Organizational Cybersecurity Journal: Practice, Process and People

Employee behavior: the psychological gateway for cyberattacks

Rahel Aschwanden, Claude Messner, Bettina Höchli and Geraldine Holenweger
University of Bern, Bern, Switzerland

Received 4 February 2023
Revised 21 August 2023
20 March 2024
Accepted 13 April 2024

Abstract

Purpose – Cyberattacks have become a major threat to small and medium-sized enterprises. Their prevention efforts often prioritize technical solutions over human factors, despite humans posing the greatest risk. This article highlights the importance of developing tailored behavioral interventions. Through qualitative interviews, we identified three persona types with different psychological biases that increase the risk of cyberattacks. These psychological biases are a basis for creating behavioral interventions to strengthen the human factor and, thus, prevent cyberattacks.

Design/methodology/approach – We conducted structured, in-depth interviews with 44 employees, decision makers and IT service providers from small and medium-sized Swiss enterprises to understand insecure cyber behavior.

Findings – A thematic analysis revealed that, while knowledge about cyber risks is available, no one assumes responsibility for employees' and decision makers' behavior. The interview results suggest three personas for employees and decision makers: experts, deportees and repressors. We have derived corresponding biases from these three persona types that help explain the interviewees' insecure cyber behavior.

Research limitations/implications – This study provides evidence that employees differ in their cognitive biases. This implies that tailored interventions are more effective than one-size-fits7-all interventions. It is inherent in the idea of tailored interventions that they depend on multiple factors, such as cultural, organizational or individual factors. However, even if the segments change somewhat, it is still very likely that there are subgroups of employees that differ in terms of their misleading cognitive biases and risk behavior.

Practical implications – This article discusses behavior directed recommendations for tailored interventions in small and medium-sized enterprises to minimize cyber risks.

Originality/value – The contribution of this study is that it is the first to use personas and cognitive biases to understand insecure cyber behavior, and to explain why small and medium-sized enterprises do not implement behavior-based cybersecurity best practices. The personas and biases provide starting points for future research and interventions in practice.

Keywords Cyber risks, Human factors in cybersecurity, Cyberpsychology, Cognitive psychology, Cognitive biases, Psychological gateway, Behavioral science

Paper type Research paper

1. Introduction

Cybercrime has become a significant problem for small and medium-sized enterprises. The number of successful attacks has increased dramatically in recent years. In 2022, 493.33 million ransomware attacks were officially documented by enterprises worldwide (Kolesnikov, 2023).

We thank Patric Vifian, Peter Hofstetter, Andreas Hölzli, Jasmine Reber, Martin Doriot, Pascal Burkhalter, Urs Fuhrer and Felix Walliser, for their helpful advice in preparing and conducting this study. In addition, we thank two anonymous reviewers for their helpful comments. This research was financially supported by Mobiliar Assurance.

Organizational Cybersecurity Journal: Practice, Process and People
Emerald Publishing Limited
e-ISSN: 2635-0289
p-ISSN: 2635-0270
DOI 10.1108/OCJ-02-2023-0004

A quarter of all small enterprises in Switzerland have already encountered cyberattacks (Peter *et al.*, 2020). Cyber criminals infiltrate networks to cause damage, make financial gains, and/or steal sensitive data, and cyberattacks can lead to reputational damage, financial losses, or even the complete closure of an enterprise (Ferro and Sapio, 2020). Addressing the resulting damages requires significant effort. Consequently, risk management for information systems is a top priority for enterprises worldwide. Most enterprises today rely on latest technology (Nobles, 2018) and invest money in technical security tools, including both software and hardware solutions. This study is motivated by the fact that small and medium-sized enterprises often neglect the human element of cyberattacks (Abass, 2018). An employee can pass on all the information an attacker needs without having to overcome any technical hurdles. Therefore, no one is safe from cyberattacks (Choras *et al.*, 2016), as the human element is the weakest link in the security chain (e.g. D'Arcy *et al.*, 2009; Proctor and Chen, 2015; Triplett, 2022). Cybercriminals exploit this vulnerability by psychologically manipulating employees and decision makers.

In addition, our study is driven by current interventions that often include information and awareness campaigns. However, these approaches have two significant drawbacks. First, they adopt a uniform, one-size-fits-all strategy for all individuals. Second, they overlook the distinct cognitive biases that drive the cyber behavior of employees and decision makers. Instead, a more effective approach would involve segmentation, considering that tailored interventions have demonstrated superior efficacy (Lustria *et al.*, 2013). Interventions should be designed based on different user characteristics (Baltuttis *et al.*, 2024) and specific biases, as this would make them more effective.

The aim of this article is to illustrate that employees and decision makers differ in the way they interpret cyber risks. They differ in their cognitive biases, which make carrying out cyberattacks easier. These cognitive biases can serve as a basis for creating tailored interventions that directly address and counter unsafe behaviors.

1.1 Influences on cyber security behaviors

An individual's cyber security behavior is influenced by various factors and rationales, and, therefore, a comprehensive understanding of the same is required to formulate successful intervention strategies. The ecological model serves as an appropriate theoretical foundation to capture the multiple determinants of cyber behavior (see Figure 1; Sallis *et al.*, 2015). Ecological models are widely used to encompass the diverse influences on one's behavior across various levels. These models include the following factors that influence behavior: individual differences

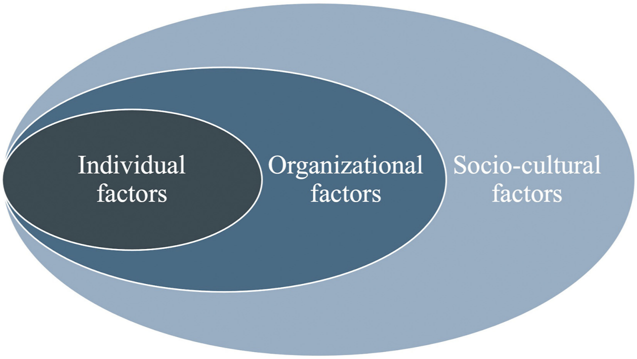


Figure 1.
Ecological model

Note(s): Factors influencing cyber behavior
Source(s): By authors

(e.g. awareness, knowledge, or attitude), organizational factors (e.g. guidelines), and socio-cultural factors (e.g. social norms; Morgan *et al.*, 2020; Williams *et al.*, 2017).

1.2 Individual factors

The primary determinants of an individual's cyber behavior stem from their understanding of cybersecurity, their knowledge, awareness, beliefs, experiences, perceptions, and attitudes (Morgan *et al.*, 2020). A lack of knowledge and awareness among employees and decision makers contributes to the high success rate of cyberattacks (Jain *et al.*, 2016). There are some misconceptions in enterprises regarding cyber risks. First, it is often assumed that the size and importance of an enterprise are relevant for a cyberattack. Employees are unaware that bots carry out automated and repetitive attacks regardless of an enterprise's size and importance (Abreu *et al.*, 2020). These bots are programmed to randomly send thousands of phishing emails with the hope that someone will fall for them. Individuals are particularly prone to clicking on links or providing information to people they trust, those making urgent appeals, and those with an authoritative status (Williams *et al.*, 2018). Second, employees believe it is easy to identify malicious emails. They underestimate not only the true risk of such attacks (Williams *et al.*, 2017; Wilson *et al.*, 2023) but also their severity (Albladi and Weir, 2018). Third, if they accidentally fall for an attack, they believe that they are either protected by firewalls or that IT specialists will solve the problem, as they are responsible for such issues. In summary, the key to the success of cyberattacks lies in the relative ease with which people's emotions and thoughts can be manipulated, which is something that employees and decision makers do not realize. Attackers manipulate their victims by developing a relationship with them to gain their trust (Mashtalyar *et al.*, 2021). The victims are then exploited and end up disclosing confidential information and sensitive data (Yaacoub *et al.*, 2020).

