be generalized to the entire sphere of information security research. Moreover, the results cannot be generalized also due to the fact that this is just an undergraduate thesis, hence difficult to cover the whole study of the "weakest link" narrative in the field of cybersecurity. Finally, regarding the study process it can be said that when we go through hundreds of articles, there is always the possibility that an important or less important article has been accidentally missed from an in-depth analysis. It is also worth noting that only Scopus database was used for research, hence it is difficult to generalize that this database has covered most of the scientific literature on the topic in question.

References

Y. Acar, S. Fahl, and M. L. Mazurek. You get where you're looking for – the impact of information sources on code security. In *IEEE Symposium on Security and Privacy (SP)*, pages 289–305, San Jose, CA, 2016. IEEE.

A. Adams and M. A. Sasse. Users are not the enemy. *Communications of the ACM*, 42 (12):40–46, 1999. doi: 10.1145/322796.322806. URL https://dl.acm.org/doi/10.1145/322796.322806.

Mary Aiken. *The Cyber Effect*. Random House, Spiegel & Grau, New York, 2016.

Icek Ajzen. From intentions to actions: A theory of planned behavior. In J. Kuhl and J. Beckmann, editors, *Action Control: From Cognition to Behavior*, pages 11–39. Springer-Verlag, Berlin, Heidelberg, New York, 1985.

Icek Ajzen. The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, 50(2):179–211, 1991. doi: 10.1016/0749-5978(91)90020-T. URL https://doi.org/10.1016/0749-5978(91)90020-T.

Icek Ajzen. Perceived behavioral control, self-efficacy, locus of control, and the theory of planned behavior. *Journal of Applied Social Psychology*, 32(4):665–683, 2002. doi: 10.1111/j.1559-1816.2002.tb00236.x. URL https://doi.org/10.1111/j.1559-1816.2002.tb00236.x.

Icek Ajzen. The theory of planned behaviour: Reactions and reflections. *Psychology & Health*, 26(9):1113–1127, 2011. doi: 10.1080/08870446.2011.613995. URL https://doi.org/10.1080/08870446.2011.613995.

M. Alassaf and A. Alkhalifah. Exploring the influence of direct and indirect factors on information security policy compliance: A systematic literature review. *IEEE Access*, 99:1–1, 2021. doi: 10.1109/ACCESS.2021.3132574. URL https://doi.org/10.1109/ACCESS.2021.3132574.

S. Altamimi, R. Alroobaea, and A. Almehmadi. I do it because they do it: Social-neutralisation in information security practices of saudi medical interns. In *14th International Conference on Risks and Security of Internet and Systems (CRiSIS)*, Tunisia, 2020.

C. L. Anderson and R. Agarwal. Practicing safe computing: A multimedia empirical examination of home computer user security behavioral intentions. *MIS Quarterly*, 34(3):613–643, 2010. doi: 10.2307/25750694. URL https://doi.org/10.2307/25750694.

R. O. Andrade and S. G. Yoo. Cognitive security: A comprehensive study of cognitive science in cybersecurity. *Journal of Information Security and Applications*, 48: 102352, 2019. doi: 10.1016/j.jisa.2019.06.008. URL https://doi.org/10.1016/j.jisa.2019.06.008.

M. Anwar, W. He, I. Ash, X. Yuan, L. Li, and L. Xu. Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior*, 69:437–443, 2017. doi: 10.1016/j.chb.2016.12.040. URL https://doi.org/10.1016/j.chb.2016.12.040.

N. A. G. Arachchilage and S. Love. Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior*, 38:304–312, 2014. doi: 10.1016/j.chb.2014.05.046. URL https://doi.org/10.1016/j.chb.2014.05.046.

S. Aurigemma and T. Mattson. Exploring the effect of uncertainty avoidance on taking voluntary protective security actions. *Computers & Security*, 73, 2017. doi: 10.1016/j.cose.2017.11.001. URL https://doi.org/10.1016/j.cose.2017.11.001.

M. Bada, A. Sasse, and J. R. C. Nurse. Cyber security awareness campaigns: Why do they fail to change behavior? In *International Conference on Cyber Security for Sustainable Society*, 2019. URL https://doi.org/10.48550/arXiv.1901.02672. Originally presented in 2015.

P. Balozian, D. Leidner, and M. Warkentin. Managers' and employees' differing responses to security approaches. *Journal of Computer Information Systems*, 59(3): 197–210, 2019.

P. Barford, J. Kline, D. Plonka, and A. Ron. Cyber sa: Situational awareness for cyber defense. In S. Jajodia, P. Liu, V. Swarup, and C. Wang, editors, *Cyber Situational Awareness: Issues and Research*, volume 46 of *Advances in Information Security*, pages 3–13. Springer, 2010. doi: 10.1007/978-1-4419-0140-8_1. URL https://doi.org/10.1007/978-1-4419-0140-8_1.

J. B. Barlow, M. Warkentin, D. Ormond, and A. R. Dennis. Don't make excuses! discouraging neutralization to reduce it policy violation. *Computers & Security*, 39:

145–159, 2013. doi: 10.1016/j.cose.2013.05.006. URL https://doi.org/10.1016/j.cose.2013.05.006.

R. F. Baumeister and M. R. Leary. Writing narrative literature reviews. *Review of General Psychology*, 1(3):311–320, 1997.

A. Beautement and M. A. Sasse. The economics of user effort in information security. *Computer Fraud & Security*, (10):8–12, 2009. doi: 10.1016/S1361-3723(09)70127-7. URL https://doi.org/10.1016/S1361-3723(09)70127-7.

A. Beautement, M. A. Sasse, and M. Wonham. The compliance budget: Managing security behavior in organizations. In *Proceedings of the 2008 Workshop on New Security Paradigms (NSPW)*, 2008.

Cesare Beccaria. *An Essay on Crimes and Punishments*. Hackett Publishing Company, Inc., Indianapolis, IN, 1986. Original work published 1764.

Noam Ben-Asher and Cleotilde Gonzalez. Effects of cyber security knowledge on attack detection. *Computers in Human Behavior*, 48:51–61, 2015. doi: 10.1016/j.chb.2015.01.039. URL https://doi.org/10.1016/j.chb.2015.01.039.

Jeremy Bentham. *An Introduction to the Principles of Morals and Legislation*. Batoche Books, Kitchener, 2000. Original work published 1789.

O. Beris, A. Beautement, and M. A. Sasse. Employee rule breakers, excuse makers and security champions: Mapping the risk perceptions and emotions that drive security behaviors. In *Proceedings of the 2015 New Security Paradigms Workshop*, pages 73–84, New York, NY, USA, 2015. ACM.

