Cyber Resilient Behavior: Integrating Human Behavioral Models and Resilience Engineering Capabilities into Cyber Security

Rick van der Kleij[1,2](✉) and Rutger Leukfeldt[1,3]

[1] Cybersecurity and SMEs Research Group,
The Hague University of Applied Sciences (THUAS),
The Hague, The Netherlands
{R.vanderkleij,E.R.Leukfeldt}@hhs.nl
[2] Department of Human Behavior and Organisational Innovations,
The Netherlands Organisation for Applied Scientific Research (TNO),
The Hague, The Netherlands
[3] Netherlands Institute for the Study of Crime and Law Enforcement (NSCR),
Amsterdam, The Netherlands

Abstract. Cybercrime is on the rise. With the ongoing digitization of our society, it is expected that, sooner or later, all organizations have to deal with cyberattacks; hence organizations need to be more cyber resilient. This paper presents a novel framework of cyber resilience, integrating models from resilience engineering and human behavior. Based on a pilot study with nearly 60 small and medium-sized enterprises (SMEs) in the Netherlands, this paper shows that the proposed framework holds the promise for better development of human aspects of cyber resilience within organizations. The framework provides organizations with diagnostic capability into how to better prepare for emerging cyber threats, while assuring the viability of human aspects of cyber security critical to their business continuity. Moreover, knowing the sources of behavior that predict cyber resiliency may help in the development of successful behavioral intervention programs.

Keywords: Security behaviors · Human aspects of cyber security · Cyber hygiene behavior

1 Introduction

Every day, companies all over the world suffer cyberattacks. The number of cyberattacks on organizations worldwide has been growing over the last six years to an average of 2.5 attacks every week for large organizations [1]. Based on 2,182 interviews from 254 companies in seven countries, the Ponemon institute [1] calculated that the average cost of cybercrime in 2017 was 11.7 million US dollars per organization. These costs are internal, dealing with cybercrime and lost business opportunities, and external, including the loss of information assets, business disruption, equipment damage and revenue loss. With the ongoing digitization of our society, it is expected that the number of cyberattacks and, consequently, the annual costs of cybercrime, will increase rapidly over the next years.

T. Ahram and W. Karwowski (Eds.): AHFE 2019, AISC 960, pp. 16–27, 2020.
https://doi.org/10.1007/978-3-030-20488-4_2

Organizations are often unprepared to face cyberattacks, to recover from attacks and lack formal incident response plans [2]. Only 32% of IT and security professionals say that their organization has a high level of *cyber resilience*, and this number is decreasing. A recent development is that security breaches are becoming more damaging to organizations, thus accelerating the need for cyber resilience [3]. As it is expected that the number of cyberattacks will also grow in the near future, the notion that organizations need to be cyber resilient is becoming increasingly popular [4]. This notion has been put forward in perspectives from multiple disciplines, including systems engineering, auditing and risk assessment. The general idea is that instead of focusing all efforts on keeping criminals out of company networks, it is better to assume they will eventually break through the organizations' defenses, and to start working on increasing cyber resilience to reduce the impact[1]. In order to ensure resilience, it is necessary to first accurately define and measure it [4]. There is, however, still a lot of confusion about what the term resilience means [5].

The notion that organizations need to be more cyber resilient is quite a recent one and, because most reports have been published by consultancy firms, commercial companies, and private research institutes working on behalf of these businesses, the scope of the scientific literature in this particular domain is fairly limited. The review of these few studies shows, however, that cyber resilience, and organizational resilience more broadly, is an emerging field [6]. Further, as pointed out by Parsons and colleagues [7], the study of this emerging field has predominantly been focused on the technical issues of cyber resilience. Consequently, measures to enhance cyber resiliency are mainly focused on improving the existing security infrastructure. It is only recently, with some exceptions, that researchers have started looking at the human aspects as potential sources of organizational resilience [8–10].