1.3 Organizational factors

Providing cybersecurity guidelines have become a standard practice in companies, which include specific instructions for employees. Although some enterprises compile technical and behavioral guidelines, employees often do not follow them. One of the problems in this regard is that following the behavioral guidelines does not provide any immediate, tangible benefit for their work. Further, the compliance costs are considerably high (Kirlappos *et al.*, 2014). It is often burdensome, for example, to constantly change passwords and to remember longer, complicated ones. This can cause fatigue with respect to security procedures, particularly when these are perceived as hindrances to employees' primary tasks (Stanton *et al.*, 2016). The increased time constraints, driven by numerous tasks and looming deadlines, amplify the risk of cyber misconduct (Chowdhury *et al.*, 2019). When decisions are made under such time constraints, there is a shift from thoughtful cognitive processing to automatic habitual responses (Wirz *et al.*, 2018). Under stress, employees often unconsciously fall back on habitual actions in pursuit of efficiency (Aggarwal and Dhurkari, 2023). Over time, they develop psychological mechanisms that reinforce their disregard for guidelines and perpetuate insecure behavior.

1.4 Socio-cultural factors

Culture is a complex, dynamic system that reflects the attitudes, norms, values, practices, communication patterns, roles, and other social regularities of a group (Kreuter and McClure, 2004). Ethnic, organizational, and cybersecurity culture are interconnected, as ethnic culture can shape organizational culture, which, in turn, shapes cybersecurity culture (Gundu *et al.*, 2019). Organizational safety culture, with its norms and values, guides employee behavior. Employees adapt their behavior by observing the actions and behaviors of others (Ferro and Sapio, 2020). For example, in a company where sharing passwords is common, an employee will typically accept this practice without questioning it and conform to the established norm. When an employee aligns with an organizational culture that does not prioritize cyber-safe practices, the likelihood of them engaging in unsafe cyber behavior increases (Morgan *et al.*, 2020). Further, there are certain differences between ethnic cultures. Individuals in collectivist cultures (e.g. Asians) have a greater tendency to conform to social norms (Iyengar and Lepper, 1999; Kim and Markus, 1999) and imitate the behavior of those around them (Van Baaren *et al.*, 2003) compared to those in individualistic cultures (e.g. Americans). In the East, individuals tend to avoid behaviors that cause social disruption and define themselves through their membership of social groups (Triandis, 1989). Rocha Flores *et al.* (2015) explored the relationship between culture and resistance to email phishing across nations (USA, Sweden, and India), revealing that culture has a substantial influence on users' behaviors and decisions in risky situations. In addition, one's perception of risk and trust differ across cultural contexts (Bada *et al.*, 2019). Cultures with a greater degree of trust are easier to deceive and, therefore, more likely to fall victim to cyberattacks (Rocha Flores *et al.*, 2014).

1.5 The current study

In many behavior change interventions, standard cyber-awareness campaigns are carried out, which often provide information without taking into account the cultural backgrounds and specific contexts involved. Consequently, such information campaigns usually fail (Bada *et al.*, 2019). For behavior change interventions to be effective, they must address the factors that hinder the desired behavior and must be tailored to the population and context in which the target behaviors are required (Michie *et al.*, 2011). Interventions tailored to specific segments are more effective at changing behavior than a general, one-size-fits-all approach (Lustria *et al.*, 2013).

This article aims to determine what types of individuals work in small and medium-sized enterprises and how they differ in their biases toward insecure cybersecurity behavior. Interviews were conducted to assess the motives and biases associated with the insecure cyber behavior of employees and decision makers, and individual, organizational, and socio-cultural factors were captured to gain a comprehensive understanding of the aspects that influence their behavior. We derive cognitive biases because, among other factors, these make people vulnerable to cyberattacks (Hong, 2012; Morgan *et al.*, 2020). Biases significantly guide one's decision-making, impacting the various daily choices they make (Kahneman, 2011). While biases can aid information processing, they can also lead to inaccurate judgments or irrational decisions, which are falsely perceived as objective. One way to successfully change individuals' behavior is to focus on these biases.

Thus, we use these biases as a basis for creating practical interventions that directly address and counter unsafe behaviors. Only a few studies have discussed personalized interventions in small and medium-sized enterprises (e.g. Morgan *et al.*, 2020). This study contributes to the existing literature by providing practical tips for changing the risky cyber behaviors of employees and decision makers, who have been shown to pose the most significant risk to cybersecurity (e.g. D'Arcy *et al.*, 2009; Proctor and Chen, 2015; Triplett, 2022).

To sum up, we address the following research question: Do different types of individuals exist in small and medium-sized enterprises that differ in their biases toward cyber behavior? The null hypothesis reflects the common practice of not differentiating between segments of employees and decision makers. This would justify using a one-size-fits-all approach, where all employees are targeted with the same intervention. Our hypothesis states that employees and decision makers differ in the way they perceive cyber risks and in terms of their cognitive biases.

2. Methodology

2.1 Design and data collection

To better understand the different types of employees and decision makers, their behavior, and the underlying biases toward cyber risks, we decided to take an exploratory approach and conduct in-depth qualitative interviews. Qualitative studies can provide rich perspectives and deep insights into individuals' attitudes, thought processes, and behaviors. We collected the data in July and August 2021. A total of 44 structured in-depth interviews were conducted, and their average duration was 60 min. The interviews were conducted in German and recorded using Microsoft Teams. We obtained ethical approval for the study from the Ethics Committee of the Faculty of Business, Economics and Social Sciences of the University of Bern (Ethical Approval Number 042023).

Our target groups were employees (n = 14), decision makers (n = 14), and IT service providers (n = 16). The interviewees were screened by a professional recruiter according to predefined criteria. They were selected in a balanced way based on age, gender, the size of the enterprise, the region (country vs city), industries, and whether they showed the desired cybersecurity behavior.

2.2 Material

We developed an interview guide to conduct the interviews in a structured manner. Our goal was to capture potential biases, barriers, and benefits associated with cyber risk-related target behaviors. Based on the literature (e.g. Jain *et al.*, 2016) and discussions with a cybersecurity expert, we identified the following cyber risk-related target behaviors for employees, decision makers, and IT service providers.

The four target behaviors identified for employees are as follows.

(1) Separating personal and professional information

(2) Not clicking on attachments or opening links in suspicious emails

(3) Choosing strong passwords and keeping your credentials private

(4) Only installing programs that come from a secure source

The four target behaviors identified for decision makers are as follows.

(1) Ensuring that employees follow the four behaviors mentioned above (a–d)

(2) Setting an example by observing the safety rules; participating in training; supporting managers/employees

(3) Using relevant IT support service providers

(4) Using relevant cyber insurance

The four target behaviors identified for IT service providers are as follows.

(1) Taking responsibility for getting employees to follow the four behaviors mentioned above (a–d)

(2) Making decision makers take responsibility for the four behaviors prescribed for employees (a–d)

(3) Getting decision makers to use relevant supporting IT service providers

(4) Getting decision makers to obtain relevant cyber insurance

To develop and structure the interview guide, we used the ecological model as a theoretical basis (Sallis *et al.*, 2015). Individual factors (e.g. knowledge and awareness) as well as organizational factors (e.g. existing measures and guidelines) and socio-cultural factors (e.g. social norms and role models) are relevant when adhering to the target behaviors mentioned above. Thus, the final interview guide was divided into corresponding sections: individual factors, organizational factors, and socio-cultural factors. To structure the individual-factors section, we used the Risks, Attitudes, Norms, Abilities, and Self-Regulation (RANAS) approach to systematic behavior change (Mosler, 2012). Based on this approach, we developed subsections with questions on the following aspects.