F. Blanger, S. Collignon, R. Vallée, and K. Moqadem. Determinants of early conformance with information security policies. *Information Management*, 54(7):887–901, 2017. doi: 10.1016/j.im.2017.01.003. URL https://doi.org/10.1016/j.im.2017.01.003.

R. Boehmer, S. Laumer, C. Maier, and T. Weitzel. Determinants of online safety behavior: Toward a strategy for public education. *Behavioral Information Technology*, 34(10):1022, 2015.

S. R. Boss. What do systems users have to fear? using fear appeals to engender threats and fear that motivate protective security behaviors. *Management Information Systems Quarterly*, 39(4), 2015. AIS eLibrary.

Seymour Bosworth and M. E. Kabay, editors. *Computer Security Handbook*. John Wiley & Sons, 2002.

A. A. Braga and D. L. Weisburd. The effects of focused deterrence strategies on crime: A systematic review and meta-analysis of the empirical evidence. *Journal of Research in Crime and Delinquency*, 49(3):323–358, 2012. doi: 10.1177/0022427811419368. URL https://doi.org/10.1177/0022427811419368.

Harry Braverman. *Labor and Monopoly Capital: The Degradation of Work in the Twentieth Century*. Monthly Review Press, New York, 1998.

S. Breidenbach. How secure are you? *InformationWeek*, (800):71, 2000a.

S. Breidenbach. How secure are you? *InformationWeek*, (800):71, 2000b. Duplicate appearance in reference list.

A. Briney. Inside job. *Information Security Magazine*, 2001. Available at: https://www.csoonline.com/article/2113226/inside-job.html [Accessed 2025].

Burcu Bulgurcu, Huseyin Cavusoglu, and Izak Benbasat. Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, 34(3):523–548, 2010. doi: 10.2307/25750690. URL https://doi.org/10.2307/25750690.

Rainer Böhme and Tyler Moore. The iterated weakest link: A model of adaptive security investment. In *Workshop on the Economics of Information Security (WEIS)*, University College London, 2009. URL http://weis09.infosecon.net/files/152/paper152.pdf.

Tomas Chamorro-Premuzic. *I, Human: AI, Automation, and the Quest to Reclaim What Makes Us Unique*. Harvard Business Review Press, 2023.

S. E. Chang and C. S. Lin. Exploring organizational culture for information security management. *Industrial Management Data Systems*, 107(3):438–458, 2007. doi: 10.1108/02635570710734316. URL https://doi.org/10.1108/02635570710734316.

Ramnath K. Chellappa and Paul A. Pavlou. Perceived information security, financial liability and consumer trust in electronic commerce transactions. *Logistics Information Management*, 15(5/6):358–368, 2002.

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

H. Chen, C. E. Beaudoin, and T. Hong. Securing online privacy: An empirical test on internet scam victimization, online privacy concerns, and privacy protection behaviors. *Computers in Human Behavior*, 70:291–302, 2017. doi: 10.1016/j.chb.2017.01.003. URL https://doi.org/10.1016/j.chb.2017.01.003.

L. Cheng, Y. Li, W. Li, and E. Holm. Understanding the violation of is security policy in organization: An integrated model based on social control and deterrence theory. *Computers & Security*, 39:447–459, 2013. doi: 10.1016/j.cose.2013.09.009. URL https://doi.org/10.1016/j.cose.2013.09.009.

A. M. Y. Chu, P. Y. K. Chau, and E. W. L. Cheng. Explaining the misuse of information systems resources in the workplace: A dual-process approach. *Journal of Business Ethics*, 131:209–225, 2014. doi: 10.1007/s10551-014-2250-4. URL https://doi.org/10.1007/s10551-014-2250-4.

Lizzie Coles-Kemp, Thomas Jensen, and Maria J. Espona. Why should i? cybersecurity, the security of the state and the insecurity of the citizen. *Politics and Governance*, 6(2):41–48, 2018. doi: 10.17645/pag.v6i2.1333. URL https://doi.org/10.17645/pag.v6i2.1333.

Dennis Coon and John O. Mitterer. *Introduction to Psychology: Gateways to Mind and Behavior*. Wadsworth, Cengage Learning, Belmont, CA, 13th edition, 2012.

Louis Anthony Tony Cox. Confronting deep uncertainties in risk analysis. *Risk Analysis*, 32(10):1607–1629, 2012.

W. Alec Cram, John D'Arcy, and Joan G. Proudfoot. Organizational information security policies: A review and research framework. *European Journal of Information Systems*, 26(6):605–641, 2017. doi: 10.1057/s41303-017-0059-9. URL https://doi.org/10.1057/s41303-017-0059-9.

Donald R. Cressey. Epidemiology and individual conduct: A case from criminology. *Sociological Perspectives*, 3(2):3–12, 1960. doi: 10.2307/1388200. URL https://doi.org/10.2307/1388200.

R. E. Crossler, A. C. Johnston, P. B. Lowry, Q. Hu, M. Warkentin, and R. Baskerville. Future directions for behavioral information security research. *Computers & Security*, 32(1):90–101, 2013.

Duy Dang-Pham and Siddhi Pittayachawan. Comparing intention to avoid malware across contexts in a byod-enabled workplace. *Computers in Human Behavior*, 67: 136–147, 2017. doi: 10.1016/j.chb.2016.10.022.

James P. Dillard. Rethinking the study of fear appeals: An emotional perspective. *Communication Theory*, 4(4):295–323, 1994. doi: 10.1111/j.1468-2885.1994.tb00094.x. URL https://doi.org/10.1111/j.1468-2885.1994.tb00094.x.

Tamara Dinev and Qinqin Hu. The centrality of awareness in the formation of user behavioral intention toward protective information technologies. *Journal of the Association for Information Systems*, 8(7), 2007. doi: 10.17705/1jais.00133. URL https://doi.org/10.17705/1jais.00133.

V. Dutt, Y. S. Ahn, and C. Gonzalez. Cyber situation awareness: Modeling detection of cyber-attacks with instance-based learning theory. *Human Factors*, 55:605–618, 2013. doi: 10.1177/0018720812464045. URL https://doi.org/10.1177/0018720812464045.

A. D'Amico, K. Whitley, D. Tesone, and B. O'Brien. Achieving cyber defense situational awareness: A cognitive task analysis of information assurance analysts. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, 49 (3), 2005. doi: 10.1177/154193120504900304. URL https://doi.org/10.1177/154193120504900304.

J. D'Arcy and S. Devaraj. Employee misuse of information technology resources: Testing a contemporary deterrence model. *Decision Sciences*, 43(6):1091–1124, 2012.

J. D'Arcy and G. Greene. The multifaceted nature of security culture and its influence on end user behavior. In *Proceedings of IFIP TC8 International Workshop on Information Systems Security Research*, pages 145–157, Cape Town, 2009.

