Why Do Organizations Fail to Practice Cyber Resilience?

Rick van der Kleij[1,2(✉)] and Tineke Hof[1]

[1] TNO, The Hague, The Netherlands
Rick.vanderkleij@tno.nl
[2] Avans University of Applied Sciences, Den Bosch, The Netherlands

Abstract. When organizations fall victim to cyber incidents, they are exposed to financial implications, data losses, and potential damage to their reputation. However, the positive news is that many of these incidents can be avoided or have a smaller impact when basic cyber-resilience practices are followed. These practices can include simple actions like regularly updating software or implementing multi-factor authentication. Although these practices might seem simple, organizations are not always taking them despite their best intentions. This may be due to various barriers that hinder practicing cyber resilience. This study investigated why organizations are not practicing cyber resilience. Discussions were held with entrepreneurs in focus groups to understand their reasons for not running a cyber-resilient digital business. We also surveyed a panel of 795 Dutch entrepreneurs about cyber risks and underlying barriers to practicing cyber resilience. A regression model shows that a lack of knowledge, skills, environmental context and resources, and protection motivation intention appear to be the strongest barriers to practicing cyber resilience, closely followed by perceived response efficacy. Implications for government agencies and future research are discussed.

Keywords: Cyber-Resilience Practices · Cyber Security · Protective Measures · Behavioral Change Interventions · Digital Business Practices

1 Introduction

1.1 Minimizing the Imbalance Between Digital Threats and Resilience

Digital security is crucial for the safe and uninterrupted functioning of our society. The digital threat for organizations, however, remains as high as ever and changes continuously. The Cyber Security Assessment Netherlands (CSAN) 2023 issues a stark reminder through the authoritative voice of the National Coordinator for Counterterrorism and Security (NCTV): Organizations must brace themselves for the unforeseen and recalibrate their security accordingly (NCTV 2023). This digital age renders every organization and sector an enticing target for malevolent actors, transcending the traditional boundaries of vulnerability. Even seemingly inconspicuous entities become potential stepping stones for cyber adversaries aiming at more prominent prey. Furthermore, the NCTV continuously warns that cyberattacks compromise the nervous system of society, asserting that cyber resilience in our society is still insufficient, with a notable discrepancy in the level of resilience observed among organizations.

A. Moallem (Ed.): HCII 2024, LNCS 14728, pp. 126–137, 2024.
https://doi.org/10.1007/978-3-031-61379-1_9

Cyber resilience is a collective term encompassing various means and methods to combat cybercrime and enhance cybersecurity (Hoekstra, De Vries, Berkenpas & Jansen 2021). It is defined as the ability to prepare, absorb, recover, and adapt to adverse effects caused by a cybersecurity incident with the aim of maintaining critical functions continuously (Dupont, Shearing, Bernier, & Leukfeldt 2023; Linkov & Kottt 2019). In practical terms, it means that organizations need four capabilities to deliver cyber resilience: (1) anticipation, (2) monitoring, (3) response, and (4) learning (Van der Kleij & Leukfeldt 2019). This implies that cyber resilience is demonstrated when organizations know (a) what to expect, (b) what to look for, (c) what actions to take, and (d) what occurred in the event of a failure. Within this context, cyber-resilience measures aim to counter both known and unknown digital threats, while also focusing more reactively on swift and effective recovery from a cyber-incident.

Reducing the imbalance between digital threats and resilience remains a significant challenge. The EU aims for a future where this imbalance is minimized, and, at the same time, increases incentives for cyber resilience in digital markets by imposing stricter requirements on digital products and services, organizational risk management, and more. A cause for this imbalance in the Netherlands is the role of the government (Brennenraedts, Den Hertog, Kleter, Ott, Smeitink, Te Velde, & Vankan 2023). Unlike countries where the government heavily invests in cyber resilience, such as Israel and Estonia, the Netherlands prioritizes issues like climate and energy over cyber resilience. And whilst there are many subsidy opportunities in the cybersecurity domain in the Netherlands, they are not always fully utilized.