(1) *R*isk factors (e.g. knowledge of the risk associated with one's behavior)

(2) *A*ttitude factors (e.g. motivation to follow the target behaviors)

(3) *N*orm factors (e.g. how employees follow the target behaviors)

(4) *A*bility factors (e.g. how clear the adherence to the target behaviors is)

(5) *S*elf-regulation factors (e.g. automation of the target behaviors)

The organizational context included questions regarding the existing measures and guidelines related to the four target behaviors for employees. The socio-cultural context included questions regarding social norms, role models, and commitments. We also included questions about the professional situation with respect to the relevant function and risks in the enterprise as well as individual experiences with cyber risks. Since the target behaviors vary according to the target group, a slightly customized interview guide was created for each group (see supplementary material on repository). Further, the initial interviews for each group were considered pilot interviews, and the interview guide was adapted to a certain extent based on the same.

2.3 Data analysis

After collecting the interview data, each interview was fully transcribed into a structured Excel sheet. We used a generic and pragmatic approach to identify the biases, the barriers that hinder the desired cyber behavior, and the benefits that foster them. We first read all the transcripts and made descriptive notes about the themes that were important (Klingman and Cohen, 2004). Using these notes, we then identified and analyzed recurrent themes to gain insights into the meaning of the responses (Braun and Clarke, 2006). We further analyzed and explored the themes to uncover similar themes, which we made tangible through three personas. Next, using these persona types as a foundation, we reread the interviews and derived appropriate biases for each of them. Then, based on the biases and the behavioral science literature, the authors discussed which behavior change interventions were appropriate. Possible interventions that focus on the identified biases have been discussed here.

3. Findings

In our thematic analysis, we found three overarching themes for employees and decision makers, which we portray using three persona types (see Figure 2). These three personas emerged from recurring statements from the interviews. All interviewed employees and decision makers could be assigned to one of these three types, as they reported similar recurring barriers and benefits for their behavior.

The first persona type is that of a self-confident *expert* who feels competent and skilled with regard to cyber issues.

> I feel pretty competent. I also test things from the outside. Yes, using all kinds of methods. I've already attended a weekly hacking course [. . .].

The second persona type is that of an insecure *deportee* who feels incompetent and shifts the responsibility to the IT service provider.

> That goes through a company, and they take care of the security. We don't have to worry about it.

The third persona type is that of a naive *repressor* who feels confident and unconcerned. A repressor believes that their enterprise is too small, uninteresting, and irrelevant for a cyberattack.

> There's not much to gain here. There are certainly other industries that are much more interesting.

The persona types identified among the IT service providers were the same. Cybersecurity issues are experienced in similar ways in this group. The IT service providers clearly state that the technical responsibility lies with them but that the responsibility for the associated behavior lies with the enterprises.

> I can take responsibility to a certain extent, but the fundamental responsibility will always remain with the employee.

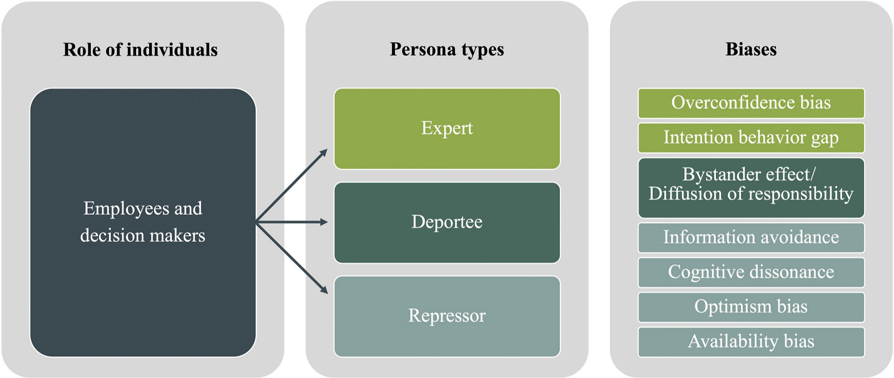
From the interview data, we derived seven cognitive biases that correspond to one of the defined persona types. Psychological theories and cognitive biases help us understand why employees and decision makers partly neglect the desired cyber behavior.

3.1 Employees and decision makers as experts

Individuals' self-confident character classifies them into the expert persona type. Such people feel competent with respect to cybersecurity and have a certain amount of relevant experience. Of the interviewees who could be assigned to this category, almost all were decision makers, and only a few were employees. They perceive the actual probability of an attack realistically and believe that no hardware and software is completely secure. Experts state that it is only a matter of time before an enterprise is hit, with luck playing a role in this context.

Cyber news is often sourced from (social) media. Interestingly, when a case is reported in the news, the issue is immediately brought up again within the enterprise. Contact is often made with the IT service provider to clarify the technical measures in place. Even among the experts, the IT service provider is simply trusted to provide the necessary security. Experts are vulnerable to overconfidence bias and/or the intention–behavior gap.

3.1.1 Overconfidence bias (experts). The overconfidence bias refers to the tendency of a person to overestimate their knowledge, abilities, or talent (see Figure 3; Pearson, 2020). Individuals consider themselves to be better than average (Proeger and Meub, 2014).



Note(s): Three persona types emerged from the interviews with the employees and decision makers. Each of these can be associated with certain misleading biases
Source(s): By authors

Figure 2. Overview of the three persona types and their corresponding biases

This belief may lead to them taking risky decisions. For example, 73% of Americans believe that they have above-average driving skills. This, in turn, can lead to risky driving behavior, as risk perception decreases and the optimism bias increases (Mohammadpour and Nassiri, 2021). The situation was similar in the enterprises we included in this study. The experts grew up with computers and worked with the device every day. This supposed experience leads to the belief that they are more sensitive to cyber risk issues than the average population. Other experts worked in larger enterprises before their current job, which led them to think that they can run smaller enterprises easily. They felt confident because their current enterprise was minor. However, the probability of an attack occurring is just as high in a small enterprise as in a larger enterprise.

3.1.2 Intention–behavior gap (experts). Different social psychological theories, such as the theory of planned behavior (Ajzen, 1985), the theory of reasoned action (Ajzen, 2012), and the protection motivation theory (Maddux and Rogers, 1983), claim that intention is a strong predictor of behavior. The underlying assumption is that when people intend to go jogging, for example, they will carry out their intentions accordingly and go jogging. The intention–behavior gap, however, describes the inconsistency between a person's intention and actual behavior (Sheeran, 2002). This gap between intention and behavior has been found in many different behaviors, such as physical activity, driving behavior, eating behavior, and IT behavior (Bhattacherjee and Sanford, 2009). Although experts know the four desired behaviors for employees and decision makers and acknowledge that humans pose the most significant risk to cybersecurity, secure behavior is not shown and encouraged. For instance, a business computer is used for private use and vice versa. Such free usage of devices is the norm in most enterprises. Regarding emails with suspicious attachments, people often rely on the spam filter and believe only emails from known senders can appear in their inbox. When choosing passwords, the same passwords are used for different accounts, are rarely changed, and are even written somewhere. Some decision makers do not know how their employees choose their passwords. When installing programs, people rely on antivirus software or trust that the program they need is secure. Various reasons are mentioned for not executing the desired behavior: time, initial effort, logistical effort, stress, and pressure at work.

