risks

MDPI

Article

Towards Diagnosing and Mitigating Behavioral Cyber Risks

Carlo Pugnetti [1,*], Albena Björck [2], Reto Schönauer [3] and Carlos Casián [4]

[1] Institute of Financial Services Zug IFZ, Lucerne School of Business, Suurstoffi 1, 63434 Rotkreuz, Switzerland
[2] ZHAW School of Management and Law, Zurich University of Applied Sciences, St.-Georgen-Platz 2, 8400 Winterthur, Switzerland; albena.bjoerck@zhaw.ch
[3] Schweizer Mobiliar Versicherungsgesellschaft AG, Bundesgasse 35, 3001 Berne, Switzerland; reto.schoenauer@mobi.ch
[4] Kessler & Co AG, Forchstrasse 95, 8032 Zurich, Switzerland; carlos.casian@kessler.ch
* Correspondence: carlo.pugnetti@hslu.ch

Abstract: A company's cyber defenses are based on a secure infrastructure and risk-aware behavior by employees. With rising cyber threats and normative training efforts showing limited impact, raising cyber risk awareness is emerging as a challenging effort. The review of the extant literature on awareness diagnosis shows interdisciplinary but mainly theoretical approaches to understanding attitudes and influencing risk behavior. We propose and test a novel methodology to combine and operationalize two tools, deep metaphor interviews and the IDEA risk communication model, to apply them for the first time in the context of behavioral cyber vulnerabilities. The results show a link between diagnosed attitudes and effective risk behavior in a real-life organizational setting, indicating the potential for an expanded diagnostic effort. We propose to develop a broader diagnostic and intervention set to improve cyber awareness and a toolkit to support the business practice of cyber risk management.

Keywords: risk; cybersecurity; cyber risk; risk behavior; risk communication; risk mitigation

Citation: Pugnetti, Carlo, Albena Björck, Reto Schönauer, and Carlos Casián. 2024. Towards Diagnosing and Mitigating Behavioral Cyber Risks. *Risks* 12: 116. https://doi.org/10.3390/risks12070116

Academic Editor: Krzysztof Jajuga

Received: 6 April 2024
Revised: 21 June 2024
Accepted: 2 July 2024
Published: 19 July 2024

1. Introduction

Cyber risks, defined as risks affecting information technology assets and threatening the confidentiality, availability, and integrity of information and entire information systems (Biener et al. 2015), pose a significant and growing threat. Cybercrimes already cost the world at least USD 6 trillion in 2021 and could lead to over USD 10 trillion worth of annual damages by 2025 (Morgan 2020). The continuous and increasing dependence on IT systems, and the surge in digitalization and the associated increase in the home office and hybrid work schedules, give attackers new opportunities to steal company data, smuggle malware into company networks, and steal money from companies using social engineering methods. While relatively new, cyber risks are among the top risks for every company—independent of size and industry (WEF 2022). The discussion of these risks in the public sphere and in the academic literature is driven primarily by technological development, individual and organizational vulnerabilities, and regulatory pressures. Academic research on the perception of cyber risks has spanned psychological, cultural, and human aspects, but cyber risk investigation remains challenging: First, with the rapid technological development and penetration of activities, new threats emerge constantly making the phenomenon highly dynamic, and any risk information and needed precautions need to be updated much faster and more often than other risks. Second, the cybercriminals and their networks remain anonymous, and a thorough investigation, if any, is not made public. Third, the technical sophistication and complexity of the topic prevent the involvement of larger stakeholder groups and the public in a wider risk discussion (Xu et al. 2021). Human error often leads to a cyber incident. For example, in the UK, 90% of cyber data breaches were caused by user errors in 2019 (CybSafe 2020). Recent

studies identified factors influencing the perception of cyber risk and responses to it such as voluntariness, immediacy, catastrophic potential, dread, the severity of consequences, lack of control, internet experience, frequency of internet use, culture, and personality (Van Schaik et al. 2017; Whitty et al. 2015). Psychological studies point out cognitive biases and the lack of motivation to adopt security solutions as primary reasons for poor cybersecurity decisions and stress the importance and urgency of cyber risk communication (West 2008; West et al. 2009).

The importance of risk and crisis communication for preventing and solving crisis events is undisputable (Coombs and Holladay 2010). Communication plays a key role before the crisis occurs, in the event of risk manifestation and effective crisis solving, and in the after-crisis period of learning and reflection (Coombs 2009). The pre-crisis phase is considered crucial to building trust and confidence, preventing future crises, and preparing the organization for quick and effective crisis resolution (Novak and Sellnow 2009; Seeger 2006). The literature highlights that effective risk messages can help raise audience perception and motivate individuals to take precautions against cyber risks (Zhang and Borden 2020), thus pointing to a promising avenue for future research. However, little research has been conducted relating to the cyber risks field, and much remains to be achieved to investigate how risks are to be communicated and how communication influences cyber risk perception and behavior (Xu et al. 2021). In recent years, the discussion on risk and crisis communication shifted from the external perspective (media and customer relations) to the internal one shedding light on the role of employees during a crisis (Frandsen and Johansen 2011). Employees are key stakeholders in a crisis (Kim 2018): they receive the organizational instructions and information and transmit them throughout and outside of the organization thus not only participating in a meaning-construction process but influencing the perception of others (Mazzei and Ravazzani 2011; Kim and Rhee 2011). Despite the key role of employees in detecting, avoiding, and managing cyber risks, internal risk and crisis communication in this context have received limited attention in the literature (Björck et al. 2024).

Against this background of significant and growing cyber threats, and the importance of human behavior in addressing this challenge, this paper aims to contribute to answering the following question:

How can we accurately diagnose and mitigate cyber vulnerabilities linked to human behavior?

To achieve this goal, we analyze the extant literature on risk diagnosis and mitigation and conduct empirical research to create a step-by-step approach to increase cyber risk awareness. This approach is innovative in several dimensions. First, we identify several factors that influence risk behavior, such as individual environments and personalized messages rather than standard settings and training. This is the result of an inductive process driven by interview responses rather than assumptions by the research team. Second, we introduce metrics for observed risk behavior, rather than self-reporting as in most current approaches. Third, we operationalize and develop modalities to deliver behavioral improvements, both of which are currently lacking in the cyber risk literature. The methodology is based on two tools: deep metaphors interviews and IDEA. While each is established in their respective contexts (market research and risk communication), their application to the field of cyber risk is novel. We present the progress to date in building and testing this approach in the context of the employees of Swiss SMEs and large companies with the support of two insurance companies, Allianz and Mobiliar.

2. A Review of the Current Literature

To address the research question, our study analyzed the literature on cyber risks, behavioral vulnerabilities, and influencing risk behavior.

Li and Liu (2021) survey cyber-attacks and cybersecurity to identify nine types of attacks and seven areas of cybersecurity to prevent and mitigate them. Six of these are described in normative terms. Operational Security, for example, includes processes and decisions made to control and protect data, such as user permissions when accessing

the network or processes that specify when and where information may be stored or shared. The sole exception is end-user training, which refers to unpredictable aspects of cybersecurity, namely individuals. Anyone can accidentally get a virus into the security system. Teaching the user to remove suspicious attachments in the email, not connecting to anonymous USBs, and other critical issues should be part of any company's corporate security plan. This technocratic and infrastructure-centric approach is a necessary but not sufficient condition for defending against cyber risks. Indeed, it can be argued that this approach severely misrepresents the true risk faced by organizations. Well-intentioned but careless employees pose a much greater risk to a company's cybersecurity than hackers on the outside (Borkovich and Skovira 2020). The Internet Crime Complaint Center reports that phishing attacks or similar incidences account for 59% of all attacks in the United States in 2021 (Federal Bureau of Investigation 2022). Some 83% of organizations experienced a successful phishing attack in 2021, up 46% from 2020, and 34% of employees did something to put themselves or their organizations at risk in 2022 (Proofpoint 2023). Phishing and other types of attacks based on employee vulnerabilities account for 66% of all initial vectors of successful attacks. These breaches take on average 277 h to fix and cost each more than USD 4.0 million for the target company (IBM Security 2022). Thus, far from being an additional and unpredictable minor component to cybersecurity, user behavior is the weakness most often exploited by hackers to breach a company's security. It therefore needs to be one of the areas of main focus to manage cyber risks. Training is often used to address these behavioral vulnerabilities. Prümmer et al. (2024) review the current literature on cybersecurity training to find significant gaps in the insights generated. While they find that the majority of the 142 studies reviewed reported a positive effect of training, they note the weakness of the current research. Most research design and intervention approaches were not anchored in theory, but rather relied on common sense. In addition, intentions rather than behavior were tested, leading to the conclusion that intervention design and evaluation need to be improved.

