WIK

Working Paper

No. 8

The effect of implicit beliefs on cybersecurity

Dr Marie-Christin Papen

Pirmin Puhl

Katrin Bürger

Bad Honnef, December 2024

WIK
Wissenschaftliches Institut
für Infrastruktur und
Kommunikationsdienste

IMPRINT

WIK WORKING PAPERS

The working papers published in the series constitute work in progress circulated to stimulate discussion and critical comments. Views expressed represent exclusively the authors' own opinions and do not necessarily reflect those of the editor.

WIK Wissenschaftliches Institut für
Infrastruktur und Kommunikationsdienste GmbH
Rhöndorfer Str. 68
53604 Bad Honnef, Germany
E-Mail: info@wik.org
www.wik.org

Person authorised to sign on behalf of the organisation

General Manager Director, Head of Administration, Head of Department	Dr Cara Schwarz-Schilling Alex Kalevi Dieke
Director, Head of Department	Prof Dr Bernd Sörries
Head of Department	Dr Christian Wernick
Head of Department	Dr Lukas Wiewiorra
Chairperson of the Supervisory Board	Dr Thomas Solbach
Registered at	Amtsgericht Siegburg, HRB 7225
Tax No.	222/5751/0722
VAT-ID	DE 123 383 795

Date: December 2024

Contents

1 Summary

The study examines the influence of implicit beliefs on cybersecurity behaviour among employees in German organizations. We address a significant gap in the existing literature related to companies‘ struggle to implement effective cybersecurity defence strategies. Despite recognizing cybercrime as a significant threat, many organizations, particularly small and medium-sized enterprises (SMEs), fail to implement adequate protective measures. Additionally, we also address a significant gap in understanding how unconscious attitudes may influence the attitude of employees towards cybersecurity.

As analytical method to gain insights in the response behaviour of employees, we use the Single Category Implicit Association Test (SC-IAT) and a questionnaire. On the basis of the Fogg Behavior Model (FBM), we investigate the behaviour of the employees and the effects of their unconscious attitudes.

Our key findings reveal that employees' implicit attitudes significantly diverge from their explicit statements about cybersecurity. With our results we demonstrate that implicit beliefs may cause a critical vulnerability in cybersecurity when it is not detected or neglected. Our research contributes to understanding the psychological mechanisms underlying cybersecurity behaviour.

2 Introduction

The German Federal Office for Information Security (BSI) stated in its annual report in 2023, that the threat in cyberspace reached an all-time high. The number of attacks is constantly increasing. Criminals no longer necessarily need to develop their own tools and attacking strategies. They can purchase cybercrime tools on the shadow market or become stakeholders in a 'cybercrime value chain'.[1] Studies estimate significant financial losses for the German economy due to cybercrime. In 2024 a potential loss of over 266 billion euros from direct and indirect cybercrime damages is to be deplored.[2]

However, the actual number of attacks remains unclear. This is likely due to a high number of unreported cases and also due to the fact that companies are often reluctant to report an attack. According to surveys, between 11% and 80% of the German companies report that they have been (likely) affected by at least one cybersecurity incident within the last twelve months.[3] In addition, companies also indicated that they anticipate a further rise in cyber-attacks over the next twelve months.[4]

In this context, the role of the 'human factor', which has been often neglected in the past, is receiving greater attention in scientific discourse.[5] This is due to the fact that numerous studies claim people to be the soft spot in the cybersecurity defence line.[6] Recent surveys appear to corroborate this. Although the surveys report different orders, the most frequently reported forms of attacks by companies are human-centric attacks, such as social engineering, (spear) phishing, and attacks on (weak) passwords.[7]

The growing danger is prompting more and more companies to take action. Consequently, there has been a notable increase in investment in cybersecurity by German companies.[8] Many companies invest in so called 'Security Education, Training, and Awareness' (SETA) programs for their employees – although, this remains often contingent upon the employee's position and seniority within the company.[9] Nevertheless, there is considerable debate regarding the extent to which activities such as awareness campaigns, security training, and security warnings are effective in addressing the challenge of reducing incidents of cybercrime, at all.[10] For example, studies show that users still ignore security policies when they do not understand them or are not motivated to follow them.[11] Also, the SETA programs might be not effective, because these programs are too generic and often don't change the employees' behaviour.[12] Additionally, 'security fatigue', a term which describes a situation in which people can tire of dealing with security measures, might emerge.[13] Other authors argue, that users are lazy, some argue that security tasks need to be made more usable, and some argue that the users are being

---

1 Bundesamt für Sicherheit in der Informationstechnik [BSI] (2023)
2 Bitkom (2024)
3 TÜV Verband (2023); Bitkom (2023a); Hiscox (2023)
4 Bitkom (2024)
5 Jeong et al. (2019); Rahman et al (2021)
6 European Network and Information Security Agency [ENISA] (2018); Alsharida et al (2023); Scholl and Schuktomow (2021)
7 TÜV Verband (2023); Bitkom (2023a)
8 TÜV Verband (2023); Statista (2024)
9 TÜV Verband (2023); Bitkom (2023b)
10 Bada et al. (2015); Herley (2009)
11 Adams and Sasse (1999)
12 Hu et al. (2021); Alshaikh et al. (2019); Kirova and Baumöl (2018)
13 Furnell and Thomson (2009)

economically rational by ignoring security advice.[14] In addition, other factors, such as time pressure for the individual, which can hardly be coped with SETA programs, play a crucial role in cybersecurity.[15]

Nevertheless, despite the advancements in cybersecurity that have occurred in recent years, the BSI states that many companies still lack necessary knowledge, even at the basic level. In particular, small and medium-sized enterprises (SMEs)[16], which constitute 99% of German companies, are unaware of the extent of cyber threats and the vulnerabilities of their own systems. Despite many companies are well aware of the necessity to allocate more resources towards cybersecurity, they still fail to do so. Furthermore, many do not even use the most basic, cost-effective preventive measures.[17]

In conclusion, it can be stated that the issue of cybersecurity represents a significant challenge for companies. Despite the recognition of cybercrime as one of the most important threats now and in the future, many companies still fail in the implementation of appropriate measures or the measures taken are not proving to be effective enough. In a consequence, employees are still a vulnerability in the cybersecurity defence system.

One objective of the present paper is to explore a potential cause for the missing success of cybersecurity activities. In particular, the gap between knowledge of the threat but lack of action suggests unconscious factors that prevent adequate behaviour. We assume a negative attitude towards cybersecurity – which is not expressed by people in recent surveys. According to scientific findings, behaviour is determined by explicit (conscious and controlled) and implicit (spontaneous and automatic) components.[18] Personal attitudes and beliefs are crucial in this regard: the objective is to determine whether an (unconscious) attitude affects the behaviour of employees. We use the Implicit Association Test (IAT) to uncover these unconscious attitudes.

A second research question of this study addresses possible approaches that can be used to create incentives for improved cybersecurity in SMEs. For this purpose, existing nudging literature is reviewed and transferred to the context of cybersecurity. Research question three examines the role of users' level of knowledge in the utilization of programs and activities.

The present paper is structured as follows: Firstly, the theoretical basis is explained. This will focus particularly on the Fogg model for behavioural change. This is followed by the empirical study, including a description of the method, sample and results. The topic of nudging in the field of cybersecurity is subsequently analysed using a literature review. The paper ends with a discussion summarizing the implications for research, companies and governments as well as a presentation of limitations and future research approaches.