The human aspects as potential sources of organizational resilience should not be underestimated. It is a well-established fact that in many cyberattacks the behaviors of employees are exploited [11–13]. Regardless of how secure a system is, the end user is often a critical backdoor into the network [14–16]. Attackers look for vulnerabilities to gain access to systems; these can come from users who exhibit cyber risky behaviors, such as by not following best practices or revealing too much personal information on social networking sites. Hence, cyber resilience includes protecting against harm that may come due to malpractice by insiders, whether intentional or accidental. Furthermore, employees can perform many different behaviors to protect themselves and their organization from computer security threats [17]. Through good practice or cyber hygiene behavior, such as using strong passwords and responding adequately to incidents, employees may help the organization to become more cyber resilient (see also [9, 18–20]). Against this background, this paper aims to (1) develop a novel comprehensive and coherent framework of cyber resilience integrating models from resilience engineering and human behavior, and (2) to test this framework in a pilot study with 56 small and medium-sized enterprises (SMEs) in the Netherlands. And although this paper focuses on the human aspects of cyber security, it also acknowledges that technological factors play an important role in cyber security at the organizational level.

[1] https://www.itgovernance.co.uk/cyber-resilience.

This paper is structured as follows. First, we start by giving an overview of current views on resilience. Then we discuss abilities necessary for resilience at the organizational level and show that these abilities are relevant in the domain of cyber security as well. We then combine a framework for understanding human behavior with a resilience engineering model and discuss a combined model of resilient behavior. Next, we describe how the framework was operationalized into a questionnaire to measure resilient behavior within the domain of cyber security and present the results of a small empirical test of the framework and instrument. We conclude with a discussion of our work and give directions for future research.

2 Resilience

Research on resilience has increased substantially over the past decades, following dissatisfaction with traditional models of risk and vulnerabilities, which focus on the results of adverse events [21]. Whereas traditional risk models have historically been useful for many applications in the past, it is difficult to apply them to cyber risks [4, 22]. Traditional risk assessment approaches tend to break down when it is difficult to clearly identify the threats, assess vulnerabilities, and quantify consequences [23, 24]. Cyber threats cannot be clearly identified and quantified through historical measures due to the rapidly changing threat environment [4]. Resilience, however, focuses on the ability to succeed under varying conditions.

Resilience was first used in medical and material sciences, relating to the ability to recover from stress or strain [25]. More recently a wider concept of resilience has emerged. Within the domain of health sciences, the Resilience and Healthy Ageing Network defined resilience as “the process of negotiating, managing and adapting to significant sources of stress or trauma. Assets and resources within the individual, their life and their environment facilitate this capacity for adaptation and ‘bouncing back’ in the face of adversity. Across the life course, the experience of resilience will vary” ([21], p. 2).

Matzenberger [25] defines resilience in a learning environment as the capacity or ability of a system to persist after disturbance and to reorganize or emerge while sustaining essentially the same function. In hazards research, resilience is understood as the ability to survive and cope with a disaster with minimum impact and damage. It holds the capacity to reduce or avoid losses, contain effects of disasters, and recover with minimal disruptions [25, 26]. In resilience engineering, a new approach to risk management, resilience is described at the generic system level as the intrinsic ability of a system to adjust its functioning prior to, during, or following changes and disturbances, so that it can sustain required operations under both expected and unexpected conditions [27]. Van der Beek and Schraagen [28] have defined resilience at the team level in crisis management situations by expanding the ability of a system with more relation-oriented abilities of leadership and cooperation.

