

# **The Weakest Link in Cybersecurity Discourse between Hembig and Evidence-Based Argumentation - A Problematizing Review**

**Early stage paper**

**Jonna Järveläinen**

University of Jyväskylä,  
Finland  
jonna.k.jarvelainen@jyu.fi

**Wael Soliman**

University of Agder, Norway  
wael.soliman@uia.no

**Peppi Porjo**

University of Turku, Finland  
peppi.a.porjo@utu.fi

## **Abstract**

*The use of concepts is a vital part of the research process as they enable scholars to sharpen their thinking and communicate clearly about the phenomena they study. Without scrutiny and critical reflection, concepts risk becoming hegemonic, ambiguous, and unnecessarily big (recently described as the ‘hembig’ problem). We suspect that one of the concepts that reached such status in the cybersecurity discourse is the ‘weakest link’ (sometimes referred to as the ‘weakest link phenomenon’). This concept seems so prevalent in cybersecurity discourse that sometimes it is merely stated as a ‘matter of fact’ without evidence, reference to prior research, or even a proper explanation of what is meant by the ‘weakest link’. Who or what the ‘weakest link’ is varies significantly from one writing to another. It may refer to an employee, an individual, an end user, or humans in general. In line with the problematization review framework, this study aims to examine how the ‘weakest link’ concept has been used and abused in the cybersecurity literature. Our analysis demonstrates that prior research fails to provide a clear definition,*

*lacks evidence to support the claim, focuses on a single point of failure in the chain instead of grasping the complexity of the whole cybersecurity system, and attempts to argue simultaneously for the deskilling and upskilling of end-users. These findings emphasize the need to (a) exercise caution when building arguments based on superlatives such as the ‘weakest link’, and (b) move forward from blaming humans towards more constructive and empowering motivations in cybersecurity research.*

### **Keywords**

Cybersecurity, Weakest Link, Human Behavior, Problematizing Review.

## **INTRODUCTION**

The use of concepts is a vital part of the research process as they enable scholars to sharpen their thinking and communicate clearly about the phenomena they study (Alvesson & Blom, 2022). Indeed, from a semantic viewpoint, scholars require clearly defined concepts that invoke shared understanding to be able to conduct and disseminate their research activities. Without such shared understanding, the accumulation of knowledge would not be possible. Furthermore, paying attention to dominant concepts in scientific discourse is crucial since, aside from their communicative quality, concepts afford a ‘performative’ function (Gond et al., 2016). From a performative viewpoint, a distinction is often made between the locutionary quality of an utterance (i.e., the literal meaning of what is said), its illocutionary quality (i.e., the intent of an utterance), and its perlocutionary quality (i.e., the actual effect of an utterance whether intended or not). In that sense, we may use concepts with a particular meaning and intent in mind that provoke unintended and undesirable consequences. Considering their communicative and performative functions, emerging concepts in scientific discourse must be challenged and refined before they

are accepted (Hirsch & Levin, 1999). Failing to do so may produce concepts that are hegemonic, ambiguous, and big (or ‘hembig’ as coined by Alvesson & Blom (2022)). We suspect that one of the concepts that reached such status in the cybersecurity discourse is the ‘weakest link’ (sometimes referred to as the ‘weakest link phenomenon’, (e.g., Siponen & Baskerville, 2018; Willison & Warkentin, 2013; Yan et al., 2018)). Readers of the cybersecurity literature may be familiar with the opening statement of academic articles and industry reports that make superlative assertions like, “humans are the weakest link in the cybersecurity chain” and “employees are the biggest cybersecurity threat” (e.g., Guo et al., 2011; Hu et al., 2015; Warkentin et al., 2016). The argument of humans being the ‘weakest link’ seems so prevalent in cybersecurity discourse that sometimes it is merely stated as a claim without any references to prior research (e.g., Kumar et al., 2008; Nguyen et al., 2021; Zhuang et al., 2020).

The argument is often used as a premise leading to a logical conclusion typically in the following manner: “since humans are the weakest link, therefore human behavior in cybersecurity is important to study”. While we have no problem with the conclusion, we take issue with the premise. The ‘weakest link’ concept is rarely defined therefore it is highly ambiguous in nature. The concept is used in various contexts such as behavioral cybersecurity, econometric models of cybersecurity services, or cybercrime reporting. Sometimes it is used to refer to end users (Li et al., 2010), to employees (Lebek et al., 2013), to IoT devices (Repetto, 2023), and even space systems (Dygnatowski, 2021).

In line with the problematization review framework (Alvesson & Sandberg, 2020), this study aims to examine and reflect how the ‘weakest link’ concept has been used and abused in the cybersecurity literature. Our search identifies 337 papers from leading academic databases which used the concept ‘weakest link’ in some form and focused on cybersecurity or information security.

In a more thorough scan of 28 selected papers, we found that the term ‘weakest link’ was used to refer to humans, employees, end-users, individuals, or similar actors. We found that the lack of definitions has led to the concept being used ambiguously, focusing on a single “root cause” to be blamed for cybersecurity breaches when there usually are numerous other contributing factors.

Against this backdrop, in the following sections, we introduce the hembig concept, present our research-in-progress methodology, and the preliminary findings and problematize the use of the ‘weakest link’ in cybersecurity research. Finally, we present recommendations for future research

## **HEMBIGS IN SCIENTIFIC DISCOURSE**

Concepts play a vital role in scientific progress for at least two reasons: First, from a communicative viewpoint, scholars need clearly defined concepts that invoke shared understanding to conduct and disseminate their research activities. Second, from a performative viewpoint, concepts do not merely describe things; they do things. In other words, as Gond et al. (2016) put it: “[a] performative utterance is one ... in which by saying something we are doing something” (p. 443). As such, emerging concepts in scientific discourse must be challenged and refined, lest they risk becoming 'hembigs', characterized by being hegemonic, ambiguous and big (i.e., having too broad scope, Alvesson & Blom, 2022).

The first characteristic, hegemony, refers to “cultural and/or linguistic dominance at the expense of other alternative expressions and vocabulary” (Alvesson & Blom, 2022, p. 60). This kind of hegemony steers the researchers to repeat popular concepts instead of more exact terms, without questioning or criticizing them.

The second characteristic, ambiguity, refers to “vagueness and uncertainty associated with multiple, incoherent meanings attributed to a phenomenon ... [which] means that a group of

informed people are likely to hold multiple meanings and/or that several plausible interpretations can be made, without more data or rigorous analysis making it possible to assess them” (Alvesson & Blom, 2022, pp. 60–61).

The third characteristic, scope, is closely related to ambiguity as it refers to “the range of meanings attributed to a concept” (Alvesson & Blom, 2022, p. 61). They clarify that a concept with a broad (i.e., big) scope “involves a large number of more or less coherent meanings, which typically also leads to the concept being applied and used in a wide-ranging set of contexts and situations” (p. 61).