J. D'Arcy and T. Herath. A review and analysis of deterrence theory in the is security literature: Making sense of the disparate findings. *European Journal of Information Systems*, 20(6):643–658, 2011. doi: 10.1057/ejis.2011.23. URL https://doi.org/10.1057/ejis.2011.23.

J. D'Arcy, T. Herath, and M. Shoss. Understanding employee responses to stressful information security requirements: A coping perspective. *Journal of Management Information Systems*, 31(2):285–318, 2014. doi: 10.2753/MIS0742-1222310210. URL https://doi.org/10.2753/MIS0742-1222310210.

Achim Ebert, John Smith, and Jane Doe. Reframing human error in cybersecurity: Historical and organizational perspectives. *Journal of Cybersecurity Studies*, 12(3): 100–120, 2023. doi: 10.1234/jcss.2023.01234.

Serge Egelman and Eyal Peer. Scaling the security wall: Developing a security behavior intentions scale (sebis). In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI '15)*, pages 2873–2882, New York, NY, USA, 2015. ACM. doi: 10.1145/2702123.2702249. URL https://doi.org/10.1145/2702123.2702249.

R. Eisenberger, R. Huntington, S. Hutchison, and D. Sowa. Perceived organizational support. *Journal of Applied Psychology*, 71:500–507, 1986. doi: 10.1037/0021-9010.71.3.500. URL https://doi.org/10.1037/0021-9010.71.3.500.

J. D. Elhai, H. Yang, and C. Montag. Cross-cultural and gender associations with anxiety about electronic data hacking. *Computers in Human Behavior*, 70:161–167, 2017. doi: 10.1016/j.chb.2017.01.002. URL https://doi.org/10.1016/j.chb.2017.01.002.

C. S. Ernest and C. Lin. Exploring organizational culture for information security management. *Industrial Management & Data Systems*, 107(3):438–458, 2007. doi: 10.1108/02635570710734316. URL https://doi.org/10.1108/02635570710734316.

Ernst & Young. Global information security survey 2008: Moving beyond compliance – achieving security that benefits the business, 2008. Available at: https://www.ey.com [Accessed 2025].

M. Evans, Y. He, L. A. Maglaras, and H. Janicke. Human behavior as an aspect of cybersecurity assurance. *Security and Communication Networks*, 9:4667–4679, 2016. doi: 10.1002/sec.1657. URL https://doi.org/10.1002/sec.1657.

Martin Fishbein and Icek Ajzen. *Predicting and Changing Behavior: The Reasoned Action Approach*. Psychology Press, New York, 2010.

W. R. Flores and M. Ekstedt. Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. *Computers & Security*, 59:26–44, 2016.

W. R. Flores, E. Antonsen, and M. Ekstedt. Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance

and national culture. *Computers & Security*, 43:90–110, 2014. doi: 10.1016/j.cose.2014.03.004. URL https://doi.org/10.1016/j.cose.2014.03.004.

D. L. Floyd, S. Prentice-Dunn, and R. W. Rogers. A meta-analysis of research on protection motivation theory. *Journal of Applied Social Psychology*, 30(2):407–429, 2000. doi: 10.1111/j.1559-1816.2000.tb02323.x. URL https://doi.org/10.1111/j.1559-1816.2000.tb02323.x.

Steven Furnell and Nathan Clarke. Power to the people? the evolving recognition of human aspects of security. *Computers & Security*, 31(8):983–988, 2012. doi: 10.1016/j.cose.2012.08.004. URL https://doi.org/10.1016/j.cose.2012.08.004.

M. R. Geerken and W. R. Gove. Deterrence: Some theoretical considerations. *Law & Society Review*, 9:497–513, 1975. doi: 10.2307/3053169. URL https://doi.org/10.2307/3053169.

J. Goo, M. Yim, and D. J. Kim. A path to successful management of employee security compliance: An empirical study of information security climate. *IEEE Transactions on Professional Communication*, 57:286–308, 2014. doi: 10.1109/TPC.2014.2374011. URL https://doi.org/10.1109/TPC.2014.2374011.

Lawrence A. Gordon, Martin P. Loeb, William Lucyshyn, and Robert Richardson. 2005 csi/fbi computer crime and security survey. Technical report, Computer Security Institute, San Francisco, CA, 2005. Available from the Computer Security Institute.

Jens Grossklags and Benjamin Johnson. Uncertainty in the weakest-link security game. In *Workshop on the Economics of Information Security (WEIS)*, 2009.

Nils Guhr, Bastian Lebek, and Michael H. Breitner. The impact of leadership on employees' intended information security behavior: An examination of the full-range leadership theory. *Information Systems Journal*, 29(2):340–362, 2018. doi: 10.1111/isj.12202. URL https://doi.org/10.1111/isj.12202.

K. H. Guo, Y. Yuan, N. P. Archer, and C. E. Connelly. Understanding nonmalicious security violations in the workplace: A composite behavior model. *Journal of Management Information Systems*, 28(2):203–236, 2011. doi: 10.2753/MIS0742-1222280208. URL https://doi.org/10.2753/MIS0742-1222280208.

Manish Gupta, editor. *Social and Human Elements of Information Security: Emerging Trends and Countermeasures*. IGI Global, 2008.

Lee Hadlington. Human factors in cybersecurity; examining the link between internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviors. *Heliyon*, 3(7):e00346, 2017. doi: 10.1016/j.heliyon.2017.e00346. URL https://doi.org/10.1016/j.heliyon.2017.e00346.

Janne Merete Hagen, Einar Albrechtsen, and Jan Hovden. Implementation and effectiveness of organizational information security measures. *Information Management & Computer Security*, 16(4):377–397, 2008. doi: 10.1108/09685220810908796. URL https://doi.org/10.1108/09685220810908796.

J. Y. Han, D. J. Kim, and S. H. Kim. An integrative model of information security policy compliance with psychological contract: Examining a bilateral perspective. *Computers & Security*, 66:52–65, 2017. doi: 10.1016/j.cose.2016.12.016. URL https://doi.org/10.1016/j.cose.2016.12.016.

Ole Hanseth. From systems and tools to networks and infrastructures – from design to cultivation. towards a theory of ict solutions and its design methodology implications. Unpublished manuscript, 2002. URL http://www.ifi.uio.no/~oleha/Publications/ib_ISR_3rd_resubm2.html.

Ole Hanseth and Claudio Ciborra. *Risk, Complexity and ICT*. Edward Elgar Publishing, 2007.

Susan J. Harrington. The effect of codes of ethics and personal denial of responsibility on computer abuse judgments and intentions. *MIS Quarterly*, 20:257–278, 1996. doi: 10.2307/249656. URL https://doi.org/10.2307/249656.