The key term to all these definitions is the system’s ability to adjust its functioning. Resilience represents the capacity (of an organizational system) to anticipate and manage risk effectively, through appropriate adaptation of its actions, systems and processes, so as to ensure that its core functions are carried out in a stable and effective relationship with the environment [29]. Although these definitions at a glance mainly seem to differ in level of analysis, ranging from the individual via the team level to the more generic organizational (system) level, Woods [5] argues that resilience is used in four different ways: (1) resilience as rebound from trauma and return to equilibrium; (2) resilience as a synonym for robustness; (3) resilience as the opposite of brittleness, i.e., as graceful extensibility when surprise challenges boundaries; (4) resilience as network architectures that can sustain the ability to adapt to future surprises as conditions evolve. The implication of this partition is that one needs to be explicit about which of the four senses of resilience is meant when studying or modeling adaptive capacities (or to expand on the four anchor concepts as new results emerge) [5]. Not all these uses of the label 'resilience' are correct according to Woods. Resilience as the increased ability to absorb perturbations confounds the labels robustness and resilience. Some of the earliest explorations of resilience confounded these two labels, and this confound continues to add noise to work on resilience [5].

The broad working definitions of resilient performance can be made more precise and operational by considering what makes resilient performance possible. Since resilient performance is possible for most, if not all, systems, the explanation must refer to something that is independent of any specific domain. Hollnagel [30] has proposed the following four abilities necessary for resilient performance (see also [27]):

- The ability to *Anticipate*. Knowing what to expect or being able to anticipate developments further into the future, such as potential disruptions, novel demands or constraints, new opportunities, or changing operating conditions. This is the ability to create foresight and to address the potential.
- The ability to *Monitor*. Knowing what to look for or being able to monitor that which is or could seriously affect the system's performance in the near term, positively or negatively. The monitoring must cover the system's own performance as well as what happens in the environment. This is the ability to address the critical.
- The ability to *Respond*. Knowing what to do, or being able to respond to regular and irregular changes, disturbances, and opportunities by activating prepared actions or by adjusting current modes of functioning. It includes assessing the situation, knowing what to respond to, finding or deciding what to do, and when to do it. This is the ability to address the actual.
- The ability to *Learn*. Knowing what has happened, or being able to learn from experience, in particular to learn the right lessons from the right experience, successes as well as failures. This is the ability to address the factual. Although this capacity is often overlooked, it is a critical aspect of resilience. By learning how to be more adaptable, systems are better equipped to respond when faced with some sort of disruption [25].

Hence, the resilience of a system is defined by the abilities to respond to the actual, to monitor the critical, to anticipate the potential, and to learn from the factual [27]. The abovementioned abilities can be thought of together as a framework for identification and classification of indicators [25]. The engineering of resilience comprises the ways in which these four capabilities can be established and managed [27]. This is of importance to organizations because being resilient can provide them with a competitive advantage [31]. Resilient organizations may also contribute to a cyber-resilient community or to more cyber resiliency at the nationwide level. McManus [32] argues that resilient organizations contribute directly to the speed and success of community resilience. Without critical services provided by resilient organizations, such as transport, healthcare and electricity, communities (or states alike) cannot respond or recover (see also [33]).

Although these four capabilities have been under debate for quite some time, and research at the employee [34] and team level [28] only partially support the four-dimensional nature of the construct as proposed by Hollnagel [27], we feel that these four dimensions have high face validity in the domain of cyber security. For instance, the recently completed NIST framework for improving Critical Infrastructure Cybersecurity encompasses five similar functions [35]. These five functions are Identify, Protect, Detect, Respond, and Recover. They aid an organization in expressing its management of cybersecurity risk by organizing information, enabling risk management decisions, addressing threats, and improving by learning from previous activities. The functions also align with existing methodologies for incident management and help show the impact of investments in cybersecurity. For example, investments in planning and exercises support timely response and recovery actions, resulting in reduced impact to the delivery of services.