2.1. Diagnosing Cyber Behavioral Vulnerability

What constitutes "good" online behavior has been investigated in several recent studies. The field, however, is still in development. Stanton et al. (2005) develop a taxonomy of password-related behavior structured along with intentionality of malicious intent and technical expertise. They find that the surveyed organizations show all behaviors in the taxonomy, albeit with different distributions and that training does not impact the behavior significantly, and they observe that self-reporting may not be an appropriate diagnostic tool for intentionally malicious behavior. Egelman and Peer (2015) point to the lack of a standardized measurement tool for end-user security behavior and develop a new scale to do so: the Security Behavior Intentions Scale (SeBIS). Starting with an initial set of 30 questions developed with security experts, they conduct a large-scale survey to validate the construct and propose a scale consisting of 16 items mapping uniquely onto four security factors: device securement, password generation, proactive awareness, and updating. Vishwanath et al. (2020) take a broader approach to define and operationalize cyber hygiene. Borrowing from the concept of personal hygiene, they define it as a set of simple daily routines, good behaviors, and occasional checkups to make sure the organization's online health is in optimal condition (ENISA 2016). Starting from a set of 39 questions, they suggest a set of 18 questions mapping onto five dimensions of cyber hygiene: storage and device, transmission, social media, authentication, and messaging.

Several recent studies attempt to establish a link between cybersecurity behavior and other factors.

Ng et al. (2009) focus on email users and link four security behaviors to nine potential influencers applying an adapted version of the health belief model (Rosenstock 1974). They find that perceived susceptibility, benefits, and self-efficacy are good predictors of email security behavior, whereas perceived barriers, cues to action, general security orientation, and perceived severity are not. Severity, however, does moderate the impact of the first

three influencers. They suggest that training programs address the specificity of individual threats and reinforce employee confidence in their ability to thwart cyber-attacks.

Parsons et al. (2014) develop the Human Aspects of Information Security Questionnaire (HAIS-Q) to examine the relationship between knowledge and attitude towards security policies and procedures and the actual behavior of employees. The tool is a self-assessment of knowledge, attitude, and behavior (KAB) along seven focus areas, each with several subareas, identified through expert interviews with senior management. Behaviors are categorized as good, neutral, or bad. In this taxonomy, good and bad behavior are deliberate, whereas neutral are security breaches where the employee meant no harm to the organization, such as sharing usernames and passwords without malicious intent. The authors find a strong correlation between knowledge and attitude. Attitude also strongly correlates with more risk-averse behavior. Thus, companies should influence their employees' attitudes towards security policies if they want to improve security. Providing generic courses will not be sufficient.

Sebescen and Vitak (2017) investigate how three sets of employee characteristics (demographic, company-specific, and skills-based) link to cyber vulnerability along four dimensions (phishing, passwords, bring-your-own-device, and company-provided laptops). Employees self-assess their behavior by responding to 21 questions by selecting between two and seven potential answers. The questions are derived from the literature and the answers are scored on a scale of 1–10 to measure their riskiness. The analysis shows that technical skills, security knowledge, gender, and recent security training do not correlate with reduced risk behavior. Being new to the company, involved in an IT organizational role, or being older reduces the cyber risk profile of the employees. Thus, broad-spectrum training by itself does not effectively address cybersecurity. Rather, training should be incorporated into everyday tasks. Compliance with security policies does not mean a lower risk, information about security risks should flow freely, and especially vulnerable employee categories should receive specific training and use special security procedures.

Hadlington (2017) links risky cybersecurity behaviors to addiction, impulsivity, and attitudes towards cybersecurity. He uses the abbreviated impulsiveness scale (ABIS) from Coutlee et al. (2014) and the online cognition scale (OCS) from Davis et al. (2002) to measure impulsivity and problematic internet use. However, he also develops two additional tools. The first is the risky cybersecurity behaviors scale (RScB), a further development of SeBIS (Egelman and Peer 2015) using input from digital forensic investigators and other law enforcement officials, and which uses self-reporting by respondents to gauge how often they engage in 20 types of risky behavior. The second is the attitudes towards cybersecurity and cybercrime questionnaire (ATC-IB), constructed with the expertise of police, digital forensics, criminal psychology, and cyberpsychology, and which asks respondents to self-score their level of agreement towards 25 attitudes. The research tests the tools on 500 respondents in the UK to find that attitude and behavior are linked, with pockets of problematic behaviors in spite of training efforts and with almost all respondents devolving responsibility for cybersecurity to management. Impulsivity and addiction are also linked to risky behaviors. Hadlington (2018) applies the tools to investigate the effect of company size and employee age to find that, while risky behaviors are widespread, employees of larger companies or who are older show less risky behavior. The reasons for this, however, are not clear. More recently, a number of studies have been conducted using these tools (e.g., Antunes et al. 2021a, 2021b).

Kennison and Chan-Tin (2020) build on the previous literature that training on security best practices may not be an effective tool to reduce cyber risks (e.g., Lorenz et al. 2013) to investigate if risky cybersecurity behavior can be predicted from a combination of knowledge personality traits and general risk-taking behavior. Respondents self-reported on their likelihood to engage in six common risky behaviors such as using a weak password, sharing passwords with others, or clicking on suspicious URLs. Knowledge of password security was estimated with a newly developed four-item diagnostic; risk-taking behavior was assessed using the SSS-V sensation-seeking scale (Zuckerman et al. 1978) and the

DOSPERT risk-taking scale (Blais and Weber 2006); and personality was captured using the Big 5 traits (Saucier 1994). Their research finds that these factors explain about a third of self-reported cyber risk behaviors and suggests that personal profiles be taken into account when estimating threat levels.

Schoenherr and Thomson (2021) develop a diagnostic of cyber hygiene behavior using a cybersecurity code (CESC) based on individual traits and motivation. They build on their previous research showing how existing behavioral and social science approaches can provide a more solid analytical foundation for analyzing insider threats and noticing how most insider threats are caused by unintentional rather than intentional behavior (Schoenherr and Thomson 2020). Cyber hygiene behavior was structured along the two dimensions of disclosure and intrusion vulnerability. Disclosure vulnerability relates to the likelihood of inadvertently disclosing sensitive information and is operationalized by the amount of use of social media. Intrusion vulnerability, on the other hand, relates to the security against cyber-attacks and is operationalized using the frequency of computer use. Following Greitzer et al. (2019), they model individual traits along the Big 5 and the Dark Triad. Motivation was modeled as promotion (i.e., focusing on gains) or prevention (i.e., focusing on loss prevention) based on Higgins (1998). The research shows that disclosure and intrusion vulnerability do not correlate with each other and that individual traits only weakly correlate through vulnerability. On the other hand, motivation plays a significant role in cyber hygiene behavior, and both promotion and prevention motivation are linked with riskier behavior.

The papers discussed are summarized in Table 1. Generalizing the insights generated by these studies, we see that several factors can influence risk behavior, with individual environments rather than static characteristics or normative settings playing the most significant role in impacting cyber risk behavior. Personalized messages rather than standard training hold the highest potential for improving this behavior. Unfortunately, none of the studies reviewed provide a structured approach to defining the contents and modality of these behavioral improvement efforts. Further, the insights are generated using risk behavior which has been self-assessed or estimated by proxy, rather than observed risk behavior. This weakens the insights significantly.

Table 1. Summary of cyber-diagnostic approaches.

Authors and Year	Method	Focus	Key Takeaways
(Ng et al. 2009)	Adapted health belief model	Email security behavior	Training to reinforce employee confidence
(Parsons et al. 2014)	Human Aspects of Information Security Questionnaire (HAIS-Q)	Link between knowledge, attitude, and behavior	Influence attitude to impact behavior
(Sebescen and Vitak 2017)	Self-assessment of behavior, expert risk scoring	Four dimensions of vulnerability and three sets of employee characteristics	Compliance with security policies does not imply lower risk
(Hadlington 2017)	Risky cybersecurity behaviors scale (RScB), attitudes towards cybersecurity and cybercrime questionnaire (ATC-IB)	Cybersecurity behavior links to addiction, impulsivity, and attitude	Attitude and behavior are linked. Risky behaviors are widespread
(Kennison and Chan-Tin 2020)	Self-reported engagement in six common risky behaviors	Cybersecurity behavior link to knowledge, personality traits, and general risk-taking	Consider personal profiles when estimating threat levels
(Schoenherr and Thomson 2021)	Vulnerability operationalized by usage of social media and frequency of computer use	Unintentional cyber behavior based on individual traits and motivation	Prospective gains and losses are linked to risk behavior
Underwriting questionnaires from insurance carriers and brokers		Focus shift from technical infrastructure to behavioral risk	
Threat assessment from law enforcement/security agencies		Confidential/not peer-reviewed	

2.2. Influencing Risk Behavior

The research on risk behavior relating to cyber investigated in Section 2.1 agrees with the broader and more established research on general risk behavior, allowing for the use of established risk diagnostic and mitigation approaches. Risk decision-making and behavior are domain-specific and linked to risk propensity and risk perception. Thus, it varies for the same person across different activities, it is linked to their personal attitude towards risk, and it depends on the subjective estimate of the risk (Weber et al. 2002). This holds both in a business setting (Sitkin and Pablo 1992) and for personal choices (Brewer et al. 2004). Several tools have been developed to measure risk propensity, both in context-specific and in more generalized settings (Meertens and Lion 2008; Zhang et al. 2018).

