Volitional Cybersecurity

Alireza Shojaifar

SIKS Dissertation Series No. 2023-22
The research reported in this thesis has been carried out under the auspices of SIKS, the Dutch Research School for Information and Knowledge Systems.

Volitional Cybersecurity
ISBN: 978-94-6469-494-9
DOI: 10.33540/1953
Cover idea: Alireza Shojaifar
Cover design: https://www.fiverr.com/velmacover/
Printed by ProefschriftMaken | www.proefschriftmaken.nl.

Volitional Cybersecurity

Vrijwillige Cybersecurity

(met een samenvatting in het Nederlands)

Proefschrift

ter verkrijging van de graad van doctor aan de
Universiteit Utrecht
op gezag van de
rector magnificus, prof.dr. H.R.B.M. Kummeling,
ingevolge het besluit van het college voor promoties
in het openbaar te verdedigen op

vrijdag 6 oktober 2023 des ochtends te 10.15 uur

door

Alireza Shojaifar

geboren op 17 Mei 1981
te Tehran, Iran

Promotoren:
Prof. dr. S. Brinkkemper
Prof. dr. M.R. Spruit

Copromotor:
Dr. S.A. Fricker

Beoordelingscommissie:
Prof. dr. S. Brad
Prof. dr. S. Fischer-Hübner
Dr. S. Jansen
Prof. dr. ir. N. Mentens
Prof. dr. K. Renaud

This thesis was accomplished with financial support from the European Union's Horizon 2020 research and innovation programme under grant agreements No. 740787 (SMESEC), partially No. 883588 (GEIGER), and the Swiss State Secretariat for Education, Research and Innovation (SERI) under contract number 17.00067.

Acknowledgments

I appreciate my supervisors' support during the wonderful and challenging PhD journey. First of all, I am grateful to Prof. dr. Samuel Fricker for the support, advice, and consistent feedback that motivated me to nurture the research ideas. I express my appreciation for all productive, insightful conversations and meetings. I also want to express my gratitude to Prof. dr. Marco Spruit for his attention to my progress, constructive feedback, and responsiveness. Thank you for creating a great professional environment for the PhD students to share their perspectives and learn. I also want to express my gratitude to Prof. dr. Sjaak Brinkkemper for his attention to my research and for warm and welcoming meetings. I sincerely acknowledge your advice.

I want to thank Dr Bilge Yiğit Özkan and Dr Farnaz Fotrousi for their valuable advice.

Alireza Shojaifar,
December 2022

Contents

CHAPTER 1

Introduction

This dissertation introduces "*Volitional Cybersecurity*" (VCS) theory as a systematic way to think about adoption and manage long-term adherence to cybersecurity approaches. Therefore, all chapters together tell the story of the construction of VCS by applying the design science research method. In this dissertation, the validation of VCS has been performed in small and medium-sized enterprises or businesses (SMEs/SMBs) context.

Cybersecurity is becoming increasingly critical for organisations. Cyberspace has become the 21st-century battleground (e.g., cyberwar), and the range of hackers' targets has expanded to government agencies and critical infrastructure providers (Sieger, 2021). The omnipresent cyber threats are one of the top concerns for organisations (Cearley et al., 2017), and according to Cybersecurity Ventures, cybercrime could cost $10.5 trillion by 2025 (Morgan, 2020). Many reports have emphasised the importance of cybersecurity and highlighted:

- 85% of breaches involved the human element (Verizon, 2021),
- 42% of people think their usernames and passwords are not valuable enough for hackers (Psychology of passwords, 2020),
- 48% of hospital executives forced a proactive shutdown in the last six months as a result of ransomware attacks (CyberMDX Philips, 2020),
- 44% of organisations lack cybersecurity training for their employees (Malwarebytes, 2020).

Cybersecurity is a multidimensional endeavour, the fusion of several sciences, and the subject of extensive interdisciplinary socio-technical research. Technical solutions alone do not resolve the cybersecurity challenges as they are related to organisational, economic, social, political, and other human dimensions that are inextricably tied to cybersecurity efforts (Craigen et at., 2014).

Cybersecurity has been considered one of the wicked problems or ill-structured problems. Carr and Lesniewska (2020) state that wicked problems are complex, interdependent, interconnected, and resistant to solutions. They emphasise that "the multilevel, transnational, cross-sectoral interconnected nature of wicked problems means that there are no simple governance or technical solutions" (Weber and Khademian, 2008). Therefore, we work to 'tame' the problems or 'cope' with them instead of 'solving' them (Daviter, 2017).

Taming strategies want to reduce wicked problems to making them more manageable. In problem taming, we transform an ill-structured problem into a more controllable and well-structured problem for decision-making. It is done by scoping and framing the problem in such a way as to align it with pre-existing administrative expertise and policy instruments.

Coping strategies want to "reflect the fragmented, uncertain and ambiguous nature of wicked problems by relying on a more disjointed and tentative process of formulating policy responses" (Daviter, 2017).

Malone and Malone (2013) explain that cyberspace has incomplete, often contradictory information with an ever-changing, interdependent architecture. It seems that there is no meaningful heuristic to steer cyberspace policy. The issues such as transparency versus security, privacy versus open access, and public space versus private property confound

policymakers. Therefore, as a wicked problem, there is neither a grand, comprehensible theory nor a simulated model to capture the paradoxes, and solutions are, at best, better or worse, not true or false (Malone and Malone, 2013).

According to (Joint Task Force, Cybersecurity Curricula 2017), cybersecurity is defined as "a computing-based discipline involving technology, people, information, and processes to enable assured operations in the context of adversaries. It involves the creation, operation, analysis, and testing of secure computer systems. It is an interdisciplinary course of study, including aspects of law, policy, human factors, ethics, and risk management."

Studies argue that cybersecurity is a journey, adoption and continuous use of solutions (e.g., Renaud and Weir, 2016). At the same time, abundant literature shows a lack of adoption of manifold cybersecurity remediations regarding tools (West, 2008), recommendations (Renaud, 2016; Renaud et al., 2019), countermeasures (Song, 2016; Beazley, 2019), standards (European Digital SME, 2020) and long-term adherence to cybersecurity approaches (e.g., Klaus, 2013; Kurpjuhn, 2015; Renaud and Weir, 2016; Heidt et al., 2019). This implies that the companies are still vulnerable because one has failed to bring the solutions to use (Renaud, 2016).

Bakry proposes the STOPE model for cybersecurity in the enterprise (Bakry, 2003), which stands for the dimensions of strategy, technology, organisation, people, and environment (AlHogail and Mirza, 2014). The strategy dimension is concerned with the future development of the enterprise and sets objectives, policies, best practices, standards, and guidelines. Technology refers to the effective use of hardware and software to make information systems secure and prevent incidents. The organisation is about the structure and culture of the organisation, including the beliefs, values, assumptions, norms, and knowledge that influence security behaviour. People are concerned with the preparedness, responsibility, and management of each individual in the enterprise. The environment is about the national culture as well as government initiatives and regulations.

Researchers (e.g., Bada et al., 2015; Li et al., 2016; Haeussinger and Kranz, 2017; Heidt et al., 2019; European Digital SME, 2020; Chang and Coppel, 2020; Donalds and Osei-Bryson, 2020; Aigbefo et al., 2022) argue that recognising the factors of adopting the desired cybersecurity behaviour is critical. Lee and Larsen (2009) applied Protection Motivation Theory (Rogers, 1983) to identify the key drivers in adopting anti-malware software. They found no significant relationship between firm size and adoption intention. Han et al. (2014) indicated that there is a lack of relevant research in this area, and further research requires an in-depth investigation of influential factors in individuals' adoption and exploitation of the new cybersecurity apps. Bada et al. (2015) explained that identifying the vital factors that may impact the effectiveness and adoption of security awareness solutions and change employees' behaviour is essential to support long-term engagement in cybersecurity practices. European Digital SME (2020) emphasised that the high complexity, lack of adaptation, and lack of awareness may be the reasons for the lack of adoption of cybersecurity standards and certification schemes.

Various approaches have been proposed for enhancing adherence to appropriate practices and the adoption of cybersecurity solutions in organisations. These approaches involve training

material and methods (ENISA, 2010; Gundu and Flowerday, 2013), awareness training solutions (Haeussinger and Kranz, 2017; Muronga et al., 2019; Ponsard et al., 2019; Wong et al., 2022), frameworks (Dojkovski et al., 2010; Heidt et al., 2019), information security management tools (Brunner et al., 2018), self-assessment tools (UK Gov., 2018; Ponsard et al., 2019), and multiple theoretical models (Lebek et al., 2014; Sommestad et al., 2014; Kuppusamy et al., 2020). Still, it is not sufficiently clear how to select and compose these approaches into solutions for meeting the profiles and needs of many diverse cybersecurity-adopting organisations (Renaud, 2016; Haeussinger and Kranz, 2017).

Existing cybersecurity research has extensively applied and examined theories from psychology, sociology, and criminology. For instance, Lebek et al.'s (2014) systematic literature review of information security awareness and behaviour identified 54 theories, mainly from the disciplines mentioned above. Kuppusamy et al.'s (2020) systematic literature review of information security compliance behaviour also identified 19 theories from almost the same disciplines. The systematic literature review of adherence to information security practices described in Chapter 2 demonstrates that these theories are also applicable to adherence to information security practices. General Deterrence Theory (GDT) and Protection Motivation Theory (PMT) are widely applied theories. Considering cybersecurity behaviour from the lens of PMT and GDT, although valuable, provides still limited insight into active, volitional behaviour.

The literature reviews, and cybersecurity studies show some open questions in the existing knowledge.

a) The diversity of context. In prior studies, the importance of incorporating diverse cybersecurity approaches for leading to well-targeted communication in heterogeneous contexts (including diverse needs and capabilities) has not been sufficiently understood or embedded in solutions. The diversity of people's risk perception, risk management and categories of security measures (Julisch, 2013; Renaud and Weir, 2016) or the diversity of theoretical variables and their influence on compliance behaviour (Sommestad et al., 2014) may be considered in approaches. Existing tools also lack a solid base in scientific knowledge and theories about considering the heterogeneity of the contexts where cybersecurity is to be applied.
b) Applied theories. The studied theories (e.g., Protection Motivation Theory, General Deterrence Theory, Theory of Planned Behaviour) mainly originated from disciplines other than information systems and cybersecurity. The theories and constructs were developed based on data, for instance, in psychology or criminology, and these seem not to fit properly for the cybersecurity context (Menard et al., 2017). Lebek et al. (2014) suggested that future studies should focus on additional factors that influence employees' behaviour instead of on measuring already confirmed existing construct relationships.
c) The diversity of motivation. A majority of scholars focused on the influence of punishments and rewards on employees' motivation. What is less understood and left almost unexplored is that the concept of motivation reflects a continuum of various qualities that need further study (Ryan and Deci, 2000).

This dissertation builds upon Self-determination Theory (SDT) and the Design Science Research Method (DSRM) as the foundations for theorising and coping with the gaps.

Self-determination theory (SDT)

SDT provides a helpful lens through which a broader understanding of individual motivation in the organisation is achieved. It classifies various types of extrinsic motivation that reflect different degrees of self-determination (Ryan and Deci, 2000). Also, SDT identifies a set of basic psychological needs to become more autonomous or self-determined. SDT defines two types of motivated behaviours: autonomous vs controlled. Autonomous forms are about conscious, active choice consistent with a person's value. However, controlled forms can be nonconscious and automatic. According to Deci and Ryan (2000), *basic psychological needs* are defined as "innate, rather than learned, psychological nutriments that are necessary for healthy development and effective functioning." Concerning this definition, Deci and Ryan explain that "the frustration of basic needs was associated with less intrinsic motivation, more controlled regulation and amotivation, and stronger extrinsic aspirations, which in turn lead to diminished experience, performance, and wellness." Moreover, Ryan and Deci (2000) indicate that volitional behaviour influences engagement quality and tends to be maintained. *Volition* is defined as "a sense of unpressured willingness to engage in the action" (Deci, Ryan, and Williams, 1996). SDT will be elaborated more in section 1.4.