We feel that the four abilities as proposed by Hollnagel [27] together seem to be sufficient without being redundant. We see no need, for instance, to split the function Anticipate into the NIST functions of Identify and Protect. We think that the Protect function, in which appropriate safeguards are developed and implemented to ensure delivery of critical infrastructure services, is a composite rather than a primary ability of a resilient organization. Implementing appropriate safeguards is a combination of the ability to Anticipate and to Learn, and possibly also the ability to Detect (see also, [30]). Moreover, the Identify function has a strong focus on understanding the contexts and the risks, while Anticipate also looks at opportunities and emerging threats. We also feel that the Recover function, to develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident, is essential, but again, we do not think of this ability as a primary function. This function is the consequence of another ability, namely Learning. For sustainable recovery to take place within organizational systems, organizations should have knowledge of what has happened, or should be able to learn from experience.

3 Human Behavior

There is an important role for employees within organizations to help the organization become more cyber resilient. In principle, one could easily envisage employees performing Monitoring, Responding, Anticipating and Learning functions to maintain resilience in cyber capabilities. To explain the four resilience functions from a behavioral perspective, a comprehensive framework for understanding human behavior can be applied that involves three essential conditions: Motivation, Opportunity, and Ability (MOA) [36]. The cyber resiliency of an organization is in part determined by employees' motivation, opportunity, and ability to perform the four generic resilience functions (see also [36]). In a recent application of this framework, capability, opportunity, and motivation interact to generate behavior, such as responding to a cyber-security incident, that in turn influences these components (the 'COM-B' system, see [37]). "Capability is defined herein as the individual's psychological and physical capacity to engage in the activity concerned. It includes having the necessary knowledge and skills. Motivation is defined as all those brain processes that energize and direct behavior, not just goals and conscious decision-making. It includes habitual processes, emotional responding, as well as analytical decision-making. Opportunity is defined as all the factors that lie outside the individual that make the behavior possible or prompt it" ([37], p. 4). Examples of Opportunity are social support and organizational climate.

Although we do not oppose the idea that the capacity to be resilient depends on the technical infrastructure of an organization, we believe that a key component of being resilient and for assessing the resilient capacity of organizations resides, for a large part, at the individual employee level. Employees need to have the psychological and physical *abilities* to act in a cyber-resilient manner. Further, employees need to have the right mindset to do so. They need to be *motivated* to behave in a cyber-resilient manner. Finally, the organization needs to provide *opportunities* to enable the desired behavior. People can be capable and motivated to behave in a resilient manner, but when there is no opportunity to do so within the organization, for instance because resources are lacking (e.g., a backup and restore system), these intentions remain in vain.

An important reason for us to utilize the COM-B system to explain resilience functions from a behavioral perspective, is that this system is part of a larger framework of behavior change interventions. Based on a systematic review of literature, Michie and colleagues [37] identified nine generic intervention functions. The nine intervention functions are aimed at addressing deficits in one or more of the conditions: capability, opportunity, and motivation. These functions are explicitly linked to one of more of these conditions. An example is 'persuasion': Using communication to induce positive or negative feelings or stimulate action. Furthermore, seven policy categories were identified that could enable those interventions to occur. An example is 'regulation', or, in other words, establishing rules or principles of behavior or practice. This means that the framework proposed in Sect. 4 hereafter, although not explicitly embedded, holds the power to link intervention functions and policy categories to an analysis of the targeted cyber resilient behavior of employees within organizations. Thus, in the context of cyber security, the framework could serve the need for more 'fit for purpose interventions' to change human cyber behavior, as stipulated by Young and colleagues [13]. For instance, when lack of motivation hinders resilient functioning of an organization, a suitable intervention function could be to apply 'modelling': providing an example for people to aspire to or imitate. A policy category that could be used to enable modeling is 'marketing': Using print, electronic, telephonic or broadcast media. Just by identifying all the potential intervention functions and policy categories this behavior change framework could prevent policy makers and intervention designers from neglecting important options [37].