3.2 Employees and decision makers as deportees

The deportee persona type is characterized by the tendency to shift the cyber responsibility to another person. Such individuals do not feel competent and do not know precisely what behaviors are safe. However, deportees know that humans pose the greatest cyber risk. They

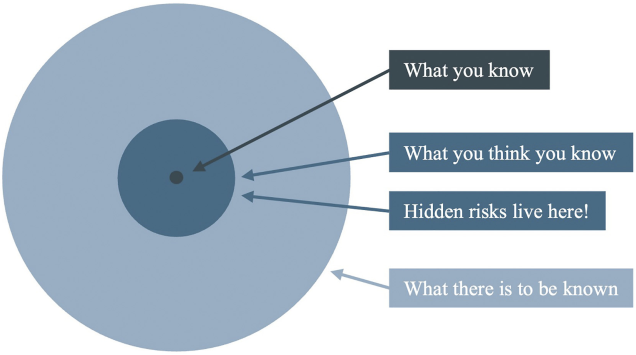


Figure 3.
Overconfidence bias

Note(s): People think they know more than they do. This overconfidence leads to hidden risks
Source(s): By courtesy of Pearson (2020)

think that the IT service provider is responsible for security and do not know what exactly the external IT service provider does in the enterprise. They know that a physical firewall is installed. It is assumed that the system is sufficiently secured by those responsible for it. One problem with cyber risks is that they are not tangible or visible. If a door is open, one can see it, or if employees are absent because of the coronavirus, for instance, it is obvious. However, cyber risks are hidden and, therefore, less obvious. Only when the enterprise is actually shut down are the effects visible. Moreover, in most companies, the focus shifts back to the core business within an hour of an attack.

Another problem is that there is often a lack of knowledge about why behaviors can be harmful. Deportees are unaware of the four desired behaviors for employees (see target behaviors for employees in the methodology section). Deportees ask themselves what can happen if personal and professional information is mixed. For convenience, several people use the same password for different programs. They know that they should have different ones, but the effort is considered to be too much. Although they know that there is sensitive data in the enterprise, such as patient or guest data, deportees are unaware of what a hacker could do with it. They believe that the data are useless to a hacker.

3.2.1 Bystander effect and diffusion of responsibility (deportees). Diffusion of responsibility describes the phenomenon in which a task is not carried out even though enough capable people are available. Each person hopes, consciously or unconsciously, that someone else will take the necessary action (Beyer *et al.*, 2017). The more people involved, the more likely each bystander will wait, believing that someone from the group will probably respond (Darley and Latane, 1968). Deportees argue that they are employed to do a specific task and not to address IT issues, such as cybersecurity. Moreover, they are not familiar with such tasks and believe that these are the responsibility of the IT service provider, who is paid for this and is an expert in the field. This is why deportees generally feel safe and consider the risk of an attack to be small. They believe that, in a worst-case scenario, the IT service provider will solve the problem. Further, situational norms and behavioral expectations in enterprises can influence a person’s responsibility. In most enterprises, cybersecurity is only addressed in the event of a technical installation or attack. Once such an incident is over, the topic is forgotten again, and the focus shifts to the important daily work. For this reason, each individual is not expected to be responsible for cybersecurity. Employees often rely on guidelines from higher-level administrators. At the latest after the first attack, cybersecurity should be a matter for decision makers. However, decision makers usually turn to the IT service providers in such situations. IT companies, by contrast, are only equipped to offer technical solutions and cannot address employees’ and decision makers’ behavior. In this study, the enterprise’s diffusion of responsibility for behavioral measures was the overarching problem. The responsibility for technical measures is clearly communicated and lies with the IT service provider. However, the responsibility for behavioral measures is shifted back and forth, and no one feels responsible for them (see Figure 4).

3.3 Employees and decision makers as repressors

The repressor persona type is characterized by reckless behavior. Such individuals are naive and underestimate the risk of an attack. Repressors argue that their enterprises are too small and uninteresting and that hackers target larger and more interesting international enterprises, such as banks. They also argue that nothing has ever happened to their enterprises, so the likelihood of them being subjected to an attack in the future is minimal. In the private setting, cyber risk and damage are given even less importance. This is even though they remember more private incidents and that more (technical) measures are implemented at work than in their private environment. Repressors are also unfamiliar with what cyber behavior is considered safe. In addition, they believe that an attack on their enterprise would not be too severe or harmful because they do not have any sensitive data; even if they do, they would store such data in a secondary location.

3.3.1 Information avoidance (repressors). Information avoidance refers to the act of intentionally avoiding or delaying the use of freely available information (Howell and Shepperd, 2016). Such actions are chosen to avoid knowing the information's potential negative consequences. Information avoidance can be active, such as asking a person not to say something, or passive, such as not asking questions to obtain necessary information (Klapper, 1961). Information about cyber dangers is made available in some enterprises (e.g. dangers in emails, installing secure programs, or choosing secure passwords), but repressors choose to ignore it. Such information alone does not lead to a change in behavior. The dangers are suppressed. One reason for this is that knowing the information can have unpleasant consequences for employees or decision makers. They would have to question their behavior and possibly modify it. Making a password more complex and consistently changing it is an effort that people prefer to avoid. Such suppression of available information is a way to release the state of tension created by cognitive dissonance.

3.3.2 Cognitive dissonance (repressors). Employees and decision makers aim to work efficiently and not take responsibility for cyberattacks, while their cybersecurity behaviors are unsafe. This reflects the cognitive dissonance theory, which states that people feel uncomfortable when they experience contradictory cognition (beliefs, thoughts, attitudes, and feelings). Cognitive dissonance occurs when one's beliefs are inconsistent with their behavior (Harmon-Jones and Mills, 2019). When an individual believes one thing but acts contrary to that belief, they usually resolve the resultant uncomfortable tension using different strategies. They may change their behaviors or attitudes or add new thoughts to rationalize their cognition. They also tend to reject or avoid new information. In addition to information avoidance, repressors discount the cyber risk based on the argument that their enterprise is too small and unattractive to attack. By claiming that the risk in their enterprise is small, the repressors can afford to behave unsafely and feel less tension. However, cyberattacks are often carried out using "bots" that systematically search for vulnerabilities. Therefore, it is only a matter of time before a weak password is cracked regardless of how uninteresting an enterprise is.

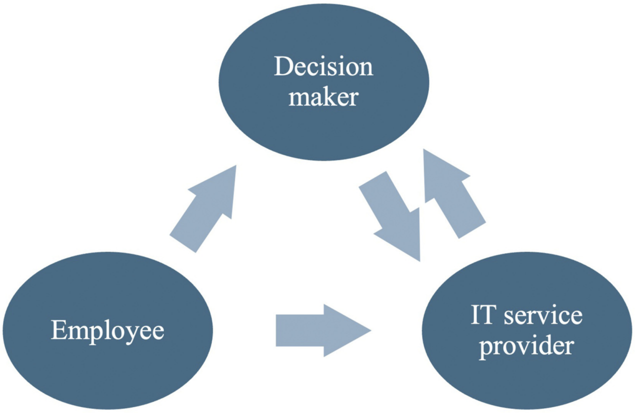


Figure 4. Diffusion of responsibility for cyber security behaviors in enterprises

Note(s): This figure illustrates the typical behavior of deportees: Employees pass on responsibility either to the decision makers or the IT service providers, decision makers pass on responsibility to the IT service providers, and IT service providers pass on responsibility for insecure behavior to the decision makers
Source(s): By authors

3.3.3 Optimism bias (repressors). The optimism bias describes the tendency to underestimate the likelihood that negative things will affect us while overestimating the likelihood that positive things will happen to us (Sharot, 2011). Typical examples of this phenomenon include how we underestimate our chances of getting into a car accident or getting divorced. We also tend to overestimate our success in the workplace and believe that our children are exceptionally talented. In cybersecurity, we mistakenly believe that the chances of one experiencing a cyberattack are lower than those for a peer or another enterprise. Overall, we tend to be over-optimistic. This tendency is further reinforced by the availability bias.

3.3.4 Availability bias (repressors). The availability bias refers to how we estimate the probability of a specific occurrence based on how easily or quickly we can think of relevant examples (Tversky and Kahneman, 1974). An example of the availability bias is estimating the divorce rate based on the number of divorced friends we have. Suppose one has never been affected by a cyberattack in one's private and business life, and they do not possess knowledge of any known attacks in their immediate environment. In such a case, the probability of an attack occurring is considered low because no specific examples come to mind.