SDT is the kernel theory ("*any descriptive theory that informs artefact construction*" Gregor and Hevner, 2013) of this study. To the best of our knowledge, this is the first time SDT has been used to design cybersecurity self-paced tools.

Design Science Research Method (DSRM)

DSRM provides a research framework for creating and evaluating artefacts. This dissertation follows the DSRM proposed by Peffers et al. (2007). This method comprises six activities:

- The identification of a problem: focus on the research problem,
- Defining objectives of a solution: focus on the objectives of a solution,
- Design and development of the artefact: focus on the artefact,
- Demonstration: focus on the use of the artefact,
- Evaluation: focus on observing and measuring,
- Communication with professionals and scholars: focus on presenting the findings.

DSRM and the activities will be elaborated more in section 1.6.

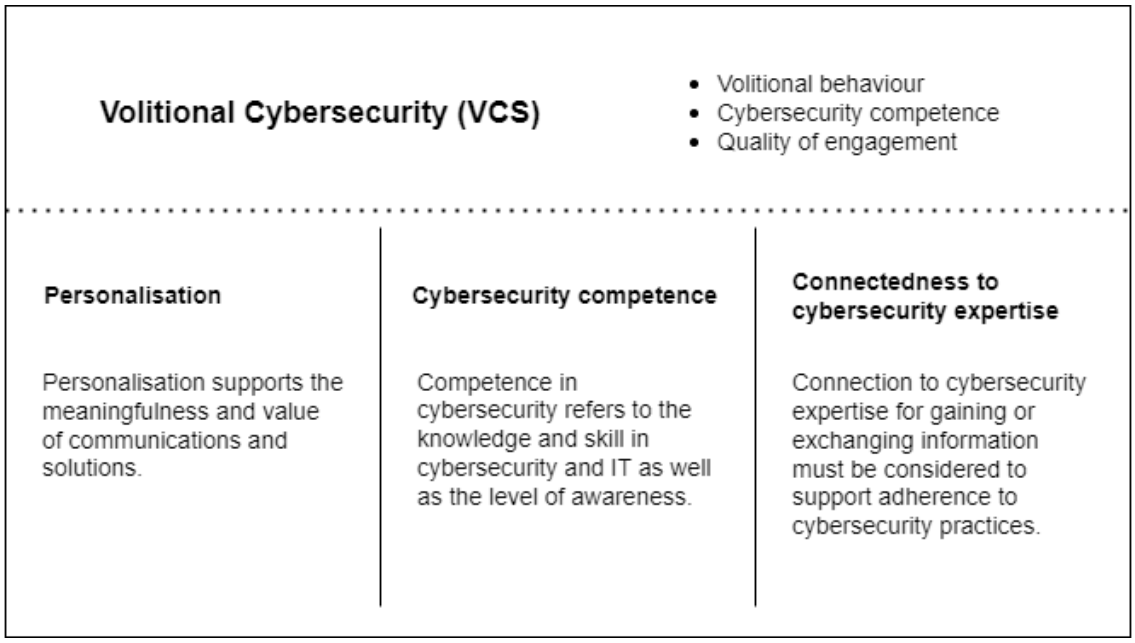
The main contribution of this dissertation is the *Volitional Cybersecurity* (VCS) theory. VCS is structured around the core concept of volitional self-determined cybersecurity behaviour. It is agreeable for a user to understand the rationale and significance behind the behaviour and consequences (e.g., performing or not performing an appropriate cybersecurity behaviour), perform cybersecurity behaviour or choose cybersecurity technologies with free will, and have relevant technical capabilities for performing the behaviour.

VCS suggests that a heterogeneous context can be classified based on the cybersecurity competence of target groups and their distinct requirements (e.g., business models) instead of

factors such as organisation size or annual turnover. The empirical findings (in Chapters 3-7) illustrate that approaches need to be tailored to cybersecurity requirements and the competence levels of each class of audience. Further, based on the analysis of the empirical findings in this research (in Chapters 3-7), VCS explicates that supporting three factors affect the adoption of cybersecurity measures and better quality of cybersecurity engagement across all classes of the context (Figure 1.1):

Figure 1.1

The constructs of the Volitional Cybersecurity theory



A) **Personalisation**. Personalisation supports the meaningfulness and value of communications and solutions. The analysis results demonstrated that users wanted to adopt approaches most suited to their daily business activities and needs. General advice and cybersecurity solutions irrelevant to the users' preferences and vulnerabilities do not support the quality of cybersecurity engagement.

B) **Cybersecurity competence**. Competence in cybersecurity (according to the findings in this research) refers to the knowledge and skill in cybersecurity and IT as well as the level of awareness. The findings illustrated that users had various levels of cybersecurity competence. The fitness of awareness training content influenced the adoption of solutions and recommendations. Also, the findings showed that the users wanted to promote their cybersecurity capabilities. It is important to entail thinking of cybersecurity competence improvement aligned with the users' competence level to influence understanding and encourage cybersecurity engagement.

C) **Connectedness to cybersecurity expertise**. Connection to cybersecurity expertise (e.g., cybersecurity providers, associations, open training materials) for gaining or exchanging information must be taken into account to support adherence to cybersecurity practices. The empirical findings demonstrated that this connection could foster volitional self-endorsed

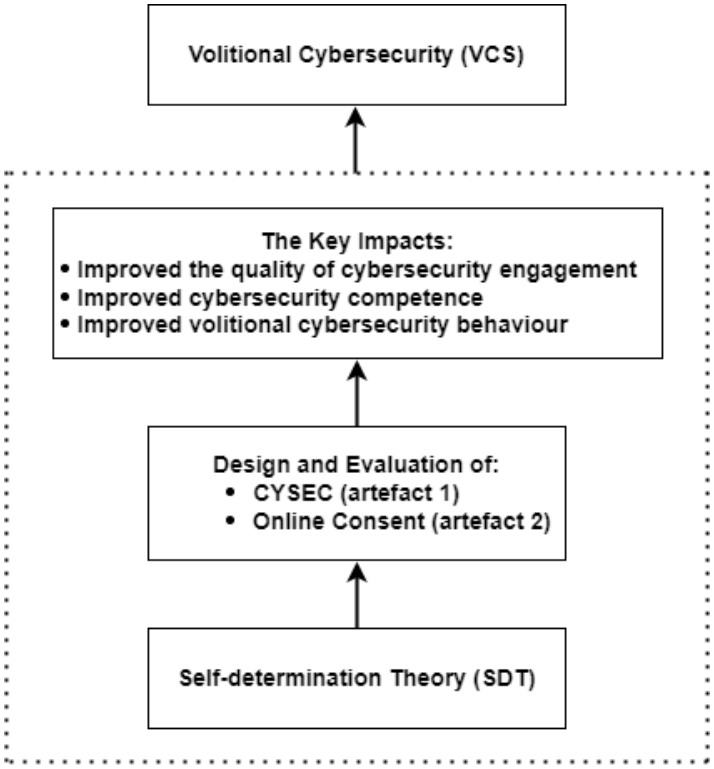
strivings since users lacking cybersecurity competence required a connection to gain knowledge or support.

Accordingly, cybersecurity approaches that ignore the personalisation of cybersecurity solutions, the cybersecurity competence of target groups, and the connectedness of recipients to cybersecurity expertise in heterogeneous contexts lead to poorer acceptance of the value or utility of solutions. Subsequently, it can cause a lack of motivation for adoption and adherence to cybersecurity solutions.

Figure 1.2 illustrates the conceptual framework of the research and theory development in this dissertation.

Figure 1.2

The conceptual framework of the research
The arrows show logical progression – from SDT in psychology to the VCS in cybersecurity



- SDT is an empirically driven psychology theory about motivation. It distinguishes between different types of motivation and proposes two basic distinct types: intrinsic and extrinsic. SDT indicates that supporting basic human needs (autonomy, competence and relatedness) enhances higher motivational quality and self-determination.
- We created and evaluated CYSEC (CyberSecurity Coach) as a self-paced tool and method for delivering cybersecurity capabilities and awareness-raising. We created and validated the Online consent prototype to tackle the challenges of lacking motivation and trust for security information sharing with CYSEC. The shared information is then applied to provide tailored advice for coaching users. CYSEC and online consent prototype supported autonomy, competence and relatedness in their features.

- CYSEC provides step-by-step instructions to assist users in cybersecurity improvement on their own. Tailored recommendations, embedded awareness training content, and stepwise series of questions facilitate learning and continuous progress. The Online Consent prototype supports users in controlling data through choices, online agreement, and familiarity with the usage of shared information.
- VCS is an empirically driven cybersecurity theory. It provides a systematic way to think about adoption and build long-term adherence to cybersecurity approaches. It suggests that a context can be classified based on the cybersecurity competence of target groups and their distinct requirements. VCS indicates that supporting personalisation, cybersecurity competence, and connectedness to expertise affect the adoption of measures and better quality of cybersecurity engagement.

Overall, this chapter delineates a background of cybersecurity activities (adherence to good practices and adoption of mitigations), VCS theory construction, and the SME context.

1.1 Research Background

Information technology (IT) adoption has become a fundamental requirement for SMEs due to its benefits (Alahmari and Duncan, 2020). Technologies such as cloud computing or e-commerce provide many opportunities to access necessary services to improve business performance, share information, facilitate communication, and reduce costs (Sultan, 2011; Alahmari and Duncan, 2020). However, it should be noted that systems vulnerabilities, cybersecurity skills and knowledge inadequacies, and malicious actors could be potential sources of cybersecurity problems, such as data breach costs or reputational damage (Heidt et al., 2019).

Han et al. (2014) explain that technology adoption and acceptance were used interchangeably by many studies; however, they are different constructs. They indicate that technology adoption studies "focus on the individual's tendency to use an emerging technology when the individual just gets to know the new technology but has not used it. Technology acceptance studies "emphasise the individual's decisions regarding whether or not to repeat using the technology after the initial adoption."

The adoption of cybersecurity solutions with corresponding investment is not a priority for many companies. Many enterprises often tend to invest in areas that will support their business growth (Kurpjuhn, 2015). It is difficult for many senior managers to see and understand the importance of investment in security technologies (Kurpjuhn, 2015; Heidt et al., 2019). Further, some companies have a naive attitude that "nobody would want to attack us" (Klaus, 2013; Renaud and Ophoff, 2021). Some of them state that the complex nature of cybersecurity needs, the novelty of threats, and the burdensome management of cybersecurity practices impede the adoption of adequate protective measures or compliance with standards (Song, 2016; Heidt et al., 2019; European Digital SME, 2020). Without actual changes in practices and policies, many companies will remain tantalising targets for cybercriminals (Berry and Berry, 2018; Alahmari and Duncan, 2020). A study by Beazley (2019) found that small businesses were hit

by 71% of the reported ransomware incidents in 2018. Cybersecurity studies demonstrate that the need to adopt appropriate countermeasures against ever-present cyberattacks is urgent.

Existing literature has investigated cybersecurity problems in organisations and proposed various recommendations, frameworks, and solutions. Dojkovski et al. (2010) explain that the success of information systems governance, risk management and compliance is achieved through developing an effective information security culture. According to the European Network and Information Security Agency (ENISA, 2017), the *cybersecurity culture* of organisations refers to "the knowledge, beliefs, perceptions, attitudes, assumptions, norms and values of people regarding cybersecurity and how they manifest in people's behaviour with information technologies." Based on this definition, ENISA (2017) explains that cybersecurity culture "is about making information security considerations an integral part of an employee's job, habits and conduct, embedding them in their day-to-day actions." Dojkovski et al. (2010) propose a framework depicting external and internal influences on information security culture. Lopes and Oliveira (2014) argue that developing a strong information security culture impacts employees' behaviour and consequently reduces information security breaches. Wiley et al. (2020) demonstrate empirical support for the relationship between organisational culture, security culture, and information security awareness. Furnell et al. (2002) state that awareness-raising programs are vital to fostering a security culture. Heidt et al. (2019), with respect to IT security investments, propose a framework of constraints in three layers: the macro-environment, the micro-environment, and the focal. The macro-environment refers to country characteristics, the institutional framework, and general globalisation pressures, which often impact smaller enterprises to a greater extent. Micro-environment factors affect companies through competitive pressure, including suppliers/partners, customers/clients, vendors/consultants, and general industry characteristics. The focal layer (internal characteristics) consists of organisational (e.g., resources, culture, and geographical insularity) and leadership (e.g., managerial skills, IS knowledge and skills, attitude, and strategic orientation) constraints. Further, Heidt et al. (2019) emphasise that future studies should consider the heterogeneity of contexts. Gundu and Flowerday (2013) propose an information security awareness process to cultivate appropriate behaviours. They explain that a well-structured information security awareness campaign helps to reduce security risks. They emphasise that there is a lack of literature on the effectiveness of information security awareness methods based on psychological theories. Renaud et al. (2019) provide a list of recommendations. ENISA (2010) proposes training material for awareness-raising. Renaud (2016) suggests a threat management model for classifying threat advice responses.