Scholars in various social science fields have begun to pay explicit attention to dominating concepts in their respective fields and question the extent to which these concepts qualify as hembigs. Solomon (2024) considers this as a necessary conceptual competence and calls it “hembig awareness” (p. 233). In organization research, it has been argued that dominating concepts, such as leadership and strategy (among others) are clear examples of hembigs (Alvesson & Blom, 2022). For instance, the ‘strategy’ concept has taken on different meanings as it traveled from its origin in the military, to organization, to the public sphere. Alvesson and Blom (2022) also note that “... as is often the case when a popular concept is travelling from domain to domain, its application, scope and meaning tend to vary ... Sometimes, organizational actors talking about strategy even deliberately reinforce the conceptual ambiguity (or ambiguities) in order to further their own agenda” (Alvesson & Blom, 2022, p. 65). The ‘leadership’ concept has been subjected to similar scrutiny, and it was noted that this concept “is often used very broadly, covering everything and nothing” (Alvesson & Blom, 2022, p. 64). Others have questioned the concept of ‘creativity’ in organization research for its vague and ambiguous nature (Karakilic & Painter, 2022). In business and management research, scholars are questioning the hegemonic ambiguity

of emerging concepts such as ‘circular economy’ (Dzhengiz et al., 2023). In accounting research, scholars have begun to question the hegemonic ambiguity of emerging concepts such as ‘social impact’ (Yang et al., 2021). Hembig awareness is present in IS research as well. Recently, Korotkova et al. (2023) have noticed the ambiguity associated with the conception of ‘trust’ and warned that the loose usage of the term may turn it into a hembig.

### **What is wrong with using hembigs?**

Aside from the obvious (as denoted by its defining elements), Alvesson and Blom (2022) pinpoint four crucial problems associated with hembigs. First, the uncritical use of hembigs may promote loose and vague thinking, leading to confusion between and within individual researchers. Second, uncritical use of hembigs may lead to ‘social amnesia’ when, at a collective level, researchers tend to “forget or ignore ... work outside [or challenges] the hembig” (Alvesson & Blom, 2022, p. 74). Third, uncritical use of hembigs may hinder creativity and novel thinking, often requiring open-mindedness to various interpretations beyond the hembig. Finally, hembigs can turn into a conceptual jungle requiring insider experts to be able to navigate them, while “newcomers and outsiders may find areas characterized by hembigs confusing, and much time and effort are called for just to get properly oriented” (Alvesson & Blom, 2022, p. 74).

### **Ambiguity and critical reflection**

So far, we have demonstrated the worries of having to deal with hembigs in various fields. Having said that, it is important not to conflate ‘hembig’ with ‘ambiguity’ which is not always seen in a negative light. For instance, Yang et al. (2021) have argued that in certain situations, ambiguity is not harmful, and can even be useful, as in the case of intentionally using ambiguous terms or concepts in scientific discourse to facilitate “attracting and gaining attention from researchers” (Yang et al., 2021, p. 315). Furthermore, ambiguity may serve as a vehicle to expand the

“interpretive space” which allows “a range of interested actors to buy into the idea [or concept], each for their own particular reasons” (Korotkova et al., 2023, p. 3). The key qualifier here is that to reap the benefits of ambiguity, it must be exercised with critical reflection. Without reflection, concepts risk becoming what Yang et al. (2021, pp. 315–316) describe as “empty ‘catch-all’ concepts”. The critical reflection and scrutiny of the use and abuse of concepts serve as the safety mechanism through which concepts in scientific discourse emerge and/or decline. From a lifecycle process perspective, concepts in a scientific field resemble the S-curve four-stage model: introduction, growth, maturity, and decline (Hirsch & Levin, 1999). In the domain of organization science, Hirsch and Levin (1999) demonstrate how a once-dominant concept of “organizational effectiveness” has gone through the four stages of (a) emerging excitement, (b) the validity challenge, and (c) tidying up efforts, before its eventual (d) construct collapse. This evolutionary perspective emphasizes the exceptional importance of the “validity challenge” phase, after which, concepts that deserve to persevere are refined and transformed, while others that do not stand the scrutiny decline and collapse. Conceptual hegemony is a real threat since “the hegemonic effect prevents or marginalizes effective critique, saving concepts from decline.” (Alvesson & Blom, 2022, p. 61).

## **METHODOLOGY**

To examine how the ‘weakest link’ concept has been used and abused in cybersecurity literature, we decided to do a problematizing literature review (Alvesson & Sandberg, 2020). We started with a systematic literature review and began from Web of Science and Scopus to find all the articles with the search phrase “weakest link” AND (“cybersecurity” OR “information security”). This search returned 123 papers from the Web of Science and 267 from Scopus, and after removing

duplicates, there were 305 papers. We included available full-text papers in English, leaving 246 papers.

We first went through all the journal articles and book chapters and checked for questions like: how many times was the ‘weakest link’ mentioned in the paper text (excluding mentions in the references)? What did the ‘weakest link’ refer to? What kind of evidence was used to support ‘weakest link’ claim? An in what context was it mentioned? This initial check left us with 21 articles that mentioned the phrase ‘weakest link’ either more than two times or in such a meaningful context that more careful examination was warranted. These papers focused on behavioral cybersecurity and mentioned humans, employees, individuals, etc. as the ‘weakest link’. Noticing that not many information systems science journals were included in the initial corpus, we decided to amend it by using the same search phrase for the Senior scholar premium list of journals. After removing the duplicates, we got 69 additions, which we inspected in the same manner. This left us 25 articles for more careful investigation and 18 possibly interesting articles, of which we decided to add three articles to the corpus since they represented an interesting category. These papers mentioned ‘weakest link’ only once, when trying to contrast the paper results against prior literature. See Appendix 1 for the literature review process. Since the work is currently in progress, we would like to emphasize that we have not yet done a backward or forward search of the literature, nor analyzed more deeply conference articles fitting the selection criteria (28).

However, as we wanted to reflect on the role of the ‘weakest link’ concept, we chose to read selectively as Alvesson and Sandberg (2020) recommended. We noticed that the articles used the concept in different sections of the paper, at the beginning (abstract and introduction), at the end (discussion and conclusions), or throughout the article. Thus, we chose to take a small sample of



each category and analyze them further. We were further inspired by Ebert et al's (2023) claim that the 'weakest link' concept stems from Taylor's scientific management and therefore we read Taylor (1919) and Braverman's (1998) critical perspective on it. As this is a research-in-progress paper, we will continue to build on those.

## **FINDINGS**

### **Locutionary use: Who (or what) is the 'weakest link'?**

The first research objective addresses the locutionary use of the 'weakest link' concept, that is, to identify who (or what) cybersecurity scholars are referring to as the 'weakest link'. Out of the 293 available papers, the 'weakest link' concept was mostly mentioned once (118 papers) or twice (102) in the text, 54 articles mentioned it 3-70 times, and 11 papers mentioned "weak link". 178 papers did not use any references linked to the concept, but stated it as a fact such as "Regardless of this trend, however, human beings are still the weakest link in the information security chain." (Chen et al., 2012) or "End users are often the weakest link in information security management." (Li et al., 2010). 114 papers used references; the most used references are listed in Appendix 2.

There was a lot of variation regarding who or what the 'weakest link' was (see Table 1), which can indicate ambiguity of the term (Alvesson & Blom, 2022). Sometimes the meaning of the 'weakest link' changed in the paper (see e.g., Borkovich & Skovira, 2020), for example, IS experts, people, IS employees, IS professionals in Ma and Cho (2022) or human beings, staff members, and human element in Mouton et al. (2016). Human(s), employee(s), people, individual(s), and user(s) or any term referring to a human agent were identified as the most common 'weakest links' in a total of 210 papers (out of 293). But there were also other more contextualized and specific weakest elements, for instance, countermeasure, cybercrime, data security, firewalls, governance

structures, home computers, insiders, IoT devices/systems, passwords, security of one system, space systems, technology, third party, etc.