Consumer research has long focused on understanding cognitive structures, i.e., belief systems and emphasizing structure over content (Olson and Reynolds 1983). However, a better term to describe and represent consumers is the mental model, which allows for nonbelief-based representations, including attitudes, feelings, images, memories, values, etc. (Christensen and Olson 2002). This is also more in line with the current cognitive neuroscience view that sees thoughts as image-based (Damasio 1989). Research and elicitation tools have evolved to attempt to capture the additional complexity of mental models—one of which is the Zaltman metaphor elicitation technique (ZMET). The theoretical assumption underlying the ZMET is, in particular, the importance of unconscious tacit content, i.e., hidden knowledge and the importance of images in mental models. The ZMET uses pictures to help informants identify and communicate content (Zaltman 1997) and has been used to elicit the deeper emotional drivers of behavior and choice among consumers (Zaltman and Zaltman 2008). The technique is based on three stages. First, respondents are asked to think about a topic and select pictures representing their thoughts and feelings on the topic. They are then interviewed to understand the meanings they assigned to the images, and connections to superordinate ideas are established using laddering probes. Finally, the findings are generated by creating consensus maps of central constructs and broad themes of meaning (Christensen and Olson 2002). The final result is a set of themes that interviewees associate with the topic being researched. There is no attempt to generate statistically significant results; instead, the focus is on bringing hidden insights to the surface. The technique has been used in several studies, including by the authors of this study for consulting projects and in published studies to investigate the experience, preferences, and risk behavior of insurance customers (Pugnetti and Bekaert 2018; Pugnetti and Casián 2021; Pugnetti et al. 2022).

Based on the deep knowledge of the audience's mental models and risk perception, effective risk communication can target awareness and behavioral change (Slovic 1987). Risk communication models leverage this insight by expressly considering how audiences act upon the communication in five steps: (a) receiving a warning message, (b) figuring out the related content (c) accepting or believing . . . the message, (d) establishing the truth with other people, and (e) taking protective actions or measures (Heydari et al. 2021). Risk internalization and understanding are the drivers behind the judgment, decisions, and behaviors of individuals, and are based on cognitive factors such as logic, rationality, and expected benefits and losses as well as emotion (Kim and Choi 2017). Further, the emotional framing of risk messages is more memorable and more likely to trigger behavioral change (de Bruijn and Janssen 2017). Effective messaging should include instructional elements to educate the audiences about the dangers while convincing them to take preventive and protective measures to prevent a crisis from occurring or mitigate its spread (Sellnow-Richmond et al. 2018). It can be assumed that the public does not know what constitutes appropriate protective action. Therefore, instructional information messages must include self-protection measures (Mileti and Peek 2000). Otherwise, the affected public will not act in the desired way, and the potential threat will not be prevented (Coombs 2009). Hence, risk and crisis communication messages must combine and include information elements of personal relevance and provide actionable directions. People have a four-stage learning cycle, which consists of specific experiences (feelings), abstract conceptualization

(thinking), reflective observation (watching), and active experimentation (doing). When all these elements are considered, a message is understandable and perceived as relevant, which subsequently leads to desired action behavior (Kolb 1984).

The IDEA (Internalization, Distribution, Explanation, and Action) model of risk communication was developed in order to design effective risk and crisis messages based on these insights. The individual elements of the model are summarized in Table 2. The model addresses active experimentation (action) and concrete experience (internalization) elements. Contrary to other risk and crisis messages, the IDEA model focuses on learning. Messages derived from the IDEA model are constructed strategically and include affective and cognitive learning to achieve behavioral change. When all four elements are combined and included in one message, comprehension, self-efficacy, and desired behavioral intention increase and subsequently enhance the effectiveness of the communication (Sellnow and Sellnow 2013). The IDEA model has been successfully applied in a wide field of research concerning risk and crisis communication (Littlefield et al. 2014; Sellnow et al. 2015). Applications of the model on emergency situations showed that most messages extensively focused on the element of explanation and were failing to integrate the element of internalization and action to create effectiveness (Björck et al. 2022; Frisby et al. 2014). Messages without instructional elements often fail to achieve compliance because they are either ignored or sustained (Sellnow-Richmond et al. 2018).

Table 2. The IDEA model (Sellnow and Sellnow 2013).

Element and Description
Internalization focuses on the recipient itself and relates to the emotional part of risk messaging. It highlights the personal relevance, potential impact, proximity, and timeliness, leading to an increased motivation to attend to the message.
Distribution deals with the choice of adequate communication channels for the message. Depending on the crisis's dimension, multiple channels may need to be used to ensure it reaches all target audiences.
Explanation covers crisis-related information, such as the current situation and the underlying reason. The information needs to come from credible sources and must be formulated in the language of the affected audience.
Action delivers instructions on how recipients can protect themselves from the threat. These messages must be stated in a precise and understandable way so that the audience can act upon them.

We expect this to be the case also in the context of cyber risks, where internalization plays a key role, and our study aims to contribute to a better understanding of internalization and its translation into instructional messages. For a more in-depth discussion of the potential application of IDEA to cybersecurity, please revert to Björck et al. (2024). This paper develops the testing of the theoretical framework in an experimental setting.

3. Methodology and Preliminary Results

Our proposed approach encompasses four phases: Understand, Baseline, Mitigate, and Validate, as shown in Figure 1. Specific frameworks have been applied to each phase, and preliminary results are available for the first two phases of the process.

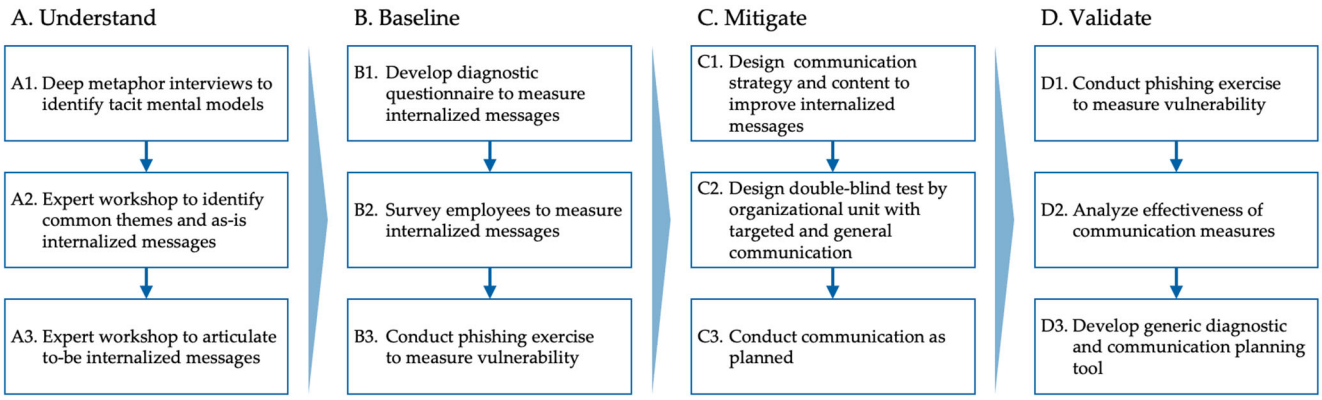

Figure 1. Development methodology.

3.1. Understand

In this phase we aim to understand the tacit mental models that employees associate with cyber risks, how these indicate current internalized messages towards cyber risks, and how these fall short of idealized to-be internalized messages.

This phase has been piloted with four SME companies that are customers of the Allianz insurance company. The results of the interviews were discussed in a series of workshops conducted by the authors to identify common themes. The to-be internalized messages resulting from these interviews are listed in Table 3 and in more detail in Table A1. The seven internalized messages have been labeled with a capital letter from A through G and will be referred to as construct A-G in the rest of the paper. These messages will be diagnosed and addressed in the phases below. For a more detailed discussion, consult Pugnetti and Casián (2021). Additional interviews have been conducted with Mobiliar employees. These results will be included in further developments of the methodology.

Table 3. Internalized to-be messages/constructs (Björck et al. 2024).