---

14 Cormac (2009), Herley (2009)
15 Chowdhury et al. (2019)
16 In this study, we use the definition of IfM Bonn for SMEs, with regard to the number of employees. This definition is widely used in Germany and defines SME as a company with up to 499 employees.
17 BSI (2024)
18 Mai and Dickel (2021)

3 Theoretical Basis

Why people act the way they do is a frequently discussed topic, and understanding individual behaviour is a challenging task. Therefore, a number of behavioural models have been developed. These models have been adapted to cybersecurity behaviour and are widely used.[19] They offer valuable insights why individuals might adopt or avoid certain cybersecurity behaviours. Many of these models are derived from the Theory of Reasoned Action[20] or the Theory of Planned Behavior.[21] They share the commonality that several factors can influence an individual's attitude towards a threat. And, in turn, affect the individuals' behavioural intentions.[22] In this context, the Fogg Behavior Model (FBM), also called B=MAP model (Behaviour = Motivation, Ability, Prompt),[23] can be used to explain the causes of (non-)behaviour in cybersecurity and to determine behavioural change.[24]

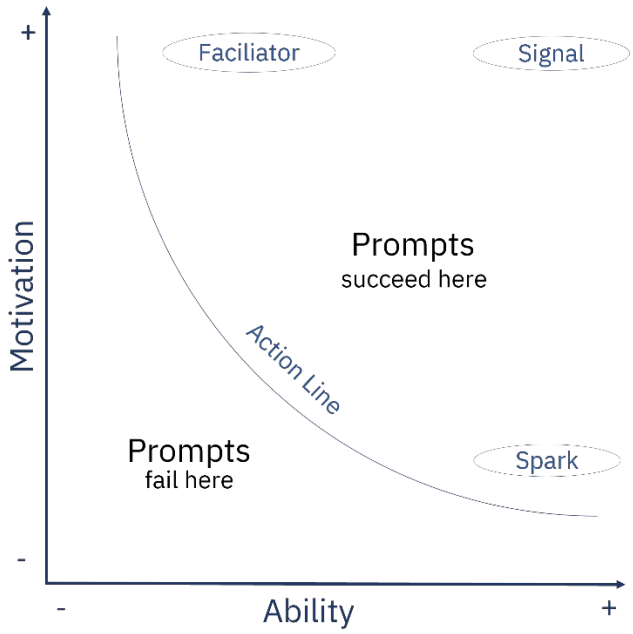
The FBM (see Figure 1) is derived from the idea that motivation and ability play a major role in the behaviour of humans. Motivation can be defined as the willingness to perform a given behaviour.[25] Ability, in this context, refers to the ease or difficulty of performing a specific behaviour. The model posits that for a targeted behaviour to occur, an individual must possess a sufficient level of motivation and a sufficient level of ability which is symbolized by the threshold called 'action line'. Both, motivation and ability can be increased to stimulate a target behaviour, when people do not have a sufficient level to exceed the action line. Elements to increase motivation (called motivators) are pleasure and pain, hope and fear as well as social acceptance and rejection. Elements to increase ability are time, money, physical effort, brain cycles, social deviance as well as non-routine.

In our study we focus on motivation and the element of brain cycles which can also be described as knowledge. When people have reached a sufficient level of motivation-ability above the threshold, it requires additionally trigger(s), which stimulate(s) the individual simultaneously, for the behaviour to occur. If, for instance, an individual exhibits a lack of motivation to perform a specific action, it needs a trigger called 'spark' to stimulate motivation. If an individual has a high motivation but lacks ability, it needs a another form of trigger ('facilitator') to ease the performance. Finally, if an individual possesses both the ability and the motivation to engage in the target behaviour, it needs a trigger called 'signal' to remind him, that a specific behaviour should be done. Only when motivation and ability are sufficiently high and when an appropriate trigger occurs, individuals may engage to perform a target behaviour (change).[26]

---

19 Alsharida et al. (2023); ENISA (2018); Briggs et al. (2017)
20 Fishbein and Ajzen (1975)
21 Ajzen (1991)
22 Briggs et al. (2017)
23 Fogg (2009)
24 ENISA (2018)
25 Fogg (2009)
26 Fogg (2009)

Figure 1: Fogg Behavior Model (FBM)



Source: Adapted from Fogg (2009)

Despite several ways to measure actual behaviour, the difficulty is, however, to measure planned behaviour (change) and reasons for behaviour (change) such as motivation and some forms of ability. Assessing intentions to perform a behaviour is a common procedure – also in the field of cybersecurity.[27] Reviews of literature in the field of cybersecurity reveal that most studies use self-report measures.[28] This results in a number of considerable issues, given that there are numerous attitudes that are probably unknown to the individual. Although there might be a strong correlation, people tend to give socially desirable answers in surveys and create a bias.[29] Also, security decisions that have a visible impact are more likely to be reported correctly.[30] These 'unconscious attitudes' are evaluations that occur outside of conscious awareness and are not the result of conscious intent. They have the potential to influence behaviour and decision-making – as well as response behaviour.[31] Research has shown that people may possess unconscious biases, despite their explicit espousal of egalitarian values.[32] Unconscious attitudes, also known as implicit biases, have already been a significant area of research in psychology and related fields for several decades.[33] The application of behavioural aspects, like unconscious attitudes, in research to cybersecurity on the other hand is a relatively new and emerging field. However, it is growing in importance as the human factor is increasingly recognised as critical to cybersecurity.[34]

27 Crossler et al. (2012); ENISA (2018)
28 ENISA (2018); Mayer et al. (2017)
29 Wash et al. (2017)
30 Wash et al. (2017)
31 Greenwald et al. (1998)
32 Barnes (2006); Norberg et al. (2007)
33 Gawronski et al. (2006)
34 ENISA (2018)

By understanding and addressing these biases, researchers may understand and enhance decision-making processes. Therefore, a valid option to observe and measure actual behaviour might be laboratory experiment methodologies.[35] A reason, underpinning the utilization of experiments and indirect measures is that they facilitate the exploration of unconscious mental associations that are challenging to discern through conventional self-report instruments.[36] To overcome the problem of self-reporting, we therefore use a questionary as well as the method of the IAT. The IAT is based on the premise that individuals tend to respond in a more consistent manner to associated concepts when they have to answer very quickly. This is closely related to the work of behavioural biases and the Dual-Process Theory.[37]

---

35 Crossler et al. (2012)
36 Gawronski et al. (2006)
37 Tversky and Kahneman (1974)

4 Empirical Study

a. Experimental Design

To answer the research questions on implicit beliefs towards cybersecurity, an online experiment was conducted.[38] An IAT is used to assess the respondents' implicit attitudes towards cybersecurity. This computer-based method measures the strength of automatic associations between concepts in the memory of the test subjects and can therefore uncover unconscious associations. Test subjects categorise words or images that are assigned to different concepts and attributes as quickly as possible. As a result, differences in reaction time can reveal implicit prejudices or preferences. Faster categorizations for congruent pairings (e.g. 'flower' and 'positive') compared to incongruent ones (e.g. 'distress' and 'positive') indicate stronger associations.[39]

Figure 2: Arrangement of the levels in the IAT in stage 2 (left) and stage 4 (right)

Source: WIK, own illustration

The standard procedure has a category level and a property level in seven stages. Both levels consist of opposing terms. In the present study, we opted for a slightly modified version and used a single category implicit association test (SC-IAT). In this modification, only one term is selected at the category level (in Figure 2, this is the word 'Cybersicherheit' (cybersecurity)), without a corresponding opposite term. The reason is that our selected category (cybersecurity) has no direct counterpart. The SC-IAT enables a simplified classification with a similarly high level of internal consistency.[40] In addition, various studies have found that the SC-IAT also leads to equivalent results to the IAT.[41]

Using the SC-IAT results in the following structure: The upper level contains the term cybersecurity (see Figure 2; category level is here in white). At the level below is the evaluative dimension in blue. In the example in Figure 2 the terms 'angenehm' and 'lästig' are used.[42] In the example in Figure 2, the term 'ermüdend' (tiring) should be assigned to the right-hand side (category annoying). In the right-hand part of the figure, the term 'Biometrie' (biometrics) in level four should also be assigned to the right-hand side. Figure 8 in the appendix shows the stimuli used for the three terms.

---

38 The experiment, including the questionnaire, was conducted in German.
39 Mai and Dickel (2021), Greenwald et al. (1998)
40 Fu and Liu (2017)
41 Fu and Liu (2017); Karpinski and Steinmann (2006), Stieger et al. (2010)
42 ‚angenehm' is the German word for 'pleasant' and 'lästig' means 'annoying'

The experiment is structured in four stages, as described by Karpinski and Steinmann.[43] Before starting the experiment, the procedure is explained to the subjects. Within the first two stages, the term 'cybersecurity' is shown on the left-hand side on the category dimension, the term 'pleasant' on the evaluative dimension below. On the right-hand side the term 'annoying' is on the evaluative dimension and nothing is displayed on the category dimension. Words that can be clearly assigned to one of the sides are displayed in the middle. For example 'firewall' can be assigned to 'cybersecurity' and 'unpleasant' can be assigned to 'annoying' (see Figure 8 in the appendix). For the third and fourth stage the only change is that the category level is on the right-hand side. Everything else remains. Table 1 shows the order of the other three levels. The first and third stage serve to familiarise participants with the categories and the general assignment method in the IAT. Stages two and four are actual experimental stages. All subjects complete the stages in the same order.[44]

Table 2: Arrangement at the category dimension and evaluative dimension the various stages

	dimensions	left (key 'e')	right (key 'i')
stage 1 (training, 24 trials)	category dimension	cybersecurity	
	evaluative dimension	pleasant	annoying
stage 2 (experimental phase, 72 trials)	category dimension	cybersecurity	
	evaluative dimension	pleasant	annoying
stage 3 (training, 24 trials)	category dimension		cybersecurity
	evaluative dimension	pleasant	annoying
stage 4 (experimental phase, 72 trials)	category dimension		cybersecurity
	evaluative dimension	pleasant	annoying

Source: WIK, own illustration

Subsequent to the SC-IAT, participants were asked to complete a questionnaire. This included information about their work, their employer, experience with cybersecurity activities and general interest in the topic of cybersecurity.[45]

Participants were recruited via the platform Prolific.[46] Subjects who completed the procedure and the questionnaire received a payment (2,54€) for taking part in the experiment. For participation, the

---

43 Karpinski and Steinmann (2006) | In difference, we use 24 trials in stages 1 and 3 and 72 trials in stages 2 and 4.
44 Karpinski and Steinmann (2006)
45 The complete questionnaire can be provided upon request.
46 Prolific is an online research platform that provides recruitment and management of participants for online research projects.

following filter criteria were used: Fluent in German, living in a German-speaking country, i.e. Germany, Austria, Liechtenstein, Luxembourg, Switzerland, age between 18 and 65 and using a computer at least 25% of the working time.