4 Conceptual Framework of Resilient Behavior

It is important to be able to measure cyber resilience. Metrics can contribute to key organizational needs, such as the need to demonstrate progress towards becoming more resilient, the need to demonstrate the effects of an intervention, or the need to link improvements in resilience with increased competitiveness [33]. As we have argued, resilience metrics could also contribute to the design of successful behavior change programs. Interventions could be tailored to the specific needs of the organization based on diagnosed sources of non-resilient behavior.

In this paper, we have combined the definitions of the four resilience functions and the three sources of behavior to create a conceptual framework of resilient behavior (see Table 1). We then tailored the model to cyber security by drawing upon metrics from the cyber security literature, primarily from [38, 39] and [9]. Further, because the aim is to measure employees' motivation, opportunity, and ability to perform the four generic resilience functions, the framework was operationalized into a questionnaire: The Cyber Resilient Behavior Questionnaire.

For each of the four resilience functions, we developed several specific capability statements, opportunity statements and motivation statements. For example, the following statements measure the function 'Respond':

Capability: "Employees in our organization know what to do in the event of cybercrime."

Opportunity: "In the event of cybercrime, our organization has clearly defined procedures on how to deal with disruptions to business operations."

Motivation: "Employees in our organization consider the ability to respond to cybercrime as something important."

5 Pilot Study

An initial version of the Cyber Resilient Behavior Questionnaire was refined based on experts' feedback and on validity testing of the survey on a small group of SMEs. The revised instrument has 42 statements, measured on a six-point Likert-type scale with no mid-point (ranging from strongly disagree to strongly agree). Even-numbered Likert scales force the respondent to commit to a certain position even if the respondent may not have a definite opinion [40]. Statements assess capacity, opportunity, and motivation regarding the performing of resilient functions to anticipate, monitor, respond, and learn within the organizational context. The statements focus predominantly on positive protective intentions of employees. This focus was chosen because respondents are probably willing to reveal these behaviors in a survey, yielding usable and reliable data (see also [19]). To reduce the chance of response bias, which is the tendency to favor one response over others [41], an - 'I do not know' - option was included for each statement. To further avoid response bias, both positively- and negatively-worded items were used in the survey [42]. Negatively-worded items may act as "cognitive speed bumps that require respondents to engage in more controlled, as opposed to automatic, cognitive processing" [43].

Table 1. Conceptual framework of resilient behavior. The left column shows the four generic resilience functions. The consecutive columns specify the abilities for resilient behavior for each of the three sources of behavior

	Capability	Opportunity	Motivation
Anticipate	Knowing what to expect	Having resources to look for developments further into the future	Willing to look for potential disruptions, novel demands or constraints, new opportunities, or changing operating conditions
Monitor	Knowing what to look for	Having resources to monitor the system's own performance as well as what happens in the environment	Willing to monitor that which is or could seriously affect the system's performance in the near term, positively or negatively
Respond	Knowing what to do	Having resources that help in taking prepared actions	Willing to respond to regular and irregular changes, disturbances, and opportunities
Learn	Knowing what has happened	Having resources to learn the right lessons from the right experience	Willing to learn from experience

Next, a pilot study was conducted, and the results were examined to identify any remaining problematic items and to establish the reliability of the main components of the survey. A total of 56 SME employees completed the pilot version of our instrument. All were high-level representatives at different SMEs. Cronbach's alpha was used as a measure of the internal consistency of the survey. This refers to the degree to which the items measure the same underlying construct, and a reliable scale should have a Cronbach's alpha coefficient above 0.70 [44]. Cronbach's alpha coefficients for each of the four main functions (i.e., Anticipate, Monitor, Respond, and Learn) all exceeded this recommended value. A series of Pearson product moment correlations were calculated to further assess the relationship between the items used to create the three main constructs. An examination of the correlation matrices revealed that all items significantly correlated at 0.3 or above with the other items in that construct.

Although the main focus of the pilot study was to test the instrument and the framework, the survey also included a set of questions concerning the incidence of cybercrime and victimization. Respondents were asked if their SME had been confronted over the last 12 months with cyberattacks and whether harms or costs were involved. We now present some preliminary results from our survey.