The 'weakest link' is specified as	Example quotation	Number of articles
Employee(s)	Introduction: "In the literature, there is a general consensus that employees are the weakest link in the chain of information security, which is similar to data protection." (Foth, 2016, p. 92)	40
Human(s)	Abstract: "While phishing has evolved over the years, it still exploits one of the weakest links in any information system — humans." (Hanus et al., 2022, p. 516)	98
Individual(s)	Introduction: "Despite the fact that more and more individuals have become alert to cybersecurity threats, they are still often the weakest link in cybersecurity attacks [30]" (Ng et al., 2021, p. 732)	14
IoT	Abstract: "Even worse, due to their inherent characteristics, IoT systems are usually the weakest link in the security chain and thus many attacks utilize IoT technologies as their key enabler." (Stellios et al., 2021, p. 157)	4
People	Informing literature and conceptual model: "People are generally considered the weakest link in an information security program and to improve staff compliance, the policies need to be precise and clear with detailed procedures to follow (von Solms and von Solms, 2004a,b)." (Goel & Chengalur-Smith, 2010, p. 283)	24
Space systems	Conclusions: "Today, however, it is clear that space systems are the weakest link in the critical infrastructure systems." (Dygnatowski, 2021, p. 144)	1
User(s)	Introduction "Despite the growing investment in information security technology, users continue to represent the weakest link in security (Furnell & Clarke, 2012)" (B. B. Anderson et al., 2016, p. 364)	40

**Table 1. Examples of the use of the ‘weakest link’ in reviewed papers (since many papers had several ‘weakest links’ the total number is larger than in the text).**

### **Illocutionary use: What is the intended use of the concept?**

The second research objective addresses the illocutionary use of the ‘weakest link’ concept, that is, to identify the intended use of the as the ‘weakest link’ concept in the various cybersecurity writings. Our analysis points to salient uses: (a) as a motivation statement, (b) as part of argument building, and (c) as an explanation of study results. We discuss each of these uses next.

#### **The concept as a motivation**

In total 170 reviewed papers used the ‘weakest link’ concept as a motivation, in the abstract or introduction, but sometimes also in the theory section. The logic often was “Since humans are the weakest link, therefore we must study the topic X” (e.g., Borkovich & Skovira, 2020; Conteh & Royer, 2021; Kannelonning & Katsikas, 2023; Klein & Zwilling, 2023; Ng et al., 2021). “X as a weakest link” motivated several studies with a specific target group in mind.

Yan et al. (2021) identified K-12 school population as the ‘weakest link’ of the cybersecurity system both in the abstract and in the introduction of the paper, in which they studied the cybersecurity judgment of middle and high school students with a quantitative experiment using real-life scenarios and a questionnaire. They aimed for “novel contributions to address [...] the weakest link phenomenon” since they saw a “need of investigating K-12 students' cybersecurity judgment and the lack of a valid and reliable measurement” (p. 778). Chamkar et al. (2022) focused on security operation centers and the professionals working in them, stating that “[t]he human factor is considered the weakest link in cybersecurity and inside the Security Operation Centers (SOC) and it represents the most important component at the same time.” (p.1) With a survey of

40 specialists, they identified challenges for analysts working in SOCs and concluded that it was unrealistic to consider the SOC analysts as ‘weakest links’ and focus attention only on them. Torten et al. (2018) continued with the same idea, by focusing on IT professionals’ desktop security behavior with a survey of 400 professionals in the US. They stated that “[s]ocial engineering concentrates on the human elements, as humans are the weakest link in the security posture of any system network” (p. 68) and therefore, IT professionals with access to several systems were an attractive target for cybercriminals. Ma and Cho (2022) had a similar target group in their interview study of Chinese IT professionals focusing on different control formats, where they concluded that if the organizational security culture would change in the hierarchical Chinese organizations “they would help Chinese IT organizations transform IS professionals from organizations’ weakest links into their strongest links” (p. 21). De Kimpe et al. (2022) noticed in their survey that people who consider themselves well-informed about cybercrime do not take so many security measures. These exemplary studies show that the ‘weakest link’ can be almost any kind of user group.

Some studies did not focus on a particular user group but took a more general approach to security behavior. For example, Spears and Barki (2010) focused on security awareness creation by involving normal users (not only IT professionals) in risk assessment activities. They motivated their study by noting the following: “While the IS security literature often portrays users as the weak link in security, the current study suggests that users may be an important resource to IS security by providing needed business knowledge that contributes to more effective security measures.” (p. 503). The human-as-a-security-sensor paper (Vielberth et al., 2021) also aimed for another perspective than the ‘weakest link’ argument proposes, to reach the “full potential” of users who can generate incident information to complement existing methods (such as security analytics systems). They claimed that since “[h]umans are commonly seen as the weakest link in

corporate information security”, prior research should be amended by using their capabilities in detecting and reporting security incidents. Heartfield and Loukas (2018) saw the human as the strongest link of security and “challenged the concept that users are the weakest link against semantic attacks, instead, empowering them to become one of its strongest links for detecting deception-based threats” (p.125). They developed a practical prototype tool for users to report possible semantic attacks. Thomson and Van Niekerk (2011) also tried to motivate their literature review by focusing on prosocial security behavior with the ‘weakest link’ argument. These papers use the weak(est) link argument to contrast their studies, and quest for rising to the next level, group level, or seeing users as an important resource or even as a security sensor.

Many papers motivate their study with the ‘weakest link’ argument, either to focus on a specific group or phenomenon (such as social engineering) or to show that humans can be seen as an asset for security management. These two different groups of studies present a stark contrast to each other, the first group embracing the argument presenting an opportunity to find more support for the argument, and the other one trying to showcase alternative perspectives for seeing humans in the security management discourse.

### **The concept as part of the argument**

The phrase was used in some papers as a part of the argument in the study. Supporting the ‘weakest link’ phrase was for example Yan et al. (2018) who found the ‘weakest links’ in the undergraduate student group. They did a literature review on the ‘weakest link’ phenomenon and argued that studying the ‘weakest link’ is important for a paradigm shift from technology emphasis in security research to a behavioral perspective in cybersecurity research, especially when focused on ordinary users by targeting the ‘weakest link’. They found that most students did not identify certain scenarios as cybersecurity problems (namely cases of missing information and leaving a laptop in

a car while visiting a bar after work) in their survey of 462 college students. They encouraged that “the cybersecurity community should focus more on tackling the most difficult aspects (i.e., the weakest link) effectively rather than on lingering with the easiest aspects (i.e., the strongest link).” (p. 380). Ani et al. (2019) also focused on finding the ‘weakest links’ of cybersecurity awareness in specific organizational settings, but instead of merely identifying the topics in which the staff has the lowest awareness, they also found specific persons who have the lowest security capabilities. In this study, a scenario-based model for identifying the ‘weakest links’ was built and tested. They state that the “weakest link refers to the personnel with least knowledge and practical proficiency in security for the implementation of ICS security objectives.” (p. 12). Nohlberg (2008) focused on explaining why humans are the ‘weakest links’ in cybersecurity. The paper introduced different manipulation tactics for deceiving humans, and emphasized that anyone may fall on these tactics, and finally gave examples of how to protect oneself against them. Siponen and Baskerville (2018) referred in their conceptual paper to the “weak link phenomenon” as an example of their call for basic research in the information system security field. They defined a “weak link, or breaking point, for information security can be a certain situation or those people who ignore all ISS messages and do not participate in surveys” (p. 253), which does not focus only on people, and emphasizes the indifference towards cybersecurity rather than knowledge or capabilities.