But there is more. When organizations fall victim to cyber incidents, they are exposed to financial implications, data losses, and potential damage to their reputation. However, the positive news is that many of these incidents can be avoided or have a reduced impact when protective cyber resilience measures are implemented. These measures can include simple actions like regularly updating software or implementing multi-factor authentication. Although these actions might seem simple, organizations are not always taking them despite their best intentions. Consequently, as mentioned above, the NCTV (2023) signals that there is a gap between organizations that have cyber resilience in order and those that do not. Organizations that lag behind need assistance in taking the right measures, such as implementing resilience management processes, enabling them to achieve an optimal level of cyber resilience. An optimal level of cyber resilience in this context refers to a level of cyber resilience appropriate for the risks to business operations and continuity of services, based on a sound risk assessment and balanced with the necessary investments to reach that level.

The challenge in closing the gap between the haves and haves-not is acute and requires a broader understanding of cyber resilience. There is little insight into relevant actors, dependencies, and mechanisms of cyber resilience and how they reverberate across cyber-resilience practices. It is also unclear how laggards can be encouraged to act appropriately to reduce this gap. This research seeks to explain why organizations fail to implement cyber-resilience measures.

1.2 Influencing Entrepreneurs to Run a Secure Digital Business

A crucial determinant of cyber resilience and, consequently, in adopting cyber resilience practices, lies in the behavior of individuals and groups within organizations. Examples of relevant behaviors in the context of this research include the extent to which management takes measures based on threat intelligence, invests in detection tools, and ensures that employees behave securely in the digital workplace. To explain these behaviors, behavioral influence models can be employed. An example is the Behavioral Change Wheel (see Michie, Van Stralen, & West 2011), which posits that behavior is driven by knowledge, opportunity, and motivation. Based on this model, we anticipate that the extent to which individuals and groups within organizations take appropriate measures to enhance cyber resilience depends on their knowledge of risks, ways to protect themselves, the opportunities available, and their motivation to act accordingly. This model also provides recommendations on how to influence cyber-resilience practices, and initial applications of this behavioral model in cyber security are promising (see, for example, Van der Kleij, Van't Hoff - De Goede, Van de Weijer, & Leukfeldt 2021; and Van der Kleij, Wijn, & Hof 2020).

As an initial exploration into the question of why organizations do not take measures to enhance their cyber resilience, and to provide for direction for the research, discussions were held with entrepreneurs in focus groups. In total, two group interviews were organized in 2022, involving 20 entrepreneurs from various sectors and working in companies of varied sizes, including self-employed individuals. The group interviews, conducted via Microsoft Teams, lasted approximately 2 h each. Entrepreneurs were recruited by the researchers through two different panels: the online DTC (Digital Trust Center) community and the entrepreneurial panel Ondernemersdenkenmee.nl, both affiliated with the Ministry of Economic Affairs and Climate. Entrepreneurs received a gift voucher as a token of appreciation for their participation.

Based on the results of the group interviews with entrepreneurs, and in line with behavioral influence models, we have formulated six explanations for why the people responsible for cyber resilience within their organization would practice unsafe digital business. These are:

- They do not see themselves as potential victims: Some entrepreneurs may not recognize the risk of digital threats and do not consider themselves potential targets of cybercriminals.
- They underestimate the consequences of cyber risks: There may be an underestimation of the consequences that may result from unsafe digital business practices.
- They do not know how to conduct cyber resilience practices: Entrepreneurs may be hindered by a lack of knowledge or guidelines on how to engage in safe digital business practices.
- They do not consider cyber resilience important: Some entrepreneurs may not place great importance on cyber resilience practices, perhaps due to other urgent business priorities.
- They do not consider taking cyber resilience measures their responsibility: There may be a perception that cyber resilience is the responsibility of others, such as the government.

- They lack the resources to take appropriate resilience measures: Entrepreneurs may be limited by a lack of social support or financial resources necessary for running a secure digital business.

This research endeavors to enhance our comprehension of the factors influencing the decisions made by individuals responsible for cyber resilience within organizations—specifically, why some take measures to bolster cyber resilience while others do not. To address this inquiry, we have undertaken a quantitative research approach, designed to test the explanations outlined earlier. In the subsequent sections of this paper, we will provide a detailed account of our research methodology, present and analyze the quantitative findings, and finally, engage in a comprehensive discussion on the implications derived from our work and directions for future research.

2 Method

2.1 Participants

A survey study was conducted among an adult sample of the Dutch general population. Participants were recruited, in conjunction with the researchers, by a panel agency. The panel is ISO-certified and consists of more than 70,000 active participants recruited online and offline. It is a good reflection of the Dutch population for characteristics such as education, age, gender, region, household composition, activity, and ethnicity.