	Internalized To-Be Messages
A	My company and I have valuable information, we are targeted by hackers, and we need to protect ourselves.
B	We can make mistakes, and we need to continue our business activities with better risk awareness.
C	I have a responsibility to do something.
D	I have to protect the company with my behavior during regular business activities.
E	I can and should do something in case of a cyber-attack. I am an important part of the response and can be creative to support our customers.
F	I know how to respond in case of a cyber-attack and have trained in alternative business processes.
G	We need to learn from cyber-attacks and continue to evolve our preparedness and response.

3.2. Baseline

In this phase, we develop a diagnostic questionnaire to identify a respondent's score along each of the seven constructs. The questionnaire is used first to baseline the risk affinity of an organization or a unit within it. The actual risk behavior is observed through phishing exercises. The two dimensions of attitude towards cyber risks and risk behavior are linked in a series of analyses.

This phase has been piloted in a number of steps. First, in the course of a pre-study, we brainstormed 201 potential questions. These questions were formulated in a number of ways, both positive and negative, as well as in a personal and group-wide manner. These

questions were linked to the seven constructs using a Q-sort analysis and reducing the number to 147. A survey was conducted to determine the diagnostic validity of each of the questions for their assigned construct. A regression analysis was used to determine both impact and statistical significance, as well as a linear fit coefficient. The number of valid questions was thus reduced to 90. Table A2 in Appendix A shows the top 10 questions ranked by linear fit R^2 to the aggregate measure. The top five questions (above the dotted line) were used in a pilot diagnostic of testing partners. Respondents were asked to rank their agreement with each statement on a 7-point Likert scale ranging from complete agreement to complete disagreement. Since the questions were formulated as positive or negative statements, the results were coded to ensure that a higher number consistently mapped onto a more risk-averse behavior. Constructs were scored using the arithmetic mean for the five questions linked to each construct.

The diagnostic was piloted in two organizational units at the Mobiliar and at six SME companies. The companies signed agreements to participate in the study, including phishing exercises and surveys. The employees were bound by previous agreements with their companies as part of their employment contract concerning data disclosure. All investigations were conducted in the respective companies' environments. At Mobiliar, we tested the 24 h assistance center (Mobi24) and the General Agency in the region Spiez (GA Spiez) with a phishing exercise focusing on Black Friday offers in November 2023. A total of 186 people were part of the organizations investigated. Of these, 128 (69%) responded to the questionnaire in January 2024. Both the phishing exercise and the questionnaire were conducted through Mobiliar's internal infrastructure. The results were coded into four categories: (a) reported the phishing attack to IT cybersecurity (44%), (b) ignored the attack and undertook no action (38%), (c) clicked on the link, then recognized it as a phishing attack and reported it to IT (10%), or (d) clicked on the link (8%). The SMEs were tested in March 2024. A total of 91 people were part of the SME organizations. Of these, 37 responded to the questionnaire (41%). The phishing exercise was carried out leveraging the platform of an IT service provider (Eraneos). The questionnaire was prepared and sent by the research team to the participating companies. The responses to the phishing exercise were coded into three categories: (a) ignored the attack and undertook no action (57%), (b) opened the email (24%), or (c) clicked on the link and/or entered data (19%). The responses to the two phishing efforts have been coded somewhat differently to reflect the options available to the different respondents. Most significantly, SME participants were not able to report the phishing to an IT expert.

The responses to the diagnostic questionnaire were tested for statistically significant differences among the response categories using a one-factor ANOVA. The results of this analysis are summarized in Table 4.

The statistical significance of the results in the pilot is encouraging but not yet sufficient. Not yet sufficient, as the *p*-values are rarely below 0.1, also for aggregate constructs. Encouraging, because in spite of a very limited set of questions and a small number of respondents, some indicators show statistically significant differences in the measured attitudes towards risk, aligning with the thesis that higher values for the internalized messages indicate more risk-averse behavior. Thus, expanding the analysis to conduct a broader diagnostic with more questions and on a broader population should produce more significant results.

Another representation and analysis of the results is shown in Figure 2. The average value by construct and overall is shown for each of the six codified responses. The linear fit R^2 is also shown in each case. In most cases, there is a visible correlation between construct value and risk behavior, especially for constructs B, C, D, and G, and for ALL constructs. These results again point to the potential of the diagnostic questionnaire pending expansion and further development. This is important for our research approach. While the results in Table 4 do not show a statistically significant difference in most instances, the direction of the correlation supports the hypothesis in almost all cases. As shown in Figure 2, higher scores are linked to more risk-aware cyber behavior.

Table 4. Pilot results—ANOVA by organization.

		Construct/Question					
ID	ALL	A	911	914	891	916	908
Mobiliar *p*-value	0.58	0.81	0.91	0.90	0.25	0.27	0.94
SME *p*-value	0.05	<0.01	0.05	0.32	0.01	<0.01	0.02
ID		B	929	925	1035	933	927
Mobiliar *p*-value		0.09	0.41	0.12	0.74	0.35	0.22
SME *p*-value		0.57	0.30	0.72	0.47	0.01	0.11
ID		C	942	939	937	944	947
Mobiliar *p*-value		0.70	0.28	0.98	0.70	0.01	0.10
SME *p*-value		0.04	<0.01	0.77	0.07	0.18	0.62
ID		D	966	977	964	972	979
Mobiliar *p*-value		0.88	0.05	0.67	0.63	0.88	0.76
SME *p*-value		0.01	0.10	<0.01	0.18	0.08	0.01
ID		E	962	952	955	956	959
Mobiliar *p*-value		0.03	0.36	0.96	0.21	0.01	0.17
SME *p*-value		0.64	0.41	0.58	0.29	0.65	0.83
ID		F	985	981	989	992	991
Mobiliar *p*-value		0.58	0.89	0.89	0.47	0.37	0.17
SME *p*-value		0.46	0.73	0.85	0.93	0.63	0.17
ID		G	1009	1021	1030	1025	1013
Mobiliar *p*-value		0.67	0.97	0.83	0.57	0.68	0.20
SME *p*-value		0.61	0.12	0.23	0.89	0.84	0.99
Legend: *p*-value	≤0.10	≤0.05	≤0.01				

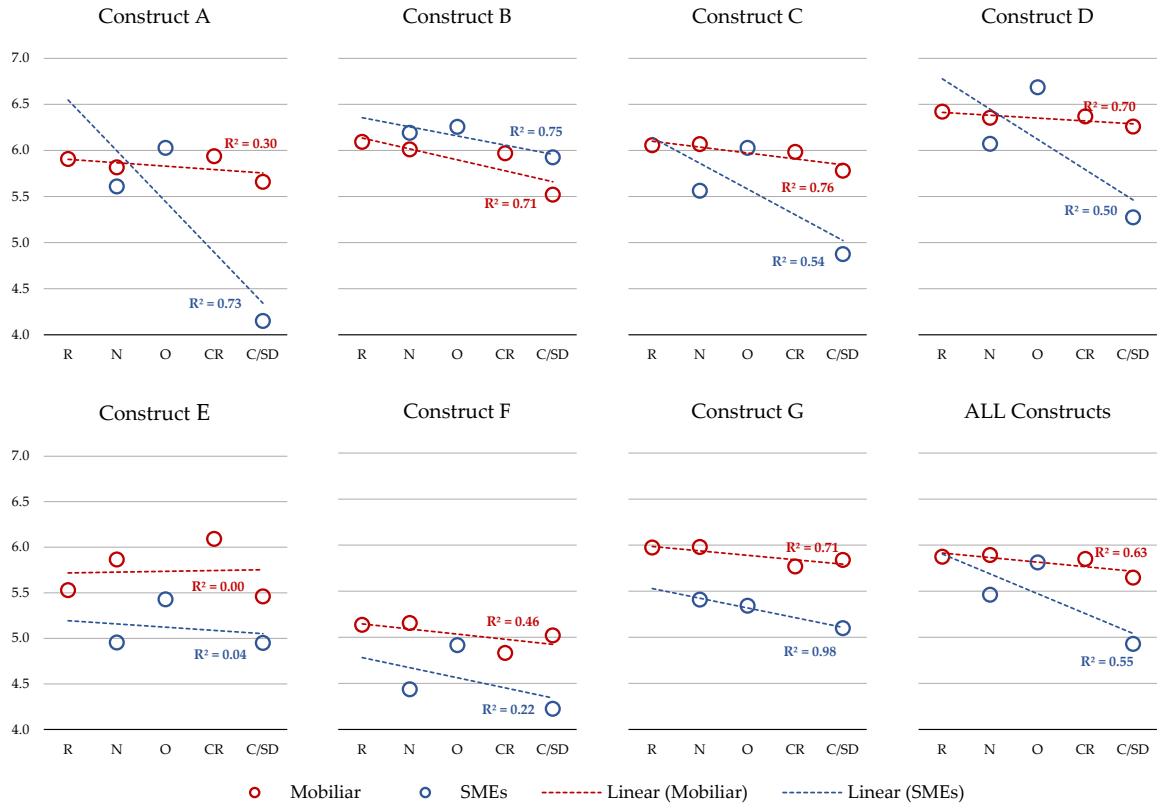

Figure 2. Values by construct and response to phishing attack (Legend: R = reported; N = no action; O = opened; CR = clicked and then reported; C/SD = clicked and/or submitted data). Constructs A-G are defined in Table 3.