Prior to the main study, a pre-test was conducted. To ensure that all survey questions could be answered by the target group and to make sure that the SC-IAT test procedure was technically reliable. The pretest was carried out in two stages: 10 participants in the first stage were informed about their role in the pretest and explicitly asked to pay attention to possible errors, ambiguities or problems. Participants were also asked to indicate their browser and device when completing the test.[47] Subsequently, some changes were made in the explanation of the SC-IAT procedure in order to clarify the test for the respondents in the main study. No changes were necessary with regard to the SC-IAT itself or the wording. In the second stage, 40 respondents were questioned via Prolific; these respondents were not informed about the pre-test. Afterwards, no changes in content were necessary. However, the announced test length was reduced from 15 to 12 minutes, as most pretest subjects required only 9-11 minutes to complete the test.

b. Sample

Of the original 579 datasets, a number of respondents were removed from the sample, particularly due to incomplete responses and incorrect answers to the attention check in the questionnaire.[48] In addition, individuals were also removed if their work status was not obvious. This applied to students, pensioners and jobseekers, in all cases without secondary current employment. This resulted in a total of 411 participants. Subsequently, to calculate the D-score according to the IAT-method, subjects who violated the specified limits of time and error rate were also removed.[49]

The final sample included 367 participants (63% male) with a mean age of 31.4 (range: 18 - 64 years). All participants were fluent in German, most (86%) were German native speakers. The majority of respondents have no IAT experience (60%), while some have already completed an IAT once (20%) or several times (19%).

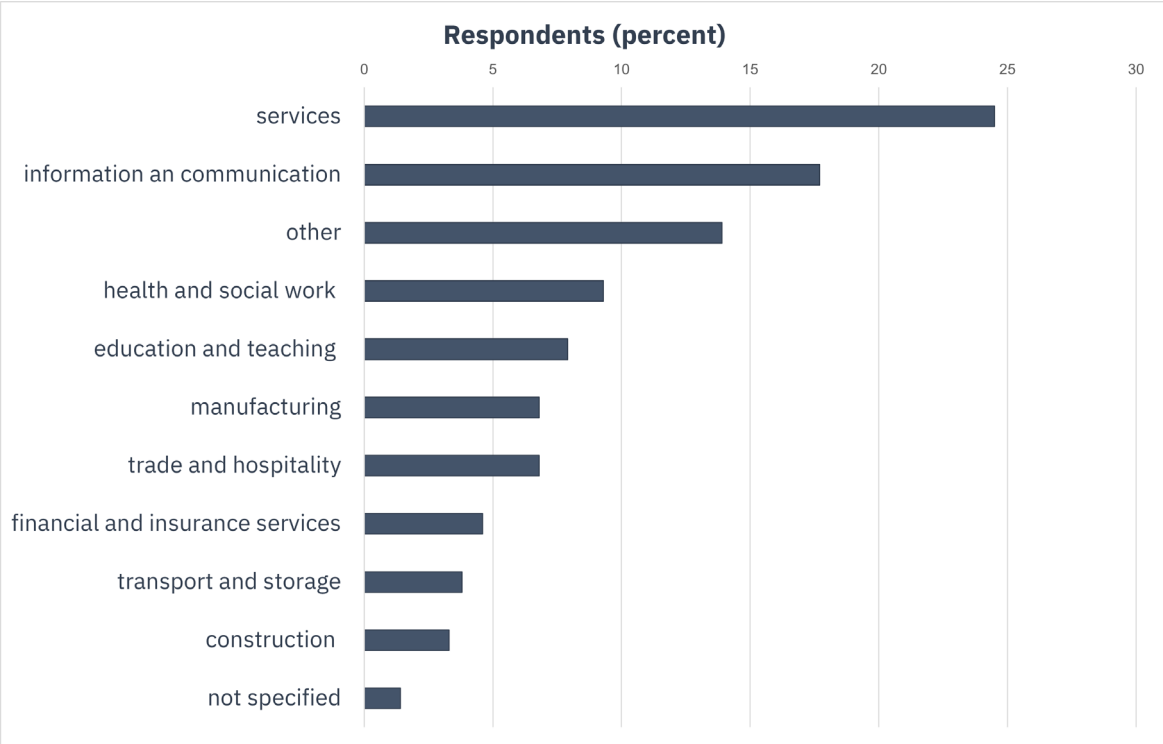
Seventy-nine percent were employees or workers, team leader or head of department (11.7%), managing directors or CEOs (4.4%) or others (5.4%, mostly freelancers). Most respondents recently joined their company (since 2022 or shorter: 51%). However, there were also long-term employees among the respondents (10 years or more: 13.1%). Approximately one quarter (26%) of respondents work in their company's IT department.

An analysis of the sectors shows a focus on services (25%) and information and communication (18%). Also other sectors are represented, including manufacturing and industry (7%), education (8%) and health and social services (9%). Around two-thirds of participants work in SMEs (59.4%), the others either work in companies with more than 500 employees (35.7%) or did not specify (4.9%) (see Figure 3 below).

---

47 All common browsers and operating systems were used in the tests, thus ensuring technical functionality.
48 In question 12 of 23 of the questionnaire, participants were asked to choose the highest number (possible answers: 4, 9, 28, 42) to ensure that they are focused and do not choose answers at random.
49 Greenwald et al. (2021)

Figure 3: Distribution of sectors within the sample



Source: WIK, own illustration

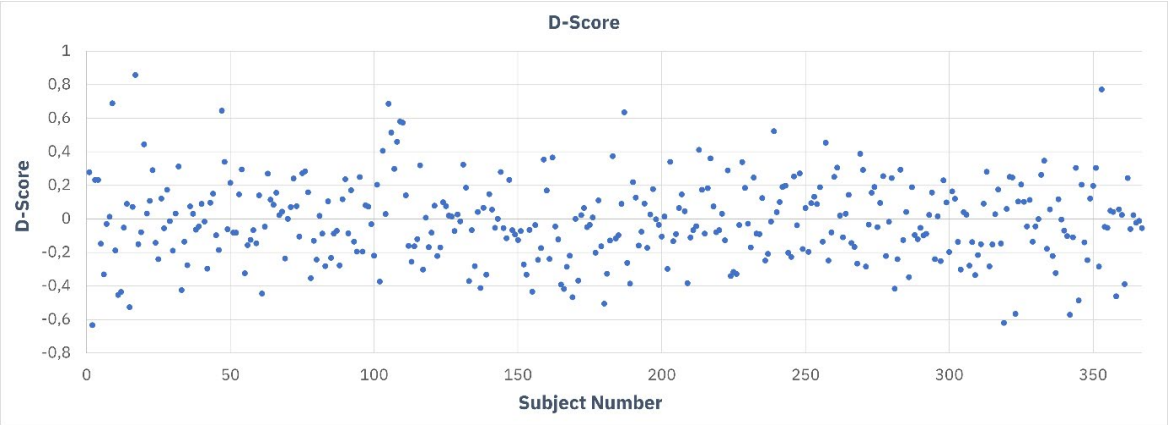
c. Results

i. Results on Implicit Beliefs

The mean error rate for the final sample amounts to 4.23% and can be considered suitable for further analysis. The D-score shows the unconscious attitude towards cybersecurity, and is calculated analogously to the procedure of Greenwald et al.[50] One adjustment involves the change resulting from the SC-IAT compared to the standard procedure described by Greenwald. This includes a reduced number of stages in the assessment, as described above. The calculation of the mean D-score shows a slightly negative trend: M_{Dsore} = *-0.0123 (SD = 0.2382*, ranges from *-0.6336 to 0.8579*, see Figure 4). Accordingly, a negative attitude towards cybersecurity is present. Based on the evaluative dimension (pleasant and annoying), it can be concluded that cybersecurity is perceived as rather annoying.