Some papers used the ‘weakest link’ to support their main argument but were against it. Many papers referred to Sasse et al.’s (2001) paper focusing on transforming the ‘weakest link’ by designing usable security. The paper started by criticizing the ‘weakest link’ concept: “labelling users as the ‘weakest link’ implies that they are to blame. In our view, this is a repeat of the ‘human error’ mindset that blighted the development of safety-critical systems until the late eighties” (p.

122). It is therefore interesting that many papers seem to refer to this paper as a source for the ‘weakest link’ argument. (e.g., C. L. Anderson & Agarwal, 2010; Bera et al., 2023; Yan et al., 2018). Another paper criticizing the argument was by Edeh (2023), which synthesized the literature on different aspects related to human factors, errors, activities, etc. The paper tried to find ways to consider human factors as a cybersecurity solution. Arce and Levy (2003) argued in their conceptual study that the security community “reiterate [the weakest link argument] ad nauseam when referring to an organization’s information security posture” (p. 72). The paper described what has been considered the ‘weakest link’ during the last decades: the mainframes in the '60s-70s, the PCs in the '80s, the networked organization in the '90s, and finally in the 2000s, the workstations. Although the paper admitted that the reasons behind the workstation’s vulnerability are 1) human factors (IT experts are well educated) 2) vulnerable software 3) exploiters attacking it and 4) instead of the backdoor, the workstation can be considered as a front door by cybercriminals. The ‘weakest link’ was not thus strictly criticized but explored, but it does give a wider perspective to the discourse, which often focuses only on humans. Bihari (2018) tackled the metaphor of security as a chain, by pointing out that 1) it focuses on individual components of security and does not consider the synergy of the whole, 2) it might give a false impression that unless “the weakest link is not broken, ‘we are fine’” (p. 3), 3) that other parts of the chain are unbreakable and 4) sometimes managing the ‘weakest link’ might be more costly than possible exploit. The paper suggested an alternative: thinking of security as an F1 car, which might have weak and strong parts, but still works if a weak part is broken. This metaphor might encourage organizations to aim to win the long-term competition, not a single race, with a high-performance machine. Evans et al. (2019) tried to find underlying causes for human errors and then corresponding preventative measures to improve information security in their multimethod

action research, where they collected data from two organizations about incident reasons. They explained that “with appropriate controls applied, the human can transform from the weakest link to the strongest link” (p.3) and created a technique of finding human error causes behind different security incidents and then appropriate measures to remedy and prevent them in the future.

The papers that use the ‘weakest link’ concept as part of their main argument have taken it for deeper examination. All the papers aimed to find better solutions to improve organizational cybersecurity whether they supported or opposed the concept. They made suggestions either by finding the ‘weakest links’ and targeting them with training (Ani et al., 2019; Yan et al., 2018), by explaining the behavior and making diverse recommendations based on the problems (Arce & Levy, 2003; Edeh, 2023; Evans et al., 2019; Nohlberg, 2008; Sasse et al., 2001), or by taking a more abstract view of suggesting alternative approaches for useful metaphors or research approaches (Bihari, 2018; Siponen & Baskerville, 2018).

However, the two existing definitions from these papers are somewhat different. Ani et al (2019) specifically focused on a person, and Siponen and Baskerville (2018) considered also situations as well as people as ‘weakest links’. The first paper also focused on the lack of knowledge or capabilities of the ‘weakest link’, and the latter on the indifference to security messages and surveys. One interpretation could be that the first definition referred to unintentional security non-compliance as the other referred to either intentional neglecters or malicious actors. Thus the ‘weakest link’ is a very ambiguous concept.

### **The concept in explaining the results**

A few papers used the ‘weakest link’ to explain their results or show the difference between their results and previous research. For example, Nguyen et al. (2021) stated in their practical implications that “Individual users are often considered the weakest link when it comes to security,



so rather than treating phishing attacks as isolated events, organisations should emphasise the need to work collectively to overcome these challenges” (p.494). Their paper introduced a collective, crowdsourcing idea to empower workgroups, helping individuals work together by harnessing the abilities of people. They focused on phishing susceptibility, the difficulty of identifying phishing emails and websites, and the trained organizational members as an additional line of defense. Davis et al. (2023) brought out that “[u]nfortunately, despite more than a decade of research on the human side of organisational InfoSec, people are often still identified as the weakest link, rooted in disinterest in security threats and the behaviours that mitigate them” (p. 203) and then explained the results of their quantitative study concerning workplace factors improving commitment to organizational cybersecurity. Also, Lin et al. (2022) contrasted their study against prior research which has either seen employees as misbehaving insiders or the ‘weakest links’ of information security. They explained the theoretical implications of their quantitative paper about proactive security behavior, where employees were seen as positive and benevolent.

All of these papers wanted to separate their study from the prior literature and take a positive approach to the human role in cybersecurity by emphasizing commitment, benevolence, or collective effort.

## **DISCUSSION**

We set out to examine and reflect the use of the ‘weakest link’ concept in cybersecurity research and found numerous papers using it, with or without a reference. It seems to permeate the cybersecurity research, and sometimes the concept is used as a fact without any reference. The findings so far point to three implications for cybersecurity research.

First, we call for definitions of the 'weakest link' concept to remove ambiguity. Although there are several statistics about humans being the root cause of many, or even most<sup>1</sup>, cybersecurity incidents, it is clear from this analysis that the concept has many different meanings and refers to many groups of humans. Thus, we recommend that if the 'weakest link' concept is used, it should be at least defined and explained why something is considered to be the 'weakest link'. When we recognize that the SOC operators managing daily security problems, the security professionals creating security controls, the managers creating ISPs, and the end-users trying to navigate the complex security landscape while focusing on their jobs, are all humans, we can probably say that 100% of cybersecurity problems can be attributed to a human actor. But how does that help us to improve cybersecurity? Should we try as researchers to be more precise and focused? The end-user groups can be anything from well-versed and knowledgeable end-users choosing to ignore the rules since they think they know better (De Kimpe et al., 2022), to novices who do not know or understand how to behave securely (Ani et al., 2019) or malicious insiders (Siponen & Baskerville, 2018). We should deal with these groups differently and try to find different solutions for them. The 'weakest link' concept is very widely used, not only in medical physics (Njeh, 2008) or economics (Hirshleifer, 1983). The concept is used broadly within cybersecurity research in the behavioral cybersecurity but also in econometric models of cybersecurity optimization (Kumar et al., 2008) as well as network (Josang et al., 2015) and technical security (Martinez et al., 2021).