The analysis was further expanded to consider each organizational unit separately, as shown in Figure 3. The relationship between diagnostic index and risk behavior is held in each of the units separately, further strengthening the indication of potential of the tool for further development.

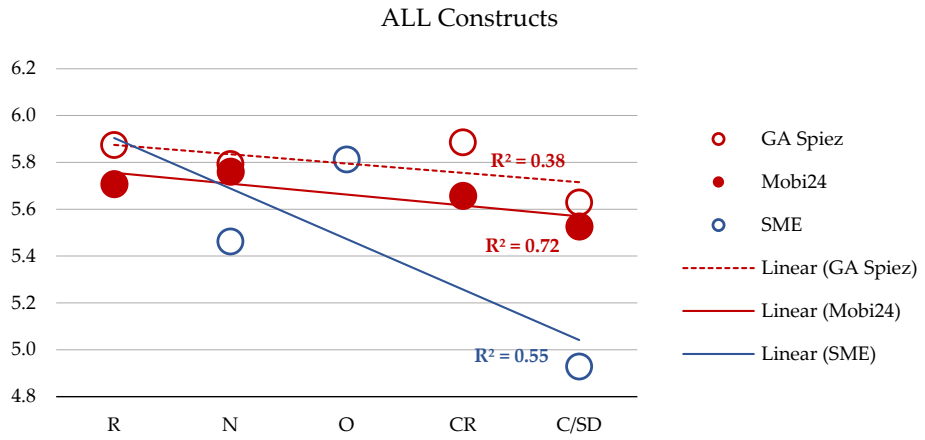

Figure 3. Analysis by organizational unit—ALL constructs.

3.3. Mitigate

In this phase, we intend to conduct a series of targeted communication efforts to mitigate the observed risk behavior. In order to understand the effectiveness of the methodology, we propose to conduct three types of interventions: (a) efforts based on the IDEA model and targeting specific constructs prioritized in the previous phase, (b) general cybersecurity communication and training per the regular company approach, and (c) no intervention. This will allow for A-B testing both of the impact on the constructs and on the risk behavior.

The IDEA model has not yet been applied in the context of cyber risk and crises. To better understand the operationalization of the four model elements, the construction of effective risk messages, the definition of risk communication strategy to influence behavior, the research team conducted a design thinking workshop with experienced academic scholars and practitioners in the field of risk communication. In a moderated sequence of three steps, five focus groups explored risk communication targeting specific employee personas. The personas have been developed based on the deep metaphor interviews. The focus group results will be used to design an experimental setting to test the messages and strategies and their impact on cyber risk internalization and behavior.

3.4. Validate

In this phase, we intend to conduct the final phishing exercises and diagnostics, following the same process as in Section 3.2. This should, on the one hand, provide a measure of the effectiveness of the communication efforts, and, on the other, establish a link between communication measures and their effectiveness on specific constructs. The best results can be collected and presented in a best-practice communication catalog for interventions. Over time and through additional projects, further examples can be developed, analyzed, and presented as suggestions for other companies.

While the first two phases have already been piloted with our partner companies, the last two phases will be tested in the near future. A broader research program to further develop the questionnaire, conduct multiple phishing exercises on a broader population, and develop a larger catalog of intervention measures is being submitted for research funding from the Swiss Innovation Agency.

4. Discussion and Next Steps

The rate of cyber-attacks and the damage they cause has been steadily increasing, and the majority are preceded by a breach of the security infrastructure due to employee behavior, typically revealing information through a phishing attack. Several approaches to estimate the risk of employee behavior have been developed, and several training programs to address this behavior have been introduced. The results, however, have not been as successful as had been hoped. Especially, normative training models have been shown to not impact behavior, and researchers have identified underlying attitudes as a potentially interesting target for training in a cybersecurity setting.

We are proposing an interdisciplinary diagnostic and intervention approach based on identifying and influencing these underlying attitudes. The former through deep metaphor interviews, and the second through the IDEA risk communication model. Both methods have been successfully deployed in other circumstances and have been shown to be useful in understanding customers' underlying motivation (Zaltman and Zaltman 2008) and influencing risk behavior (Sellnow et al. 2019). Further, we propose a four-step development methodology that can be used to develop the content for a self-service or self-led tool and implemented iteratively to refine and further enrich the tool for different audiences, settings, and timeframes.

This paper summarizes the status of the research efforts that have taken place over the last several years, first with the publication of a study on employee attitudes in Switzerland (Pugnetti and Casián 2021) using deep metaphors, followed by a paper linking cyber attitudes and the IDEA model (Björck et al. 2024). In parallel, a first diagnostic questionnaire was developed and in the current phase of this research effort, we are piloting a shortened version of the diagnostic questionnaire composed of the top five questions for each of the seven risk attitude constructs identified and linking the results to observed rather than theorized risk behavior. There are several insights relating to both the process and results from this piloting work.

First, the deep metaphor interview process can produce to-be internalized messages. In this research, we develop seven to-be internalized messages. The current set of messages, however, is potentially overlapping in the minds of survey respondents. Future analysis should investigate the reduction in constructs to generate a streamlined and understandable set of diagnostic dimensions. Further, we have noticed in the second set of interviews how the setting of the interviews (for the second set, on-site at the company) potentially influences the mental framing and therefore the content of the interviews. We recommend that future planning of the setting should include this factor and its impact should be better analyzed.

Second, the preliminary set of questions developed can quantify the dimensions investigated, in general showing both internal consistency within the construct and independence from other constructs. In this research, we developed a preliminary set of 70 questions. Further development, however, is necessary to (a) develop a much larger set of questions to investigate, (b) potentially reduce the dimensions to ensure orthogonality on a much larger set of respondents, and (c) determine which combination of questions can best be combined to provide a diagnostic metric linked to risk behavior. This work will necessarily be part of the next project phases.

Third, phishing exercises provide a credible, reality-based indicator for risk behavior. This is a valuable addition to the current published methodology. In the course of the pilot, we identified the following two issues that should be addressed in future work to improve the process: (a) The rate of response depends significantly on the quality of the phishing attack. This may be due to both the credibility of the phishing email and the timeliness of the topic used. This was observed in both organizational settings, and phishing emails with very low responses produce less useful analytical results, implying that several attacks on several platforms will be necessary to derive accurate and informative results to develop the tool. (b) The administrative work necessary to coordinate phishing attacks on SMEs places a significant workload on the project team. Both the need to inform a distributed

set of responsible people and managing access to the network requires significantly more effort than working with a large organization with internally managed IT security and communication infrastructure. This may influence future work towards a smaller number of larger research partners.

Fourth, there is a logical and data-driven link between the diagnostic and risk behavior. In this study, we show statistically significant links for five out of seven constructs and for thirteen of the individual questions, with the clearest link shown for the importance of the information available to the users and the commitment needed to safeguard the company. However, the link is not yet sufficiently strong to warrant a broad implementation at this stage. Further work is necessary with larger diagnostic questionnaires and more penetration tests as described above to improve the validity of the results. Especially important will be a much broader data set in multiple settings and a more developed analysis to identify the appropriate combination of questions for diagnostic purposes.

An important component of the methodology has not yet been developed and tested. This will be the focus of the next phase. Based on the existing partnership, we are planning to test several communication measures, both driven by the diagnostic and according to the IDEA model, and placebo interventions. The purpose of this work is to pilot the last two phases of the methodology proposed in Figure 1. In addition, the results of the pilot indicate the need to expand the work, potentially with additional sources of funding and including an understanding of the attitude towards cyber risks in the broader population as a baseline rather than in specific companies.

This work expands the current research approach by including the use of established market research and risk communication tools in the cyber risk literature and proposing an iterative diagnostic and mitigation model to address the weaknesses of current approaches. The first weakness addressed is the lack of systemic success linked to the introduction of current training and mitigation approaches. The second is the reluctance to include observed risk behavior in the development and testing of mitigation approaches. Self-reported and proxy indicators may not be as reliable. Addressing these weaknesses, however, requires a well-structured project with multiple data collection, analytical, and intervention activities to generate usable insights and self-service tools to improve cybersecurity.

Author Contributions: Conceptualization, C.P. and A.B.; methodology, C.P., A.B. and C.C.; analysis, C.P.; investigation, C.P., A.B., C.C. and R.S.; writing—original draft preparation, C.P.; writing—review and editing, A.B. and R.S.; funding acquisition, C.P., C.C. and R.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded in part by Schweizer Mobiliar Versicherungsgesellchaft AG and Allianz Suisse Versicherungsgesellschaft AG.