50 Greenwald et al (2021)

Figure 4: Distribution of the D-score



Source: WIK, own illustration

There is a significant difference in the D-score when distinguishing between employees from the IT department and other employees (M_{IT} = *-0.0576;* M_{notIT} = *-0.0033; t(366) = -2.361 p = .019*). This is a rather negative attitude among employees in the IT department. A possible, but yet to prove assumption could be that an cybersecurity incident requires a considerable amount of work for the IT department's employees. For example, if a company's employees receive an increased number of phishing emails, these are often forwarded to the IT department for investigation. The IT department therefore has additional tasks of reviewing and answering questions from staff besides its 'normal' activities and may perceive this as an additional effort.

The analysis also shows that the D-score negatively impacts the assessment of personal knowledge about cybersecurity (*b = -0.544, t(366) = -2.147, p = 0.032*). Further significant differences and relationships with the variables surveyed, such as company size or attendance of cybersecurity training, were not identified.

ii. Results on Motivation

The Fogg model (see Chapter 3) considers motivation to be particularly decisive for behavioural change. Accordingly, the analysis in this study also focused on factors that in turn influence employee motivation.

The age of the respondents is a personal factor that positively affects motivation.[51] Accordingly, a higher age is associated with slightly higher motivation (*b = 0.023, t(366) = 2.988, p = 0.003*). The same applies to the time that the respondent has been employed by the current company (*b = 0.023, t(366) = 2.143, p = 0.033*). However, it should be noted that the two variables, age and length of employment, are correlated.

51 The specific statement in the survey was: *'I generally feel motivated to engage with the topic of cybersecurity'. (7-point scale)*

Furthermore, the concern of becoming a victim of a cybersecurity attack[52] also shows a significant influence on motivation (*b = 0.143, t(366) = 2.984, p = 0.003*), suggesting that risk awareness is an important factor for motivation, but does not fully explain it. However, based on the available data it remains unclear which other factors promote motivation. The further analysis shows that the occurrence of cybersecurity incidents in one's own employer and being personally affected by a cybersecurity incident have no effect on motivation.

iii. Results on Knowledge

In addition to motivation, the second component in the Fogg model is analysed in detail. We see knowledge ('brain cycles') as one prominent component of ability. Here, the occurrence of a cybersecurity incident in the company and one's own involvement in an incident also do not matter. Similar to motivation, it can be observed that the concern of becoming a victim of a cybersecurity incident affects the assessment of one's own knowledge about cybersecurity[53] (*b = -0.202, t(366) = -5.075, p < 0.001*). However, the results show an inverse effect. The assessment of one's own knowledge decreases with increasing threat expectation. One possible explanation involves the Dunning-Kruger effect.[54] Their key finding is that individuals with low competences tend to rate their own competence higher than it actually is, while individuals with high competence tend to rate their own competence lower than it actually is. In the present case, the interpretation is that a high level of awareness and reflection on the topic of cybersecurity strengthens the awareness that the knowledge on the topic of cybersecurity is (still) limited. Hence, perceived threat makes the individual more vigilant and rates its own competence lower than if they do not perceive a threat.

Examining motivation as an impact factor on the assessment of personal knowledge reveals a positive effect (*b = 0.211, t(366) = 4.879, p < 0.001*), i.e. the higher the motivation, the higher one's own knowledge is assessed. The number of trainings shows a similar result: The more trainings the respondents attended, the higher they rated their own knowledge (*b = 0.070, t(197) = 3.335, p < 0.001*).[55]

iv. Results on Behaviour

In addition to the parameters used in the Fogg model, the present study also focuses on behaviour with regard to cybersecurity activities. Therefore, the respondents were asked about how strictly they follow the cybersecurity policies and guidelines of their employer.[56] Similar to most other questions in the questionnaire, respondents were asked to make an self-assessment (in this case about their own behaviour), which needs to be considered when interpreting the results.

---

52 The specific question in the survey was: *'How would you rate your personal risk of becoming a victim of cybercrime?' (7-point scale)*

53 The specific question in the survey was: *'How would you rate your knowledge of cyber security?' (7-point scale)*

54 Kruger and Dunning (1999)

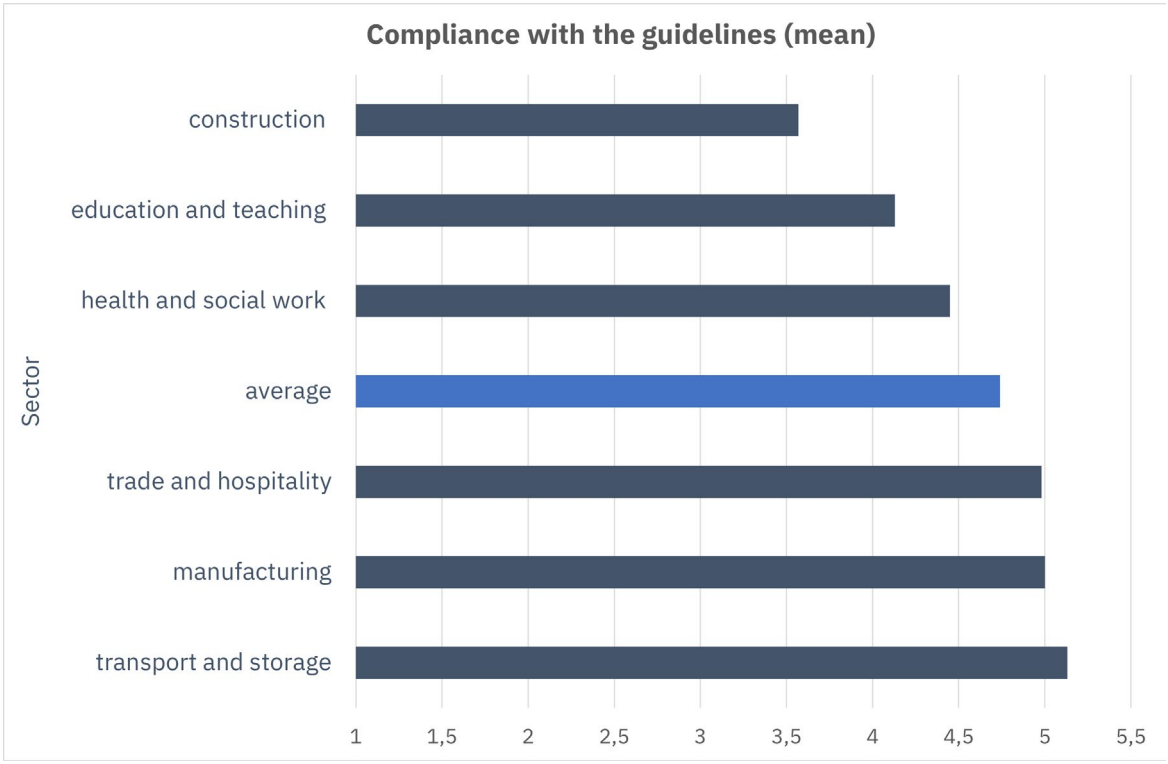
55 It should be noted that this is a reduced sample; only subjects who had previously stated that they had ever attended a training course were asked about the number of trainings.

56 It should be noted that the respondents were first asked whether their company had guidelines on the topic of cybersecurity. In the next step, the individuals for whom this was the case were then asked how strictly they adhere to them; the exact question was: '*How strictly do you comply with these policies and guidelines? (7-point scale)*

A number of factors were found to impact behaviour in relation to guidelines. Motivation (*b = 0.184, t(213) = 3.657, p < 0.001*), knowledge (*b = 0.299, t(213) = 4.714, p < 0.001*), as well as the assessment of the relevance of cybersecurity (*b = 0.279, t(213) = 3.175, p = 0.002*)[57] have a significantly positive effect on acting in accordance with the guidelines.

The examination of cybersecurity training activities reveals a higher level of conformity to guidelines when training is perceived as helpful (*b = 0.176, t(146) = 3.122, p = 0.002*). A difference also emerges between the extent to which the guidelines are followed between companies that offer training vs. companies that don't ($M_{training}$ = *4.90;* $M_{notraining}$ = *4.40; t(213) = 2.883 p = 0.002*). However, it should be noted that there is a relationship between the binary variable of presence of guidelines and the presence of trainings (*χ2=52.218; p<0.001*). Accordingly, a part of the difference may be attributed to the company's fundamental attitude of considering cybersecurity issues seriously.