---

<sup>1</sup> Ebert et al. (2023) raise a good point about the fact that determining the role of humans in incidents not an objective endeavor, but rather a social constructive one. That is "what you look for is what you find, and what you find is what you fix." (p. 1)

Therefore, the ‘weakest link’ is clearly becoming a buzzword that covers ‘everything and nothing’ (Alvesson & Blom, 2022). The ‘weakest link’ refers to varied human entities and is rarely defined in cybersecurity studies. The ‘weakest link’ thus has a lot of variances, as do human factors, but that variance is reduced and oversimplified when we adopt the concept of ‘the weakest link’. When the concept is defined, it can refer to malicious insiders and ill-informed employees, who accidentally may break the information security policy. All cybersecurity problems can be traced back to humans, but the weakest link is usually those with less power who do not have the power to respond. Thus, we call for using more precise names for the specific agent groups, to break the current hegemony of the ‘weakest link’ concept and find more precise solutions for cybersecurity threats caused by the different human factors.

Second, we should question the value of seeing cybersecurity as a chain, which is actually a multifaceted and multilayered network of technical, procedural, cultural and social practices (cf. Soomro et al., 2016). Bihari (2018) found several problems in using the chain metaphor. For instance, if we believe that the “chain” of cybersecurity can be broken from only the ‘weakest link’ point, i.e. human actor, then we 1) might not care for the other parts of the chain or 2) get a false sense of security or 3) invest in securing the ‘weakest link’, although the cost of that investment is larger than the exploitation damage would be. Ebert et al. (2023) also criticized the focus on finding a single root cause of cybersecurity breaches in humans, since several other contributing factors should be investigated also. For example, zero-day vulnerabilities can be exploited although end-users are well trained and aware of those threats. The oversimplification of the ‘weakest link’ idea thus adds ambiguity to the security discourse, and can limit our focus to the ‘weakest link’ or to the surrounding areas, when a more holistic approach would be needed (Ebert et al., 2023; Soomro et al., 2016)

Third, we should either promote deskilling or upskilling, but we cannot demand both. Ebert et al (2023) have compared safety science with current cybersecurity discourse and argue that portraying humans as the ‘weakest link’ has roots in scientific management, sometimes called Taylorism. Taylor (1919) had a negative perception of workers. In Taylor’s view, workers try to work slower and cannot understand how the work should be organized. He wrote that (p.14) “the greatest evil with which the working-people of both England and America are now afflicted” is that “this man deliberately plans to do as little as he safely can - to turn out far less work than he is well able to do” (p.13). He recognized that the tradespersons teach other tradespersons as one reason for slow work, but systematically re-engineered work would give the optimal output. Therefore, he saw that “the workman who is best suited to actually doing the work is incapable of fully understanding this science, without the guidance and help of those working with him or over him, either through lack of education or through insufficient mental capacity.” (p. 26). Thus, he believed that actual labor and planning of how labor is done should be separated (Braverman, 1998).

The ‘human as the weakest link’ argument used in cybersecurity literature reflects a similar negative perspective of workers. Braverman (1998) summarizes scientific management into three principles. The first principle is “dissociation of the labor process from the skills of the workers” (p.113), which means that the skills of the experienced workers should not be used but the labor process should be optimized elsewhere. Thus, the second principle “separation of conception from execution” (p.114) or planning the optimal work process should be focused on a planning department, which systematically can study the work. Therefore, the third principle is the “use of this monopoly over knowledge to control each step of the labor process and its mode of execution.” (p.119). The workers are “neither encouraged nor permitted to understand his or her work” (p.132).

Braverman (1998) interprets that in scientific management the requirements of managers are rational, but employees' ideas are irrational.

When security experts formulate the ISP, they try to spare the burden of becoming experts from normal employees but this will lead to deskilling. Security experts have a monopoly on cybersecurity knowledge. Thus, the conception of ISPs is separate from execution or compliance, which is expected from employees. The intention of creating the ISP by experts is good, then the other employees could merely follow the rules and attend trainings, and thus be able to detect those attacks not caught by technical controls.

However, sophisticated cyberattacks (such as phishing) cannot be detected by generalized rules in the ISP but require upskilling of end-users. Humans must be well trained and mindful and able to interpret whether an email, QR code, link, video, image etc. is reliable or not. This is expected simultaneously when employees should do their work tasks with maximum efficiency and fast pace. Many end-users are using their computers for tasks demanding skill and expertise, but with generalized ISP rules, we expect them to follow them mindlessly, without questioning, although many cyberattacks are virtually impossible to detect without expertise.

So we call for picking the upskilling or deskilling route, both are not feasible simultaneously. If we want to continue the path of mindless compliance of generalized ISPs, then perhaps technical security measures should become so sophisticated that they can find the cyberattacks before they reach the end-users (Soliman & Järveläinen, 2024). If we however want to use the upskilling route then we should concentrate on ISP localization (Niemimaa & Niemimaa, 2019) and various role-based training approaches.

## CONCLUSION

The purpose of this paper is to examine and reflect on the use and abuse of the 'weakest link' concept in cybersecurity research with the help of a problematizing literature review. Our preliminary findings point out that it is used in hundreds of cybersecurity papers, often as a motivation for the study, but sometimes as part of the argument or in explaining the results. We further observe that the concept has not been defined in many papers, leading to the ambiguity of the concept. Further, the scope of the concept use is very wide also in the cybersecurity field, and it seems to have a hegemonic position. Thus, we suspect that it is becoming a hembig concept. As research implications, we call for more precise definitions, question the use of chain metaphor in the cybersecurity field, and choose either upskilling or deskilling of end-users. Future researchers could thus focus on the impact of language on cybersecurity behavior (such as self-perception and consequent behavior), performativity of language, identification of human actor groups, and finding different solutions for ensuring cybersecurity based on the identified groups.

## REFERENCES

- Alvesson, M., & Blom, M. (2022). The hegemonic ambiguity of big concepts in organization studies. *Human Relations*, 75(1), 58–86. <https://doi.org/10.1177/0018726720986847>
- Alvesson, M., & Sandberg, J. (2020). The Problematizing Review: A Counterpoint to Elsbach and Van Knippenberg's Argument for Integrative Reviews. *Journal of Management Studies*, 57(6), 1290–1304. <https://doi.org/10.1111/joms.12582>
- Anderson, B. B., Vance, A., Kirwan, C. B., Eargle, D., & Jenkins, J. L. (2016). How users perceive and respond to security messages: A NeuroIS research agenda and empirical study. *European Journal of Information Systems*, 25(4), 364–390. <https://doi.org/10.1057/ejis.2015.21>
- Anderson, C. L., & Agarwal, R. (2010). Practicing Safe Computing: A Multimethod Empirical Examination of Home Computer User Security Behavioral Intentions. *MIS Quarterly*, 34(3), 613–A15. <https://doi.org/10.2307/25750694>
- Ani, U. D., He, H., & Tiwari, A. (2019). Human factor security: Evaluating the cybersecurity capacity of the industrial workforce. *Journal of Systems and Information Technology*, 21(1), 2–35. Scopus. <https://doi.org/10.1108/JSIT-02-2018-0028>
- Arce, I., & Levy, E. (2003). The weakest link revisited. *IEEE Security and Privacy*, 1(2), 72–76. Scopus. <https://doi.org/10.1109/MSECP.2003.1193216>