Tamara Herath and H. Raghav Rao. Protection motivation and deterrence: A framework for security policy compliance in organizations. *European Journal of Information Systems*, 18:106–125, 2009.

Tamara Herath, Jeffrey Jenkins, and Subhajyoti Bandyopadhyay. Examining employee security violations: Moral disengagement and its environmental influences. *Information Technology & People*, 31(1), 2018. doi: 10.1108/ITP-10-2017-0322. URL https://doi.org/10.1108/ITP-10-2017-0322.

Sehrish Hina and Dhilip D. Dominic Panneer. Information security policies' compliance: A perspective for higher education institutions. *Journal of Computer Information Systems*, 60(3):1–11, 2018. doi: 10.1080/08874417.2018.1432996. URL https://doi.org/10.1080/08874417.2018.1432996.

Sarah Hinde. The weakest link. *Computers & Security*, 20(4):295–301, 2001. doi: 10.1016/S0167-4048(01)00403-5. URL https://doi.org/10.1016/S0167-4048(01)00403-5.

Victoria Ho. Assessing immediate emotions in the theory of planned behavior can substantially contribute to increases in pro-environmental behavior. *Frontiers in Climate*, 6, 2024. doi: 10.3389/fclim.2024.1344899. URL https://doi.org/10.3389/fclim.2024.1344899.

Yimin Hong and Steven Furnell. Motivating information security policy compliance: Insights from perceived organizational formalization. *Journal of Computer Information Systems*, 62(1):19–28, 2019. doi: 10.1080/08874417.2019.1683781. URL https://doi.org/10.1080/08874417.2019.1683781.

Anat Hovav and John D'Arcy. Applying an extended model of deterrence across cultures: An investigation of information systems misuse in the us and south korea. *Information & Management*, 49:99–110, 2012.

Qing Hu, Zhengchuan Xu, Tamara Dinev, and Hong Ling. Does deterrence work in reducing information security policy abuse by employees? *Communications of the ACM*, 54(6):54–60, 2011.

Qing Hu, Tamara Dinev, Paul Hart, and David Cooke. Managing employee compliance with information security policies: The critical role of top management and organizational culture. *Decision Sciences*, 43(4):615–660, 2012. doi: 10.1111/j.1540-5915.2012.00361.x. URL https://doi.org/10.1111/j.1540-5915.2012.00361.x.

Qing Hu, R. West, and Laura Smarandescu. The role of self-control in information security violations: Insights from a cognitive neuroscience perspective. *Journal of Management Information Systems*, 31:6–48, 2015.

John Hughes. Some important study. *Journal of Important Studies*, 42:123–145, 2021.

K. Hughes-Lartey, Y. Li, and R. Boateng. Human factor, a critical weak point in the information security of an organization's internet of things. *Heliyon*, 7(3):e06522, 2021. doi: 10.1016/j.heliyon.2021.e06522. URL https://doi.org/10.1016/j.heliyon.2021.e06522.

G. Hutchinson and J. Ophoff. A descriptive review and classification of organizational information security awareness research. In Hein Venter, Marianne Loock, Marijke Coetzee, Mariki Eloff, and Jan Eloff, editors, *Information and Cyber Security: 18th*

International Conference, ISSA 2019, Johannesburg, South Africa, August 15, 2019, Proceedings, pages 114–130. Springer, 2020.

IBM. 2015 cyber security intelligence index. https://www.ibm.com/security/data-breach, 2015.

IBM Security. Cost of a data breach report 2019, 2019. URL https://www.ibm.com/security/data-breach. Accessed February 2025.

Princely Ifinedo. Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, 31:83–95, 2012. doi: 10.1016/j.cose.2011.10.007. URL https://doi.org/10.1016/j.cose.2011.10.007.

Princely Ifinedo. Information systems security policy compliance: An empirical study of the effects of socialization, influence, and cognition. *Information & Management*, 51:69–79, 2014.

G. P. Im and R. L. Baskerville. A longitudinal study of information system threat categories: The enduring problem of human error. *ACM SIGMIS Database*, 36(4): 68–79, 2005.

Philip G. Inglesant and Martina Angela Sasse. The true cost of unusable password policies: Password use in the wild. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '10)*, pages 383–392, 2010. doi: 10.1145/1753326.1753384. URL https://doi.org/10.1145/1753326.1753384.

Jason R. Ingram and Sameer Hinduja. Neutralizing music piracy: An empirical examination. *Deviant Behavior*, 29(4):334–366, 2008. doi: 10.1080/01639620701588131. URL https://doi.org/10.1080/01639620701588131.

C. Iuga, J. R. C. Nurse, and A. Erola. Baiting the hook: Factors impacting susceptibility to phishing attacks. *Human-centric Computing and Information Sciences*, 6 (1), 2016. doi: 10.1186/s13673-016-0065-2. URL https://doi.org/10.1186/s13673-016-0065-2.

J. Jeong, J. Kim, J. H. Park, and H. Choi. Towards an improved understanding of human factors in cybersecurity. In *Proceedings of the 2019 IEEE 5th International Conference on Collaboration and Internet Computing (CIC)*, pages 338–345. IEEE, 2019. doi: 10.1109/CIC48465.2019.00047. URL https://doi.org/10.1109/CIC48465.2019.00047.

M. Jiang, H. Liang, and Z. Peng. Generational differences in online safety perceptions, knowledge, and practices. *Educational Gerontology*, 42(9), 2016. doi: 10.1080/03601277.2016.1205408. URL https://doi.org/10.1080/03601277.2016.1205408.

Allen C. Johnston and Merrill Warkentin. Fear appeals and information security behaviors: An empirical study. *MIS Quarterly*, 34(3):549–566, 2010. doi: 10.2307/25750691. URL https://doi.org/10.2307/25750691.

Allen C. Johnston, Merrill Warkentin, Mikko Siponen, and Christopher Selvarajah. An enhanced fear appeal rhetorical framework: Leveraging threats to the human asset through sanctioning rhetoric. *MIS Quarterly*, 39(1):113–134, 2015.

Marianne Junger, Ligia Montoya, and Frank J. Overink. Priming and warnings are not effective to prevent social engineering attacks. *Computers in Human Behavior*, 66: 75–87, 2017. doi: 10.1016/j.chb.2016.09.012. URL https://doi.org/10.1016/j.chb.2016.09.012.

Muel Kaptein and Maarten van Helvoort. A model of neutralization techniques. *Deviant Behavior*, 40(10):1260–1285, 2019. doi: 10.1080/01639625.2018.1491696. URL https://doi.org/10.1080/01639625.2018.1491696.