Data Availability Statement: Data are available from the corresponding author upon request.

Acknowledgments: We would like to extend our gratitude to Ulrich Moser, Philipp Schirmer, Adrian Anderegg, Christoph Svoboda, Michael Adamer, Cornelia Ginggen, Mario Guarino, Doreen Pietsch, Gregor Huber, Urs Schell, Giota Kokalis, and Pascal Grand-Guillaume-Perrenoud for their support and contribution to this research effort.

Conflicts of Interest: The authors declare no conflicts of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript; or in the decision to publish the results.

Appendix A

Table A1. Internalized to-be messages (constructs A–G) (Björck et al. 2024).

	Internalized to-Be Messages	Description
A	My company and I have valuable information, we are targeted by hackers, and we need to protect ourselves.	Even though we think we may be small, our company has valuable information on customers, technology, markets, and bank accounts, and this information is valuable. I, as an employee, have access to this important information. Both I and the company can be targeted, and we need to be alert at all times and protect ourselves.
B	We can make mistakes, and we need to continue our business activities with better risk awareness.	My coworkers and I can make mistakes if/when we are not paying attention. We need to therefore pay attention. On the other hand, it is not possible to not make any mistakes at all while conducting business, so we need to learn to recognize them, communicate openly when they occur, develop ways to cope with them, and continue to try to minimize them.
C	I have a responsibility to do something.	Defending my company's valuable information is not somebody else's job. It is also my job. Other people also carry a responsibility (the CEO, management, the IT department, IT consultants, all employees), but I carry my fair share of this responsibility. I therefore have to pay attention, communicate openly, and take corrective action as needed.
D	I have to protect the company with my behavior during regular business activities.	My behavior while conducting normal business transactions (email with clients and partners, entering the facilities, etc.) can create vulnerabilities for hackers to exploit. I therefore have to remain vigilant not just at special times but throughout my activities.
E	I can and should do something in case of a cyber-attack. I am an important part of the response and can be creative to support our customers.	The response in case of a cyber-attack is the responsibility of all employees, not just of a few IT specialists and management. It is my responsibility to ensure the impact on our customers and partners is kept to a minimum. This can only be carried out by the people who have interacted with our external partners before and understand their needs. Sometimes it may require being creative and flexible regarding the best solution, rather than waiting for the situation to normalize or just following orders.
F	I know how to respond in case of a cyber-attack and have trained in alternative business processes.	Responding to an attack in progress can be somewhat chaotic and proper responses need to be prepared and trained prior to an event in order to be effective. In the case of cyber, they may involve alternative processes less reliant on company technology—for example personal mobile phones, pens, and paper. It is important to train these processes and understand how to carry them out under the proper conditions—much in the same way that a ship's crew conducts firefighting drills.
G	We need to learn from cyber-attacks and continue to evolve our preparedness and response.	Each attack, both the successful and unsuccessful, provides important information about vulnerabilities and capabilities to respond. It is important to understand what these breaches or near misses signal and how to integrate this knowledge into our training and responses. This information needs to therefore be shared with and understood by employees.

Table A2. Internalized to-be messages and ranked preliminary diagnostic questions (Björck et al. 2024).

ID	Internalized to-Be Messages	ID	Question	R^2
A	My company and I have valuable information, we are targeted by hackers, and we need to protect ourselves.	911	My company is not a target for hackers.	0.98
		914	My company fits the target profile of hackers.	0.92
		891	Our company data are only valuable to us	0.70
		916	My company is not threatened by hackers.	0.70
		898	I can be targeted by hackers because of my access.	0.68
		908	I am a potential target for hackers.	0.68
		901	Hackers are interested in our company.	0.67
		917	My company's data are worth being protected.	0.60
		906	My company has been attacked by hackers.	0.59
		907	We are targeted by hackers.	0.55
B	We can make mistakes, and we need to continue our business activities with better risk awareness.	929	I may make mistakes that expose the company to cyber-attacks.	0.72
		925	Making mistakes regarding cybersecurity is nothing to be ashamed of.	0.65
		1035	To defend the company against hackers means to communicate openly about mistakes.	0.65
		933	We need to recognize cybersecurity mistakes fast.	0.60
		927	We need to communicate openly when we notice mistakes regarding cybersecurity.	0.58
		934	I have made mistakes regarding cybersecurity, but I have learned from them.	0.53
		936	I have made cybersecurity mistakes in the past.	0.49
		1034	I have to pay attention to my behavior and take corrective actions if needed to ensure the safety of the company's data.	0.48
		935	We should share our cybersecurity mistakes to learn and minimize future risks.	0.47
		930	Mistakes at work can expose the company to cyber-attacks.	0.45
C	I have a responsibility to do something.	942	Our IT department alone is responsible for cybersecurity.	0.75
		939	Defending the company's valuable information is everyone's job, independent of their position and function.	0.55
		937	Paying attention to cybersecurity is not part of my job.	0.54
		944	I can and should motivate my colleagues to help me defend company data.	0.53
		947	I am an essential part of the defense against cyber-attacks.	0.53
		1038	The company's cybersecurity depends on my behavior.	0.52
		1036	I have to be careful with our company data and information.	0.51
		1044	I handle company data and information vigilantly.	0.51
		946	I do not have any responsibility for the safeguarding of company data.	0.50
		1045	I have to be careful with company data and information.	0.48
D	I have to protect the company with my behavior during regular business activities.	966	Only at special times do I need to be aware of cyber risks when conducting business activities.	0.83
		977	My behavior during regular business activities influences the cybersecurity of the company.	0.83
		964	I need to be cybersecurity-aware throughout the day, not only during extraordinary times.	0.78
		972	My behavior while working can protect the company from hacker attacks.	0.78
		979	My behavior has an impact on our cybersecurity.	0.76
		976	Being constantly attentive to cyber risks when conducting business is not necessary.	0.72
		973	My behavior can create vulnerabilities that hackers can exploit.	0.71
		970	My behavior during everyday business activities does not affect the safety of company data.	0.68
		967	I should always keep careful watch throughout my business activities to protect the company from cyber-attacks.	0.62
		978	I should be attentive when sending emails and even when entering the company facilities.	0.62

Table A2. *Cont.*

ID	Internalized to-Be Messages	ID	Question	R^2
E	I can and should do something in case of a cyber-attack. I am an important part of the response and can be creative to support our customers.	962	I should do something in case of a cyber-attack because I am an important part of the response to it.	0.79
		952	I should do something in case of a cyber-attack.	0.73
		955	I am part of the response in case of a cyber-attack.	0.61
		956	My creativity can be an important part of the response to cyber-attacks.	0.59
		959	Not only can I, but I also should do something in case of a cyber-attack.	0.56
		1048	I want to provide information and inputs on my business processes and alternatives in case of a cyber-attack.	0.56
		948	I am an important part of the response against cyber-attacks.	0.55
		957	There is not much I can do once a cyber-attack on our company is successful.	0.55
		951	I am not an essential part of the response to a cyber-attack as there is nothing I can do.	0.54
		950	To minimize the impact of a cyber-attack, I should know my business partners and their needs.	0.53
F	I know how to respond in case of a cyber-attack and have trained in alternative business processes.	985	I have alternative processes in place in case of a cyber-attack.	0.81
		981	I feel well prepared for a cyber-attack.	0.75
		989	The processes to follow in case of a cyber-attack are well known.	0.70
		992	The company has guidelines in place in case of a cyber-attack.	0.66
		982	I know how to deal with a cyber-attack.	0.65
		991	I do not know how to react in case of a cyber-attack.	0.65
		988	I have trained in cyber responses in the last 12 months.	0.64
		997	I have trained in alternative business processes I can use in case of a cyber-attack.	0.62
		1004	We received training on how to respond in case of a cyber-attack.	0.62
		986	Our company informed us about how to react to cyber-attacks.	0.61
G	We need to learn from cyber-attacks and continue to evolve our preparedness and response.	1009	Cyber-attacks are a recurring topic in our company.	0.82
		1021	Learning from past cyber-attacks is part of our cybersecurity strategy.	0.77
		1030	We have learned from past cyber-attacks.	0.74
		1025	It is essential to learn from past cyber-attacks to be better prepared for the future.	0.66
		1013	We are informed about the latest developments in cybersecurity.	0.65
		1018	We have updated our response to cyber-attacks in the last 12 months.	0.62
		1006	We have regular company updates on cyber-attacks and cybersecurity.	0.59
		1023	We discuss cyber-attacks in our company.	0.59
		1026	I am more aware when I receive information on cyber risk/-attacks on a regular basis.	0.58
		1011	Learning from past or failed cyber-attacks helps to increase our preparedness and response.	0.54