- Bera, D., Ogbanufe, O., & Kim, D. J. (2023). Towards a thematic dimensional framework of online fraud: An exploration of fraudulent email attack tactics and intentions. *Decision Support Systems*, 171, 113977. <https://doi.org/10.1016/j.dss.2023.113977>
- Bihari, E. (2018). WEAKEST LINK, OR.... *EDPACS*, 57(6), 1–7. Scopus. <https://doi.org/10.1080/07366981.2018.1476312>
- Borkovich, D. J., & Skovira, R. J. (2020). WORKING FROM HOME: CYBERSECURITY IN THE AGE OF COVID-19. *Issues in Information Systems*, 21(4), 234–246. Scopus. [https://doi.org/10.48009/4\\_iis\\_2020\\_234-246](https://doi.org/10.48009/4_iis_2020_234-246)
- Braverman, H. (1998). *Labor and Monopoly Capital: The Degradation of Work in the Twentieth Century*. NYU Press.
- Chamkar, S. A., Maleh, Y., & Gherabi, N. (2022). THE HUMAN FACTOR CAPABILITIES IN SECURITY OPERATION CENTER (SOC). *EDPACS*, 66(1), 1–14. Scopus. <https://doi.org/10.1080/07366981.2021.1977026>
- Chen, Y., Ramamurthy, K., & Wen, K. W. (2012). Organizations' information security policy compliance: Stick or carrot approach? *Journal of Management Information Systems*, 29(3), 157–188. <https://doi.org/10.2753/MIS0742-1222290305>
- Conteh, N. Y., & Royer, M. D. (2021). The unprecedented rise in cybercrime and the role of the human vulnerability factor. In *Ethical Hacking Techniques and Countermeasures for Cybercrime Prevention* (pp. 32–43). Scopus. <https://doi.org/10.4018/978-1-7998-6504-9.ch003>
- Davis, J., Agrawal, D., & Guo, X. (2023). Enhancing users' security engagement through cultivating commitment: The role of psychological needs fulfilment. *European Journal of Information Systems*, 32(2), 195–206. <https://doi.org/10.1080/0960085X.2021.1927866>
- De Kimpe, L., Walrave, M., Verdegem, P., & Ponnet, K. (2022). What we think we know about cybersecurity: An investigation of the relationship between perceived knowledge, internet trust, and protection motivation in a cybercrime context. *Behaviour and Information Technology*, 41(8), 1796–1808. Scopus. <https://doi.org/10.1080/0144929X.2021.1905066>
- Dygnatowski, S. (2021). Space systems as the weakest link. *Advances in Military Technology*, 16(1), 133–147. Scopus. <https://doi.org/10.3849/aimt.01409>
- Dzhengiz, T., Miller, E. M., Ovaska, J.-P., & Patala, S. (2023). Unpacking the circular economy: A problematizing review. *International Journal of Management Reviews*, 25(2), 270–296. <https://doi.org/10.1111/ijmr.12329>
- Ebert, N., Schaltegger, T., Ambuehl, B., Schöni, L., Zimmermann, V., & Knieps, M. (2023). Learning from safety science: A way forward for studying cybersecurity incidents in organizations. *Computers & Security*, 134, 103435. <https://doi.org/10.1016/j.cose.2023.103435>
- Edeh, N. C. (2023). Cybersecurity and Human Factors: A Literature Review. In *Cybersecurity for Decision Makers* (pp. 45–56). Scopus. [https://doi.org/10.1201/9781003319887\\_3](https://doi.org/10.1201/9781003319887_3)
- Evans, M., He, Y., Luo, C., Yevseyeva, I., Janicke, H., Zamani, E., & Maglaras, L. (2019). Real-Time Information Security Incident Management: A Case Study Using the IS-CHEC Technique. *IEEE ACCESS*, 7, 142147–142175. <https://doi.org/10.1109/ACCESS.2019.2944615>
- Foth, M. (2016). Factors influencing the intention to comply with data protection regulations in hospitals: Based on gender differences in behaviour and deterrence. *European Journal of Information Systems*, 25(2), 91–109. <https://doi.org/10.1057/ejis.2015.9>