Various tools were proposed to facilitate awareness-raising and capability improvement in organisations. Brunner et al. (2018) introduce a tool for supporting continuous risk-driven and context-aware information security management according to the ISO 27001 standard. They argue that the tool supports changes and maintains the connections between assets, information security risks and derived security requirements. Ponsard et al. (2019) present several cybersecurity approaches and awareness-raising tools. For instance, the Cyber Essentials framework in the UK (HM Government UK, 2014) provides basic countermeasures and a self-

assessment tool (UK Gov., 2018). Geiger (2020) has recently proposed an easy and affordable cybersecurity toolbox for training and risk assessment in micro and small enterprises. To our knowledge, there are no statistics on adopting cybersecurity tools.

1.2 AWARENESS TRAINING STRATEGIES

Drawing on the mentioned solutions presented in section 1.1, researchers have considered awareness training solutions as an effective means to influence the adoption of secure behaviours and the main prerequisite for enhancing cybersecurity capacity and facilitating cybersecurity culture development (Bulgurcu et al., 2010; Lebek et al., 2014; Bada et al., 2015; Li et al., 2016; Haeussinger and Kranz, 2017; ENISA, 2017; European Digital SME, 2020; Chang and Coppel, 2020). Consistent training awareness programs are required to build a strong cybersecurity culture (ENISA 2017).

Also, many studies well recognise that cybersecurity awareness-raising measures should be one of the top priorities for organisations. Organisations' staff are considered the first line of defence, and a lack of awareness among staff leads to misbehaviours and thus reduces the strength of this line (PwC, 2010; Haeussinger and Kranz, 2017). A study by Manso et al. (2015) shows that security experts believe that limited awareness is one of the primary barriers to embracing standards. Osborn (2015) argues that awareness programs are more required than tool implementation for facilitating self-assessed risks.

According to the NIST (Wilson and Hash, 2003):

> *"Awareness is not training. The purpose of awareness presentations is simply to focus attention on security. Awareness presentations are intended to allow individuals to recognise IT security concerns and respond accordingly. In awareness activities, the learner is a recipient of information, whereas the learner in a training environment has a more active role. Awareness relies on reaching broad audiences with attractive packaging techniques."*

Haeussinger and Kranz (2017) indicate that information security awareness is "a cognitive state of mind, which is characterised by recognising the importance of information security and being aware and conscious of information systems security (ISS) objectives, risks, and threats, and having an interest in acquiring the required knowledge to use IS responsibly." Furnell and Clarke (2005), concerning NIST (1996), differentiate between awareness, training, and education and emphasise that awareness is desirable for all employees:

- *Awareness – Enables of recognition of what needs to be protected.*
- *Training – Provides skill in how the protection can be achieved.*
- *Education – Provides deeper understanding of why protection is required.*

According to Corallo et al. (2022), the goals of cybersecurity and information security awareness are the same: "both increase the employees' level of knowledge about possible security threats, system vulnerabilities and security risks, and allow them to be responsible in terms of information security and aware of possible cyberattacks, thus ensuring that the information, systems and networks they interact with are well protected."

Different types of awareness were identified in the literature. Bulgurcu et al. (2010) conceptualise that information security awareness consists of two types: general information security awareness and information security policy (ISP) awareness. General information security awareness refers to "an employee's overall knowledge and understanding of potential issues related to information security and their ramifications." Further, ISP awareness is defined as "an employee's knowledge and understanding of the requirements prescribed in the organisation's ISP and the aims of those requirements." Bulgurcu et al. (2010) argue that both types of awareness impact an employee's attitude to comply with the ISP directly and indirectly through the employee's outcome beliefs (e.g., rewards, sanctions, costs).

Han et al. (2014) explain two types of awareness of an individual: threat awareness and technology awareness.

a) *The individual's threat awareness* is considered the fundamental determinant of an effective defence strategy and is about the consciousness of security breaches. It is considered that individuals with threat awareness are more likely to take preventive actions before a threat occurs or implement security strategies.
b) *The individual's technology awareness* is about the awareness of the existence and functionality of available protective technologies and users' perception of the benefits and costs of the adoption and actual use of these technologies.

Han et al. (2014) explain that an effective information security strategy should consider approaches to increasing both types of awareness. Moreover, they recommend that future research examine the user's self-efficacy influence on the adoption of free third-party cybersecurity apps. This suggestion has been incorporated into this dissertation.

The findings about cybersecurity awareness in this dissertation (e.g., Chapter 6) are consistent with prior works (Bulgurcu et al., 2010; Han et al., 2014; Donalds and Osei-Bryson, 2020; Renaud and Ophoff, 2021). The findings revealed that users of our tool have different types (or levels) of awareness, and it has an influence on their cybersecurity needs and, consequently, the adoption of our tool. Some CEOs or chief information security officers (CISOs) of the SMEs (Chapters 6 and 7) know about the general potential cybersecurity threats and safeguards. Some of them indicate that they have a cybersecurity policy or a partially written policy in some focus areas and put a high value on best practices. However, in addition to Bulgurcu et al. (2010) study, the author discovered that some CEOs of CISOs have another type of awareness. It is *awareness of the dynamic essence of cybersecurity*. Some CEOs or CISOs know that threats are ever-changing (e.g., new COVID-19-related cybersecurity threats and vulnerabilities (Chapman, 2020; Lallie et al., 2021)), and cybersecurity topics become obsolete. Thus, they have a long-term attitude, regularly review their policy, and adapt their rules. Further, the author used this type of awareness as one of the indicators for the context classification. Users with this type of awareness want to keep up with the new IT advancements and the latest updates in the cybersecurity threat landscape (in Chapter 7).

In a literature review, Haeussinger and Kranz (2017) identified several information security awareness antecedents and classified them into institutional, individual, and socio-environmental.

Institutional antecedents mainly rely on an organisation's security management practices and encompass managerial security awareness; management support, communication, and commitment; security, education, training, and awareness (SETA) program (generic measure); e-learning; online game-based training; password security; conceptual change pedagogy; discussion, checklist, e-tutorial; phishing mail exercise; media richness; user participation; and information security policy provision (ISPP).

Individual antecedents focus on employees' factors, including information systems knowledge, negative experience with ISS threats, individual education, and User security perception.

Socio-environmental antecedents include factors about situational contexts and individuals' interactions with a social environment. These factors are about secondary sources (e.g., mass media, news), peer behaviour (e.g., with respect to significant others), and stakeholders (e.g., business partners).

Haeussinger and Kranz (2017) argue that understanding the antecedents of information security awareness is necessary for IT security management to develop more effective awareness strategies and support policy-compliant behaviour. They indicate that on the institutional level, managers' awareness and support positively correlate with employees' information security levels. They explain that future research may investigate how the knowledge of factors that specifically build managerial information security awareness can be utilised to customise awareness programs more specifically aimed at different target groups. On the individual level, they suggest that future research can investigate the effect of tailored feedback and information (e.g., the consequences of specific policy violations) on security awareness. Further, they recommend that future research may study information security awareness in real work environments. Haeussinger and Kranz's (2017) suggestions for future research have inspired this dissertation.

The impact of cybersecurity awareness on employees' and managers' behaviours was demonstrated in the literature. According to the definition of awareness, changing behaviour for best practices is the aim of awareness-raising solutions (Bada et al., 2015; Muronga et al., 2019). Siponen and Pahnila (2010) state that awareness of cybersecurity threats and their severity is key to motivating employees to comply with security policy. *Security policy compliance intention* is defined as "an employee's intention to protect the information and technology resources of the organisation from potential security breaches" (Bulgurcu et al., 2010). Employees' awareness of organisational information security policies affects cybersecurity behaviour (Li et al., 2019). Awareness of policies also has a deterrent effect on information systems (IS) misuse intention. This effect is achieved indirectly through the perceived certainty and severity of organisations' sanctions (D'Arcy et al., 2009). Also, information security awareness exerts a significantly positive influence on the cost of non-compliance (Bulgurcu et al., 2010). Further, Barlette and Jaouen (2019) explain that awareness-raising activities impact CEOs' protective and supportive actions. Protective actions refer to taking personal charge of information security, including implementing security measures and

performing technical behaviours. Supportive actions refer to validating security measures or budgets or raising employees' awareness.

One significant issue about designing awareness training programs is their effectiveness. Cybersecurity recommendations provided monotonically by security experts alone are not enough and do not actually increase awareness or appropriately change behaviour (Bada et al., 2015). An awareness training program can be effective if the content is interesting, current, and simple enough to be followed (Bada et al., 2015). Further, it is important to help companies identify the value of the recommendations regarding their business models and goals. Prior studies have shown that CEOs and employees usually have a good understanding of their company's assets and processes. Linking cybersecurity best practices to this understanding increases effectiveness and motivation and helps develop cybersecurity tailored to the business needs (Wilson and Hash, 2003; Amankwa et al., 2015; Beyer et al., 2015; Manso et al., 2015).

Many studies indicate that the aim of implementing awareness training programs is changing employees' behaviour for adherence to best practices. ENISA (2012) emphasises that cybersecurity is a matter of cultural challenge and behavioural change and motivating people to act is a major challenge. Several theories (e.g., protection motivation theory, theory of planned behaviour) have been considered and used to explain the enabling or inhibiting factors that inform cybersecurity awareness and the individual's behaviour. These theories were then used as a basis for proposing methods supporting management in assessing and improving cybersecurity in their enterprise. Haeussinger and Kranz (2017) argue that scholars and practitioners recently shifted their attention more towards the human dimension of cybersecurity by applying behaviourism and social psychology theories.

1.3 THE ROLE OF HUMAN ASPECTS IN CYBERSECURITY

Human vulnerabilities have been considered a challenging cybersecurity problem. Understanding and incorporating human-related factors into organisational cybersecurity can improve the organisation's cybersecurity defence capacity and prevent adverse security outcomes. Around 85% of data breaches in companies are related to a human element (Verizon, 2021). Furnell and Clarke (2012) state that human aspects of security are prone to receiving significantly less attention than technical issues since the human aspects are a more challenging problem to approach, and they cannot be easily approached with a product-based solution.

The way individuals perceive the concept of risk affects their cybersecurity behaviour. West (2008) argues that the primary users' problem in security systems is about how people think of the risk that guides their behaviour. West (2008) explains that risk and uncertainty are extremely difficult concepts for individuals to evaluate. Julisch (2013) states that individuals' cognitive biases may lead to suboptimal decisions. He explains four types of biases:

a) Most people are risk-seekers and prefer to take their chances that future loss will not occur.
b) Individuals generally believe that they are less exposed to risks than other parties.
c) Most people are more afraid of risks if they are clearly described, easy to imagine, memorable, and have occurred recently.

d) Most people have a bias to ignore evidence that contradicts their preconceived notions.

Psychological and behavioural characteristics are among the significant influencing factors of information security incidents (Hong and Furnell, 2022). Dhillon (2001) explains that security controls' effectiveness depends on the competency and dependability of the employees using them. Consistent with Dhillon, Gundu (2019) indicates that the success or failure of organisations' cybersecurity initiatives ultimately depends on their employees' behaviour. Kraemer et al. (2009) consider the complex relationship between human and organisational factors and demonstrate that these factors play a significant role in the development of security vulnerabilities that technical remedies cannot fix. Stanton et al. (2005) state that one organisational constraint that influences effective security is the end user behaviours, and motivational interventions can improve the organisation's security status. Safa et al. (2016) argue that human, organisational, and technological aspects play a core integrative role in information security. They identify two key human aspects of information security in organisations: information security knowledge sharing and information security collaboration. Furnell and Clarke (2012) delineate that human aspects have a direct overlap in the technical area with topics such as the usability and acceptability of technology solutions with an impact on protective measures in organisations.