The cognitive biases and theories described above can explain why it is difficult to change one's behavior despite having the necessary knowledge. Further, we can design better solutions if we better understand what leads to undesired behavior.

4. Discussion

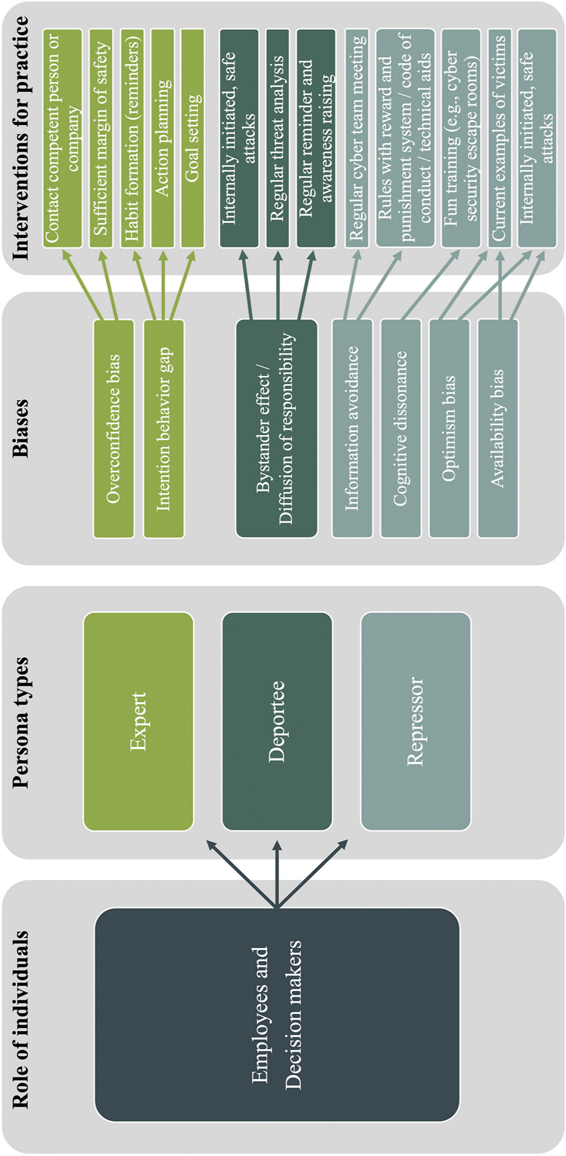
4.1 Implications for practice

Many attacks by cyber criminals are successful because they use psychology to exploit employee behavior to gain access to protected computer systems. Thus, in addition to implementing technical measures, it is crucial to take psychological measures to successfully defend an enterprise against cyberattacks. Based on the biases, barriers, and benefits related to the employees' and decision makers' behavior, this study contributes to practice by formulating potential tailored interventions that fit the three persona types (see Figure 5). It is important that the measures do not represent additional barriers for the employees and decision makers, and, instead, they should be easy and fun to implement.

4.1.1 Practical measures for experts. For the expert persona type, different measures can help counter the overconfidence bias and the intention–behavior gap. The first thing that can help with the *overconfidence bias* is the understanding that most people tend to be overconfident. The experts are probably well versed in specific fields but most likely not in the cyber domain, as they are either employed by an enterprise or are decision makers in a non-IT company. If experts recognize the limits of their cyber knowledge, they may be more willing to contact a suitable competent person or enterprise, which could be an IT person or a cyber insurance company that also addresses behavioral risks.

Another option is to plan for a sufficient margin of safety. This means investing more rather than less in cybersecurity, as we tend to underestimate the associated risk. For instance, cyber insurance can be implemented, employee training can be conducted, and regular security checks can be performed.

The *intention–behavior gap* implies that experts do not put their intentions into action. In other words, while experts intend to follow the four safe behaviors, many do not implement them. The COM-B model of behavior change is based on three components to implement any behavior. An individual needs to have the *c*apability, *o*pportunity, and *m*otivation to perform a *b*ehavior (Michie *et al.*, 2011). Experts possess the required physical and psychological capability—they can follow the four desired behaviors and know about cyber risks. They also have reflective motivation, as they intend to adhere to the four desired behaviors. However, they lack automatic motivation and physical and social opportunities. First, they do


Role of individuals
Employees and Decision makers
Persona types
Expert
Deportee
Repressor
Biases
Overconfidence bias
Intention behavior gap
Bystander effect / Diffusion of responsibility
Information avoidance
Cognitive dissonance
Optimism bias
Availability bias
Interventions for practice
Contact competent person or company
Sufficient margin of safety
Habit formation (reminders)
Action planning
Goal setting
Internally initiated, safe attacks
Regular threat analysis
Regular reminder and awareness raising
Regular cyber team meeting
Rules with reward and punishment system / code of conduct / technical aids
Fun training (e.g., cyber security escape rooms)
Current examples of victims
Internally initiated, safe attacks

Source(s): By authors

Figure 5. Overview of employees' and decision makers' personas, biases, and ideas regarding interventions for practice

not have the habit of following the four behaviors. Second, they do not have the financial resources to adhere to these behaviors, especially in small enterprises. They may also experience time pressure at work and lack the initial and logistical efforts to implement secure cyber behavior. Third, experts may fail to set cyber goals or social norms in enterprises.

The following behavior change techniques can help experts overcome the barriers mentioned above.

(1) Habit formation: Automatic reminders on their laptops or via emails may encourage experts to repeat the four behaviors and establish routines and habits. Repeating the behavior in the same context can also be prompted so that the context elicits the behavior. This means, for example, scheduling time for cyber topics in the first few minutes of each team meeting.

(2) Action planning: Experts can be encouraged to plan the implementation of the specific desired behaviors; thus, they can be aware of the time and day of the week when the cyber issue will be brought up and addressed. Once such a plan is in place, not much time is needed to execute it.

(3) Goal setting: Establishing a common goal, such as a team score with zero tolerance, can further motivate employees to adhere to a desired behavior (Wegge and Haslam, 2005). The success of this measure will increase if team members define goals together. In other words, it will be more effective when the goal is not imposed from above but, rather, when all team members have a say in the process. The IKEA effect, named after the famous Swedish furniture giant, describes how people value an item more if they have made it themselves (Norton *et al.*, 2012). In the context of cyber risk, the IKEA effect suggests that we will tend to take operation-specific threats more seriously when we can determine which behaviors to change or when we discover unsafe cybersecurity behaviors ourselves (e.g. old or shared passwords and unattended computers). If all employees share the common goal of contributing to cybersecurity, this reduces the intention–behavior gap. The common goal makes people pay more attention to cyber issues. No one wants to be a team member who does not achieve the common goal.

4.1.2 Practical measures for deportees. There are several ways for deportees to ensure that they do not shift cyber responsibility to another person but instead consider themselves responsible (*diffusion of responsibility*). First, there must be clarity between the decision makers and the IT service providers regarding who is responsible for which area and how to execute their responsibilities. Ideally, the risks that the IT service providers can cover (technical measures) and cannot cover (behavioral measures) should be clear from the very first meeting. The IT service providers are not responsible for what the employees and decision makers click on. If the decision makers do not feel competent enough to take responsibility for the behavior of the employees, it is best to involve a neutral party. This can be, for instance, an insurance company through which an enterprise can introduce the necessary behavioral measures.

A regular threat analysis (by the IT service provider) should reveal the areas that are the most accessible to attackers and what clever strategies they use. A fake cyberattack can be carried out to make deportees aware that they also bear responsibility for such incidents and that anyone can be affected. If deportees experience a fake cyberattack, they could realize how little is needed for a successful attack. This experience could make them more cautious in similar situations in the future. Regular reminders and awareness campaigns can be powerful determinants for bystanders' decision to follow the desired behavior (*bystander effect*). If behavioral expectations are not communicated, they cannot be expected. The communication of expectations can lead to the creation of new, beneficial norms in the enterprise.