Almost half of the SMEs in our sample (48% or 22 SMEs) had been the victim of at least one cyberattack in the last 12 months. Phishing (32%) and viruses (11%) were reported most. Seven SMEs (12%) reported that damage was caused, for instance in the form of financial damage or business disruption. The overall score for cyber resilience of the SMEs was considered poor to average. SMEs scored 3.5 on the six-point Likert type scale. SMEs in our sample were best at responding to cyberattacks, and worst at learning from attacks (3.7 and 3.2, respectively). Because of the small sample size, no analyses were performed at the behavioral level for each of these functions. Nevertheless, this pilot study clearly shows that there is ample room for improvement in the cyber resiliency of the SMEs in our sample.

6 Discussion and Way Ahead

The cyber security field is in need of techniques to evaluate and compare the security design of organizations [8]. Many techniques have been proposed and explored, but these typically focus on auditing systems and technologies rather than on people. Our work is aimed at measuring cyber resilience of organizations through its employees rather than just with the technologies on which they rely [33]. Our framework gives an overview of relevant cyber resilient behaviors of employees within organizations. Accordingly, our conceptual framework allows for better development of human aspects of cyber resilience. It provides organizations with diagnostic capability to better prepare themselves for emerging cyber threats, while assuring the viability of those cyber assets critical to their business continuity [45]. Moreover, knowing what sources of behavior play a role in being cyber resilient, may help in the development of successful behavior change intervention programs. In future work, investigating how to link behavior change interventions to resilient behavior of employees, might prove important.

The Cyber Resilient Behavior Questionnaire is intended to investigate the capabilities, opportunities and motivation of people from all levels and functions of the organization. Many cyber security measurement tools used by organizations rely on information from only one or few organizational members, often specialists or managers responsible for cyber security [33]. This produces biased results, based on a single or few experiences, often with a vested interest in the results or scores achieved. The results that are produced with the Cyber Resilient Behavior Questionnaire are based on responses from a significant number of the company's employees. It is therefore more likely to tell us what the organization is actually doing and whether measures and policies have been embedded in the organization's social system [33]. However, in our pilot study, for practical reasons, only responses from high-level representatives from a small sample of SMEs were collected. Future research would benefit from the use of a larger sample of employees from all levels within organizations. Moreover, the SMEs in our sample were mostly small retailers. It is essential to validate our framework and instrument within other categories of the economy as well, for instance with large businesses in the industrial or financial sector.

Funding and Acknowledgments. This work was partially supported by the municipality of The Hague. The authors would like to thank Dr. Susanne van 't Hoff - de Goede, Michelle Ancher, Iris de Bruin and students from HBO ICT at THUAS for their assistance with this research effort. Further we would like to thank Dr. Jan Maarten Schraagen and Dr. Heather Young for their thoughtful and detailed comments that greatly improved the quality and readability of the manuscript. We are also grateful to the SMEs who agreed to participate in the surveys.