Figure 5: Compliance with cybersecurity guidelines in different sectors



Source: WIK, own illustration

Differences in compliance with the guidelines can be seen between sectors (*t(213) = 2.168 p =.021*, see Figure 5).[58] Branches with strict compliance or a mean value exceeding the overall means are manufacturing and industry ($M_{manufac}$ = *5.00*); transport and storage ($M_{transport}$ = *5.13*) and trade and hospitality (M_{trade} = *4.89*). Respondents in the construction (M_{const} = *3.57*), education and teaching (M_{teach} = 4.13) and health and social work (M=4.45) sectors adhere to the guidelines to a below-average extent.

57 The statement was: *'In general, the topic of cybersecurity is relevant.' (7-point scale)*

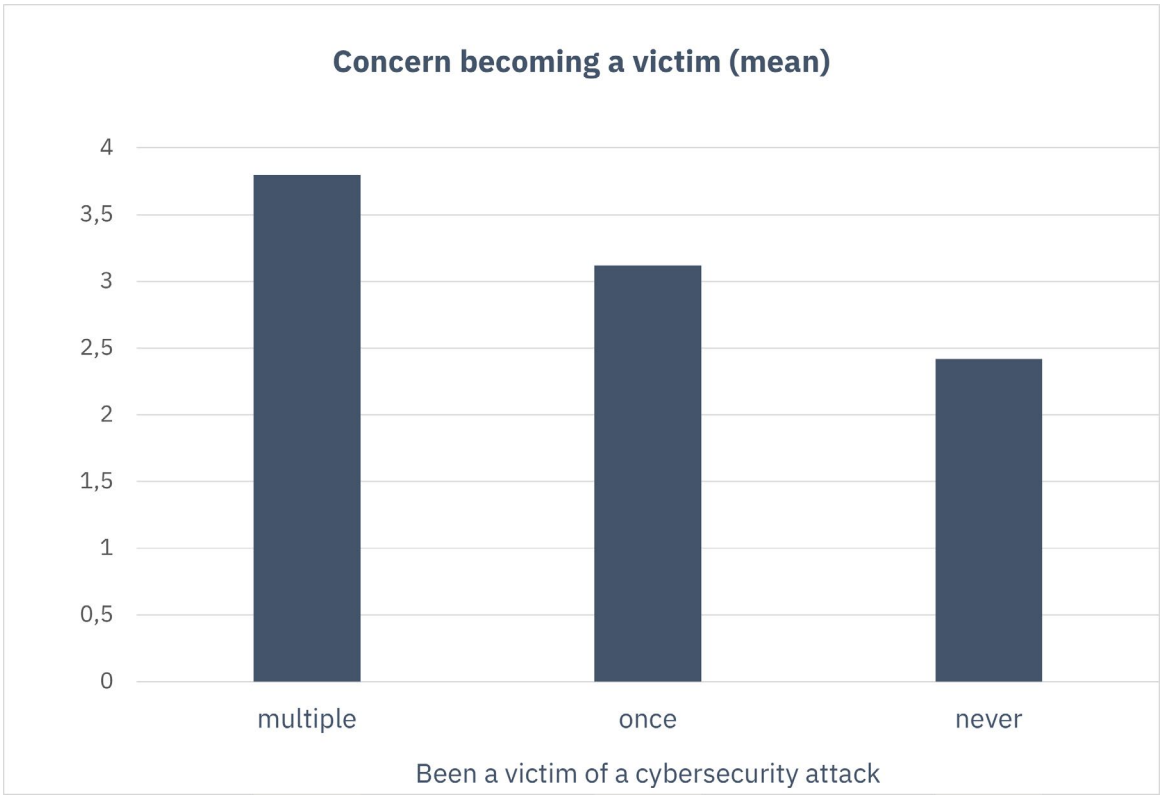
58 When interpreting the differences between sectors, it should be noted that some sectors are only represented by a very small number of respondents.

Interestingly, neither an incident in the company the person works, nor personal involvement, nor the concern of becoming a victim of a cybersecurity incident affect compliance to guidelines. It also does not matter whether the respondents hold a management role or not.

v. Further Results

The analysis of further results shows variables that affect the concern of becoming a victim of a cybersecurity incident. An incident in the company does not lead to any differences in the expectation of becoming a victim. However, if the respondent has personally been the victim of an incident, it increases the concern that this could happen again. This is particularly the case when the respondent has been affected several times (M_{mult} = *3.80*; M_{once} = *3.12*; M_{never} = *2.42*; $t(367) = 16.717$ $p < 0.001$; see Figure 6 below).

Figure 6: Mean values of concern of becoming a victim of a cybersecurity attack in relation of being an actual victim of an attack



Source: WIK, own illustration

The distinction between SMEs and large companies reveals only one difference between the company types. SMEs are significantly less likely to offer any training on cybersecurity for employees ($\chi 2$ = *20.380; p < 0.001*). In SMEs, 52.75% of respondents stated that their organization does not offer any training on cybersecurity, compared to only 31.30% in large companies.

Furthermore, respondents were asked in an open question about topics covered in recent trainings. These were clustered by topic (see Figure 7). The most frequently mentioned topics were phishing emails (43 mentions), cybersecurity in general (34 mentions) and data protection (18 mentions). The

‘other’ cluster (13 mentions) included topics like external storage media, the risk of hacking and dealing with social media.

Figure 7: Most frequent topics of trainings

Source: WIK, own illustration. Number of mentions: Phishing = 43, Cybersecurity = 34, Data protection = 18, Passwords = 8, Social Engineering (without Phishing) = 7, Patient data/files = 4, Policies = 3, Best Practice = 3, Other = 13. Font size in relation to number of mentions.

5 Nudging

The literature research and our empirical research shows that the employees are aware of the cybersecurity threats, but have negative associations with the subject and do not always act to sufficiently ensure cybersecurity. To enhance the activity level of the employees with regard to cybersecurity, nudging might be an effectful way to improve the level of cybersecurity.

Thaler and Sunstein[59] define nudges as '*any aspects of the choice architecture that alters people's behaviour in a predictable way without forbidding any options or significantly changing their economic incentives'*. Applied to the present paper, the idea is primarily that unconscious rejection or low motivation towards cybersecurity topics or low ability/knowledge can be altered. That is supposed to be achieved without making users feel manipulated and without using explicit (such as financial) incentives.

There are numerous publications on nudging in general. The analysis by Beshears and Kosowsky,[60] for example, examines the effectiveness of different nudging methods as part of a meta-study. According to their findings, multiple types of nudging are effective, particularly if they also automate parts of the decision-making process. Nudging can generally be carried out in different ways; Weinmann et al.[61] provide six examples of principals of digital nudging, including incentives (make incentives clearer to enhance their effectiveness), defaults (preselection of options by defining standard options), giving feedback (feedback to users on whether they are performing well or make mistakes).

The paper by Schmauder et al.[62] focuses on the use of AI for customized nudge creation. Accordingly, algorithmically personalized nudges have the potential to improve human decision-making by tailoring interventions to individual needs. However, relying on 'black box' AI systems can obscure the underlying cognitive processes that make these nudges effective. In their conceptional paper, the authors recommend an interdisciplinary regulation to ensure that the ethical and cognitive implications of AI-driven nudges are properly addressed.

Some studies emphasize specific use cases within the field of cybersecurity. One paper focuses the issue of inadequate support for users in managing cybersecurity behaviours, using password authentication as a specific example.[63] Through two experimental studies, the paper explores how active user support, including guidance, feedback, and gamification, can positively influence password choices. The findings suggest that such interventions can lead to improved user behaviour, and similar approaches could be applied to other areas of user-facing security.

The study by Hartwig and Reuter[64] also addresses the application of passwords. In contrast to most analyses, a whitebox procedure is considered. This method enables users to understand the steps between input and output. In contrast to black box methods, this ensures greater transparency, but can also lead to information overload and thus overwhelm users. The paper also addresses the topic of personalization of nudges. The users were categorized according to their decision-making and information processing styles. Results show that dynamic radar charts provide a reasonably effective nudge for stronger passwords. Contrary to expectations, the personalization approach did not show any significant advantage.