The sample was realized as follows. Panel members were selected based on the following selection question: To what extent are you involved in cyber resilience within your company/organization. Respondents who were responsible for cyber resilience were selected for the survey. Based on this selection, we were able to achieve a net sample of n = 795 (co-)responsible/(co-)decision-makers for cyber resilience, spread across different company sizes and sectors. Participation was voluntary.

2.2 Measures

Dependent Variable: Cyber-resilience Practices. *Cyber-resilience practices.* Was considered as a dependent variable in this study. This variable was measured by presenting statements to the respondents related to taking cyber resilience measures in a business environment (11 items, Cronbach's $\alpha = .890$). The items were organized around the following 5 topics and adapted from the Dutch Digital Trust Center (DTC) Cyber-resilience scan (for more information, see: The five basic principles of running a secure digital business[1]): 1. Identify cyber risks; 2. Choose secure settings; 3. Install updates; 4. Limit access; 5. Prevent viruses and other malware. Answer options for each item were: always, often, sometimes, rarely, or never (5-point Likert-type scale) or not applicable. The highest score is assigned to the safest answer option for each statement.

[1] https://business.gov.nl/running-your-business/business-management/cyber-security/the-5-basic-principles-of-running-A-secure-digital-business/.

Independent Variables. For each of the six possible explanations for why the people responsible for cyber resilience within their organization would or would not take the appropriate measures to increase the level of cyber resilience, we searched in the literature for related constructs, validated measuring scales or items. Below we summarize the constructs that were used in this study.

They Do Not See Themselves as Potential Victims. To understand whether respondents see themselves as potential victims of cyber incidents we used *Perceived vulnerability*. This construct refers to the assessment of one's own vulnerability to a threat and was adapted from Van't Hoff-de Goede, Leukfeldt, Van der Kleij, and Van de Weijer (2021). It was measured with the following item: 'How likely do you think it is that your organization will fall victim to a cyber incident in the next 12 months?' This item involved a 7-point Likert scale to indicate a respondent's level of agreement with the statement regarding the likelihood of victimization.

They Underestimate the Consequences. The following 2 constructs were included in our study to assess how respondents interpret the consequences of unsafe digital business practices: *Perceived severity* and *Response efficacy*. *Perceived severity* was measured with 3 items (Cronbach's $\alpha = .878$) and refers to an individual's beliefs about the seriousness of consequences of an incident or situation (Champion & Skinner 2008, Dodel and Mesch 2017). An example question is: 'I believe that cyber incidents pose a serious problem for my organization.' *Response efficacy* was also measured with 3 items (Cronbach's $\alpha = .860$). This refers to beliefs as to whether the recommended action step will actually avoid the threat (Herath & Rao 2009). An example question is: 'Engaging in safe digital business practices reduces the likelihood of falling victim to a cyber incident.' Each item involved a 7-point Likert scale to indicate a respondent's level of agreement with the statements.

They Do Not Know How to Conduct Safe Digital Business Practices. To access if entrepreneurs may be hindered by a lack of knowledge or guidelines on how to engage in safe digital business practices, we included the constructs *Knowledge* and *Skills* in the questionnaire. Knowledge was measured with 2 items (Cronbach's $\alpha = .898$) based on Cane, O'Connor, and Michie (2012) and Connell, Carey, De Bruin, Rothman, Johnston, Kelly, and Michie (2019) and refers to an awareness of the existence of something. An example question is: 'I know how to do digital business safely.' Skills was measured with 2 items (Cronbach's $\alpha = .744$). This construct refers to an ability or proficiency acquired through practice (Connell, et al. 2019). Items were adapted from Huijg, Gebhardt, Dusseldorp et al. (2014) and Amemori, Michie, Korhonen, Murtomaa, and Kinnunen (2011). An example question is: 'I have the skills to conduct digital business safely.' Each item involved a 7-point Likert scale to indicate a respondent's level of agreement with the statements.