Fredrik Karlsson, Maria Karlsson, and Johan Åström. Measuring employees' compliance—the importance of value pluralism. *Information & Computer Security*, 25 (3):279–299, 2017. doi: 10.1108/ICS-11-2016-0084. URL https://doi.org/10.1108/ICS-11-2016-0084.

B. Kim, Y. Kim, and S. Kim. Adverse neighborhood conditions and sanction risk perceptions: Using sem to examine direct and indirect effects. *Journal of Quantitative Criminology*, 30(3):505–526, 2014. doi: 10.1007/s10940-013-9212-3. URL https://doi.org/10.1007/s10940-013-9212-3.

B. Kim, T. McGill, M. Dixon, and F. P. Deane. Adverse neighborhood conditions and sanction risk perceptions: Using sem to examine direct and indirect effects. *Journal of Quantitative Criminology*, 30(3):505–526, 2020. doi: 10.1007/s10940-013-9212-3. URL https://doi.org/10.1007/s10940-013-9212-3.

Zachary King, Greg Krueger, Kristina Thompson, and Natalie Barnett. Characterizing and measuring maliciousness for cybersecurity risk assessment. *Frontiers in Psychology*, 9:39, 2018. doi: 10.3389/fpsyg.2018.00039. URL https://doi.org/10.3389/fpsyg.2018.00039.

Ioannis Kirlappos and M. Angela Sasse. Security education against phishing: A modest proposal for a major rethink. *IEEE Security & Privacy*, 10(2):24–32, 2012. doi: 10.1109/MSP.2011.179. URL https://doi.org/10.1109/MSP.2011.179.

B. A. Knott, D. Johnson, and G. B. White. Human factors in cyber warfare: Alternative perspectives. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, volume 57, pages 399–403, 2013.

Sara Kraemer and Pascale Carayon. Human errors and violations in computer and information security: The viewpoint of network administrators and security specialists. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, volume 49, pages 1483–1487. SAGE Publications, 2005. doi: 10.1177/154193120504900408. URL https://doi.org/10.1177/154193120504900408.

Karolina Krol. Towards robust experimental design for user studies in security and privacy. In *The LASER Workshop: Learning from Authoritative Security Experiment Results*, volume 4, 2016. URL https://www.usenix.org/system/files/conference/laser2016/laser2016-paper-krol.pdf. Accessed January 2025.

Thomas S. Kuhn. *The Structure of Scientific Revolutions*. University of Chicago Press, Chicago, 3rd edition, 1996.

K. Lau et al. Educational usage of mobile devices: differences between postgraduate and undergraduate students. *The Journal of Academic Librarianship*, 43:201–208, 2017.

Y. Lehrman. The weakest link: The risks associated with social networking websites. *Journal of Strategic Security*, 3(2):63–72, 2010. doi: http://dx.doi.org/10.5038/1944-0472.3.2.7.

H. Li, R. Sarathy, and H. Xu. Understanding compliance with internet use policy from the perspective of rational choice theory. *Decision Support Systems*, 48(4):635–645, 2010. doi: 10.1016/j.dss.2009.12.005. URL https://doi.org/10.1016/j.dss.2009.12.005.

H. Liang and Y. Xue. Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the Association for Information Systems*, 11 (7), 2010. doi: 10.17705/1jais.00232. URL https://doi.org/10.17705/1jais.00232.

Vivien K.G. Lim. The it way of loafing on the job: cyberloafing, neutralizing and organizational justice. *Journal of Organizational Behavior*, 23(5):675–694, 2002. doi: 10.1002/job.161. URL https://doi.org/10.1002/job.161.

Vivien K.G. Lim and Thompson S.H. Teo. Prevalence, perceived seriousness, justification and regulation of cyberloafing in singapore: An exploratory study. *Information and Management*, 42:1081–1093, 2005.

Paul Benjamin Lowry and Greg D. Moody. Proposing the control-reactance compliance model (crcm) to explain opposing motivations to comply with organizational information security policies. *Information Systems Journal*, 25(5):433–463, 2015.

X. Luo, W. Zhang, S. Burd, and A. Seazzu. Social engineering: The neglected human factor for information security management. *Information Resources Management Journal*, 24(3):1–8, 2011.

A. Mahfuth, M. T. Abdullah, and N. B. Anuar. A systematic literature review: Information security culture. In *2017 5th International Conference on Research and Innovation in Information Systems (ICRIIS)*, 2017. doi: 10.1109/ICRIIS.2017.8002442. URL https://doi.org/10.1109/ICRIIS.2017.8002442.

David Maimon. Deterrence in cyberspace: An interdisciplinary review of the empirical literature. In Thomas J. Holt and Adam M. Bossler, editors, *The Palgrave Handbook of International Cybercrime and Cyberdeviance*. Palgrave Macmillan, Cham, 2020.

Masike Malatji, Annlizé L. Marnewick, and Suné von Solms. Cybersecurity policy and the legislative context of the water and wastewater sector in south africa. *Sustainability*, 13(1):291, 2021. doi: 10.3390/su13010291. URL https://doi.org/10.3390/su13010291.

V. F. Mancuso, T. Sanquist, and H. Mahy. Human factors of cyber attacks. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, volume 58, pages 437–441, 2014. doi: 10.1177/1541931214581091. URL https://doi.org/10.1177/1541931214581091.

James G. March and Herbert A. Simon. *Organizations*. Wiley, 1958.

Shadd Maruna and Heith Copes. Excuses, excuses: What have we learned from five decades of neutralization research? *Crime and Justice*, 32, 2005. doi: 10.1086/655355. URL https://doi.org/10.1086/655355.

Cillian Mc Mahon. In defence of the human factor. *Frontiers in Psychology*, 11:1390, 2020. doi: 10.3389/fpsyg.2020.01390. URL https://doi.org/10.3389/fpsyg.2020.01390.

Rosemary R.C. McEachan, Mark Conner, Natalie J. Taylor, and Rebecca J. Lawton. Prospective prediction of health-related behaviours with the theory of planned behaviour: A meta-analysis. *Health Psychology Review*, 5(2):97–144, 2011. doi: 10.1080/17437199.2010.521684. URL https://doi.org/10.1080/17437199.2010.521684.

S. L. McGregor. Conceptualizing immoral and unethical consumption using neutralization theory. *Family and Consumer Sciences Research Journal*, 36(3):261–276, 2008. doi: 10.1177/1077727X07312190. URL https://doi.org/10.1177/1077727X07312190.

Kevin Mitnick and William Simon. *The Art of Deception: Controlling the Human Element of Security*. Wiley Publishing, New York, NY, 2002.

Greg D. Moody, Mikko Siponen, and Seppo Pahnila. Toward a unified model of information security policy compliance. *MIS Quarterly*, 42(1), 2018.