4.1.3 Practical measures for repressors. Different interventions can help repressors better assess cyber risk and behave less naively. To counteract *information avoidance*, decision makers should proactively address desired behaviors regularly. Expectations can be discussed, for example, in a monthly team meeting before being fixed on the agenda so that no one can avoid the topic.

In addition, creating cyber rules should become a standard practice in every enterprise. It is crucial for decision makers to discuss the essential points with the employees and jointly determine the rules followed in the enterprise. Compliance with the rules should be rewarded, and non-compliance should be punished. Each team should devise its reward and punishment systems. Such systems could increase the motivation of the repressors to comply with the established rules. This code of conduct should be prominently posted in the office so that people are confronted with it and reminded of it daily. If the rules are followed repeatedly, they will eventually become the enterprise norm. In addition, technical aids, such as a password manager, can simplify work processes. Technical aids should lower the barriers to performing safe behaviors.

To counteract *cognitive dissonance*, repressors should learn that the likelihood of an attack is not dependent on the size or attractiveness of an enterprise and that the attacks are usually carried out using bots that systematically search for gaps. For this, repressors should experience such situations firsthand and undergo relevant training. Interventions for employees, such as training, must be fun and provide direct benefits. Easily understandable documents with visual cues can make such training more effective (Cuchta *et al.*, 2019). If the training is playful, competition occurs, and feedback can be provided, which will make the intervention more exciting and successful. Playful approaches, or so-called gamification, are entertaining and, thus, increase motivation (Alsawaier, 2018), as employees receive direct feedback on their behavior. Various providers offer games (Ferro and Sapio, 2020) or so-called cybersecurity escape rooms (e.g. Infosequre, 2020; Sectricity, 2020). There are also online adventure rooms that are less time-consuming (Jagmetti, 2018; Ludwig, 2019; SUPSI, 2019). These are fun and entertaining ways to assess and understand cyber risks.

Repressors also need a change in awareness to exhibit desirable behaviors. A possible way to achieve this is through internally initiated (and safe) cyberattacks to counter *optimism and availability biases*. By becoming the victim of a fake cyberattack, an individual can increase their awareness of the relevant potential risks. Accordingly, their estimation of the likelihood of becoming a victim of a cyberattack becomes more accurate, and over- or underestimations can be minimized. Further, there is another advantage of internally initiated attacks: When a phishing email is successfully detected and reported, one can be congratulated, which serves as an immediate reward. By receiving immediate positive or negative personal feedback, people can learn to attribute their behavior correctly. Another way to raise awareness among repressors is to show them current cyberattack examples experienced by other enterprises. The aim should be to illustrate how the attack occurred and how similar enterprises may be targeted.

4.2 Limitations and future work

Our results contribute to a deeper understanding of individuals who do not adhere to cybersecurity best practices. When interpreting the findings, it is important to consider the limitations of the employed methodology. The qualitative approach was appropriate for identifying factors that influence cyber behavior. However, more evidence is required regarding what works or does not work in practice. The interventions we discuss remain to be validated and measured through quantitative empirical methods. Using fail-fasts, adjustments can be made, and experience can be gained for future projects.

Another factor is that the research took place in Switzerland with a Swiss sample. The sample of employees, decision makers, and IT providers from different industries offers a comprehensive insight into cyber behavior practices. Since perceptions of security awareness, risk, or trust differ across cultures and nations (Rocha Flores *et al.*, 2015; Schomakers *et al.*, 2020), the proposed interventions are tailored only to the specific target group. Tailored interventions are inherently context- and time-specific. Employees of larger enterprises or from other countries could reveal other persona types and cognitive biases. This may limit the transferability of our results to other cultures. Future studies could examine cultural differences in this context, which could help identify additional factors that influence cyber behavior. Further, the same individuals may answer the interview questions in a different way a few years later.

5. Conclusion

Technical security tools alone are not enough to prevent cyberattacks, as it is often human behavior that can provide cyber criminals with the access they need. Human behavior interventions require little effort compared to technical solutions, which are usually sophisticated. Changing behavior requires consideration of the barriers and benefits as well as the context of a particular behavior. To understand why employees and decision makers are vulnerable to cyberattacks at work, a range of factors, such as personal, organizational, and socio-cultural factors, need to be considered. This article does not offer a validated program to change employees' and decision makers' behavior. Instead, this article aims to highlight the necessity of developing tailored behavioral interventions to strengthen the human factor and, thus, prevent cyberattacks. We argue that for cyber security issues, tailored interventions are necessary and more effective than uniform one-size-fits-all interventions, such as information campaigns or awareness programs. In small and medium-sized enterprises, employees and decision makers differ in their cognitive biases regarding insecure cyber behavior and therefore require different interventions. The contribution of this article is that it discusses 13 interventions that correspond to seven psychological biases and three persona types. These findings can serve as starting points for future research and interventions in practice.

References

Abass, I.A.M. (2018), "Social engineering threat and defense: a literature survey", *Journal of Information Security*, Vol. 9 No. 4, pp. 257-264, doi: 10.4236/jis.2018.94018.

Abreu, J.V.F., Fernandes, J.H.C., Gondim, J.J.C. and Ralha, C.G. (2020), "Bot development for social engineering attacks on Twitter", *arXiv*. doi: 10.48550/ARXIV.2007.11778.

Aggarwal, A. and Dhurkari, R.K. (2023), "Association between stress and information security policy non-compliance behavior: a meta-analysis", *Computers and Security*, Vol. 124, 102991, doi: 10.1016/j.cose.2022.102991.

Ajzen, I. (1985), "From intentions to actions: a theory of planned behavior", in Kuhl, J. and Beckmann, J. (Eds), *Action Control*, Springer, Heidelberg, Berlin, pp. 11-39, doi: 10.1007/978-3-642-69746-3_2.

Ajzen, I. (2012), "Martin Fishbein's legacy: the reasoned action approach", *The Annals of the American Academy of Political and Social Science*, Vol. 640 No. 1, pp. 11-27, doi: 10.1177/0002716211423363.

Albladi, S.M. and Weir, G.R.S. (2018), "User characteristics that influence judgment of social engineering attacks in social networks", *Human-Centric Computing and Information Sciences*, Vol. 8 No. 1, p. 5, doi: 10.1186/s13673-018-0128-7.

Alsawaier, R.S. (2018), "The effect of gamification on motivation and engagement", *The International Journal of Information and Learning Technology*, Vol. 35 No. 1, pp. 56-79, doi: 10.1108/IJILT-02-2017-0009.

Bada, M., Sasse, A.M. and Nurse, J.R.C. (2019), "Cyber security awareness campaigns: why do they fail to change behaviour?", *arXiv*. doi: 10.48550/ARXIV.1901.02672.

Baltuttis, D., Teubner, T. and Adam, M.T.P. (2024), "A typology of cybersecurity behavior among knowledge workers", *Computers and Security*, Vol. 140, 103741, pp. 1-17, doi: 10.1016/j.cose.2024.103741.

Beyer, F., Sidarus, N., Bonicalzi, S. and Haggard, P. (2017), "Beyond self-serving bias: diffusion of responsibility reduces sense of agency and outcome monitoring", *Social Cognitive and Affective Neuroscience*, Vol. 12 No. 1, pp. 138-145, doi: 10.1093/scan/nsw160.

Bhattacherjee, A. and Sanford, C. (2009), "The intention–behaviour gap in technology usage: the moderating role of attitude strength", *Behaviour and Information Technology*, Vol. 28 No. 4, pp. 389-401, doi: 10.1080/01449290802121230.