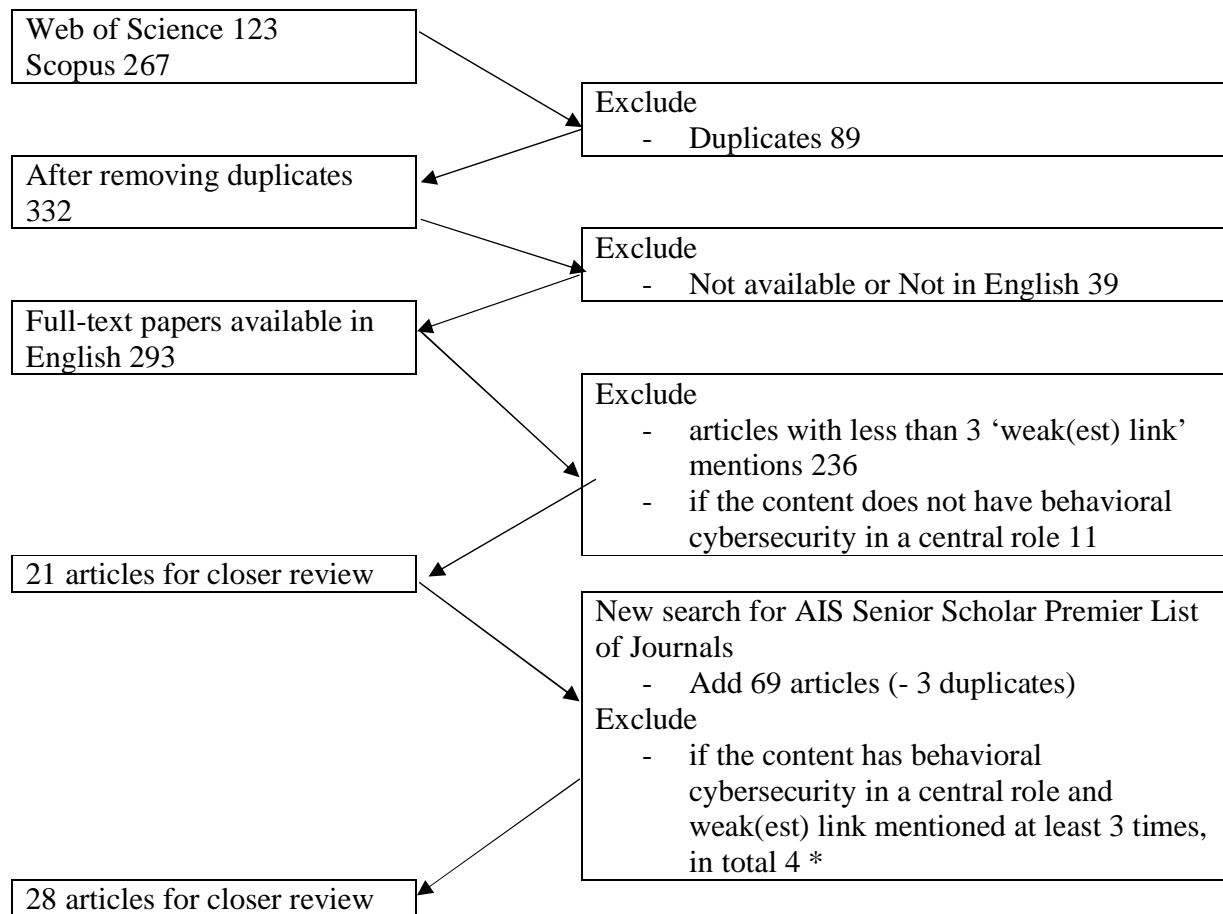
- Goel, S., & Chengalur-Smith, I. N. (2010). Metrics for characterizing the form of security policies. *The Journal of Strategic Information Systems*, 19(4), 281–295. <https://doi.org/10.1016/j.jsis.2010.10.002>
- Gond, J.-P., Cabantous, L., Harding, N., & Learmonth, M. (2016). What Do We Mean by Performativity in Organizational and Management Theory? The Uses and Abuses of Performativity. *International Journal of Management Reviews*, 18(4), 440–463. <https://doi.org/10.1111/ijmr.12074>
- Guo, K. H., Yuan, Y., Archer, N. P., & Connelly, C. E. (2011). Understanding nonmalicious security violations in the workplace: A composite behavior model. *Journal of Management Information Systems*, 28(2), 203–236. <https://doi.org/10.2753/MIS0742-1222280208>
- Hanus, B., Wu, Y. A., & Parrish, J. (2022). Phish Me, Phish Me Not. *Journal of Computer Information Systems*, 62(3), 516–526. Scopus. <https://doi.org/10.1080/08874417.2020.1858730>
- Heartfield, R., & Loukas, G. (2018). Detecting semantic social engineering attacks with the weakest link: Implementation and empirical evaluation of a human-as-a-security-sensor framework. *Computers & Security*, 76, 101–127. <https://doi.org/10.1016/j.cose.2018.02.020>
- Hirsch, P. M., & Levin, D. Z. (1999). Umbrella Advocates Versus Validity Police: A Life-Cycle Model. *Organization Science*, 10(2), 199–212. <https://doi.org/10.1287/orsc.10.2.199>
- Hirshleifer, J. (1983). From weakest-link to best-shot: The voluntary provision of public goods. *Public Choice*, 41(3), 371–386. <https://doi.org/10.1007/BF00141070>
- Hu, Q., West, R., & Smarandescu, L. (2015). The role of self-control in information security violations: Insights from a cognitive neuroscience perspective. *Journal of Management Information Systems*, 31(4), 6–48. <https://doi.org/10.1080/07421222.2014.1001255>
- Josang, A., Miralabé, L., & Dallot, L. (2015). It's not a bug, it's a Feature: 25 Years of Mobile Network Insecurity. In N. Abouzakhar (Ed.), *University of Oslo* (WOS:000361690600016; pp. 129–136).
- Kannelonning, K., & Katsikas, S. (2023). A systematic literature review of how cybersecurity-related behavior has been assessed. *INFORMATION AND COMPUTER SECURITY*. <https://doi.org/10.1108/ICS-08-2022-0139>
- Karakilic, E., & Painter, M. (2022). The (un)surprising nature of creativity: A Deleuzian perspective on the temporality of the creative process. *Ephemera: Theory and Politics in Organization*, 22(2), Article 2. <http://www.ephemerajournal.org/contribution/unsurprising-nature-creativity-deleuzian-perspective-temporality-creative-process-0>
- Klein, G., & Zwilling, M. (2023). The Weakest Link: Employee Cyber-Defense Behaviors While Working from Home. *Journal of Computer Information Systems*. Scopus. <https://doi.org/10.1080/08874417.2023.2221200>
- Korotkova, N., Benders, J., Mikalef, P., & Cameron, D. (2023). Maneuvering between skepticism and optimism about hyped technologies: Building trust in digital twins. *Information & Management*, 60(4), 103787. <https://doi.org/10.1016/j.im.2023.103787>
- Kumar, R. L., Park, S., & Subramaniam, C. (2008). Understanding the Value of Countermeasure Portfolios in Information Systems Security. *Journal of Management Information Systems*, 25(2), 241–280. <https://doi.org/10.2753/MIS0742-1222250210>
- Lebek, B., Uffen, J., Neumann, M., & Hohler, B. (2013). *Towards a needs assessment process model for security, education, training and awareness programs: An action design research study*. ECIS 2013 - Proceedings of the 21st European Conference on Information Systems.



- Scopus. <https://www.scopus.com/inward/record.uri?eid=2-s2.0-84905845324&partnerID=40&md5=146c26a7392745d6497c14ea9d10713a>
- Li, H., Zhang, J., & Sarathy, R. (2010). Understanding compliance with internet use policy from the perspective of rational choice theory. *Decision Support Systems*, 48(4), 635–645. <https://doi.org/10.1016/j.dss.2009.12.005>
- Lin, C., Wittmer, J. L. S., & Luo, X. (Robert). (2022). Cultivating proactive information security behavior and individual creativity: The role of human relations culture and IT use governance. *Information & Management*, 59(6), 103650. <https://doi.org/10.1016/j.im.2022.103650>
- Ma, X., & Cho, H. (2022). Access to user data stored by organizations-divides surrounding information security professionals in Chinese IT organizations. *CHINESE JOURNAL OF COMMUNICATION*, 15(1), 1–33. <https://doi.org/10.1080/17544750.2021.1954962>
- Martinez, M. M., Marin-Tordera, E., & Masip-Bruin, X. (2021). *Scalability analysis of a blockchain-based security strategy for complex IoT systems*. 2021-June. Scopus. <https://doi.org/10.1109/HPSR52026.2021.9481865>
- Mouton, F., Leenen, L., & Venter, H. S. (2016). Social engineering attack examples, templates and scenarios. *Computers and Security*, 59, 186–209. Scopus. <https://doi.org/10.1016/j.cose.2016.03.004>
- Ng, K. C., Zhang, X., Thong, J. Y. L., & Tam, K. Y. (2021). Protecting Against Threats to Information Security: An Attitudinal Ambivalence Perspective. *Journal of Management Information Systems*, 38(3), 732–764. <https://doi.org/10.1080/07421222.2021.1962601>
- Nguyen, C., Durcikova, A., Jensen, M. L., & Wright, R. T. (2021). *A comparison of features in a crowdsourced phishing warning system*. January 2020, 1–41. <https://doi.org/10.1111/isj.12318>
- Niemimaa, M., & Niemimaa, E. (2019). Abductive innovations in information security policy development: An ethnographic study. *European Journal of Information Systems*, 28(5), 566–589. <https://doi.org/10.1080/0960085X.2019.1624141>
- Njeh, C. F. (2008). Tumor delineation: The weakest link in the search for accuracy in radiotherapy. *Journal of Medical Physics*, 33(4), 136. <https://doi.org/10.4103/0971-6203.44472>
- Nohlberg, M. (2008). Why humans are the weakest link. In *Social and Human Elements of Information Security: Emerging Trends and Countermeasures* (pp. 15–26). Scopus. <https://doi.org/10.4018/978-1-60566-036-3.ch002>
- Repetto, M. (2023). Adaptive monitoring, detection, and response for agile digital service chains. *COMPUTERS & SECURITY*, 132. <https://doi.org/10.1016/j.cose.2023.103343>
- Sasse, M. A., Brostoff, S., & Weirich, D. (2001). Transforming the ‘Weakest Link’—A Human/Computer Interaction Approach to Usable and Effective Security. *BT Technology Journal*, 19(3), 122–131. <https://doi.org/10.1023/A:1011902718709>
- Siponen, M., & Baskerville, R. (2018). Intervention effect rates as a path to research relevance: Information systems security example. *Journal of the Association for Information Systems*, 19(4), 247–265. <https://doi.org/10.17705/1jais.00491>
- Soliman, W., & Järveläinen, J. (2024). RECONCEPTUALIZING THE HUMAN IN THE LOOP: A PROBLEMATIZATION OF TAKEN-FOR-GRANTED METAPHORS IN CYBERSECURITY RESEARCH. *ECIS 2024 Proceedings*. [https://aisel.aisnet.org/ecis2024/track02\\_general/track02\\_general/5](https://aisel.aisnet.org/ecis2024/track02_general/track02_general/5)
- Solomon, M. (2024). Five conceptual competences in psychiatry. *World Psychiatry*, 23(2), 233–234. <https://doi.org/10.1002/wps.21195>

- Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management*, 36(2), 215–225. <https://doi.org/10.1016/j.ijinfomgt.2015.11.009>
- Spears, J. L., & Barki, H. (2010). User participation in information systems security risk management. *MIS Quarterly*, 34(3), 503.
- Stellios, I., Kotzanikolaou, P., Psarakis, M., & Alcaraz, C. (2021). Risk Assessment for IoT-Enabled Cyber-Physical Systems. In *Learning and Analytics in Intelligent Systems* (Vol. 14, pp. 157–173). Scopus. [https://doi.org/10.1007/978-3-030-41196-1\\_8](https://doi.org/10.1007/978-3-030-41196-1_8)
- Taylor, F. W. (1919). *The principles of scientific management*. Harper & Brothers Publishers.
- Thomson, K., & Van Niekerk, J. (2011). *Combating information security apathy by encouraging prosocial organisational behaviour*. 1–10. Scopus.
- Torten, R., Reaiche, C., & Boyle, S. (2018). The impact of security awareness on information technology professionals' behavior. *COMPUTERS & SECURITY*, 79, 68–79. <https://doi.org/10.1016/j.cose.2018.08.007>
- Vielberth, M., Englbrecht, L., & Pernul, G. (2021). Improving data quality for human-as-a-security-sensor. A process driven quality improvement approach for user-provided incident information. *INFORMATION AND COMPUTER SECURITY*, 29(2), 332–349. <https://doi.org/10.1108/ICS-06-2020-0100>
- Warkentin, M., Johnston, A. C., Shropshire, J., & Barnett, W. D. (2016). Continuance of protective security behavior: A longitudinal study. *Decision Support Systems*, 92, 25–35. <https://doi.org/10.1016/j.dss.2016.09.013>
- Willison, R., & Warkentin, M. (2013). Beyond Deterrence: An Expanded View of Employee Computer Abuse. *MIS Quarterly*, 37(1), 1–20.
- Yan, Z., Robertson, T., Yan, R., Park, S., Bordoff, S., Chen, Q., & Sprissler, E. (2018). Finding the weakest links in the weakest link: How well do undergraduate students make cybersecurity judgment? *COMPUTERS IN HUMAN BEHAVIOR*, 84, 375–382. <https://doi.org/10.1016/j.chb.2018.02.019>
- Yan, Z., Xue, Y., & Lou, Y. (2021). Risk and protective factors for intuitive and rational judgment of cybersecurity risks in a large sample of K-12 students and teachers. *COMPUTERS IN HUMAN BEHAVIOR*, 121. <https://doi.org/10.1016/j.chb.2021.106791>
- Yang, C., O'Leary, S., & Tregidga, H. (2021). Social impact in accounting: Is it at risk of becoming a hembig concept and does this matter? *Qualitative Research in Accounting & Management*, 18(3), 313–331. <https://doi.org/10.1108/QRAM-05-2021-0093>
- Zhuang, Y., Choi, Y., He, S., Leung, A. C. M., Lee, G. M., & Whinston, A. (2020). Understanding Security Vulnerability Awareness, Firm Incentives, and ICT Development in Pan-Asia. *Journal of Management Information Systems*, 37(3), 668–693. <https://doi.org/10.1080/07421222.2020.1790185>

## APPENDIX 1. LITERATURE SEARCH PROCEDURE



**Figure 1. Literature review process (\* except the three articles which were included since they represented a third category, explaining the results, and mentioned the ‘weakest link’ only once).**

## APPENDIX 2. MOST USED REFERENCES

Article name and authors	Example quotation	Times used as reference	Used by

Mitnick, K. D., Simon, W. L (2002)	“As Mitnick and Simon [39] note, people who interact with the information assets of the organization are “truly security’s weakest link” (p. 4).” (Cavusoglu et al 2015)	10	Lin et al, 2022; Nord et al, 2020; Bulgurcu et al, 2010; Aurigemma, 2013; Heartfield & Loukas, 2018; Ani et al, 2019; Greulich et al, 2024; Malatji et al, 2020; Cavusoglu et al, 2015; Danet, 2021
Crossler, R. E. et al 2013	“Compliance with such rules entirely depends on employees’ motivation to conform, while various sources refer to humans as the weakest link in the security chain [9].” (Connolly et al, 2017)	10	Guhr et al, 2018; Mady et al, 2023; Warkentin et al, 2016; Luecke & Simon, 2014; Klein & Zwilling, 2023; Silic & Lowry, 2020; Connolly et al, 2017(a); Connolly et al, 2017(b); Belanger & Crossler, 2019; Djajadikerta et al, 2015
Warkentin, M., Willison, R. (2009).	“Employees are often the weakest link in information security (Mitnick and Simon 2002; Warkentin and Willison 2009).” (Nord et al 2020)	9	Lin et al, 2022; Nord et al, 2020; Bulgurcu et al, 2010; Aurigemma, 2013; Wang et al, 2015; Guhr et al, 2018; Mady et al, 2023; Warkentin et al, 2016; Luecke & Simon, 2014
Schneier, B. (2000)	“Literature review suggests human users as the weakest link [8, 9, 10, 11, 12].” (Shah & Agarwal, 2020)	8	Dlamini et al, 2011; Heartfield & Loukas, 2018; Shah & Agarwal, 2020; Martins & Eloff, 2002; Alohalo et al, 2018; Zaman, 2020; Mahfuth et al, 2017; Sasse et al, 2001
Sasse et al. 2001	“Many people in the security business regard the human factor as the weakest link in security solutions [2].” (Zakaria & Katuk, 2013)	7	Dlamini et al, 2011; Ifinedo, 2014; Morgan et al, 2020; Zakaria & Katuk, 2013; Bera et al, 2023; Anderson & Agarwal, 2010; Velki et al, 2014
Vroom, C., & Von Solms, R. (2004)	“According to Vroom and Von Solms (2004, p. 193), “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.” (McFadzean et al, 2011)	5	Ifinedo, 2014; McFadzean et al, 2011; Posey et al, 2013; Ma & Cho, 2022; Leering et al, 2022

Spears JL, Barki H (2010)	“Information security (IS) is a function of technology, policy, process, and users, among which users are often considered to be the weakest link (Spears and Barki 2010, Warkentin and Willison 2009).” (Wang et al, 2015)	5	Wang et al, 2015; Lebek et al, 2013(a); Lebek et al, 2014; Lebek et al, 2013(b); Ahmed et al, 2014
Bulgurcu, B.; Cavusoglu, H. & Benbasat, I. (2010):	“Since researchers refer to employees as the weakest link in information security (e.g. Bulgurcu et al., 2010; Spears & Barki, 2010) security education, training, and awareness (SETA) programs have garnered increasing attention.” (Lebek et al, 2013)	5	Lebek et al, 2013; Lin et al, 2022; Ani et al, 2019; Lowry & Moody, 2015; Hu et al, 2015