They Do Not Consider Safe Digital Business Practices Important. To understand the role of motivation, we used Protection motivation intention, Normative beliefs, Priority, and Intention to practice cybersecurity. Protection motivation intention is defined as the motivation of people to engage in protective behaviors and is measured with 2 items (Cronbach's $\alpha = .746$) adapted from Van't Hoff-de Goede et al. (2021). An example question is: 'We are willing to do everything to protect the organization against cyber

incidents.' Normative beliefs refer to the belief about whether most people approve or disapprove of the behavior. It relates to a person's beliefs about whether peers and people of importance to the person think he or she should engage in the behavior (Ajzen 1991). This construct is measured with 2 items (Cronbach's $\alpha = .771$). An example item is: 'We aspire to be a role model for other organizations in the field of safe digital business practices.' Priority refers to mental representations of outcomes or end states that an individual wants to achieve. Three items were adapted from Huijg et al. (2014) (Cronbach's $\alpha = .883$). An example item is: 'Other topics on the agenda have a higher priority than safe digital business practices.' The Intention to Practice Cyber Security construct was defined by Glanz, Rimer, Orleans, and Viswanath (2015) as a reflective variable consisting of expectations, plans, and desires to perform a particular behavior. To measure people's intentions or willingness to engage in safe digital business practices 2 items (Cronbach's $\alpha = .859$) were adapted from Alanazi, Freeman, and Tootell (2022). An example item is: 'Our organization intends to take measures in the next 12 months to enhance cyber resilience.' A 7-point Likert type scale was used for most variables, except for priority, ranging from 'completely disagree' to 'completely agree', with the highest score always being assigned to the safest answer option. A 5-point Likert type scale was used for Priority.

They Do Not Consider Safe Digital Business Practices Their Responsibility. To understand the role of responsibility, one construct was used in our study. Two *Locus of control* items were adopted from Workman, Bommer, and Straub (2008). These items attempted to gauge individual's belief that he/she is personal responsible for cyber resilience within their organization (internal) or the control of others (external). But due to insufficient internal reliability (Cronbach's $\alpha = .49$) both items could not be combined into a single scale. Consequently, each item was treated as a separate construct. Locus of control was measured with the following sliding-scale item: 'To what extent do you agree that safe digital entrepreneurship is outside the control of your organization (as opposed to within the control of your organization)?' *Perceived responsibility* was measured with the following sliding-scale item: 'Safe digital business practices are the responsibility of my organization (as opposed to others).'

They Lack the Resources to Engage in Safe Digital Business Practices. The construct *Environmental context and resources* was used in the study to investigate whether respondents lack the resources to practice cyber resilience. The construct was measured with 3 items (Cronbach's $\alpha = .739$) and was defined as 'aspects of a person's situation or environment that discourage or encourage the behavior' (Connell et al. 2019). Items were adapted from Van der Kleij et al. (2021). An example item is: 'My organization has sufficient financial resources to conduct safe digital business.' Each item involved a 7-point Likert scale to indicate a respondent's level of agreement with the statements.

Table 1. Scale ranges, means, and standard deviations.

#	Variable	Scale range	Mean	SD
1	Cyber-resilience practices	1–7	5.38	0.93
2	Knowledge	1–7	5.14	1.17
3	Skills	1–7	4.80	1.28
4	Priority	1–5	2.85	0.83
5	Perceived severity	1–7	3.60	1.49
6	Environmental context and resources	1–7	4.85	1.23
7	Protection motivation intention	1–7	5.02	1.20
8	Normative beliefs	1–7	4.52	1.44
9	Intention to practice cyber security	1–7	4.71	1.35
10	Response efficacy	1–7	5.38	1.08
11	Locus of control	1–7	5.21	1.45
12	Perceived responsibility	1–7	2.91	1.74
13	Perceived vulnerability	1–7	3.56	1.47

Control Variables. To explicitly consider the possible effects of being self-employed (41%), outsourcing IT services (including cybersecurity) (53.6%), economic activities[2], victimization in the past 12 months (11.4%), and level of digitalization[3], we controlled for these variables in all analyses.

2.3 Analysis

In this study, two types of analyses were conducted. Firstly, bivariate relationships between all variables were estimated using Pearson correlations. Secondly, multivariate regression analyses were employed to estimate the multivariate relationships, incorporating control variables as mentioned above.

3 Results

3.1 Descriptive Statistics

The scale ranges, means, and standard deviations of the dependent and independent variables are presented in Table 1. Pearson correlation was used to assess the relationship among all study variables. The relationship between the dependent variable and all independent variables was statistically significant. Interestingly, respondents who

[2] The list of economic activities was based on the Standard Industrial Classifications (Dutch SBI 2008, NACE and ISIC).