---

59 Thaler and Sunstein (2008, p. 6)
60 Beshears and Kosowsky (2020)
61 Weinmann et al. (2016)
62 Schmauder et al. (2023)
63 Furnell et al. (2019)
64 Hartwig and Reuter (2021)

An experimental study investigates behavioral change through priming and framing in the context of phishing emails.[65] The findings indicate that framing, positive or negative, does not affect users' behavior. In line with the authors assumptions, priming users with information about security risks effectively reduces risk-taking behavior. Additionally, the results reveal a number of further relationships between the components of risk orientation: risk-averse behavior is associated with greater confidence in the action, greater perceived severity of cybersecurity risks, lower perceived susceptibility to cybersecurity risks and lower trust in the provided download link.

For the purposes of the present study, literature shows some approaches for using nudges in the field of cybersecurity. In particular, a combination of nudging types seems to offer a suitable approach if there is a reasonable level of motivation and knowledge (see chapter 3, Fogg-Modell). For example, in case of passwords, a combination of ‘feedback’ and ‘default’ appears useful. In cases of rather low knowledge or low motivation, the use of ‘ease and convenience’ with the objective of automating the decision-making process seems suitable.

---

65 Sharma et al. (2021)

6 Conclusions, Implications, Limitations and Outlook

a. Conclusions and Implications for Research, Companies and Government

The role of implicit beliefs in cybersecurity contexts is an understudied topic. To our knowledge, there are hardly any existing studies that use the IAT method in the context of cybersecurity.[66] The key finding of the present study, i.e. the existing negative attitude towards cybersecurity, emphasizes the role of implicit beliefs in research and practice.

The findings provide support for the assumption that employees who use computers tend to have a negative implicit attitude towards cybersecurity. Engaging with the topic is perceived as annoying rather than pleasant.

However, the implicit attitude towards cybersecurity does not appear to affect a lot of the variables assessed in this study. The only variable in our study that is impacted by the implicit attitude is self-assessed knowledge, with a negative connection. Accordingly, a negative implicit attitude towards cybersecurity leads to a lower assessment of one's own knowledge. Additionally, there might be further implicit attitudes influencing cybersecurity behaviour, than those assessed.[67] Accordingly, the IAT method offers promising potential for future applications in the field of cybersecurity.

As illustrated with the FBM (see chapter 3), more cybersecurity might occur, when individuals are motivated to engage with the topics. They should also get easier access to knowledge and receive support to improve their abilities (e.g. through knowledge transfer) to foster the desired behaviour. The theoretical model is corroborated by the findings of our empirical investigation. Our findings allow us to propose recommendations for businesses and governments. One possible solution would be to implement SETA measures.

1. Companies need to provide their employees with training. The objective of the training should thereby not only be to qualify employees but also enhance employees' motivation to engage with cybersecurity.

Our results show that employees who take part in training on cybersecurity tend to strictly follow the cybersecurity guidelines and specifications of their employer. Moreover, the implementation of such trainings positively influences the employees' self-assessed knowledge. By identifying and offering training on cybersecurity to their employees, companies can enhance the ability of their workforce, and consequently impact their behaviour to address cybersecurity. As SMEs offer less training for their employees than large companies, this recommendation is particularly important for them.

Trainings, which also increase the motivation of people to deal with cybersecurity seem particularly suitable. Since our results show that the self-assessed knowledge increases with higher motivation, it seems suitable to focus on motivation in cybersecurity trainings as well.

Additionally, our findings indicate that managing directors are more likely than employees to assess their level of expertise as high. This discrepancy may indicate a knowledge gap, because management

---

66 Di Gioia et al (2019); Moceriono (2024)
67 Ajzen and Dasgupta (2015)

is unaware of the gaps in employees' knowledge. It is crucial for management to recognize this gap and address the needs of employees, rather than assume their own self-assessed knowledge as standard.

2. Awareness and training programs is advised to teach participants that they are prone to become victims in the future.

This is derived from our results that individuals who perceive the risk of becoming victims of a cyberattack to be high are more motivated to engage with this topic. Our results also indicate that this perception is associated with a more reflected (and hence lower) self-assessment of knowledge.

In contrast, the occurrence of cybersecurity incidents at one's own employer and being personally affected by a cybersecurity incident have no effect on motivation and self-assessed knowledge. We assume that the mere awareness of incidents, even when they occur at one's own employer, is too abstract for employees to draw conclusions by themselves. Consequently, they are not more motivated to engage with the topic and they do also not increase their knowledge. One possible explanation can be a lack of feedback provided to the individual. The same applies to personal security incidents, which are probably too abstract to be able to draw lessons for motivation and knowledge. This could explain why the concern of becoming a victim increases with the number of personal incidents without having an effect on motivation and self-assessed knowledge.

We conclude that employees must learn from existing incidents in order to be able to realistically assess the dangers of cyberattacks. When specific security incidents are used as bad-practice the employees must learn how they might (or might not) behave in a particular situation. For employees who have previously become victim to an attack, it is crucial to undertake additional measures to enhance their motivation, such as providing reassurance and offering feedback on their past security incident.

Our findings also indicate that individuals who perceive the risk of becoming a victim of a cyberattack as high tend to rate their knowledge of cybersecurity as low while individuals who perceive this risk as low do the other way round (Dunning-Kruger Effect).[68] The negative, but presumably more realistic assessment demonstrates the necessity for training measures to be targeted and individualized. Training measures should not necessarily be based on self-assessed knowledge, as this can result in misjudgments of needs. Rather, the actual needs are to be assessed individually in test procedures in order to identify those who overestimate it and require training and to prevent 'security fatigue' among those who already possess a high level of knowledge but underestimate it. This result demonstrates again that awareness and training measures is better aimed at increasing employees' awareness of their risk of falling victim to a cyberattack so that their actual knowledge – and not their self-assessed knowledge – is enhanced.

3. In the implementation and realization process of policies and guidelines, such as an information security management system (ISMS), it is important that companies involve their employees to ensure compliance.

Our results show that a high level of motivation and highly valued knowledge increases the likelihood of employee adherence to policies and guidelines. Also providing high-quality training that employees perceive as useful increases the likelihood of employee adherence to company policies and guidelines. In

---

68 Kruger and Dunning (1999)

contrast, it is insufficient to merely raise awareness of security incidents. This does not necessarily result in employees adhering to policies and guidelines.

We assume that the introduction of guidelines without accompanying measures is unlikely to result in a desired level of adherence by the employees because they do not understand the importance. Consequently, companies should implement supporting measures for their employees when they introduce policies and guidelines. This recommendation is particularly relevant for companies in the construction and education sectors, where our survey results show that policies and guidelines are even less strictly adhered to.

4. People should to be made aware of the potential unconscious attitudes.

Based on our results, it can be concluded that cybersecurity is perceived as rather annoying. We also assume that there are more implicit beliefs and unconscious attitudes towards cybersecurity which we did not investigate. Since it is one of the characteristics for this phenomena, people will not be aware of these attitudes. It would be beneficial to raise awareness for this topic. Government and authorities can play a crucial role as impartial mediators, facilitating the implementation of effective measures to raise awareness about unconscious attitudes among companies and their employees. Relevant findings could be adopted in publicly funded measurements, such as awareness campaigns.

Furthermore, it is essential to develop strategies to address and counteract these negative attitudes. We propose to use elements of nudging to ease behaviour change towards a more cybersecure behaviour in cases, where unconscious attitudes constitute obstacles.

b. Limitations and Outlook

The present study provides valuable insights into unconscious beliefs about cybersecurity, as well as other aspects of cybersecurity. Nevertheless, there are some limitations that need to be considered when interpreting the results. These limitations also offer potential for future research.

One important limitation of the present study relates to the survey method within the questionnaire. Most of the items are recorded via direct questions. Thus, results for the items (e.g. on knowledge, relevance and implementation of the cybersecurity guidelines) are solely based on self-assessment and therefore highly subjective. Self-assessment is based on the principle that people reflect on their own mental processes and actions, bearing the risk that the answers may be influenced by social desirability or unconscious bias. Future research could address this: Questions to identify the subject's knowledge on cybersecurity, for example, could be answered directly using knowledge questions in order to obtain objective data. Another option might be using latent constructs.[69] This involves a set of questions that at least provide a better approximation of an objective response compared to direct questions.

The present study demonstrates that influential factors still remain unknown. Moreover, it is not entirely clear what possible interaction effects influence actual behaviour in the cybersecurity context. For example, the consideration of individual risk behaviour[70] or regulatory focus is conceivable in this context. Research on regulatory focus theory suggests that different foci lead to different approaches to problem solving.[71] The promotion focus emphasizes positive outcomes and opportunities, whereas the

---

69 Bollen (2002)
70 Sharma et al. (2021)
71 Higgins (2012)

‘prevention’ focus concentrates on possible negative outcomes and risks. Accordingly, it can be assumed that individuals in the prevention focus are more likely to be motivated to follow guidelines if the risks of non-compliance are highlighted. In contrast, people in the promotion focus are more likely to be motivated by the benefits of complying with guidelines.