Braun, V. and Clarke, V. (2006), "Using thematic analysis in psychology", *Qualitative Research in Psychology*, Vol. 3 No. 2, pp. 77-101, doi: 10.1191/1478088706qp063oa.

Choras, M., Kozik, R., Churchill, A. and Yautsiukhin, A. (2016), "Are we doing all the right things to counter cybercrime?", in Akhgar, B. and Brewster, B. (Eds), *Combatting Cybercrime and Cyberterrorism – Challenges, Trends and Priorities*, Springer International Publishing AG, Switzerland, pp. 279-294.

Chowdhury, N.H., Adam, M.T.P. and Skinner, G. (2019), "The impact of time pressure on cybersecurity behaviour: a systematic literature review", *Behaviour and Information Technology*, Vol. 38 No. 12, pp. 1290-1308, doi: 10.1080/0144929X.2019.1583769.

Cuchta, T., Blackwood, B., Devine, T.R., Niichel, R.J., Daniels, K.M., Lutjens, C.H., Maibach, S. and Stephenson, R.J. (2019), "Human risk factors in cybersecurity", *paper presented at the SIGITE '19: The 20th Annual Conference on Information Technology Education*, Tacoma, WA, 3-5 October, available at: https://www.doi.org/10.1145/3349266.3351407 (accessed 21 August 2023).

Darley, J.M. and Latane, B. (1968), "Bystander intervention in emergencies: diffusion of responsibility", *Journal of Personality and Social Psychology*, Vol. 8 No. 4, pp. 377-383, Pt.1, doi: 10.1037/h0025589.

D'Arcy, J., Hovav, A. and Galletta, D. (2009), "User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach", *Information Systems Research*, Vol. 20 No. 1, pp. 79-98, doi: 10.1287/isre.1070.0160.

Ferro, L.S. and Sapio, F. (2020), "Another week at the office (AWATO) – an interactive serious game for threat modeling human factors", in Moallem, A. (Ed.), *HCI for Cybersecurity, Privacy and Trust*, Springer International Publishing, Cham, Vol. 12210, pp. 123-142, doi: 10.1007/978-3-030-50309-3_9.

Gundu, T., Maronga, M. and Boucher, D. (2019), "Industry 4.0 businesses environments: fostering cyber security culture in a culturally diverse workplace" in Njenga, K. (Ed.), *paper presented at the Proceedings of 4th International Conference on the Internet, Cyber Security and Information Systems 2019*, Johannesburg, South Africa, Kalpa Publications in Computing, pp. 85-94, available at: https://www.doi.org/10.29007/r64x (accessed 15 August 2023).

Harmon-Jones, E. and Mills, J. (2019), "An introduction to cognitive dissonance theory and an overview of current perspectives on the theory", in Harmon-Jones, E. (Ed.), *Cognitive Dissonance: Reexamining a Pivotal Theory in Psychology*, 2nd ed., American Psychological Association, Washington, pp. 3-24, doi: 10.1037/0000135-001.

Hong, J. (2012), "The state of phishing attacks", *Communications of the ACM*, Vol. 55 No. 1, pp. 74-81, doi: 10.1145/2063176.2063197.

Howell, J.L. and Shepperd, J.A. (2016), "Establishing an information avoidance scale", *Psychological Assessment*, Vol. 28 No. 12, pp. 1695-1708, doi: 10.1037/pas0000315.

Infosequre (2020), "Race against the clock to gain security awareness and escape before the bang", *Security Awareness Escape Room*, available at: https://www.infosequre.com/security-awareness-escape-room (accessed 15 August 2023).

Iyengar, S.S. and Lepper, M.R. (1999), "Rethinking the value of choice: a cultural perspective on intrinsic motivation", *Journal of Personality and Social Psychology*, Vol. 76 No. 3, pp. 349-366, doi: 10.1037/0022-3514.76.3.349.

Jagmetti, S. (2018), "Hack the hacker – it's on!", *SWITCH*, available at: https://www.switch.ch/de/stories/escape-room-hack-the-hacker/ (accessed 15 August 2023).

Jain, A., Tailang, H., Goswami, H., Dutta, S., Singh Sankhla, M. and Kumar, R. (2016), "Social engineering: hacking a human being through technology", *Journal of Computer Engineering (IOSR-JCE)*, Vol. 18, pp. 94-100, doi: 10.9790/0661-18050594100.

Kahneman, D. (2011), *Thinking, Fast and Slow*, Macmillan, New York, NY.

Kim, H. and Markus, H.R. (1999), "Deviance or uniqueness, harmony or conformity? A cultural analysis", *Journal of Personality and Social Psychology*, Vol. 77 No. 4, pp. 785-800, doi: 10.1037/0022-3514.77.4.785.

Kirlappos, I., Parkin, S. and Sasse, M.A. (2014), "Learning from 'shadow security: 'why understanding non-compliant behaviors provides the basis for effective security", *paper presented at Proceedings 2014 Workshop on Usable Security*, San Diego, CA, available at: https://www.doi.org/10.14722/usec.2014.23007 (accessed 16 August 2023).

Klapper, J.T. (1961), "The effects of mass communication: an analysis of research on the effectiveness and limitations of mass media in influencing the opinions, values and behavior of their audiences", *Communications*, Vol. 1 No. 1, pp. 202-205, Persée – Portail des revues scientifiques en SHS.

Klingman, A. and Cohen, E. (2004), "The generic intervention approach and principles", in Klingman, A. and Cohen, E. (Eds), *School-Based Multisystemic Interventions for Mass Trauma*, Springer US, Boston, MA, pp. 87-91, doi: 10.1007/978-1-4419-9104-1_9.

Kolesnikov, N. (2023), "50+ cybersecurity statistics for 2023 you need to know – where, who & what is targeted", *Techopedia*, available at: https://www.techopedia.com/cybersecurity-statistics (accessed 16 August 2023).

Kreuter, M.W. and McClure, S.M. (2004), "The role of culture in health communication", *Annual Review of Public Health*, Vol. 25 No. 1, pp. 439-455, doi: 10.1146/annurev.publhealth.25.101802.123000.

Ludwig, L. (2019), "Cybersecurity awareness escape rooms – join the fun!", *Activity at Security Professionals Conference*, available at: https://events.educause.edu/special-topic-events/security-professionals-conference/2019/agenda/cybersecurity-awareness-escape-rooms–join-the-fun (accessed 15 August 2023).

Lustria, M.L.A., Noar, S.M., Cortese, J., Van Stee, S.K., Glueckauf, R.L. and Lee, J. (2013), "A meta-analysis of web-delivered tailored health behavior change interventions", *Journal of Health Communication*, Vol. 18 No. 9, pp. 1039-1069, doi: 10.1080/10810730.2013.768727.

Maddux, J.E. and Rogers, R.W. (1983), "Protection motivation and self-efficacy: a revised theory of fear appeals and attitude change", *Journal of Experimental Social Psychology*, Vol. 19 No. 5, pp. 469-479, doi: 10.1016/0022-1031(83)90023-9.

Mashtalyar, N., Ntaganzwa, U.N., Santos, T., Hakak, S. and Ray, S. (2021), "Social engineering attacks: recent advances and challenges", in Moallem, A. (Ed.), *HCI for Cybersecurity, Privacy and Trust*, Springer International Publishing, Cham, Vol. 12788, pp. 417-431, doi: 10.1007/978-3-030-77392-2_27.

Michie, S., van Stralen, M.M. and West, R. (2011), "The behaviour change wheel: a new method for characterising and designing behaviour change interventions", *Implementation Science*, Vol. 6 No. 1, p. 42, doi: 10.1186/1748-5908-6-42.

Mohammadpour, S.I. and Nassiri, H. (2021), "Aggressive driving: do driving overconfidence and aggressive thoughts behind the wheel, drive professionals off the road?", *Transportation Research F: Traffic Psychology and Behaviour*, Vol. 79, pp. 170-184, doi: 10.1016/j.trf.2021.04.008.