Herath and Rao (2009) indicate that research in behavioural information security has started focusing attention on employee intentions to follow policies. Aigbefo et al. (2022) demonstrate that personality traits (habit and hardiness) significantly affect the employees' cybersecurity compliance intention. Behaviour is driven by behavioural intention (Ajzen, 1991). Padayachee (2012) defines *information security behaviour* as "a set of core information security activities that have to be adhered to by end users to maintain information security as defined by information security policies." In our self-paced tool (CYSEC), we supported step-by-step instructions to assist users in information security behaviour on their own. CYSEC provided five themes (Patch Management, Access Control and Audit, Malware Scans, User Training and Backup). Chapters 4 and 6 discuss the tool evaluation results and user behaviour.

The significant role of management in information security was discussed in many studies (e.g., Soomro et al., 2016). Ifinedo (2014) explains that management has a principal role in shaping employees' beliefs and attitudes and providing an environment for increasing information security policy compliance. Consistent with Ifinedo, Shih et al. (2016) indicate that IS security is related to management rather than technology issues from the human behaviour perspective. Motivating employees to comply with policies is essential since employees are the Achilles' heel in IS security management. Clapper and Richmond (2016) demonstrate that small business managers' beliefs about their peers' behaviour are positively associated with the intention to comply with information security policies.

Applying theoretical models from other disciplines (e.g., economics, criminology, psychology) has been attracting more attention to explain human aspects of cybersecurity and predict compliance behaviour and attitudes. Siponen et al. (2007) have been the first ones to show that theory-driven and empirically validated approaches may be effective. They have shown that (1) the Protection Motivation Theory (PMT), (2) the General Deterrence Theory

(GDT), and (3) the Theory of Reasoned Action (TRA) could be used to explain employees' compliance with cybersecurity policy (Siponen et al., 2007). These theories will be discussed in Chapter 2.

In the following, the author of this dissertation elaborates on four systematic literature reviews that study human aspects of cybersecurity awareness, policy compliance, and adherence and adoption in organisations.

Lebek et al. (2014) provide a literature review of theories used in the field of employees' information systems security behaviour. They studied 113 papers published between 2000 and 2013 and classified 54 theories from social psychology and criminology. They identify cognitive determinants and principles that have been proven to influence employees' awareness and need to be considered in designing effective training and awareness programs. Their findings illustrate that the Theory of Planned Behaviour (TPB), TRA, GDT, and PMT are the dominantly applied behavioural theories. They indicate that the quantitative empirical research method is dominant in the examined research field.

Lebek et al. (2014) emphasise that more studies should focus on the differences in awareness. Also, they indicate that future empirical studies need to focus on additional factors influencing employees' information security awareness and behaviour instead of measuring already confirmed core construct relationships. They also explain that very few publications studied employees' actual behaviour. These suggestions and research gaps have been incorporated in this dissertation. We paid attention to the importance of literature review, conducted qualitative empirical research and inductive analysis to identify additional factors, and considered the significance of awareness levels in employees' cybersecurity behaviour. Additionally, several findings within the dissertation are based on studying the actual behaviour of end-users in their companies.

Kuppusamy et al.'s (2020) literature review identifies behavioural theories that influence information security policies compliance behaviour. They identify 29 papers published between 2014 and 2019 and classify 19 theories from psychology, criminology, health, and management. Their findings, consistent with Lebek et al.'s (2014) study, illustrate that TPB, PMT, and GDT are widely applied theories. Kuppusamy et al.'s (2020) study demonstrates that Self-determination Theory (SDT) is one of the less explored theories (only applied in two studies) in this context. However, SDT provides a comprehensive overview of various theoretical constructs (Padayachee, 2012). Padayachee classifies information security compliance behaviour antecedents grounded in SDT. The findings of these studies suggest that future research may be built on SDT to address the gap and construct novel theoretical and practical insights.

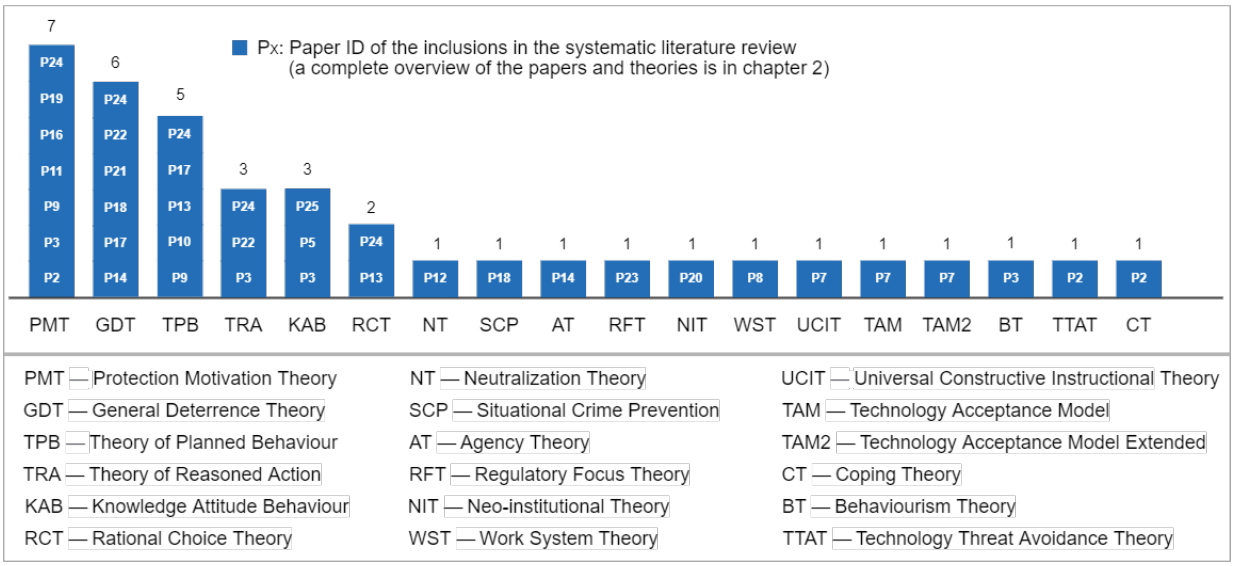
Sommestad et al. (2014) provide the first systematic literature review on variables that influence information security policies compliance (and incompliance) and identify how significant these variables are. They selected 29 papers published until May 2012 and identified 61 variables (theoretical constructs such as threat appraisal and attitude) drawn from psychological theories. Their findings show that each of the variables and theoretical models only explains a small part of the variation in people's behaviour. Also, the findings of multiple

studies may show a considerable variation in a variable. Further, they indicate that decision-makers should recognise that many variables probably influence employees' compliance.

Chapter 2 reports our literature review, focusing on the proposed theoretical foundations and the extent of empirical evidence for adherence to information security practices. The author used the snowballing strategy and selected 25 papers published between 2003 and mid-2020. The findings show that there is a proliferation of research published after 2015. The findings revealed that the common goals across these studies were twofold: tackling the challenges of information security policy compliance and management practices. Also, the study demonstrated that only one paper proposed and evaluated the utility of a cybersecurity tool (for information security management) based on a well-established theory. Further, the study identified 18 theories from different disciplines (e.g., psychology, criminology, health), as shown in Figure 1.3. In line with prior literature reviews, the findings demonstrated that PMT, GDT, and TPB are the most prevalent applied theories. However, no prior research has applied Self-determination Theory to design and evaluate a cybersecurity tool.

Figure 1.3

Distribution of the applied theories for studying adherence to cybersecurity approaches in the context of SMEs



1.4 SELF-DETERMINATION THEORY

According to the literature review, PMT, GDT, and TPB have dominated information security studies for years (Chapter 2). Motivation is a key concept in these theories and across many cybersecurity studies. Understanding the factors that motivate employees to comply with their organisation's policy is central to solving behavioural issues in information security management (Bulgurcu et al., 2010). Using approaches that motivate users to adopt information security recommendations may support the effectiveness of cybersecurity communication (Cranor, 2008). However, most scholars have focused on the influence of punishments, rewards, and fear appeals on employees' motivation. What is less understood is that motivation can be intrinsic and extrinsic, with various types and qualities.

Deci et al. (1999) demonstrated that all tangible and expected rewards for desirable performance tend to undermine autonomy and intrinsic motivation. Deci et al. (2001) explain that the effects on the intrinsic motivation of external events such as rewards are a function of how these events impact an individual's perceptions of competence and self-determination. Rewards have two aspects. The informational aspect promotes self-determined competence and tends to enhance intrinsic motivation and can be reflected by behaviour that persists with a minimum of external support. In contrast, the controlling aspect prompts an externally perceived locus of causality (experienced as pressure toward specific outcomes) and thus diminishes intrinsic motivation (Deci et al., 2001). Further, controlling orientation (e.g., the use of punishments) is more related to pressured compliance, would be negatively related to performance on the heuristic activities, and tends to be effective for short-term behaviour change. In some instances, controlling communication may lead to doing just the opposite of what is demanded or acts of contravention (Deci and Ryan, 1985). Thomson and Van Niekerk (2012) consider the motivation of employees from an organisational perspective and explain that a coercive environment undermines employees' autonomy and, consequently, their intrinsic motivation for complying with the information security goals of management.

With respect to the Theory of Planned Behaviour (TPB), Sommestad et al. (2015) argue that the TPB lacks a component concerning the negative emotion or risk of not being compliant with information security policy. They explain that for studying information security behaviour, TPB needs to be improved by adding new constructs, anticipated regret and the threat appraisal process.

With respect to the Protection Motivation Theory (PMT), Menard et al. (2017) note the inconsistencies and misspecification of PMT, that is the nature of a person's cognitive processes related to individual health care. However, in information security research, threat and coping processes are related to the protection of information belonging to the individual. Moreover, at the organisational level, with low psychological ownership of the data, the individuals' perception of relevance further decreases (Barki et al., 2008).

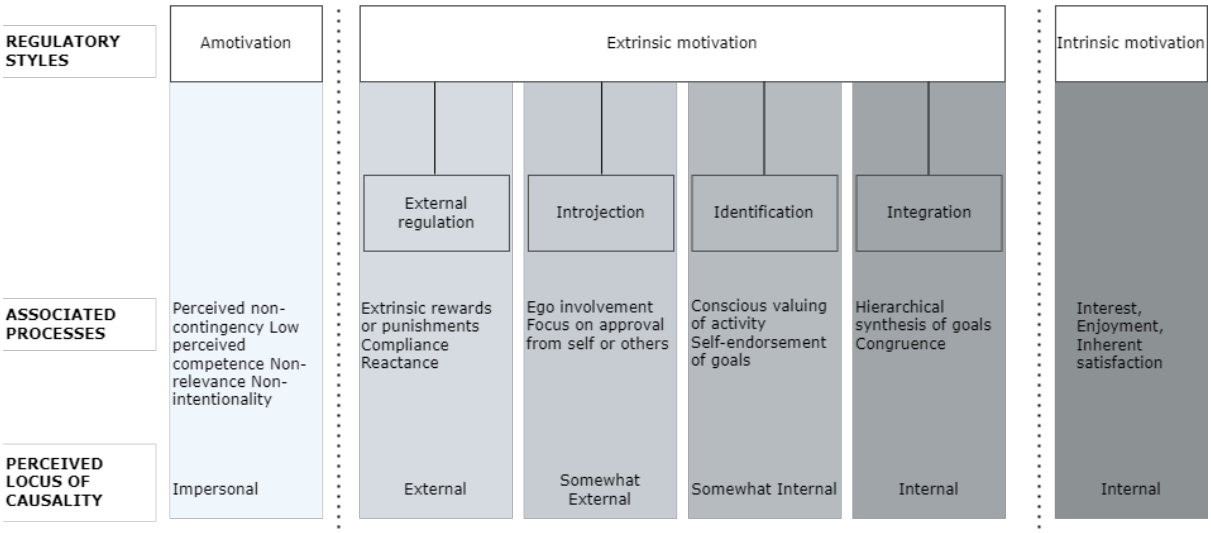
Therefore, to extend the domain of applied theories and understand the factors that may accentuate or diminish motivation, this dissertation applied the self-determination theory (Deci and Ryan, 1985; Deci, 1992; Ryan and Deci, 2000) to study cybersecurity behaviour. To the best of our knowledge, this is the first time that SDT has been used for designing and evaluating cybersecurity self-paced tools.