References

1. Ponemon Institute: Cost of cybercrime study (2017). https://www.accenture.com/t20171006T095146Z__w__/us-en/_acnmedia/PDF-62/Accenture-2017CostCybercrime-US-FINAL.pdf#zoom=50
2. Ponemon Institute: 2016 Cost of Cyber Crime Study & the Risk of Business Innovation (2016). https://www.ponemon.org/local/upload/file/2016%20HPE%20CCC%20GLOBAL%20REPORT%20FINAL%203.pdf
3. Accenture: Gaining ground on the cyber attacker. State of Cyber Resilience (2018). https://www.accenture.com/t20180416T134038Z__w__/us-en/_acnmedia/PDF-76/Accenture-2018-state-of-cyber-resilience.pdf#zoom=50
4. DiMase, D., Collier, Z.A., Heffner, K., Linkov, I.: Systems engineering framework for cyber physical security and resilience. Environ. Syst. Decis. **35**(2), 291–300 (2015)
5. Woods, D.D.: Four concepts for resilience and the implications for the future of resilience engineering. Reliab. Eng. Syst. Saf. **141**, 5–9 (2015)
6. Brown, C., Seville, E., Vargo, E.: Measuring the organizational resilience of critical infrastructure providers: a New Zealand case study. Int. J. Crit. Infrastruct. Prot. **18**, 37–49 (2017)
7. Parsons, K.M., Young, E., Butaviciu, M.A., Mc Cormac, A., Pattinson, M.R., Jerram, C.: The influence of organizational information security culture on information security decision making. J. Cogn. Eng. Decis. Mak. **9**(2), 117–129 (2015)
8. Bowen, P., Hash, J., Wilson, M.: Information Security Handbook: A Guide for Managers-Recommendations of the National Institute of Standards and Technology (2012)
9. Cain, A.A., Edwards, M.E., Still, J.D.: An exploratory study of cyber hygiene behaviors and knowledge. J. Inf. Secur. Appl. **42**, 36–45 (2018)
10. Yoon, C., Hwang, J.W., Kim, R.: Exploring factors that influence students' behaviours in information security. J. Inf. Syst. Educ. **23**(4), 407 (2012)
11. Leukfeldt, E.R.: Phishing for suitable targets in the Netherlands: routine activity theory and phishing victimization. Cyberpsychol. Behav. Soc. Netw. **17**(8), 551–555 (2014)
12. Leukfeldt, E.R., Kleemans, E.R., Stol, W.P.: A typology of cybercriminal networks: from low-tech all-rounders to high-tech specialists. Crime Law Soc. Change **67**(1), 21–37 (2017)
13. Young, H., van Vliet, T., van de Ven, J., Jol, S., Broekman, C.: Understanding human factors in cyber security as a dynamic system. In: International Conference on Applied Human Factors and Ergonomics, pp. 244–254. Springer, Cham (2018).
14. Bulgurcu, B., Cavusoglu, H., Benbasat, I.: Roles of information security awareness and perceived fairness in information security policy compliance. In: Proceedings of the AMCIS, pp. 419–430 (2009)
15. Dodge, R.C., Carver, C., Ferguson, A.J.: Phishing for user security awareness. Comput Secur. **26**(1), 73–80 (2007)
16. Talib, S., Clarke, N.L., Furnell, S.M.: An analysis of information security awareness within home and work environments. In: Proceedings of the International Conference on Availability, Reliability, and Security, pp. 196–203 (2010)
17. Crossler, R.E., Bélanger, F., Ormond, D.: The quest for complete security: an empirical analysis of users' multi-layered protection from security threats. Inf. Syst. Front. 1–15 (2017)
18. Da Veiga, A., Eloff, J.H.: A framework and assessment instrument for information security culture. Comput. Secur. **29**(2), 196–207 (2010)
19. Stanton, J.M., Stam, K.R., Mastrangelo, P., Jolton, J.: Analysis of end user security behaviors. Comput. Secur. **24**(2), 124–133 (2005)