References

Antunes, Mário, Carina Silva, and Frederico Marques. 2021a. An Integrated Cybernetic Awareness Strategy to Assess Cybersecurity Attitudes and Behaviours in School Context. *Applied Sciences* 11: 11269. [CrossRef]

Antunes, Mário, Marisa Maximiano, Ricardo Gomes, and Daniel Pinto. 2021b. Information Security and Cybersecurity Management: A Case Study with SMEs in Portugal. *Journal of Cybersecurity and Privacy* 1: 219–38. [CrossRef]

Biener, Christian, Martin Eling, and Jan Hendrik Wirfs. 2015. Insurability of cyber risk: An empirical analysis. *The Geneva Papers on Risk and Insurance—Issues and Practice* 40: 131–58. [CrossRef]

Björck, Albena, Audra Diers-Lawson, and Felix Dücrey. 2022. Evolution and effectiveness of the governmental risk and crisis communication on Twitter in the COVID-19 pandemic: The Case of Switzerland. *Proceedings of the International Crisis and Risk Communication Conference* 5: 27–30. [CrossRef]

Björck, Albena, Carlo Pugnetti, and Carlos Casián. 2024. Communicating to Mitigate Behavioral Cyber Risks: The Case of Employee Vulnerability. In *Handbook of Communicating Safety and Risk*. Edited by Timothy L. Sellnow and Deanna D. Sellnow. Berlin and Boston: De Gruyter Mouton, pp. 585–606. [CrossRef]

Blais, Ann-Renée, and Elke U. Weber. 2006. A domain-specific risk-taking (DOSPERT) scale for adult populations. *Judgment and Decision Making* 1: 33–47. [CrossRef]

Borkovich, Debra J., and Robert J. Skovira. 2020. Working from Home: Cybersecurity in the Age of COVID-19. *Issues in Information Systems* 21: 234–46. [CrossRef]

Brewer, Noel T., Neil D. Weinstein, Cara L. Cuite, and James E. Herrington. 2004. Risk perceptions and their relation to risk behavior. *Annals of Behavioral Medicine* 27: 125–30. [CrossRef]
Christensen, Glenn L., and Jerry C. Olson. 2002. Mapping Consumers' Mental Models with ZMET. *Psychology and Marketing* 19: 477–502. [CrossRef]
Coombs, W. Timothy. 2009. Crisis, Crisis Communication, Reputation, and Rhetoric. In *Rhetorical and Critical Approaches to Public Relations II*. New York: Routledge, pp. 249–64.
Coombs, W. Timothy, and Sherry J. Holladay, eds. 2010. Handbook of Crisis Communication. Malden, MA: Wiley-Blackwell, pp. xxvi–xxvii. [CrossRef]
Coutlee, Christopher G., Cary S. Politzer, Rick H. Hoyle, and Scott A. Huettel. 2014. An Abbreviated Impulsiveness Scale Constructed Through Confirmatory Factor Analysis of the Barratt Impulsiveness Scale Version 11. *Archives of Scientific Psychology* 2: 1–12. [CrossRef]
CybSafe. 2020. Human Error to Blame for 9 in 10 UK Cyber Data Breaches in 2019. Available online: https://www.cybsafe.com/press-releases/human-error-to-blame-for-9-in-10-uk-cyber-data-breaches-in-2019/ (accessed on 9 January 2022).
Damasio, Antonio R. 1989. Time-locked multiregional retroactivation: A systems-level proposal for the neural substrates of recall and recognition. *Cognition* 33: 25–62. [CrossRef] [PubMed]
Davis, Richard A., Gordon L. Flett, and Avi Besser. 2002. Validation of a New Scale for Measuring Problematic Internet Use: Implications for Pre-employment Screening. *Cyberpsychology & Behavior* 5: 331–45. [CrossRef]
de Bruijn, Hans, and Marjin Janssen. 2017. Building cybersecurity awareness: The need for evidence-based framing strategies. *Government Information Quarterly* 34: 1–7. [CrossRef]
Egelman, Serge, and Eyal Peer. 2015. Scaling the security wall: Developing a Security Behavior Intentions Scale (SeBIS). Paper presented at CHI'15: Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems, Seoul, Republic of Korea, April 18–23, pp. 2873–82. [CrossRef]
European Union Agency for Network and Information Security ENISA. 2016. *Review of Cyber Hygiene Practices (December 2016)*. Available online: https://www.enisa.europa.eu/publications/cyber-hygiene/at_download/fullReport (accessed on 6 April 2024).
Federal Bureau of Investigation. 2022. Internet Crime Report 2021. Available online: https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf (accessed on 6 April 2024).
Frandsen, Finn, and Winni Johansen. 2011. The study of internal crisis communication: Towards an integrative framework. *Corporate Communications: An International Journal* 16: 247–365. [CrossRef]
Frisby, Brandi N., Shari R. Veil, and Timothy L. Sellnow. 2014. Instructional Messages During Health-Related Crises: Essential Content for Self-Protection. *Health Communication* 29: 347–54. [CrossRef]
Greitzer, Frank L., Justin Purl, D. E. Sunny Becker, Paul J. Sticha, and Yung Mei Leong. 2019. Modeling expert judgments of insider threat using ontology structure: Effects of individual indicator threat value and class membership. Paper presented at 52nd Hawaii International Conference on Systems, Grand Wailea, HI, USA, January 8–11, pp. 3202–11. Available online: https://hdl.handle.net/10125/59756 (accessed on 6 April 2024).
Hadlington, Lee. 2017. Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity and risky cybersecurity behaviours. *Heliyon* 3: e00346. [CrossRef] [PubMed]
Hadlington, Lee. 2018. Employees Attitude towards Cyber Security and Risky Online Behaviours: An Empirical Assessment in the United Kingdom. *International Journal of Cyber Criminology* 12: 269–81. [CrossRef]
Heydari, Seyed Taghi, Lella Zarei, Ahmad Kalateh Sadati, Najmeh Moradi, Maryam Akbari, Gholamhossin Mehraliary, and Kamran Bagheri Lankarani. 2021. The effect of risk communication on preventive and protective behaviours during the COVID-I9 outbreak: Mediating role of risk perception. *BMC Public Health* 21: 54. [CrossRef] [PubMed]
Higgins, E. Tory. 1998. Promotion and prevention: Regulatory focus as a motivational principle. In *Advances in Experimental Social Psychology*. Amsterdam: Elsevier, vol. 30, pp. 1–46, ISBN 067-2601/98.
IBM Security. 2022. Cost of a Data Breach Report 2022. Available online: https://www.ibm.com/reports/data-breach (accessed on 6 April 2024).
Kennison, Sheila K., and Eric Chan-Tin. 2020. Taking Risks with Cybersecurity: Using Knowledge and Personal Characteristics to Predict self-Reported Cybersecurity Behaviors. *Frontiers in Psychology* 11: 546546. [CrossRef]
Kim, Jeong-Nam, and Yunna Rhee. 2011. Strategic Thinking about Employee Communication Behavior (ECB) in Public Relations: Testing the Models of Megaphoning and Scouting Effects in Korea. *Journal of Public Relations Research* 23: 243–68. [CrossRef]
Kim, Mikyoung, and Yoonhyeung Choi. 2017. Risk communication: The roles of message appeal and coping style. *Social Behavior and Personality* 45: 773–84. [CrossRef]
Kim, Young. 2018. Enhancing employee communication behaviors for sensemaking and sensegiving in crisis situations: Strategic management approach for effective internal crisis communication. *Journal of Communication Management* 22: 451–75. [CrossRef]
Kolb, David A. 1984. *Experiential Learning: Experience as the Source of Learning and Development*. Englewood Cliffs: Prentice-Hall. ISBN 0132952610.
Littlefield, Robert S., Kimberly Beauchamp, Derek Lane, Deanna D. Sellnow, Timothy L. Sellnow, Steven Venette, and Bethany Wilson. 2014. Instructional Crisis Communication: Connecting Ethnicity and Sex in the Assessment of Receiver-Oriented Message Effectiveness. *Journal of Management and Strategy* 5: 6–23. [CrossRef]