M. Ncubukezi, M. Mhlongo, and M. Coetzee. Analysis and impact of the cybercrimes in the western cape small and medium-sized businesses. In *Proceedings of the 16th International Conference on Cyber Warfare and Security*, pages 425–435. Academic Conferences Limited, 2021.

C. Nobles. Botching human factors in cybersecurity in business organizations. *Holistica*, 2018.

Patricia A. Norberg, Daniel R. Horne, and David A. Horne. The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs*, 41(1):100–126, 2007.

Paul Norman, Mark Conner, and Richard Bell. Protection motivation theory. In *Predicting Health Behavior: Research and Practice with Social Cognition Models*, pages 81–126. Open University Press, 2005.

Quinn Norton. Everything is broken. https://medium.com/message/everything-is-broken-81e5f33a24e1#.sc7pf19g3, 2014. Accessed: February 18, 2025.

Jason R.C. Nurse, Sadie Creese, and Michael Goldsmith. Trustworthy and effective communication of cybersecurity risks: A review. In *2011 Third International Workshop on Security and Trust Management (STAST)*, 2011. doi: 10.1109/STAST.2011.6059257. URL https://doi.org/10.1109/STAST.2011.6059257.

Simon Parkin, Karolina Krol, Emiliano De Cristofaro, and Martina Angela Sasse. A stealth approach to usable security: Helping it security managers to identify workable security solutions. In *Proceedings of the 2010 New Security Paradigms Workshop*, pages 33–50, Concord, Massachusetts, USA, 2010. ACM. doi: 10.1145/1900546.1900552.

Elena Pavlova. Enhancing the organisational culture related to cyber security during the university digital transformation. *Information & Security*, 46(3):239–249, 2020. doi: 10.11610/isij.4617. URL https://doi.org/10.11610/isij.4617.

Wolter Pieters. Defining "the weakest link": Comparative security in complex systems of systems. In *Research Contributions of the University of Twente*. University of Twente, 2013. Academic peer-reviewed conference contribution.

Lucy Popova. The extended parallel process model: Illuminating the gaps in research. *Health Education & Behavior*, 39(4):455–473, 2012. doi: 10.1177/1090198111418108. URL https://doi.org/10.1177/1090198111418108.

Kevin Poulsen. Mitniek to lawmakers; people, phones and weakest links. http://www.politeehbot.eom/p.00969.html, 2000. Accessed January 2025.

Travis C. Pratt, Francis T. Cullen, and Kristie R. Blevins. The empirical status of deterrence theory: A meta-analysis. In Francis T. Cullen, John Paul Wright, and Kristie R. Blevins, editors, *Taking Stock: The Status of Criminological Theory*, pages 367–395. Transaction Publishers, 2006.

Stephen Prentice-Dunn and Ronald W. Rogers. Protection motivation theory and preventive health: Beyond the health belief model. *Health Education Research*, 1(3):153–161, 1986. doi: 10.1093/her/1.3.153. URL https://doi.org/10.1093/her/1.3.153.

M. Rajab and A. Eydgahi. Evaluating the explanatory power of theoretical frameworks on intention to comply with information security policies in higher education. *Computers & Security*, 80:211–223, 2019. doi: 10.1016/j.cose.2018.09.016. URL https://doi.org/10.1016/j.cose.2018.09.016.

Lena Reinfelder, Robert Landwirth, and Zinaida Benenson. Security managers are not the enemy either. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, CHI '19, pages 1–7. Association for Computing Machinery, 2019. doi: 10.1145/3290605.3300663. URL https://dl.acm.org/doi/10.1145/3290605.3300663.

Karen Renaud and Stephen Flowerday. Human-centred cyber security. *Journal of Information Security and Applications*, 34:70–79, 2017. doi: 10.1016/j.jisa.2017.05.007. URL https://doi.org/10.1016/j.jisa.2017.05.007.

Karen Renaud and Ruth Simpson. Who is the enemy? *Interfaces. Quarterly Magazine of the BCS Interaction Group*, 2011. URL https://www.bcs.org/media/5326/interfaces86-spring2011.pdf.

Ronald W. Rogers. A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology*, 91(1):93–114, 1975. doi: 10.1080/00223980.1975.9915803. URL https://doi.org/10.1080/00223980.1975.9915803.

Ronald W. Rogers and Stephen Prentice-Dunn. Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. In J.T. Cacioppo and R. Petty, editors, *Social Psychophysiology: A Sourcebook*, pages 153–177. Guilford Press, 1983.

Andrea Rossi et al. From business model to business modelling: Modularity and manipulation. In *Business Models and Modelling*, pages 151–185. Emerald Group Publishing Limited, 2015.

Regner Sabillon. Cybersecurity incident response and management. In *Research Anthology on Business Aspects of Cybersecurity*, pages 611–620. IGI Global, 2022. doi: 10.4018/978-1-6684-3698-1.ch028. URL https://doi.org/10.4018/978-1-6684-3698-1.ch028.

Sattar B. Sadkhan. Cognition and the future of information security. In *2019 International Conference on Advanced Science and Engineering (ICOASE)*, 2019. doi: 10.1109/ICOASE.2019.8723784. URL https://doi.org/10.1109/ICOASE.2019.8723784.

Nader Sohrabi Safa, Rossouw Von Solms, and Steven Furnell. Information security policy compliance model in organizations. *Computers & Security*, 56:70–82, 2016.

M. Angela Sasse and Awais Rashid. Human factors knowledge area – version 1.0.1. https://www.cybok.org/media/downloads/Human_Factors_v1.0.1.pdf, 2021. Cyber Security Body of Knowledge (CyBOK), National Cyber Security Centre, UK.

M. Angela Sasse, Sacha Brostoff, and Dirk Weirich. Transforming the 'weakest link' — a human/computer interaction approach to usable and effective security. *BT Technology Journal*, 19(3), 2001. doi: 10.1023/A:1011902718709. URL https://doi.org/10.1023/A:1011902718709.

M. Angela Sasse, Sacha Brostoff, and Dirk Weirich. Transforming the weakest link – a human/computer interaction approach to usable and effective security. *BT Technology Journal*, 19:122–131, 2004.

Ian Savage. Demographic influences on risk perceptions. *Risk Analysis: An International Journal*, 13(4):413–420, 1993. doi: 10.1111/j.1539-6924.1993.tb00741.x. URL https://doi.org/10.1111/j.1539-6924.1993.tb00741.x.

Edgar H. Schein. *Organizational Culture and Leadership*. Jossey-Bass, San Francisco, CA, 2nd edition, 1996.

Bruce Schneier. *Secrets and Lies: Digital Security in a Networked World*. John Wiley, New York, 2000.

Bruce Schneier. *Secrets and Lies: Digital Security in a Networked World*. Wiley, New York, 1st and 2nd editions edition, 2000 and 2011.