[3] A 5-point Likert type scale was used ranging from ‘not digitized’ to ‘completely digitized’.

perceive cyber resilience as the responsibility of others tend to report a higher level of cyber-resilience practices ($r = .17$; $p < .01$). Also, the higher the estimated likelihood of becoming a victim, the more likely respondents are to practice cyber resilience ($r = .08$; $p < .05$). Additionally, companies that have been victims of an incident in the past year report cyber-resilience practices more often than those that have not been victims ($r = .09$; $p < .01$). Furthermore, there is a noticeable positive relationship between company size and cyber-resilience practices. Sole proprietors are practicing cyber resilience to a lower extent than larger companies ($r = .15$; $p < .01$).

3.2 Multivariate Regression Analysis

The results of the multivariate regression analysis are presented in Table 2. We tested one model that included all variables, including control variables. All variables together explain 64% of the variance in cyber-resilience practices, which can be considered an impressive result.

The model shows that the control variables for self-employed worker ($B = 0.137$; $p = 0.015$) and the level of digitization ($B = 0.076$; $p = 0.004$) are related to our dependent variable. Outsourcing of IT services is negatively related ($B = -0.121$; $p = 0.020$). This implies that larger organizations, organizations that are more digitalized, and organizations that are not outsourcing IT services are taking more cyber resilience measures. The economic sector in which a company operates is not related to practicing cyber resilience.

Of the assumed barriers of taking cyber resilience measures, lack of knowledge ($B = 0.221$; $p = 0.000$), skills ($B = 0.139$; $p = 0.000$), environmental context and resources ($B = 0.131$; $p = 0.000$), protection motivation intention ($B = 0.149$; $p = 0.000$), and response efficacy ($B = 0.081$; $p = 0.006$) are indeed significantly explaining variance of the dependent variable. This means that the people responsible for cyber resilience within their organization who better understand what they need to do, are more capable of practicing cyber resilience, have more resources at their disposal, are more willing to take these measures, and more strongly belief that this helps to mitigate threats, are more often practicing cyber resilience. The coefficients of normative beliefs and perceived vulnerability are marginally significant and strong conclusions cannot be drawn on their basis.

Table 2. Results of multivariate regression analysis for practicing cybersecurity behavior.

	B	*SE*	t	Sig
(Constant)	0.934	0.263	3.549	0.000
Knowledge	0.221	0.036	6.089	0.000
Skills	0.139	0.035	4.006	0.000
Priority	0.044	0.031	1.394	0.164
Perceived severity	0.036	0.022	1.644	0.101
Environmental context and resources	0.131	0.028	4.646	0.000
Protection motivation intention	0.149	0.033	4.459	0.000
Normative beliefs	0.052	0.027	1.908	0.057
Intention to practice cyber security	0.034	0.024	1.420	0.156
Response efficacy	0.081	0.029	2.783	0.006
Locus of Control	0.003	0.020	0.132	0.895
Responsibility	0.024	0.017	1.394	0.164
Perceived vulnerability	−0.040	0.021	−1.890	0.059
Victimization in the past 12 months (vs NO)	0.071	0.083	0.853	0.394
Self-employed (vs NO)	0.137	0.056	2.440	0.015
Manufacturing & energy (vs Agri & Mining)	−0.021	0.192	−0.110	0.913
Construction (vs Agri & Mining)	−0.164	0.185	−0.890	0.374
Wholesale, retail trade & food serving (vs Agri & Mining)	−0.190	0.163	−1.166	0.244
Publishing & telecommunication (vs Agri & Mining)	−0.110	0.166	−0.662	0.508
Financial & insurance services (vs Agri & Mining)	−0.032	0.169	−0.189	0.851
Real estate activities (vs Agri & Mining)	−0.131	0.197	−0.664	0.507
Professional & support service activities (vs Agri & Mining)	−0.197	0.159	−1.237	0.216
Public administration (vs Agri & Mining)	-0.076	0.215	−0.353	0.724
Education (vs Agri & Mining)	0.036	0.179	0.199	0.842
Health care & social work (vs Agri & Mining)	−0.014	0.169	−0.080	0.936

(*continued*)

Table 2. (*continued*)

	B	*SE*	t	Sig
Arts, sports & recreation (vs Agri & Mining)	−0.097	0.184	−0.524	0.600
Other service activities (vs Agri & Mining)	−0.130	0.169	−0.768	0.443
Outsourcing IT services (vs YES)	−0.121	0.052	−2.325	0.020
Digitalization	0.076	0.027	2.877	0.004

Notes. $R^2 = 64\%$; $N = 795$; B = unstandardized regression coefficient; SE = standard error.