20. Winnefeld Jr., J.A., Kirchhoff, C., Upton, D.M.: Cybersecurity's human factor: lessons from the Pentagon. Harv. Bus. Rev. **93**(9), 87–95 (2015)
21. Windle, G., Bennett, K.M., Noyes, J.: A methodological review of resilience measurement scales. Health Qual. Life Outcomes **9**(1), 8 (2011)
22. Linkov, I., Anklam, E., Collier, Z.A., DiMase, D., Renn, O.: Risk-based standards: integrating top–down and bottom–up approaches. Environ. Syst. Decis. **34**(1), 134–137 (2014)
23. Cox Jr., L.A.: Some limitations of "risk=threat x vulnerability x consequence" for risk analysis of terrorist attacks. Risk Anal. **28**, 1749–1761 (2008)
24. Frick, D.E.: The fallacy of quantifying risk. Def. AT&L **228**, 18–21 (2012)
25. Matzenberger, J.: A novel approach to exploring the concept of resilience and principal drivers in a learning environment. Multicultural Educ. Technol. J. **7**(2/3), 192–206 (2013)
26. Cutter, S.L., et al.: A place-based model for understanding community resilience to natural disasters. Glob. Environ. Change **18**(4), 598–606 (2008)
27. Hollnagel, E.: RAG – the resilience analysis grid. In: Hollnagel, E., Pariès, J., Woods, D.D., Wreathall, J. (eds.) Resilience Engineering in Practice. A Guidebook. Ashgate, Farnham (2011)
28. Van der Beek, D., Schraagen, J.M.: ADAPTER: analysing and developing adaptability and performance in teams to enhance resilience. Reliab. Eng. Syst. Saf. **141**, 33–44 (2015)
29. McDonald, N.: Organisational resilience and industrial risk. In: Hollnagel, E., Woods, D.D., Leveson, (eds.) Resilience Engineering, pp. 155–180. CRC Press, Boca Raton (2006)
30. Hollnagel, E.: Introduction to the Resilience Analysis Grid (RAG) (2015). http://erikhollnagel.com/onewebmedia/RAG%20Outline%20V2.pdf
31. Parsons, D.: National Organisational Resilience Framework Workshop: The Outcomes. National Organisational Resilience Framework Workshop (2007). http://www.tisn.gov.au/Documents/FINAL1Workshop.pdf. Accessed 22 Nov 2012
32. McManus, S., Seville, E., Vargo, J., Brunsdon, D.: Facilitated process for improving organizational resilience. Nat. Hazards Rev. **9**(2), 81–90 (2008)
33. Lee, A.V., Vargo, J., Seville, E.: Developing a tool to measure and compare organizations' resilience. Nat. Hazards Rev. **14**(1), 29–41 (2013)
34. Ferreira, P., Clarke, T., Wilson, J.R., et al.: Resilience in rail engineering work. In: Hollnagel, E., Paries, J., Woods, D.D., Wreathall, J. (eds.) Resilience in Practice, pp. 145–156. Ashgate, Aldershot (2011)
35. NIST: Framework for Improving Critical Infrastructure Cybersecurity, v 1.1, April 2018. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
36. MacInnis, D.J., Moorman, C., Jaworski, B.J.: Enhancing and measuring consumers' motivation, opportunity, and ability to process brand information from ads. J. Mark. **55**, 32–53 (1991)
37. 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)
38. Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., Jerram, C.: Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q). Comput. Secur. **42**, 165–176 (2014)
39. Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., Zwaans, T.: The human aspects of information security questionnaire (HAIS-Q): two further validation studies. Comput. Secur. **66**, 40–51 (2017)
40. Brown, J.D.: What issues affect likert- scale questionnaire formats? JALT Test. Eval. SIG **4**, 27–30 (2000)

41. Randall, D.M., Fernandes, M.F.: The social desirability response bias in ethics research. J. Bus. Ethics **10**(11), 805–817 (1991)
42. Spector, P.E.: Summated Rating Scale Construction: An Introduction, no. 82. Sage, Thousand Oaks (1992)
43. Chen, Y.H., Rendina-Gobioff, G., Dedrick, R.F.: Detecting Effects of Positively and Negatively Worded Items on a Self-Concept Scale for Third and Sixth Grade Elementary Students (2007). Online Submission
44. Cronbach, L.J.: Coefficient alpha and the internal structure of tests. Psychometrika **16**(3), 297–334 (1951)
45. Linkov, I., Eisenberg, D.A., Plourde, K., Seager, T.P., Allen, J., Kott, A.: Resilience metrics for cyber systems. Environ. Syst. Decis. **33**(4), 471–476 (2013)