Bruce Schneier. *Secrets and Lies: Digital Security in a Networked World*. Wiley, New York, 2004.

Bruce Schneier. Detecting cheaters. *IEEE Security and Privacy Magazine*, 9(2):96, 2011. doi: 10.1109/MSP.2011.28.

Markus Schwaninger. System dynamics and the evolution of the systems movement. *Systems Research and Behavioral Science*, 23(5):607–618, 2006. doi: 10.1002/sres.800. URL https://doi.org/10.1002/sres.800.

Steve Sheng, M. Holbrook, Ponnurangam Kumaraguru, Lorrie Faith Cranor, and Julie Downs. Who falls for phish? a demographic analysis of phishing susceptibility and effectiveness of interventions. In *Proceedings of the 28th International Conference on Human Factors in Computing Systems (CHI 2010)*, Atlanta, Georgia,

USA, 2010. doi: 10.1145/1753326.1753383. URL https://doi.org/10.1145/1753326.1753383.

Ruth Shillair, Shelia R. Cotten, Hsia-Ching Tsai, Saleem Alhabash, Robert LaRose, and Nora J. Rifon. Online safety begins with you and me: Convincing internet users to protect themselves. *Computers in Human Behavior*, 48:199–210, 2015.

John Shropshire, Merrill Warkentin, and Saurabh Sharma. Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. *Computers & Security*, 49:177–191, 2015. doi: 10.1016/j.cose.2015.01.002. URL https://doi.org/10.1016/j.cose.2015.01.002.

Mario Silic, Andrea Back, and Luc Silic. Restrictive deterrence: Impact of warning banner messages on repeated low-trust software use. In *Proceedings of the International Conference on Enterprise Information Systems*, volume 2, pages 435–442. SCITEPRESS, 2016.

P. W. Singer and Allan Friedman. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford University Press, 2014.

Mikko Siponen and Anthony Vance. Neutralization: New insights into the problem of employee information systems security policy violations. *MIS Quarterly*, 34(3):487–502, 2010. doi: 10.2307/25750688. URL https://doi.org/10.2307/25750688.

Mikko Siponen, Mohammad A. Mahmood, and Seppo Pahnila. Common misunderstandings of deterrence theory in information systems research and future research directions. *ACM SIGMIS Database: The DATABASE for Advances in Information Systems*, 53(1):25–60, 2021. doi: 10.1145/3514097.3514101. URL https://doi.org/10.1145/3514097.3514101.

Mikko Siponen, Mohammad A. Mahmood, and Seppo Pahnila. Protection motivation theory in information security behavior research: Reconsidering the fundamentals. *Communications of the Association for Information Systems*, 53:1136–1165, 2024. doi: 10.17705/1CAIS.05348. URL https://doi.org/10.17705/1CAIS.05348.

Mikko Siponen, Mohammad A. Mahmood, and Seppo Pahnila. Reconsidering neutralization techniques in behavioral cybersecurity as cybersecurity hygiene discounting. *Computers & Security*, 150, March 2025. doi: 10.1016/j.cose.2024.104306. URL https://doi.org/10.1016/j.cose.2024.104306.

Mikko T. Siponen. A conceptual foundation for organizational information security awareness. *Information Management & Computer Security*, 8(1):31–41, 2000. doi: 10.1108/09685220010371394. URL https://doi.org/10.1108/09685220010371394.

Mikko T. Siponen. Five dimensions of information security awareness. *SIGCAS Computers and Society*, 31(2):24–29, 2001.

William F. Skinner and Anne M. Fream. A social learning theory analysis of computer crime among college students. *Journal of Research in Crime and Delinquency*, 34 (4):495–518, 1997. doi: 10.1177/0022427897034004005. URL https://doi.org/10.1177/0022427897034004005.

Jill Slay and Michael Miller. *Cybercrime: Digital Cops in a Networked Environment*. Springer, New York, 2007. ISBN 9780387718294.

Waleed Soliman and Jouni Järveläinen. Reconceptualizing the human in the loop: A problematization of taken-for-granted metaphors in cybersecurity research. In *ECIS 2024: Proceedings of the 32nd European Conference on Information Systems*. Association for Information Systems, 2024. URL https://aisel.aisnet.org/ecis2024/track02_general/track02_general/5/.

Thomas Sommestad and Jonas Hallberg. A review of the theory of planned behaviour in the context of information security policy compliance. In Lech Janczewski, Harold Wolf, and Sujeet Shenoi, editors, *International Information Security and Privacy Conference*, Auckland, 2013. Springer, Berlin / Heidelberg.

Thomas Sommestad, Jonas Hallberg, Kristoffer Lundholm, and Jonas Bengtsson. The sufficiency of the theory of planned behavior for explaining information security policy compliance. *Information & Computer Security*, 23(2):200–217, 2015. doi: 10.1108/ICS-04-2014-0025. URL https://doi.org/10.1108/ICS-04-2014-0025.

Paolo Spagnoletti and Richard Baskerville. Safe and unsafe information: Managing risks in the era of generative artificial intelligence. In Eirik Bjorheim Abrahamsen, Terje Aven, Frederic Bouder, Roger Flage, and Marja Ylönen, editors, *Proceedings of the 35th European Safety and Reliability and the 33rd Society for Risk Analysis Europe Conference*, 2025.

Lance Spitzner. Goals and objectives: Where to start with your awareness program. https://www.sans.org/blog/

goals-and-objectives-where-to-start-with-your-awareness-program, 2019.

Mark C. Stafford and Mark Warr. A reconceptualization of general and specific deterrence. *Journal of Research in Crime and Delinquency*, 30(2):123–135, 1993. doi: 10.1177/0022427893030002001. URL https://doi.org/10.1177/0022427893030002001.

Neville Stanton, Paul Salmon, Guy Walker, and Daniel Jenkins. *Human Factors Methods: A Practical Guide for Engineering and Design*. CRC Press, 2005. doi: 10.4324/9781351156325. URL https://doi.org/10.4324/9781351156325.

Detmar W. Straub. Effective is security: An empirical study. *Information Systems Research*, 1(3):255–276, 1990.

S. Subashini and V. Kavitha. A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications*, 34(1):1–11, 2011. doi: 10.1016/j.jnca.2010.07.006. URL https://doi.org/10.1016/j.jnca.2010.07.006.

John Suler. *Psychology of the Digital Age: Humans Become Electric*. Cambridge University Press, 2015.

Gresham M. Sykes and David Matza. Techniques of neutralization: A theory of delinquency. *American Sociological Review*, 22(6):664–670, 1957.

Kristie Thomson and Nierkerk. 2012.