SDT (Ryan and Deci, 2000) provides a helpful lens through which a broader understanding of human motivation is achieved. It proposes two basic distinct types of motivation: intrinsic and extrinsic. "Intrinsic motivation refers to doing something because it is inherently interesting, and extrinsic motivation refers to doing something because it leads to a separable outcome." SDT classifies different types of extrinsic motivation that reflect different degrees of autonomy or self-determination. It indicates that two processes describe the autonomous extrinsic motivation for behavioural regulations. "Internalisation is the process of taking in a value or regulation, and integration is the process by which individuals more fully transform the regulation into their own so that it will emanate from their sense of self." Also, SDT

identifies a set of basic psychological needs to become more self-determined: competence, autonomy, and relatedness. Autonomy refers to a desire to participate in activities with a choice of freedom or a sense of volition. Competence refers to individuals' desire to interact effectively with the environment to produce desired outcomes and prevent undesired results. Relatedness reflects a sense of connectedness and belonging to others or a social environment (Deci, 1992; Vallerand, 1997). Figure 1.4 depicts the taxonomy of human motivation in SDT.

Figure 1.4

A taxonomy of human motivation. Based on (Ryan and Deci, 2000), Self-determination theory



Amotivation or unwillingness refers to a state of lacking the intention to act due to coercion, leading to failed goal achievement. Amotivation results from not valuing an activity, not feeling competent to do it, or not expecting the activity to yield a desired outcome.

Extrinsic motivation is based on external regulation, a continuum from coercion to stimulating intrinsic motivation. It refers to performing an activity because it leads to an expected outcome.

External regulation is the least autonomous type of extrinsic motivation. External regulation is associated with control or alienation, and actions are perceived imposed by external regulators. External regulation is achieved with salient rewards or threats.

Introjection is more internalised than external regulation, but it is still quite controlling. Introjection describes a form of regulation that is not accepted as one's own. However, behaviours are performed to maintain a feeling of worth, e.g., to avoid guilt or anxiety or attain pride.

Identification is a more self-determined form of extrinsic motivation. Identification occurs when an individual has understood the personal importance and value of an activity.

Integrated regulations are the most autonomous form of extrinsic motivation, fully assimilated to the self as a result of evaluation and bringing the regulations into congruence with one's other values and needs.

Intrinsic motivation refers to performing a behaviour because it is inherently interesting or enjoyable. Such motivation results from the individual's personality, habits, and skills. An individual with intrinsic motivation tends to seek out novelty and challenges to explore, learn, and exercise one's capacities, even without specific rewards.

Although SDT is an infrequently used theory for studying cybersecurity behaviour, there are studies that have considered and empirically supported SDT in this domain. Pham et al. (2017) applied the self-determination continuum to highlight the gap between experts' views of security compliance and users' views. They argued that experts use external regulation by focusing on rewards and punishments. However, the end-users want to be self-determined. Therefore, designing a human system that allows for self-determination in compliance without increasing the risk to the organisation is required. Padayachee (2012) studied the extrinsic and intrinsic motivations that affect the propensity toward information security compliance behaviour. The study proposed a classification of the research done on compliant behaviour from an end-user perspective and based on self-determination theory. Menard et al. (2017) explained that understanding end users' motivation to perform information secure behaviours would lead to greater adoption of safeguards. They demonstrated that an alternate form of security appeals based on autonomy, competence, and relatedness leads to a greater intrinsic desire to protect information and the intention to engage in secure behaviour among employees. They argued that motivating behaviour using fear might not be the most effective means of eliciting secure behaviours, and a motivational model based on SDT, rather than on PMT, explains more variance in employees' intention to perform secure behaviour.

This dissertation aims to demonstrate that an SDT theoretical perspective can boost our understanding of how enterprises (with respect to CEOs' and employees' roles) may be motivated to adopt good practices for diverse levels of motivation that range from amotivation to intrinsic motivation. Enterprises have different types and business models and, consequently, needs. Executives as the main role in the decision-making process for supporting cybersecurity compliance in their companies (Lange et al., 2000; Da Veiga and Eloff, 2007; Lee and Larsen, 2009; Ifinedo's study, 2014; Njenga and Jordaan, 2016; Barlette and Jaouen, 2019; Heidt et al., 2019) also have various cognitive capacities, knowledge, and experience in cybersecurity. Therefore, providing general solutions and recommendations cannot support motivation, nor can it assist adherence and adoption of best practices. It means that it is required to pay sufficient attention to personalised strategies for supporting long-term planning for adherence according to this diversity. For example, enterprises that are not aware of the value and importance of basic cybersecurity mitigations may need to establish a connection with a cybersecurity expert and peers. They should not be given information about contemporary advancements and changes in the threat landscape. Knowing how to promote active and volitional forms of cybersecurity behaviour with respect to the context heterogeneity may support better cybersecurity engagement.

Our literature review (Chapter 2) highlighted the key issues and avenues for future research (Table 1.1). The findings in Table 1.1 influenced the author's research approach and will be discussed in more detail in the following chapters.

Table 1.1

Potential directions and themes for future research were identified in the literature review (chapter 2) and then considered in the subsequent chapters.

Theme	Suggestions for future study in information security adherence	Chapter
Behavioural Theory	Self-determination theory of motivation. • Studying different types of motivation (not only punishment / reward) • Studying hypothesised effects of autonomy, competence, and relatedness on employees' compliance, adherence, and adoption	3, 4, 5
Goal of Adherence	Considering the importance of • Effectiveness of information security communication • Risk perception • Awareness-raising	4, 5, 6, 7
Research Methodology	Considering additional research methods • Experiment • **Design science** and action research	2 - 7
Context Heterogeneity	Proposing tailored solutions • Design and evaluation of volitional self-endorsed cybersecurity approaches • Classification of heterogeneous contexts for effective communication	3, 4, 6, 7

1.5 RESEARCH QUESTIONS

In this section, the research questions are presented. According to the structure of this research, the research questions were mapped to the design science research method's activities proposed by Peffers et al. (2007) for the construction and utility evaluation of our artefacts. Peffers et al.'s research method will be elaborated on in section 1.6. Further, using the self-determination theory of motivation as the theoretical foundation of this study guided the author in formulating research questions to produce knowledge about the self-determined cybersecurity behaviours concerning the use of our self-paced tool. Thus, the arguments for users' behaviour can be traced back to the SDT constructs. Table 1.2 illustrates a holistic view of the integration of the research questions, research activities, iterative design cycles, knowledge contributions, and chapters.

The main research question (MRQ) of this study is:

MRQ: How can we support volitional forms of behaviour with a self-paced tool to increase the quality of cybersecurity engagement?

The MRQ assisted in discovering how to promote more active and volitional forms of cybersecurity behaviour, identifying the design objectives of a self-paced tool for effective communication, organising the evaluation approaches, and accumulating knowledge for effective cybersecurity interventions. Further, it supported the author in formulating the following research questions concerning the practical and knowledge problems during the research process.

"Practical problems call for a change of the world so that it better agrees with some stakeholder goals. Knowledge problems, by contrast, do not call for a change of the world but a change of our knowledge about the world" (Wieringa and Heerkens, 2006; Wieringa, 2009).

Chapter 2 has four research questions.

RQ1: What theories are in use to explain adherence to good information security practices?

RQ1.1**: What are the goals of adherence that can be explained with these theories?**

RQ1.2**: What is the state of empirical validation of these theories for explaining adherence?**

RQ2: How do the characteristics of small- and medium-sized enterprises affect the adherence to information security?

These research questions want to acquire available knowledge about the studied theories and the context characteristics. Bada et al. (2015) argue that attention to psychological theories is important in information security since changing employees' behaviour plays a crucial role in awareness campaigns. Haeussinger and Kranz (2017) indicate that scholars and practitioners recently shifted their attention to behaviourism and social psychology theories to explain the human aspects of information security. Therefore, the research questions in chapter 2 investigated the current knowledge about the applied theories to guide the other design science steps. RQ1 aims to recognise theories from different disciplines that have been considered in the context of SMEs' information security behaviour. RQ1.1 wants to identify and consolidate the main goals of adherence to information security practices. RQ1.2 contributes to exploring and synthesising the state of empirical support and evaluation methods that have been used. Finally, RQ2 wants to identify the specific characteristics which can affect information security engagement.

Chapter 3 focuses on one research question.

RQ3: How is SDT operationalised in a self-paced tool to facilitate end-users' self-endorsed cybersecurity behaviour?

Several scholars have emphasised the importance of cybersecurity tools for fostering good cybersecurity practices and assisting in awareness-raising (Furnell et al., 2002; Brunner et al., 2018; Ponsard et al., 2019). The European Network and Information Security Agency (ENISA, 2020) highlights the need for the right tools to help SMEs be protected against cyber threats before they happen. However, there is resistance to adopting cybersecurity tools and changing the behaviour of employees (West, 2008). Many studies emphasise the importance of employees' motivation in order to support the adoption of best practices and behaviour change. Therefore, SDT has been applied in the design of our self-paced tool to facilitate volitional cybersecurity behaviour.

Chapter 4 seeks to answer two research questions.

RQ4: How do the available features of cybersecurity tools influence the effectiveness of communicating cybersecurity to motivate users' adoption of desired behaviour?

RQ5: Do the SME human end-users perceive the tool to be useful as a tool assisting do-it-yourself cybersecurity assessment?

Wieringa (2009) explains that design and research are closely related activities. He indicates that "design science emphasises the connection between knowledge and practice by showing that we can produce scientific knowledge by designing useful things."

In the formative evaluation of the artefact (CYSEC), the author posed RQ4 and RQ5 to assess how the CYSEC features supported desired behaviour and how users experienced the self-assessment tool's usefulness. The results provided us with essential feedback to identify the key areas for improvement of the CYSEC design. In RQ4, the author evaluated the effectiveness of communication by observing users' behaviour, attention, comprehension, and theoretical cause-effect relationships. In RQ5, the author examined the users' attitudes about the tool's acceptance and usefulness.

Chapter 5 focuses on one research question.

RQ6: Do the choice of anonymity and the elaboration of how shared information will be used motivate SMEs to share security information?

After the formative evaluation of CYSEC, it was evident that security information sharing is a significant concern for CISOs and CEOs. Security information sharing is an important measure for companies (Lewis et al., 2014). So, the research centred around information sharing. An online consent prototype has been designed to tackle the challenges of lacking motivation and trust. Trust influences a user's willingness to share security information (Bedrijfsrevisoren et al., 2015). As a knowledge task, the author asked the CISOs whether the online consent prototype would motivate them to share security information if implemented. The study focused on the impact of motivational constructs, controlling over data through choices, online agreement, and familiarity with the usage of shared information.

Chapter 6 wants to answer one research question.

RQ7: What are the reasons that result in the intended use and usefulness of the tool for cybersecurity competence improvement?

In the summative evaluation of CYSEC, the author posed RQ7 to discover how CYSEC is relevant and valuable for the users after the incremental improvements. For this evaluation, a cloud version of CYSEC was available within the context of twelve companies for two months. The study yielded important lessons learned about the impacts of CYSEC and the influential factors that affected its use and usefulness. Identifying the vital factors that may impact the effectiveness and adoption of awareness-raising solutions is essential to support sustained engagement in cybersecurity practices (Bada et al., 2015).

Chapter 7 seeks to answer one research question.

RQ8: How can we classify the heterogeneous SME context to reduce the complexity of approaching effective cybersecurity?