4 Discussion

When analyzing the reasons why the people responsible for cybersecurity within their organizations fail to take the necessary measures for better protection, this research reveals a diverse range of justifications. Some lack the knowledge and skills required to implement the necessary measures. For instance, they may not know how or where to start, or where to find this knowledge. There may also be contextual factors that discourage practicing cyber resilience, including a shortage of suitable talent, insufficient funds for acquiring cybersecurity tools, or a lack of encouragement from leadership to invest (see also Pawar & Palivela 2022). Moreover, certain ingrained beliefs or myths about cybersecurity can hinder safe digital business practices. For instance, entrepreneurs might be unmotivated to take measures because they underestimate the consequences of neglecting cyber resilience or do not perceive safe digital business practices as crucial. Low motivation can also be attributed to a lack of cybersecurity training and persistent misinformation (O'Donnell 2022).

This research provides a deeper understanding of why lagging companies are not adopting adequate cyber resilience measures. It also highlights the crucial role of psychology in addressing barriers to cyber resilience practices within organizations. Behavioral models offer insights into how individuals responsible for cyber resilience perceive and respond to cyber risks. This understanding is essential for developing behavioral change interventions that effectively address these barriers and resonate with those overseeing cyber resilience. Principles from behavioral economics, such as incentives and nudges, can be employed to motivate entrepreneurs to adopt cyber-resilient practices. Positive reinforcement and rewards can influence compliance with cyber resilience guidelines.

Future research should delve into identifying specific intervention functions that are likely to be effective in promoting the widespread adoption of effective cyber resilience practices within organizational settings. While our current findings shed light on various barriers, a more nuanced exploration is needed to understand the intricacies of these challenges and design targeted solutions. The group interviews conducted as part of this study have unveiled differences in the channels entrepreneurs use to inform themselves about cybersecurity. This emphasizes the necessity of adopting a tailor-made approach in the development of interventions. Recognizing these diverse information sources will

be crucial in crafting strategies that are accessible and resonate with a broad spectrum of entrepreneurs. It is imperative to assess the effectiveness of these interventions over time, taking into consideration evolving cyber threats and technological advancements.

In conclusion, future research endeavors should aim for a comprehensive understanding of the intricate dynamics surrounding the adoption of cyber resilience practices within organizations. This involves further exploring intervention strategies, considering the evolving threat landscape, and recognizing the influence of organizational culture and leadership commitment. This nuanced approach will contribute to the development of targeted, effective, and sustainable cyber resilience practices in diverse organizational settings.

Acknowledgements. The authors would like to thank Silke Mergler for her help with the project administration, funding acquisition, and conceptualization of the research. We thank Martin Muller and Bram van der Lelij with their help in collecting and analyzing the data. This work was funded by the Digital Trust Center (DTC) of the Dutch Ministry of Economic Affairs and Climate Policy.

References

1. Ajzen, I.: The theory of planned behavior. Organ. Behav. Hum. Decis. Process. **50**(2), 179–211 (1991)
2. Alanazi, M., Freeman, M., Tootell, H.: Exploring the factors that influence the cybersecurity behaviors of young adults. Comput. Hum. Behav. **136**, 107376 (2022)
3. Amemori, M., Michie, S., Korhonen, T., Murtomaa, H., Kinnunen, T.: Assessing implementation difficulties in tobacco use prevention and cessation counselling among dental providers. Implement Sci. **6**, 50–10 (2011). 1186/1748-5908-6-50
4. Brennenraedts, R., et al.: De economische kansen van de cybersecuritysector. Report 2022.130.2308. Dialogic. The Netherlands, Utrecht (2023)
5. Cane, J., O'Connor, D., Michie, S.: Validation of the theoretical domains framework for use in behaviour change and implementation research. Implement. Sci. **7**, 37 (2012). https://doi.org/10.1186/1748-5908-7-37
6. Champion, V.L., Skinner, C.S.: The health belief model. Health Behav. Health Educ. Theory Res. Pract. **4**, 45–65 (2008)
7. Connell, L.E., et al.: Links between behavior change techniques and mechanisms of action: an expert consensus study. Ann. Behav. Med. **53**(8), 708–720 (2019)
8. Dodel, M., Mesch, G.: Cyber-victimization preventive behavior: a health belief model approach. Comput. Hum. Behav. **68**, 359–367 (2017)
9. Dupont, B., Shearing, C., Bernier, M., Leukfeldt, R.: The tensions of cyber-resilience: from sensemaking to practice. Comput. Secur. **132**, 103372 (2023)
10. Glanz, K., Rimer, B.K., Orleans, C.T., Viswanath, K.: Health Behavior and Health Education Theory, Research, and Practice, 4th edn. Jossey-Bass, USA (2015)
11. Herath, T., Rao, H.R.: Protection motivation and deterrence: a framework for security policy compliance in organisations. Eur. J. Inf. Syst. **18**, 106–125 (2009)
12. Hoekstra, M., De Vries, S., Berkenpas, M., Jansen, J.: De werking van de basisscan cyberweerbaarheid. Thorbecke academie, NHL Stenden (2021)
13. Huijg, J.M., Gebhardt, W.A., Dusseldorp, E., et al.: Measuring determinants of implementation behavior: psychometric properties of a questionnaire based on the theoretical domains framework. Implementat. Sci. **9**, 33 (2014). https://doi.org/10.1186/1748-5908-9-33