Morgan, P.L., Asquith, P.M., Bishop, L.M., Raywood-Burke, G., Wedgbury, A. and Jones, K. (2020), "A new hope: human-centric cybersecurity research embedded within organizations", in Moallem, A. (Ed.), *HCI for Cybersecurity, Privacy and Trust*, Springer International Publishing, Cham, Vol. 12210, pp. 206-216, doi: 10.1007/978-3-030-50309-3_14.

Mosler, H.-J. (2012), "A systematic approach to behavior change interventions for the water and sanitation sector in developing countries: a conceptual model, a review, and a guideline", *International Journal of Environmental Health Research*, Vol. 22 No. 5, pp. 431-449, doi: 10.1080/09603123.2011.650156.

Nobles, C. (2018), "Botching human factors in cybersecurity in business organizations", *HOLISTICA – Journal of Business and Public Administration*, Vol. 9 No. 3, pp. 71-88, doi: 10.2478/hjbpa-2018-0024.

Norton, M.I., Mochon, D. and Ariely, D. (2012), "The IKEA effect: when labor leads to love", *Journal of Consumer Psychology*, Vol. 22 No. 3, pp. 453-460, doi: 10.1016/j.jcps.2011.08.002.

Pearson, T. (2020), "Overconfidence bias: what it is and how to overcome it - Reality has a surprising amount of detail", available at: https://taylorpearson.me/overconfidence-bias/ (accessed 16 August 2023).

Peter, M.K., Hölzli, A., Kaelin, A.W., Mändli Lärch, K., Vifian, P. and Wettstein, N. (2020), "Digitalisierung, Home-Office und Cyber-Sicherheit in KMU", Ein Beitrag zum Verständnis und zur Stärkung von Schweizer KMU mit 4-49 Mitarbeitenden im Umfeld von Corona (COVID-19), gfs-zürich, Markt- und Sozialforschung, Bern, pp. 1-30.

Proctor, R.W. and Chen, J. (2015), "The role of human factors/ergonomics in the science of security: decision making and action selection in cyberspace", *Human Factors: The Journal of the Human Factors and Ergonomics Society*, Vol. 57 No. 5, pp. 721-727, doi: 10.1177/0018720815585906.

Proeger, T. and Meub, L. (2014), "Overconfidence as a social bias: experimental evidence", *Economics Letters*, Vol. 122 No. 2, pp. 203-207, doi: 10.1016/j.econlet.2013.11.027.

Rocha Flores, W., Holm, H., Svensson, G. and Ericsson, G. (2014), "Using phishing experiments and scenario-based surveys to understand security behaviours in practice", *Information Management and Computer Security*, Vol. 22 No. 4, pp. 393-406, doi: 10.1108/IMCS-11-2013-0083.

Rocha Flores, W.R., Holm, H., Nohlberg, M. and Ekstedt, M. (2015), "Investigating personal determinants of phishing and the effect of national culture", *Information and Computer Security*, Vol. 23 No. 2, pp. 178-199, doi: 10.1108/ICS-05-2014-0029.

Sallis, J.F., Owen, N. and Fisher, E. (2015), "Ecological models of health behavior", in Glanz, Z., Rimer, B.K. and Viswanath, K. (Eds), *Health Behavior: Theory, Research, and Practice*, 5th ed., Jossey-Bass, San Francisco, CA, pp. 435-461.

Schomakers, E.-M., Biermann, H. and Ziefle, M. (2020), "Understanding privacy and trust in smart home environments", in Moallem, A. (Ed.), *HCI for Cybersecurity, Privacy and Trust*, Springer International Publishing, Cham, Vol. 12210, pp. 513-532, doi: 10.1007/978-3-030-50309-3_34.

Sectricity (2020), "Cyber security escape truck", available at: https://sectricity.com/en/security-awareness-en/cyber-security-escape-room/ (accessed 15 August 2023).

Sharot, T. (2011), "The optimism bias", *Current Biology*, Vol. 21 No. 23, pp. R941-R945, doi: 10.1016/j.cub.2011.10.030.

Sheeran, P. (2002), "Intention–behavior relations: a conceptual and empirical review", *European Review of Social Psychology*, Vol. 12 No. 1, pp. 1-36, doi: 10.1080/14792772143000003.

Stanton, B., Theofanos, M.F., Prettyman, S.S. and Furman, S. (2016), "Security fatigue", *IT Professional*, Vol. 18 No. 5, pp. 26-32, doi: 10.1109/MITP.2016.84.

SUPSI (2019), "Hack the internet. Escape room developed by the Laboratorio tecnologie e media in educazione Dipartimento formazione e apprendimento, SUPSI, Switzerland", available at: http://www.school-break.eu/escape-rooms-2?tx_category=fr (accessed 15 August 2023).

Triandis, H.C. (1989), "The self and social behavior in differing cultural contexts", *Psychological Review*, Vol. 96 No. 3, pp. 506-520, doi: 10.1037/0033-295X.96.3.506.

Triplett, W.J. (2022), "Addressing human factors in cybersecurity leadership", *Journal of Cybersecurity and Privacy*, Vol. 2 No. 3, pp. 573-586, doi: 10.3390/jcp2030029.

Tversky, A. and Kahneman, D. (1974), "Judgment under uncertainty: heuristics and biases: biases in judgments reveal some heuristics of thinking under uncertainty", *Science*, Vol. 185 No. 4157, pp. 1124-1131, doi: 10.1126/science.185.4157.1124.

Van Baaren, R.B., Maddux, W.W., Chartrand, T.L., De Bouter, C. and Van Knippenberg, A. (2003), "It takes two to mimic: behavioral consequences of self-construals", *Journal of Personality and Social Psychology*, Vol. 84 No. 5, pp. 1093-1102, doi: 10.1037/0022-3514.84.5.1093.

Wegge, J. and Haslam, S.A. (2005), "Improving work motivation and performance in brainstorming groups: the effects of three group goal-setting strategies", *European Journal of Work and Organizational Psychology*, Vol. 14 No. 4, pp. 400-430, doi: 10.1080/13594320500349961.

Williams, E.J., Beardmore, A. and Joinson, A.N. (2017), "Individual differences in susceptibility to online influence: a theoretical review", *Computers in Human Behavior*, Vol. 72, pp. 412-421, doi: 10.1016/j.chb.2017.03.002.

Williams, E.J., Hinds, J. and Joinson, A.N. (2018), "Exploring susceptibility to phishing in the workplace", *International Journal of Human-Computer Studies*, Vol. 120, pp. 1-13, doi: 10.1016/j.ijhcs.2018.06.004.

Wilson, M., McDonald, S., Button, D. and McGarry, K. (2023), "It won't happen to me: surveying SME attitudes to cyber-security", *Journal of Computer Information Systems*, Vol. 63 No. 2, pp. 397-409, doi: 10.1080/08874417.2022.2067791.

Wirz, L., Bogdanov, M. and Schwabe, L. (2018), "Habits under stress: mechanistic insights across different types of learning", *Current Opinion in Behavioral Sciences*, Vol. 20, pp. 9-16, doi: 10.1016/j.cobeha.2017.08.009.

Yaacoub, J.-P.A., Salman, O., Noura, H.N., Kaaniche, N., Chehab, A. and Malli, M. (2020), "Cyber-physical systems security: limitations, issues and future trends", *Microprocessors and Microsystems*, Vol. 77, pp. 1-33, doi: 10.1016/j.micpro.2020.103201.

Supplementary material

Supplementary material available at: https://osf.io/6mycn/?view_only=28ddc74208374c409156e463144d4acc

Corresponding author

Claude Messner can be contacted at: claude.messner@unibe.ch