Further future research with IAT for specific aspects of cybersecurity might be helpful. In the present working paper, the topic of cybersecurity was considered as a whole; focusing on a specific sub-topic could provide deeper insights into selected characteristics. For the selection of the specific field, areas that focus on spontaneous human behaviour are particularly suitable, e.g. various types of social engineering. The recent study by Moceriono[72] focuses on a similar topic; Cognitive processes in the context of phishing emails and their characteristics are analysed. For future research, other communication channels that require a quick response, e.g. chats or phone calls, would also be a suitable field of investigation.

72 Moceriono (2024)

Literature

Adams, A., Sasse, M. A. (1999). Users are not the enemy. In: Commun. ACM 42, 12 (Dec. 1999), 40-46. https://doi.org/10.1145/322796.322806

Ajzen, I. (1991). The Theory of Planned Behavior. In: Organizational Behavior and Human Decision Processes. 50. 179-211. 10.1016/0749-5978(91)90020-T.

Ajzen, I., & Dasgupta, N. (2015). Explicit and implicit beliefs, attitudes, and intentions: The role of conscious and unconscious processes in human behavior. In P. Haggard & B. Eitam (Eds.), The sense of agency, pp. 115-144. Oxford University Press.

Alshaikh, M., Naseer, H., Ahmad, A., & Maynard, S.B. (2019). Toward Sustainable behaviour Change: an Approach for Cyber Security Education Training and Awareness. European Conference on Information Systems.

Alsharida, R., Al-rimy, B., Al-Emran, M., Zainal, A. (2023). A systematic review of multi perspectives on human cybersecurity behavior. Technology in Society. 73. 102258. 10.1016/j.techsoc.2023.102258.

Bada, M., Sasse, A.M., & Nurse, J.R. (2015). Cyber Security Awareness Campaigns: Why do they fail to change behaviour? 10.48550/arXiv.1901.02672.

Barnes, S. B. (2006). A privacy paradox: Social networking in the United States. In: First Monday, 11(9). https://doi.org/10.5210/fm.v11i9.1394

Beshears, J., & Kosowsky, H. (2020). Nudging: Progress to date and future directions. In: Organizational behavior and human decision processes, 161, pp. 3-19.

Bitkom (2023a). Wirtschaftsschutz 2023. https://www.bitkom.org/sites/main/files/2023-09/Bitkom-Charts-Wirtschaftsschutz-Cybercrime.pdf

Bitkom (2023b). IT-Sicherheit: 8 von 10 Unternehmen schulen Beschäftigte. https://www.bitkom.org/Presse/Presseinformation/IT-Sicherheit-8-von-10-Unternehmen-schulen-Beschaeftigte

Bitkom (2024). Wirtschaftsschutz 2024. https://www.bitkom.org/sites/main/files/2024-08/240828-bitkom-charts-wirtschaftsschutz-cybercrime.pdf

Bollen, K. A. (2002). Latent variables in psychology and the social sciences. Annual review of psychology, 53(1), pp. 605-634.

Briggs, P., Jeske, D., Coventry, L. (2017). Behavior Change Interventions for Cybersecurity. In: Behavior Change Research and Theory. Psychological and Technological Perspectives 2017, pp. 115-136. 10.1016/B978-0-12-802690-8.00004-9.

BSI (2023). Die Lage der IT-Sicherheit in Deutschland 2023. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2023.pdf?__blob=publicationFile&v=8

BSI (2024). Die Lage der IT-Sicherheit in Deutschland 2024. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2024.pdf?__blob=publicationFile&v=5

Chowdhury, N. H., Adam, M. T. P., Skinner, G. (2019). The impact of time pressure on cybersecurity behaviour: a systematic literature review, In: Behaviour and Information Technology, Taylor & Francis Journals, 38(12), pp. 1290-1308, December. https://ideas.repec.org/a/taf/tbitxx/v38y2019i12p1290-1308.html

Cormac H. (2009). So long, and no thanks for the externalities: the rational rejection of security advice by users. In Proceedings of the 2009 workshop on New security paradigms workshop (NSPW '09). Association for Computing Machinery, New York, NY, USA, 133–144. https://doi.org/10.1145/1719030.1719050

Crossler, R., Johnston, A., Lowry, P. B., Hu, Q., Warkentin, M., Baskerville, R. (2012). Future Directions for Behavioral Information Security Research (September 26, 2012). In: Computers & Security, Vol. 32(1), pp. 90-101. doi:10.1016/j.cose.2012.09.010

Di Gioia, R., Di Pomponio, I., Gemo, M., & Chaudron, S. (2019). Attitudes towards cyber risks Implicit and self-report measures. Publications Office of the European Union.

ENISA (2018). Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity. https://www.enisa.europa.eu/sites/default/files/publications/WP2018%20O.3.3.2.%20Review%20of%20Behavioural%20Sciences%20Research%20in%20the%20Field%20of%20Cybersecurity.pdf

Fishbein, M., Ajzen, I. (1975). Predicting and understanding consumer behavior: Attitude-behavior correspondence. In: Ajzen, I. & Fishbein, M. (eds.). Understanding Attitudes and Predicting Social Behavior (pp. 148-172). Englewood Cliffs, NJ: Prentice Hall.

Fogg, B. J. (2009). A behavior model for persuasive design. In: Proceedings of the 4th International Conference on Persuasive Technology (Persuasive '09). Association for Computing Machinery, New York, NY, USA, Article 40, 1–7. https://doi.org/10.1145/1541948.1541999

Fu, H., & Liu, X. (2017). Research on the phenomenon of Chinese residents' spiritual contagion for the reuse of recycled water based on SC-IAT. Water, 9(11), 846-854. 10.3390/w9110846

Furnell, S. M., Alotaibi, F., & Esmael, R. (2019). Aligning security practice with policy: guiding and nudging towards better behavior. Proceedings of the 52nd Hawaii International Conference on System Sciences (HICSS), pp. 5618-5627.

Furnell, S. & Thomson, K.-L. (2009). Recognising and addressing 'security fatigue'. ECU Publications. 2009. 10.1016/S1361-3723(09)70139-3.

Gawronski B., Hofmann W., Wilbur C.J. (2006). Are "implicit" attitudes unconscious? In: Conscious Cogn, 15(3), pp.485-99. doi: 10.1016/j.concog.2005.11.007.

Greenwald, A. G., McGhee, D. E., & Schwartz, J. L. K. (1998). Measuring individual differences in implicit cognition: The implicit association test. Journal of personality and social psychology, 74(6), pp. 1464-1480. 10.1037/0022-3514.74.6.1464

Greenwald, A. G., Brendl, M., Cai, H., Cvencek, D., Dovidio, J. F., Friese, M., & Wiers, R. W. (2021). Best research practices for using the Implicit Association Test. In: Behavior research methods, 54, pp. 1161-1180. https://doi.org/10.3758/s13428-021-01624-3

Hartwig, K. and Reuter, C. (2021). Nudging users towards better security decisions in password creation using whitebox-based multidimensional visualisations. In: Behaviour & Information Technology, 41(7), pp. 1357-1380. 10.1080/0144929X.2021.1876167

Higgins, E. T. (2012). Regulatory focus theory. In: P.M. Van Lange et al (eds.), Handbook of theories of social psychology, vol. 1, pp. 483-504). Thousand Oaks, CA: Sage

Hiscox (2023). Hiscox Cyber Readiness Report 2023. https://www.hiscox.com/documents/Hiscox-Cyber-Readiness-Report-2023.pdf

Hu, S., Hsu, C., & Zhou, Z. (2021). Security Education, Training, and Awareness Programs: Literature Review. In: Journal of Computer Information Systems, 62(4), pp. 752-764. https://doi.org/10.1080/08874417.2021.1913671

Jeong, J. J., Mihelcic, J., Oliver, G. C., Rudolph, C. (2019). Towards an Improved Understanding of Human Factors in Cybersecurity. Proceedings - 2019 IEEE 5th International Conference on Collaboration and Internet Computing, CIC 2019, p. 338-345. 10.1109/CIC48465.2019.00047.

Karpinski, A., & Steinman, R. B. (2006). The single category implicit association test as a measure of implicit social cognition. In: Journal of personality and social psychology, 91(1), pp. 16-32.10.1037/0022-3514.91.1.16.