The summative evaluation clarified that it is necessary to understand SME heterogeneity and recognise their distinctions to advance the knowledge about approaching cybersecurity in SMEs. While studies commonly distinguish between SMEs based on the number of employees (e.g., Gupta and Hammond, 2005), it does not point out SME cybersecurity capabilities and

vulnerabilities. This understanding raised a new question (RQ8), and the author investigated the SME classification based on their cybersecurity competence, connectedness to cybersecurity expertise, and personalisation of needs. Classification allows us to go beyond the information given and better perceive the world structure (Rosch, 1978; Smith and Medin, 2013). Then the author proposed cybersecurity remedies (according to the use cases' feedback) most suited to each class of SME. The classification framework provides a simplifying tool that may help systematically describe and compare SME cybersecurity needs, communicate effectively with them, apply research findings to propose tailored solutions, and predict future improvement areas.

The next section explains the research framework, the main artefact, the research context (SME), the research process, and the applied methods for theory development.

Table 1.2

An overview of the research activities and the dissertation chapters

Main RQ	**Method/Strategy**	**Main Activity**	**Design Science Iteration**	**Focal Knowledge Contribution**	**Chapter**
RQ1, RQ2	Literature Review	Problem Identification	1	A report of the current state of the knowledge: applied theories – identifying the gaps and proposing SDT and the avenues for future cybersecurity research	Chapter 2
RQ3	Design Science, Lessons Learned	Design, Inductive Evaluation	1	Implementing SDT for designing the self-paced tool and method (CYSEC)	Chapter 3
RQ4, RQ5	Case study (observation), Questionnaire	Deductive Evaluation	1	Describing the effectiveness of CYSEC for supporting cybersecurity communication	Chapter 4
RQ6	Design Science, Semi-structured Interview	Design, Deductive Validation	2	Implementing SDT for designing an online consent – describing the effectiveness of the prototype for security information sharing	Chapter 5
RQ7	Survey, Structured Interview	Design, Inductive Evaluation	3	VCS appraisal, identifying the influential cybersecurity behaviour factors – describing the effectiveness of CYSEC product	Chapter 6
RQ8	Conceptual Modelling	Categorisation	3	Proposing an original SME classification framework – identifying the improvement needs by each class	Chapter 7

1.6 RESEARCH FRAMEWORK AND THEORY DEVELOPMENT

This section provides an overview of the design science research process for the construction of VCS and the context in which the validation of VCS has been performed. In design science studies, theory development is based on the design and evaluation of artefacts (Gregor and Hevner, 2013). Gregor and Hevner (2013) study the knowledge contributions of design science research (DSR). They indicate "one process of maturation in a body of knowledge and theory development, beginning with the development of a novel artefact." The development of theories about the artefacts that meet business needs produces knowledge that aids in the shared knowledge base of design scientists (Hevner et al., 2004; Wieringa, 2009).

During the research process, the author was involved in a sustained connection with 14 SME use cases (at first four and then ten new enterprises) and one SME association. The main artefact, CYSEC, was demonstrated in the context of use to evaluate its utility and effects on cybersecurity behaviour. According to Muronga et al. (2019), the evaluation of the effectiveness of awareness training tools for SMEs has not received adequate attention. To bridge this gap and improve the quality of the CYSEC and the quality of produced knowledge, the author conducted two artefact evaluations, formative and summative.

The formative evaluation of CYSEC provided empirically based knowledge that helped us identify several improvement features. The author applied a deductive approach in this evaluation phase due to the selection of SDT as the kernel theory. "The deductive research starts with existing theory, sets out hypotheses for the research, and finally makes observations" (Runeson et al., 2012). According to Runeson et al.'s recommendation for deductive research in software engineering, the explanatory multi-case study (observation strategy) and short survey were applied in this step. When we have a developed theory as a template, the model of generalisation is the analytic generalisation (Yin, 2009).

The summative evaluation surfaced the influential factors that may affect the usage and success of cybersecurity tools. The author applied an inductive thematic approach in this phase of evaluation. "In inductive research, the researcher [...] sets up tentative hypotheses, and relates them to existing theory or develops new theory" (Runeson et al., 2012). Thematic analysis is a method for identifying, analysing, and reporting themes or patterns within collected data (Braun and Clarke, 2006). According to Runeson et al.'s recommendation for inductive research, the exploratory case study (structured interview) and a questionnaire survey were applied. "A case study will never provide conclusions of statistical significance" (Runeson et al., 2012).

This study investigates the qualitative evaluation of the artefacts. The qualitative research fitted well with the author's goals to understand the heterogeneity of the context. It provided significant insights into the tacit knowledge that was of interest and was only available in the minds of CEOs and CISOs. The qualitative evaluation approach is aligned with the Runeson et al. (2012) recommendation in empirical studies and Hevner et al. (2004) recommendation in design science research. Qualitative methods have been used to study cybersecurity behaviour, SDT in cybersecurity, and cybersecurity for organisations (e.g., Dojkovski et al., 2010; Njenga and Jordaan, 2016; Pham et al., 2017; Kabanda et al., 2018; Choi et al., 2018; Heidt et al.,

2019). Qualitative studies may add value to the training and awareness research field due to the dominance of quantitative work (Lebek et al., 2014). A qualitative study is a more useful alternative to determine richer insights with a small number of subjects (Lee, 2003). When the study sample size is rather small, hard statistical indexes are not of particular importance (Jarvinen, 2001; Tryfonas et al., 2001). Accordingly, interpretive research and empirical evaluation are deemed to be appropriate (Klein and Myers, 1999; Tryfonas et al., 2001). Qualitative assessment is needed to understand the interaction of people, organisations, and technology for theory development or problem-solving (Hevner et al., 2004; Klein and Meyers, 1999).

1.6.1 CYSEC, the Main Artefact

By applying the design science research method, we designed and evaluated a self-paced method and tool, CyberSecurity Coach (CYSEC), for the delivery of cybersecurity capabilities and awareness-raising. The CYSEC method is designed to allow users easy access to the repository for many cybersecurity remedies. It provides Do It Yourself (DIY) step-by-step instructions to assist users in information security control implementation, intra-organisational information exchange, and continuous progress. The design of the tool is grounded in the rigorous psychology theory of motivation (Self-determination theory) for the sustainability of the improvements.

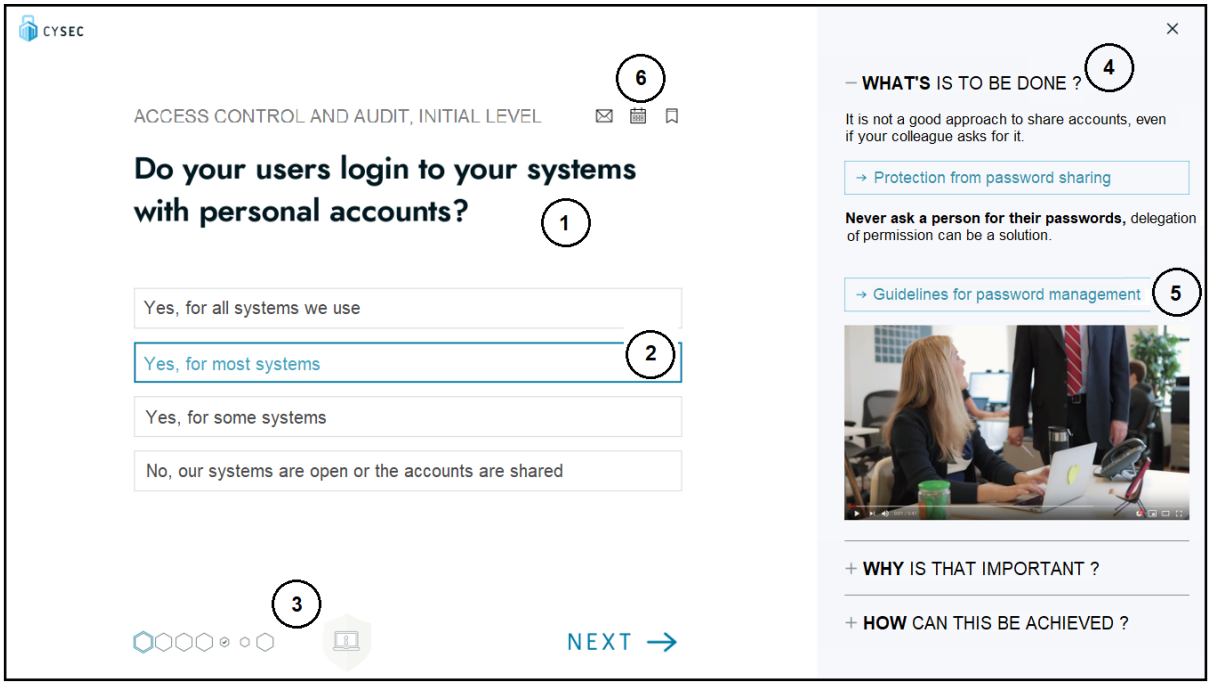
CYSEC has two main interfaces (Capability Improvement Dashboard and Capability Work Area), and each interface has several components (described in more detail in chapters 3, 4 and 6).

The Capability Improvement Dashboard shows an overview of the available capability areas, recommendations, and summary section. Capability areas are thematic blocks that consist of stepwise series of questions and training content. CYSEC has six capability areas, including Company, Patch Management, Access Control and Audit, Malware Scans, User Training, and Backup. Recommendations offer tailored solutions according to the users' answers to the self-assessment questionnaires and specify the improvement requirements to help users who are unsure of the next steps. The summary section demonstrates the progress status and latest achievements.

The Capability Work Area encompasses self-assessment questionnaires (Ozkan and Spruit, 2018), embedded awareness training content, and a summary page, see Figure 1.5. The questionnaires and pertinent awareness content together a) facilitate learning and diagnosis of potential threats and vulnerabilities and b) supply users with guidance on implementing controls for each capability in a DIY manner. The order of questions has an easy to advanced capability pattern, and users' responses influence the adaptation of questions. At the end of each capability area, a summary page is shown, and users have the option to start a new capability area or get back to the dashboard.

Figure 1.5

Example of a questionnaire screen in the work area. 1: question. 2: answers with immediate feedback. 3: progress for achieving an information security goal. 4: What, why, how guidance. 5: learning module. 6: involvement of employees and planning follow-ups.



1.6.2 The Context of the Research: SME

Organisational size has been considered as a variable that may have a relation to employees' cybersecurity behaviour and the organisation's cybersecurity culture. Many studies have found it positively related to policy compliance intention or behaviour (e.g., Parsons et al., 2015; Song, 2016; Mijnhardt et al., 2016; Solomon and Brown, 2020; Aigbefo et al., 2022). For instance, Parsons et al. (2015) indicate that organisational information security culture and information security decision-making tend to improve as the size increases. Solomon and Brown (2020) argue that organisational size is significantly relevant to compliance behaviour. However, many studies argue that organisational size offers no causal explanation of employees' cybersecurity behaviour (e.g., Lee and Larsen, 2009; Herath and Rao, 2009; Bulgurcu et al., 2010; Guo and Yuan, 2012). For instance, Lee and Larsen (2009) argue that firm size has no significant effect on adopting protective solutions. However, executives' adoption intention and IT budget significantly influence the adoption of cybersecurity solutions in SMEs.

This research was performed in the SME context. Studies commonly distinguish between SMEs based on the number of employees (Gupta and Hammond, 2005). However, there is no standard international definition of SMEs (OECD, 2017). This dissertation refers to the European Commission's (2003) definition. Accordingly, SMEs are "enterprises which employ fewer than 250 persons and which have an annual turnover not exceeding EUR 50 million, and/or an annual balance sheet total not exceeding EUR 43 million." SMEs make substantial

contributions to the national economic growth and are central to the efforts to achieve environmental sustainability (Lange et al., 2000; OECD, 2017). They represent 99% of all businesses in the EU (European Commission, 2003).

Literature indicates some characteristics of SMEs (Ghobadian and Gallear, 1996; Huang et al., 2010; Gundu and Flowerday, 2012; Njenga and Jordaan, 2016; Mijnhardt et al., 2016). The systematic literature review in chapter 2 highlighted that the constraints of a) technical skills, b) knowledge and awareness, and c) financial resources are the frequently mentioned SME characteristics. Renaud and Weir (2016) indicate that "an SME that acknowledges the likelihood of attacks is still at risk of implementing insufficient measures." These characteristics demonstrate that SMEs need a great demand for remediation actions to enhance their cybersecurity understanding and ward off ever-present cyber threats.