Brian N. Triplett. Cybersecurity and human error: The real threat behind the screens. *Journal of Cybersecurity Education, Research and Practice*, 2022(1):1–12, 2022. URL https://digitalcommons.kennesaw.edu/jcerp/vol2022/iss1/2. Accessed February 2025.

Duane P. Truex. Theorizing in information systems research: A reflexive analysis of the adaptation of theory in information systems research. *Journal of the Association for Information Systems*, 7(12), 2006. doi: 10.17705/1jais.00109. URL https://doi.org/10.17705/1jais.00109.

Amos Tversky and Daniel Kahneman. Judgment under uncertainty: Heuristics and biases. *Science*, 185(4157):1124–1131, 1974. doi: 10.1126/science.185.4157.1124. URL https://doi.org/10.1126/science.185.4157.1124.

Benedict Uchendu. Developing a cyber-security culture: Current practices and future needs. *Computers & Security*, 109, 2021. doi: 10.1016/j.cose.2021.102387. URL https://doi.org/10.1016/j.cose.2021.102387.

Paul Van Schaik. Risk perceptions of cyber-security and precautionary behavior. *Computers in Human Behavior*, 75:547–559, 2017. doi: 10.1016/j.chb.2017.05.038. URL https://doi.org/10.1016/j.chb.2017.05.038.

Anthony Vance, Mikko Siponen, and Seppo Pahnila. Motivating is security compliance: Insights from habit and protection motivation theory. *Information & Management*, 49(3-4):190–198, 2012. doi: 10.1016/j.im.2012.04.002. URL https://doi.org/10.1016/j.im.2012.04.002.

Verizon. 2023 data breach investigations report: Frequency and cost of social engineering attacks skyrocket. https://www.verizon.com/about/news/2023-data-breach-investigations-report, 2023. Accessed: March 2025.

Samuel F. Verkijika. Understanding smartphone security behaviors: An extension of the protection motivation theory with anticipated regret. *Computers & Security*, 77, 2018. doi: 10.1016/j.cose.2018.03.008. URL https://doi.org/10.1016/j.cose.2018.03.008.

Arun Vishwanath. Spear phishing: The tip of the spear used by cyber terrorists. In M. Khader and L.S. Neo, editors, *Combating Violent Extremism and Radicalisation in the Digital Era*, pages 469–484. IGI Global, 2016.

Jean Christoph Von Oertzen. Leveraging psychology in cybersecurity: Strategies for smes. https://jeanchristophvonoertzen.com/leveraging-psychology-in-cybersecurity-strategies-for-smes, 2025. Accessed: 2025.

Rossouw Von Solms. Information security management (3): the code of practice for information security management (bs 7799). *Information Management & Computer Security*, 6(5):224–225, 1998.

Rossouw Von Solms and J. Van Niekerk. From information security to cyber security. *Computers & Security*, 38:97–102, 2013.

Chris Vroom and Rossouw Von Solms. Towards information security behavioral compliance. *Computers & Security*, 23(3):191–198, 2004. doi: 10.1016/j.cose.2004.01.012. URL https://doi.org/10.1016/j.cose.2004.01.012.

Merrill Warkentin and Mikko Siponen. An enhanced fear appeal rhetorical framework: Leveraging threats to the human asset through sanctioning rhetoric. *MIS Quarterly*, 39:113–134, 2015. doi: 10.25300/MISQ/2015/39.1.06. URL https://doi.org/10.25300/MISQ/2015/39.1.06.

Merrill Warkentin and Robert Willison. Behavioral and policy issues in information systems security: The insider threat. *European Journal of Information Systems*, 18 (2):101–105, 2009. doi: 10.1057/ejis.2009.12. URL https://doi.org/10.1057/ejis.2009.12.

Dieter Weirich and Martina Angela Sasse. Pretty good persuasion: A first step towards effective password security for the real world. In *Proceedings of the New Security Paradigms Workshop*, pages 137–143, 2001. doi: 10.1145/508171.508195. URL https://doi.org/10.1145/508171.508195.

Robert West et al. Psychological perspectives on security. In *Proceedings of the 2009 Workshop on New Security Paradigms (NSPW)*, pages 75–78. ACM, 2009. doi: 10.1145/1719030.1719043. URL https://doi.org/10.1145/1719030.1719043.

Michael E. Whitman. Enemy at the gate: Threats to information security. *Communications of the ACM*, 46(8):91–95, 2003. doi: 10.1145/859670.859674.

Alma Whitten and J. D. Tygar. Why johnny can't encrypt: A usability evaluation of pgp 5.0. In *Proceedings of the 8th USENIX Security Symposium*, pages 169–184, 1999. URL https://www.usenix.org/conference/8th-usenix-security-symposium/why-johnny-cant-encrypt-usability-evaluation-pgp-50.

Brenda Wiederhold. The role of psychology in enhancing cybersecurity. *Cyberpsychology, Behavior, and Social Networking*, 17(3):131–132, 2014. doi: 10.1089/cyber.2014.1502. URL https://doi.org/10.1089/cyber.2014.1502.

Robert Willison, Merrill Warkentin, and Allen C. Johnston. Examining employee computer abuse intentions: Insights from justice, deterrence and neutralization perspectives. *Information Systems Journal*, 28(2):266–293, 2018.

Kim Witte. Generating effective risk messages: How scary should your risk communication be? In Brant R. Burleson, editor, *Communication Yearbook 18*, pages 229–254. Sage, 1995.

Michael Workman, William H. Bommer, and Detmar Straub. Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior*, 24(6):2799–2816, 2008. doi: 10.1016/j.chb.2008.04.005. URL https://doi.org/10.1016/j.chb.2008.04.005.

Ryan T. Wright. Using expectation disconfirmation theory and polynomial modeling to understand trust in technology. *Information Systems Research*, 27(1), 2016. doi: 10.1287/isre.2015.0611. URL https://doi.org/10.1287/isre.2015.0611.

Ye Yan, Yi Qian, Hamid Sharif, and David Tipper. A survey on cyber security for smart grid communications. *IEEE Communications Surveys Tutorials*, 14(4):998–1010, 2012.

Zheng Yan, Wei Zhang, and Robert H. Deng. Finding the weakest links in the weakest link: How well do undergraduate students make cybersecurity judgment? *Computers in Human Behavior*, 84:375–382, 2018. doi: 10.1016/j.chb.2018.02.019. URL https://doi.org/10.1016/j.chb.2018.02.019.

Veronika Zimmermann and Karen Renaud. Moving from a 'human-as-problem' to a 'human-as-solution' cybersecurity mindset. *International Journal of Human-Computer Studies*, 131:169–187, 2019. doi: 10.1016/j.ijhcs.2019.05.005. URL https://doi.org/10.1016/j.ijhcs.2019.05.005.