Li, Yuchong, and Qinghui Liu. 2021. A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports* 7: 8176–86. [CrossRef]
Lorenz, Birgy, Kaido Kikkas, and Aare Klooster. 2013. The four most-used passwords are love, sex, secret, and god: Password security and training in different user groups. In *Human Aspects of Information Security, Privacy, and Trust: First International Conference, HAS 2013, Held as Part of HCI International 2013, Las Vegas, NV, USA, July 21-26, 2013. Proceedings 1*. Berlin and Heidelberg: Springer, pp. 276–83.
Mazzei, Alessandra, and Silvia Ravazzani. 2011. Manager-employee communication during a crisis: The missing link. *Corporate Communications: An International Journal* 16: 243–54. [CrossRef]
Meertens, Ree M., and René Lion. 2008. Measuring an Individual's tendency to Take Risks: The Risk Propensity Scale. *Journal of Applied Social Psychology* 38: 1506–20. [CrossRef]
Mileti, Dennis S., and Lori Peek. 2000. The social psychology of public response to warnings of a nuclear power plant accident. *Journal of Hazardous Materials* 75: 181–94. [CrossRef]
Morgan, Steve. 2020. *Cybercrime to Cost the World $10.5 Trillion Annually By 2025*. Northport: Cybercrime Magazine. Available online: https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/ (accessed on 9 January 2022).
Ng, Boon-Yuen, Atreyi Kankanhalli, and Yunjie C. Xu. 2009. Studying users' computer security behavior: A health belief perspective. *Decision Support Systems* 46: 815–25. [CrossRef]
Novak, Julie M., and Timothy L. Sellnow. 2009. Reducing Organizational Risk through Participatory Communication. *Journal of Applied Communication Research* 37: 349–73. [CrossRef]
Olson, Jerry C., and Thomas J. Reynolds, eds. 1983. Understanding consumers' cognitive structures: Implications for advertising strategy. In *Advertising and Consumer Psychology*. Lexington: Lexington Books, pp. 77–90.
Parsons, Kathryn, Agata McCormac, Marcus Butavicius, Malcolm Pattinson, and Cate Jerram. 2014. Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers & Security* 42: 165–76. [CrossRef]
Proofpoint. 2023. State of the Phish 2023. Available online: https://www.proofpoint.com/us/resources/threat-reports/state-of-phish (accessed on 6 April 2024).
Prümmer, Julia, Tommy van Stehen, and Bibi van den Berg. 2024. A systematic review of current cybersecurity training methods. *Computers & Security* 136: 103585. [CrossRef]
Pugnetti, Carlo, and Carlos Casián. 2021. *Cyber Risks and Swiss SMEs: An Investigation of Employees' Attitudes and Behavioral Vulnerabilities*. Winterthur: ZHAW School of Management and Law. [CrossRef]
Pugnetti, Carlo, and Xavier Bekaert. 2018. *A Tale of Self-Doubt and Distrust. Onboarding Millennials: Understanding the Experience of New Insurance Customers*. Winterthur: ZHAW School of Management and Law. ISBN 978-3-03870-021-0.
Pugnetti, Carlo, Pedro Henriques, and Ulrich Moser. 2022. Goal Setting, Personality Traits, and the role of Insurers and Other Service Providers for Swiss Millennials and Generation Z. *Journal of Risk and Financial Management* 15: 185. [CrossRef]
Rosenstock, Irwin M. 1974. The Health Belief Model and Preventive Health Behavior. *Health Education Monographs* 2: 354–86. [CrossRef]
Saucier, Gerard. 1994. Mini-Markers: A brief version of Goldberg's unipolar Big-Five markers. *Journal of Personality Assessment* 63: 506–16. [CrossRef] [PubMed]
Schoenherr, Jordan Richard, and Robert Thomson. 2020. Insider Threat Detection: A Solution in Search of a Problem. Paper presented at IEEE 2020 International Conference on Cyber Security and Protection of Digital Services (Cyber Security), Dublin, June 15–19.
Schoenherr, Jordan Richard, and Robert Thomson. 2021. The Cybersecurity (CSEC) Questionnaire: Individual Differences in Unintentional Insider Threat Behaviours. Paper presented at IEEE 2021 International Conference on Cyber Security Awareness, Data Analytics and Assessment (CyberSA), Dublin, June 14–18. [CrossRef]
Sebescen, Nina, and Jessica Vitak. 2017. Securing the Human: Employee Security Vulnerability Risk in Organizational Settings. *Journal of the Association for Information Science and Technology* 68: 2237–47. [CrossRef]
Seeger, Matthew W. 2006. Best Practices in Crisis Communication: An Expert Panel Process. *Journal of Applied Communication Research* 34: 232–44. [CrossRef]
Sellnow, Deanna D., Bengt Johansson, Timothy L. Sellnow, and Derek R. Lane. 2019. Toward a global understanding of the effects of the IDEA model for designing instructional risk and crisis messages: A food contamination experiment in Sweden. *Journal of Contingencies and Crisis Management* 27: 102–15. [CrossRef]
Sellnow, Deanna D., Derek Lane, Robert S. Littlefield, Timothy L. Sellnow, Bethany Wilson, Kimberly Beauchamp, and Steven Venette. 2015. A Receiver-Based Approach to Effective Instructional Crisis Communication: Instructional Crisis Communication. *Journal of Contingencies and Crisis Management* 25: 149–58. [CrossRef]
Sellnow-Richmond, Deborah, Amiso George, and Deanna D. Sellnow. 2018. An IDEA model analysis of instructional risk communication in the time of Ebola. *Journal of International Crisis and Risk Communication Research* 1: 135–66. [CrossRef]
Sellnow, Timothy L., and Deanna D. Sellnow. 2013. The role of instructional risk messages in communicating about food safety. Food Insight: Current Topics in Food Safety and Nutrition 3. Available online: https://www.academia.edu/9111360/The_Role_of_Instructional_Risk_Messages_in_Communicating_about_Food_Safety_The_IDEA_Model (accessed on 6 April 2024).
Sitkin, Sim B., and Amy L. Pablo. 1992. Reconceptualizing the Determinants of Risk Behavior. *Academy of Management Review* 17: 9–38. [CrossRef]
Slovic, Paul. 1987. Perception of Risk. *Science* 236: 280–85. [CrossRef]

Stanton, Jeffrey M., Kathryn R. Stam, Paul Mastrangelo, and Jeffrey Jolton. 2005. Analysis of end user security behaviors. *Computers & Security* 24: 124–33. [CrossRef]
Van Schaik, Paul, Debora Jeske, Joseph Onibokun, Lynne Coventry, Jurjen Jansen, and Petko Kusev. 2017. Risk perceptions of cyber-security and precautionary behaviour. *Computers in Human Behavior* 75: 547–59. [CrossRef]
Vishwanath, Arun, Loo Seng Neo, Pamela Goh, Seyoung Lee, Majeed Khader, Gabriel Ong, and Jeffery Chin. 2020. Cyber hygiene: The concept, its measure, and its initial tests. *Decision Support Systems* 128: 113160. [CrossRef]
Weber, Elke U., Ann-Renée Blais, and Nancy E. Betz. 2002. A domain-specific risk-attitude scale: Measuring risk perceptions and risk behaviors. *Journal of Behavioral Decision Making* 15: 263–90. [CrossRef]
West, Ryan. 2008. The psychology of security. *Communications of the ACM* 51: 34–40. [CrossRef]
West, Ryan, Christopher Mayhorn, Jefferson Hardee, and Jeremy Mendel. 2009. The Weakest Link: A Psychological Perspective on Why Users Make Poor Security Decisions. In *Social and Human Elements of Information Security: Emerging Trends and Countermeasures*. Hershey: IGI Global, pp. 43–60.
Whitty, Monica, James Doodson, Sadie Creese, and Duncan Hodges. 2015. Individual differences in cyber security behaviors: An examination of who is sharing passwords. *Cyberpsychology, Behavior, and Social Networking* 18: 3–7. [CrossRef]
World Economic Forum. 2022. *Global Cybersecurity Outlook 2022*. Geneva: Insight Report.
Xu, Wei, Finbarr Murphy, Xian Xu, and Wenpeng Xing. 2021. Dynamic communication and perception of cyber risk: Evidence from big data in media. *Computers in Human Behavior* 122: 106851. [CrossRef]
Zaltman, Gerald. 1997. Rethinking Marketing Research: Putting People Back In. *Journal of Marketing Research* 34: 424–37. [CrossRef]
Zaltman, Gerald, and Lindsey H. Zaltman. 2008. *Marketing Metaphoria: What Deep Metaphors Reveal about the Minds of Consumers*. Boston: Harvard Business Press.
Zhang, Don C., Scott Highhouse, and Christopher D. Nye. 2018. Development and validation of the General Risk propensity Scale (GRiPS). *Behavioral Decision Making* 32: 152–67. [CrossRef]
Zhang, Xiaochen Angela, and Jonathan Borden. 2020. How to communicate cyber-risk? An examination of behavioral recommendations in cybersecurity crises. *Journal of Risk Research* 23: 1336–52. [CrossRef]
Zuckerman, Marvin, Sybil B. Eysenck, and Hans J. Eysenck. 1978. Sensation seeking in England and America: Cross-cultural, age and sex comparisons. *Journal of Consulting and Clinical Psychology* 46: 139. [CrossRef] [PubMed]