14. Linkov, I., Kott, A.: Fundamental concepts of cyber resilience: introduction and overview. In: Kott, A., Linkov, I. (eds.) Cyber Resilience of Systems and Networks, pp. 1–25 (2019)
15. Michie, S., Van Stralen, M.M., West, R.: The behaviour change wheel: a new method for characterising and designing behaviour change interventions. Implement. Sci. **6**(1), 42 (2011)
16. Michie, S., Johnston, M.: Behavior change techniques. In: Gellman, M.D., Turner, J.R. (eds.) Encyclopedia of Behavioral Medicine, pp. 182–187. Springer, New York (2013). https://doi.org/10.1007/978-1-4419-1005-9_1661
17. NCTV: Cyber Security Assessment Netherlands 2023. Expect the unexpected. Ministry of Justice and Security, 9 January 2023. https://english.nctv.nl/documents/publications/2023/07/03/cyber-security-assessment-netherlands-2023
18. O'Donnell, B.: 5 cybersecurity myths and how to address them. Techtarget, 16 March 2022. https://www.techtarget.com/whatis/post/5-cybersecurity-myths-and-how-to-address-them
19. Pawar, S., Palivela, H.: LCCI: a framework for least cybersecurity controls to be implemented for small and medium enterprises (SMEs). Int. J. Inf. Manag. Data Insights **2**(1), 100080 (2022)
20. van der Kleij, R., Leukfeldt, R.: Cyber resilient behavior: integrating human behavioral models and resilience engineering capabilities into cyber security. In: Ahram, T., Karwowski, W. (eds.) AHFE 2019. AISC, vol. 960, pp. 16–27. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-20488-4_2
21. van der Kleij, R., van't Hoff-De Goede, S., van de Weijer, S., Leukfeldt, R.: How safely do we behave online? An explanatory study into the cybersecurity behaviors of dutch citizens. In: Zallio, M., Raymundo Ibañez, C., Hernandez, J.H. (eds.) AHFE 2021. LNNS, vol. 268., pp. Springer, Cham (2021). https://doi.org/10.1007/978-3-030-79997-7_30
22. Van der Kleij, R., Wijn, R., Hof, T.: An application and empirical test of the capability opportunity motivation-behaviour model to data leakage prevention in financial organizations. Comput. Secur. **97**, 101938 (2020). https://doi.org/10.1016/j.cose.2020.101970
23. van't Hoff-de Goede, M.S., Leukfeldt, E.R., van der Kleij, R., van de Weijer, S.G.A.: The online behaviour and victimization study: the development of an experimental research instrument for measuring and explaining online behaviour and cybercrime victimization. In: Weulen Kranenbarg, M., Leukfeldt, R. (eds.) Cybercrime in Context. Crime and Justice in Digital Society, vol. I, pp. 21–41 . Springer, Cham (2021). https://doi.org/10.1007/978-3-030-60527-8_3
24. Workman, M., Bommer, W.H., Straub, D.: Security lapses and the omission of information security measures: a threat control model and empirical test. Comput. Hum. Behav. **24**(6), 2799–2816 (2008)