Kirova, D., Bauмöl, U. (2018). Factors that Affect the Success of Security Education, Training, and Awareness Programs: A Literature Review. In: Journal of information technology in theory and application, 19(4), pp 56-83.

Kruger, J., & Dunning, D. (1999). Unskilled and unaware of it: how difficulties in recognizing one's own incompetence lead to inflated self-assessments. Journal of personality and social psychology, 77(6), pp. 1121-1134.

Mai, R., & Dickel, P. (2023). What we say= what we think? How implicit beliefs shape nascent entrepreneurial behavior. Journal of Small Business Management, 61(6), pp. 2986-3026.

Mayer, P., Kunz, A., Volkamer, M. (2017). Reliable Behavioural Factors in the Information Security Context. In: Proceedings of the 12th International Conference on Availability, Reliability and Security (ARES '17). Association for Computing Machinery, New York, NY, USA, Article 9, pp. 1-10. https://doi.org/10.1145/3098954.3098986

Moceriono, G. E. (2024): Implicit Association Tests for Understanding Human Factor in Phishing Beyond Awareness (Work in Progress)

Norberg, P.A., Horne, D.R. and Horne, D.A. (2007). The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors. In: Journal of Consumer Affairs, 41, pp. 100-126. https://doi.org/10.1111/j.1745-6606.2006.00070.x

Rahman, T., Rohan, R., Pal, D. and Kanthamanon, P. (2021). Human Factors in Cybersecurity: A Scoping Review. The 12th International Conference on Advances in Information Technology, Article No. 5. https://doi.org/10.1145/3468784.3468789

Schmauder, C., Karpus, J., Moll, M., Bahrami, B., & Deroy, O. (2023). Algorithmic nudging: The need for an interdisciplinary oversight. In: Topoi, 42(3), pp. 799-807.

Scholl, M., Schuktomow, R. (2021): The Current State of ―Information Security Awarenessǁ in German SMEs. In: International Journal of Emerging Technology and Advanced Engineering, 11(12) DOI: 10.46338/ijetae1221_16

Sharma, K., Zhan, X., Nah, F. F. H., Siau, K., & Cheng, M. X. (2021). Impact of digital nudging on information security behavior: an experimental study on framing and priming in cybersecurity. In: Organizational Cybersecurity Journal: Practice, Process and People, 1(1), pp. 69-91.

Statista (2024). Statista Market Insights. Durchschnittliche Ausgaben je Arbeitnehmer nach Segment. https://de.statista.com/outlook/tmo/cybersecurity/deutschland#umsatz

Stieger, S., Göritz, A. S., & Burger, C. (2010). Personalizing the IAT and the SC-IAT: Impact of idiographic stimulus selection in the measurement of implicit anxiety. In: Personality and individual differences, 48(8), pp. 940-944.

TÜV Verband (2023). TÜV Cybersecurity Studie 2023 – Cybersicherheit in deutschen Unternehmen. https://www.tuev-verband.de/studien/cybersicherheit-in-deutschen-unternehmen

Tversky, A., Kahneman, D. (1974). Judgment under uncertainty: Heuristics and biases. In: Science 185, pp. 1124-1131. DOI:10.1126/science.185.4157.1124

Wash, R., Rader, E., Fennell, C. (2017). Can people self-report security accurately? Agreement between self-report and behavioral measures. In: Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (CHI '17). Association for Computing Machinery, New York, NY, USA, pp. 2228-2232. https://dl.acm.org/doi/10.1145/3025453.3025911

Weinmann, M., Schneider, C., & Brocke, J. V. (2016). Digital nudging. In: Business & information systems engineering, 58, pp. 433-436.

Appendix

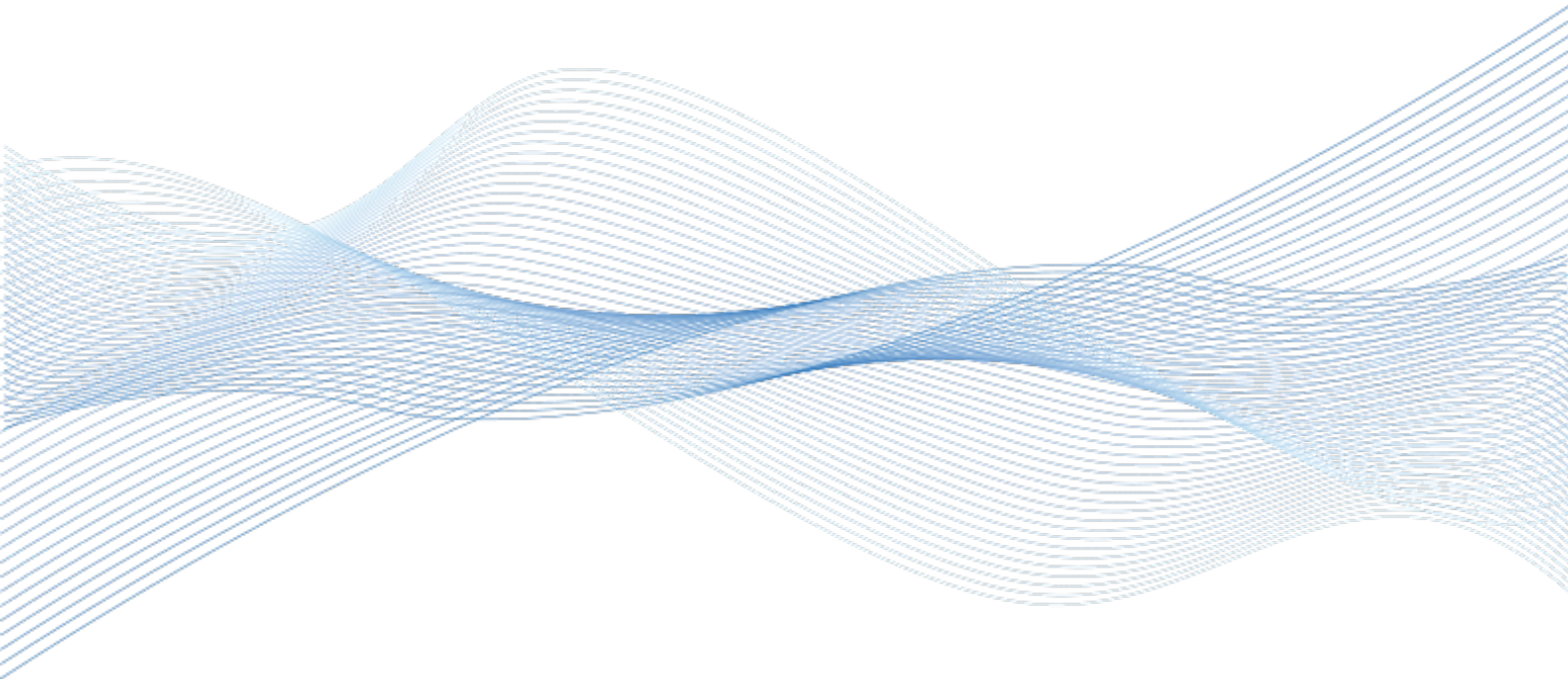
Figure 8: Overview on used stimuli for each term.

Cybersicherheit / cybersecurity (white text):
- Backup
- Starkes Passwort
- Datenverschlüsselung
- Frühwarn-System
- Firewall
- Authentifizierung
- Antivirus
- Biometrie
- Datenschutz
- Sicherheits-Zertifikate
- Zwei-Faktor-Authentifizierung
- Passwortmanager
- Update
- Datensicherung
- IT-Sicherheit
- Cybersicherheitsschulung
- Cybersicherheitsleitlinien
- IT-Sicherheitsrichtlinien
- Passwortschutz

Lästig / annoying (lightblue):
- ärgerlich
- anstrengend
- unangenehm
- nervig
- mühsam
- hinderlich
- unbequem
- unliebsam
- langwierig
- langweilig
- störend
- beschwerlich
- ermüdend
- belastend
- zermürbend
- erschöpfend
- stressig
- frustrierend
- unerfreulich

Angenehm / pleasant (lightblue):
- interessant
- toll
- optimal
- erfreulich
- schön
- glücklich
- freundlich
- entspannt
- optimal
- beeindruckend
- wundervoll
- fantastisch
- perfekt
- hervorragend
- herrlich
- friedlich
- Gut
- einfach
- bequem

Source: WIK, own illustration



WIK Wissenschaftliches Institut für
Infrastruktur und Kommunikationsdienste GmbH
Rhöndorfer Str. 68
53604 Bad Honnef, Germany
www.wik.org

ISSN 2750-5448 (Online)