The participating organisations provided a rich diversity of SMEs, differentiating in size, business interests (IT intensive and non-IT intensive), cybersecurity maturity, IT maturity, awareness level, implemented measures, and information security policy availability. Three of them were cybersecurity providers, and three had written information security policies. One of them had no skills in cybersecurity and IT (even basic knowledge). The participating SMEs came from six EU countries (France, Spain, UK, Greece, Italy, and Switzerland).

The research focused on CEOs' and CISOs' behaviours. All the subjects were CISOs or senior managers, and all except one subject have been responsible for cybersecurity tasks within their companies. Three of the subjects were cybersecurity experts. Abundant literature emphasises the significant roles and responsibilities of top management in preventive efforts and commitment to effective cybersecurity in organisations (e.g., Kankanhalli et al., 2003; Da Veiga and Eloff, 2007; Lee and Larsen, 2009; Dojkovski et al., 2010; Njenga and Jordaan, 2016; Heidt et al., 2019; Barlette and Jaouen, 2019). For instance, Lee and Larsen (2009) explain that SME executives could adequately assess their companies' collective capabilities for the adoption of cybersecurity tools. They are willing to adopt solutions when they are confident in their organisation's ability to use them.

1.6.3 The Research Process

Peffers et al. (2007) propose a method for performing design science research in information systems. This research method "*provides a nominal process model for doing design science (DS) research, and it provides a mental model for presenting and evaluating DS research in IS.*" Figure 1.6 depicts the application of this method in this dissertation. Peffers et al. (2007) delineated six activities for the DS process:

Activity 1: Problem identification and motivation. "*Define the specific research problem and justify the value of a solution.*"

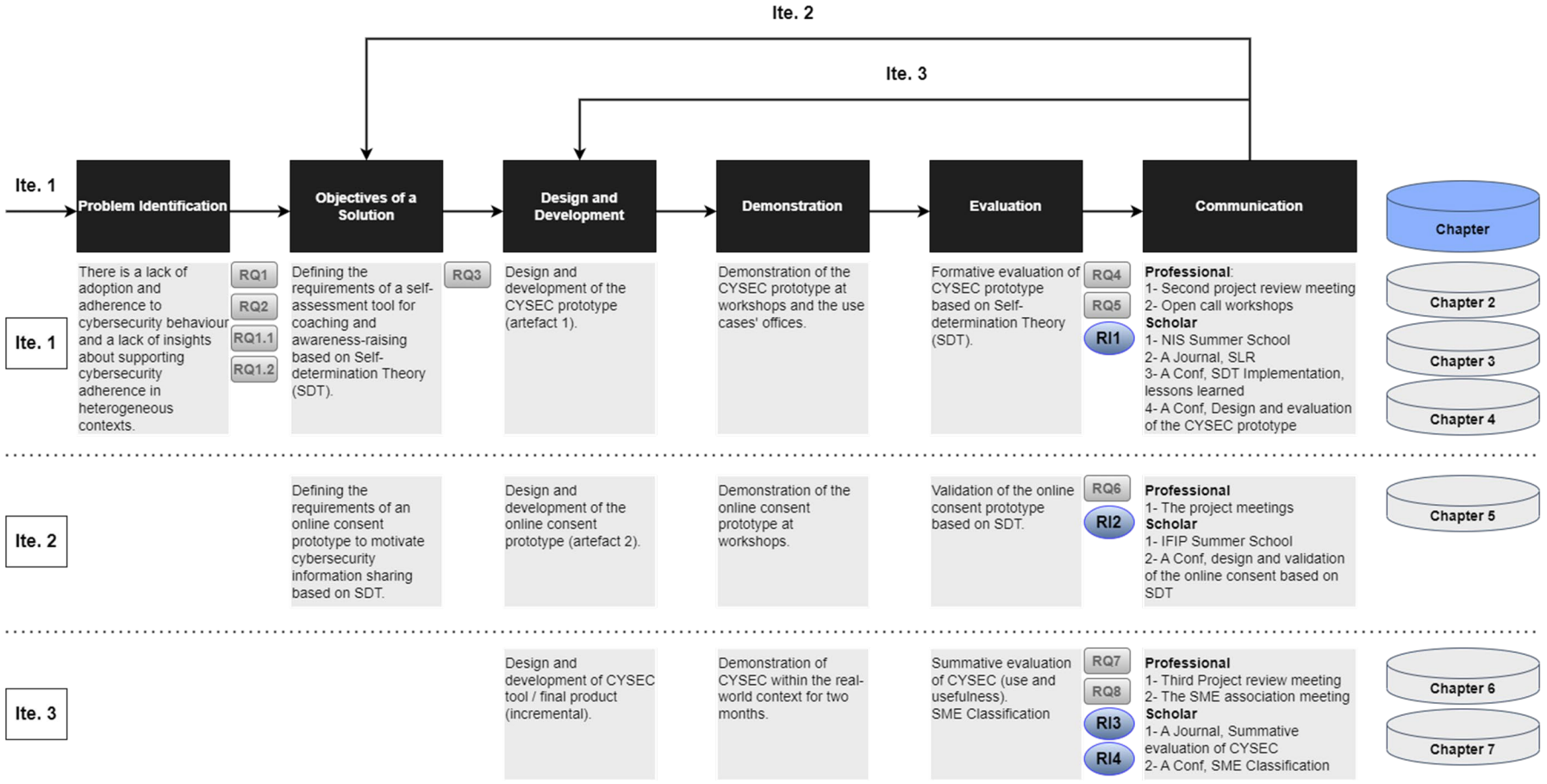
Activity 2: Define the objectives for a solution. "*Infer the objectives of a solution from the problem definition and knowledge of what is possible and feasible.*"

Activity 3: Design and development. "*Create the artefact*."

Activity 4: Demonstration. "*Demonstrate the use of the artefact to solve one or more instances of the problem*."

Figure 1.6

Design science research process in this dissertation (Based on Peffers et al. (2007))



Activity 5: Evaluation. "*Observe and measure how well the artefact supports a solution to the problem*."

Activity 6: Communication. "*Communicate the problem and its importance, the artefact, its utility and novelty, the rigour of its design, and its effectiveness to researchers and other relevant audiences such as practising professionals, when appropriate."*

Peffers et al. DSRM serves as the primary research framework for creating and evaluating our artefacts. Our research process has three consecutive iterations; Peffers et al. activities were applied in each iteration. At the end of each iteration, the findings are communicated first to the project partners (e.g., in the second and third project review meetings, meetings with the SME association representatives) to check the accuracy of the qualitative findings and then submitted to the conference proceedings or journals (Figure 1.6).

Iteration 1

This iteration started with problem identification and motivation. The adoption of cybersecurity tools and adherence to appropriate behaviour have been aptly noted as essential for improving cybersecurity posture in organisations. Therefore, two activities have been done in this step. A) a survey to recognise the users' needs and realise the problem situation in the use cases; and B) a systematic literature review (snowballing strategy; Wohlin (2014)) to identify the applied theories that studied cybersecurity behaviour and the empirical state of their validation. The findings of the survey provided us with knowledge about the use cases. The findings of the literature review influenced the selection of the research methods. Also, the author found the theory gap that exists in SME cybersecurity studies, and SDT has been proposed as the kernel theory of this dissertation. "Knowledge of the underlying theoretical background would help practitioners and scholars to understand why a particular IS security awareness approach is expected to have the desired impact on users' information security behaviour" (Puhakainen, 2006). Then, the author identified the requirements and operationalised the SDT constructs in the CYSEC design to support effective counselling communication and facilitate daily self-determined cybersecurity behaviour.

Research Impact 1 (RI1). The design knowledge and idea, based on SDT constructs and the relationship between requirements and features, have been subsequently used in the follow-up project design (van Haastrecht et al., 2021).

Then several workshops were organised to demonstrate the CYSEC prototype in the users' offices to see if the design worked as intended. A multi-case study using an observation strategy (Runeson et al., 2012) and a post-observation questionnaire (to understand the users' attitudes and support the triangulation) were applied. The study goes beyond just evaluating intentions or theoretical relationships as in the common survey-based studies. This approach provided us with first-hand experience of CYSEC's use and usefulness in SMEs.

Then the author conducted the formative evaluation (deductive analysis) of the artefact features. The findings helped to identify the new needs that influence tool usage and capability

improvement. The author also discovered that CYSEC should have considered SME confidentiality concerns for sharing security information with a third-party tool.

Confidentiality concerns may impact SME responses to adopting the tool and effective cybersecurity communication. This finding activated the second iteration. Further, the author found that the tool needs to support a) personalised recommendations for cybersecurity tools, b) immediate feedback, c) new cybersecurity capabilities (e.g., Backup), d) the adaptation according to the company requirements, e) progress summary and f) easy-to-apply awareness training content. These findings activated the third iteration.

Iteration 2

According to the identified problem in the first iteration, this iteration started with defining of objectives of the solution. The author applied an SDT model for knowledge sharing in virtual communities (Yoon and Rolland, 2012) to identify the objectives of the solution and support users' motivation for security information sharing. Afterwards, an online consent prototype was designed. Then the artefact was validated by applying semi-structured interviews (deductive analysis). The findings showed that users' perception of control over information sharing (providing choices to have selective permission controls) influences their motivation for security information sharing. The findings, at first, were presented in a summer school and then at a conference.

Research Impact 2 (RI2). The design knowledge and idea of supporting security information sharing have been subsequently used in the follow-up project (van Haastrecht et al., 2021).

Iteration 3

According to the newly identified requirements in the first evaluation, the CYSEC design was improved, and new features were developed. Then, the author conducted the summative evaluation (inductive analysis) to rigorously evaluate the utility of the designed solution and identify the drivers and impediments that influenced the effectiveness and adoption of CYSEC. For this evaluation, CYSEC was placed in operation in real SME environments for two months. The author applied a survey study and then structured interviews. The findings revealed three types of cybersecurity awareness and their impact on user adherence and adoption. Also, the findings showed that personalisation, cybersecurity competence, and connectedness to cybersecurity expertise influenced adoption and adherence in the heterogeneous context. The findings demonstrated that CYSEC had an impact on awareness-raising and cybersecurity behaviour.

Research Impact 3 (RI3). The need for connectedness to cybersecurity defenders has been subsequently considered in the follow-up project (van Haastrecht et al., 2021).

Through the inductive analysis of the summative evaluation, it was evident that SMEs were heterogeneous. They exhibited diverse cybersecurity needs, perceptions, and capabilities. Therefore, it offered the notion of classification and identifying the improvement needs for each class. Therefore, five concepts or names to represent five types of companies were

formulated (Abandoned, Unskilled, Expert-connected, Capable, and Provider) and the exemplars were provided. Accordingly, cybersecurity interventions that are effective for one class of SMEs are not necessarily effective for another. The author argues that when we classify SMEs and approach them with well-targeted cybersecurity awareness training content aligned with their own needs and values, we can reduce communication complexity and support a better quality of cybersecurity engagement. SME classification and identifying associated needs with respect to awareness types demystify the topics of awareness-raising and organise the body of knowledge in the fields of SME cybersecurity. We can identify **what class of SMEs lack what type of awareness** and propose tailored compatible solutions instead of using the common ambiguous sentence: "many SMEs have a lack of awareness" and providing untargeted solutions.

Research Impact 4 (RI4). The proposed SME classification framework has been subsequently applied to the follow-up project requirements deliverable, and its usefulness has been confirmed (D1.1, Geiger, 2020).

1.7 THE CHAIN OF CHAPTERS

This dissertation has eight chapters. Chapter 1 provides the introduction to the study. Chapters 2 to 7 are structured around the design science research method's activities supported by Peffers et al. (2007) and together tell one story. The main proposed avenue for future research in each chapter is studied in the next chapter (the chain of chapters). These chapters have been published or are currently under review in conference proceedings and journals. Chapter 8 concludes the dissertation and proposes future research avenues.

Chapter 1. This chapter presents an overview of all chapters and studied concepts. A background of barriers deterring cybersecurity behaviour, available solutions for improving adherence to good practices, and their limitations are discussed. The significant concepts about human-related cybersecurity concerns and awareness training strategies are described. Several systematic literature reviews and their links to this dissertation are studied. Afterwards, Volitional Cybersecurity theory is introduced, and the research questions, research framework, applied methods, and knowledge contributions are elaborated to assist readers in gaining an understanding of the structure of this research and its outcomes.

Chapter 2. This chapter elaborates on the systematic literature review about adherence to information security practices. This chapter investigates the proposed theoretical foundations and the extent of empirical evidence that information security adherence has been validated. This is the first literature review in this context (for SMEs), selecting 25 papers published between 2003 and mid-2020. The snowballing strategy based on the Wohlin (2014) guidelines is applied. This chapter specifies a series of research avenues (Table 1.1) studied in the following chapters to understand the context and address some gaps regarding adherence to cybersecurity measures.

A shortened instance of chapter 2 is submitted to a journal as Shojaifar, A., Fricker, S., Spruit, M. (2022). Adherence to Information Security in Small and Medium-Sized Enterprises.

Chapter 2 indicates that "*to extend the domain of applied theories for SMEs, self-determination theory as a new research focus to study information security adherence is proposed*", which is being studied in Chapter 3.

Chapter 3. This chapter introduces CYSEC, the main artefact that implements the self-determination theory to prompt end-users to sustainable self-endorsed forms of behaviour and guide them to carry out the cybersecurity recommendations in an iterative process on their own. The chapter presents the synthesised findings through the lessons learned from the use of CYSEC. The chapter makes a design knowledge contribution to the follow-up project.

Chapter 3 is published as Fricker, S., Shojaifar, A. (2022). Self-endorsed Cybersecurity Capability Improvement for SMEs. In Proceedings of the 28th annual Americas Conference on Information Systems (AMCIS 2022), Minneapolis. Association for Information Systems.

Chapter 3 indicates a need "*to study how we can support effective communication between security experts and SMEs*", which is being studied in Chapter 4.

Chapter 4. This chapter offers insights into how the CYSEC features influence the effectiveness of counselling communication between a cybersecurity expert and SME employees to motivate users' adoption of desired behaviour. The author conducts a formative deductive evaluation of CYSEC through a multi-case study using an observation strategy based on the think-aloud protocol (Runeson et al., 2012) to study the actual use of the artefact in real-world settings. Before conducting the case studies, a pilot workshop is performed. Then six workshops in France, Greece, Switzerland, and Spain are conducted for the tool usage and data collection. The observation in each workshop is supplemented with a post-observation questionnaire to understand users' attitudes about the tool's acceptance and usefulness.

Chapter 4 is published as Shojaifar, A., Fricker, S. A., & Gwerder, M. (2020). Automating the Communication of Cybersecurity Knowledge: Multi-Case Study. In IFIP World Conference on Information Security Education (pp. 110-124). Springer, Cham.

Chapter 4 indicates that "*we discovered a potential barrier that should be addressed by future research: confidentiality. We observed resistance to documenting and sharing security-related information. Alleviating confidentiality worries is crucial for improving the method's success*" which is being studied in Chapter 5.

Chapter 4 indicates that "*the findings of the study suggest that one challenge of motivating and supporting SMEs is the choice of knowledge that is being communicated. The wrong knowledge, extraneous security awareness details, or knowledge gaps reduce motivation and influence the adoption of security recommendations*", which is being studied in Chapter 6.

Chapter 5. This chapter presents an online consent prototype (that engenders trust in CISOs) and its validation results. The formative evaluation reveals that confidentiality concerns about cybersecurity information sharing impact users' willingness to adopt our tool and quality of engagement. Therefore, an online consent prototype with multiple options for indicating a suitable level of agreement is designed and then validated. At first, a pilot study and then semi-

structured interviews with CISOs are conducted. A theoretical model based on self-determination theory is chosen to analyse the CISOs' information-sharing motivation. The chapter makes a knowledge contribution to the follow-up project.

Chapter 5 is published as Shojaifar, A., & Fricker, S. A. (2020). SMEs' Confidentiality Concerns for Security Information Sharing. In International Symposium on Human Aspects of Information Security and Assurance (pp. 289-299). Springer, Cham.

Chapter 6. This chapter offers insights into the summative inductive evaluation of CYSEC. It advances the understanding of cybersecurity activities in SMEs by studying the adoption of CYSEC. The findings demonstrate that SMEs are heterogeneous, with various vulnerabilities, training needs, and capabilities. The research applies a two-phase data collection process: a survey and then structured interviews. The chapter makes a design knowledge contribution to the follow-up project.

A shortened instance of chapter 6 is published as Shojaifar, A., Fricker, S. (2022). Design and Evaluation of a Self-paced Cybersecurity Tool. Information and Computer Security.

Chapter 6 indicates that "*Our future work will investigate SME heterogeneity. We intend to differentiate SME needs and vulnerabilities. We believe that well-targeted awareness training content can support the effectiveness of CYSEC.*", which is being studied in Chapter 7.

Chapter 7. This chapter investigates context heterogeneity. A classification framework with an outline of improvement needs in each class is proposed in this chapter. In addition, the study presents the framework's usage in the sampled use cases (exemplar). Not only does this chapter make a knowledge contribution to the follow-up project, but it also provides a topic for further discussion in the European Digital SME Alliance.

Chapter 7 is published as Shojaifar, A., & Järvinen, H. (2021). Classifying SMEs for Approaching Cybersecurity Competence and Awareness. In The 16th International Conference on Availability, Reliability and Security (pp. 1-7).

Chapter 8. This chapter summarises this research. It provides an overview of all the design and evaluation research activities and knowledge contributions. Further, the answers to the research questions, the main study limitations, significant dimensions for future research and reflections are elaborated on.

CHAPTER 2

The Theoretical Foundations of Information Security Behaviours

Information security is becoming increasingly critical for organisations, especially small and medium-sized enterprises (SMEs). Studies have shown that cyberattacks have shifted from targeting large organisations to SMEs. This changed attack pattern implies that not just a few large organisations with dedicated cybersecurity staff need to be protected, but many SMEs with neither the resources nor skills to the same extent as the large ones. This chapter investigates the research performed on factors affecting adherence to information security practices in SMEs. The chapter investigates the proposed theoretical foundations and the extent of empirical evidence that information security adoption and adherence have been validated. We conducted the first literature review in this context by selecting 25 papers published between 2003 and mid-2020. We used the snowballing strategy based on the Wohlin guidelines. 18 theories were identified that were used to explain adherence. The chapter offers a synthesis of these results and the main adherence goals with an in-depth discussion of the relevance of these theories and avenues for future research. The presented results have been used in the sketching of a research agenda for researchers and advice to practitioners to make information security feasible for SMEs.

A shortened instance of this chapter is submitted for publication:
Shojaifar, A., Fricker, S., Spruit, M. (2022). Adherence to Information Security Practices in Small and Medium-Sized Enterprises.

2.1 INTRODUCTION

Information security has received much attention in the media and trade journals in recent years. Data and systems have become critical assets in most organisations, and the threat of attack is continuing to grow. A recent study shows that there has been a marked increase in cyber criminality, including theft of information and communication technology (ICT) resources for coin-mining, injection of malware, and ransomware with an increased targeting of mobile and Internet-of-Things (IoT) devices (Cleary et al., 2018). The omnipresent threat of cybercrime implies that many companies view security as one of their top concerns (Cearley et al., 2017), and global spending on information security in 2018 has increased to $144 billion at a growth rate of 12.4 percent, from the last years (Moore and Keen, 2018).

Organisations are exposed to a wide range of attacks, including data theft, financial fraud, viruses, insider net abuse, and sabotage (Gupta and Hammond, 2005; Warren, 2002). A cyberattack can destroy, corrupt, deny access, or result in the theft of assets. Hackers are doing so for illicit financial gain, malicious damage to business operations, using an attacked system for further attacks, espionage, or as an act of war or terrorism (Kapur et al., 2015). In the context of the Internet, messages may be intercepted and manipulated, the validity of documents denied, and personal data illicitly collected (Spinellis et al., 1999). An incident may also happen due to negligence or inattention of an employee or user of the company's assets (Gundu and Flowerday, 2013). The consequences for the victim company are manyfold: they may include financial loss, legal and ethical responsibility, business service interruption, and quality problems (Ban and Heng, 1995; Ponemon 2018).

Small and medium-sized enterprises (SMEs) have become an important target for cyberattacks. According to the Symantec 2016 Internet Security Threat Report, SMEs are attacked increasingly frequently, and attacks on them have started to outnumber the attacks on large enterprises (Symantec 2016). SMEs face the same security challenges as larger companies, even though the priorities of the issues differ (Knapp et al., 2006). SMEs worry most about employee awareness and management support for information security, while large organisations are more concerned with patch management and malware.

Many SMEs have less effective procedures, policies, and controls in place to counteract cyber threats than large companies (Spinellis et al., 1999; Gupta and Hammond, 2005; Dojkovski et al., 2010; Kurpjuhn, 2015; Heidt et al., 2019). In an ideal situation, organisations would formally coordinate security, promote awareness of security-related issues during day-to-day activities, and train their staff (Furnell et al., 2002). However, SMEs often do not have staff with security expertise, lack financial resources to buy consultancy or training, lack understanding of risks, and are unable to focus on information security. These constraints prevent them from addressing information security comprehensively and make them more vulnerable to attacks from outsiders as well as from insiders with direct access to the company's systems.

To cope with the increase of cyber threats, not only technical solutions but also appropriate management methods, policies, and an information security culture with awareness training programs are necessary (Furnell et al., 2002; Julisch, 2013). Researchers criticized the currently

present ad-hoc practice for developing and deploying information security, however, and suggested that adherence methods be theoretically grounded and empirically evaluated for their effectiveness. Siponen et al. have been the first ones to show that theory-driven and empirically validated approaches may be effective (Siponen et al., 2007). They have shown that the Protection Motivation Theory, General Deterrence Theory, and the Theory of Reasoned Action could be used to explain employees' compliance to information security policy (Siponen et al., 2007). Other researchers have shown that individual factors can moderate the validity of aggregate-level theories. For example, D'arcy and Hovav have shown that the profile of an individual, e.g., measured with computer self-efficacy and status in the social organisation of the team, moderate the impact of policy, awareness and training programs, and computer monitoring on misuse intentions (D'Arcy and Hovav, 2009). Also, characteristics of an asset under protection, such as the quality of protected information, may play a role (Pahnila et al., 2007).

To more thoroughly comprehend the theories that may be used to understand and reason about adoption and adherence to information security in SMEs, we have performed a systematic literature review following the snowballing protocol proposed by Wohlin (Wohlin, 2014; Badampudi et al., 2015). To analyse the data extracted from the identified papers and synthesise the findings, we tabulated extracted information according to the research questions and followed the guidelines (Kitchenham and Charters, 2007).

The remainder of the chapter is structured as follows. Section 2 gives an overview of related works on information security and motivates our study. Section 3 outlines the research method. Section 4 describes the results of the systematic search. Section 5 interprets the findings of the data extracted from the papers. Section 6 discusses the implications, future research avenues, and study limitations. Section 7 summarises and concludes.

2.2 INFORMATION SECURITY IN THE ENTERPRISE

Information security in organisations has been the subject of extensive research. The secondary research that we describe here gives a broad overview of how to describe and analyse information security, of the theories used to explain the factors that influence information security, and of the frameworks that were proposed to build information security in the enterprise. We use the concepts presented here as a framework to analyse the information security behaviour of an enterprise.

2.2.1 Dimensions of information security

A common basis for describing information security in the enterprise is Bakry's STOPE model (AlHogail and Mirza, 2014), which stands for the dimensions of strategy, technology, organisation, people, and environment (Bakry 2003). The strategy dimension is concerned with the future development of the enterprise and sets objectives, policies, best practices, standards, and guidelines for information security. Technology is concerned with the effective use of hardware and software to make information systems secure and prevent incidents. Organisation is concerned with the structure and culture of the organisation, including the beliefs, values, assumptions, norms, and knowledge that influence security behaviour. People are concerned

with the preparedness, responsibility, and management of each individual in the enterprise. The environment refers to the national culture as well as government initiatives and regulations.

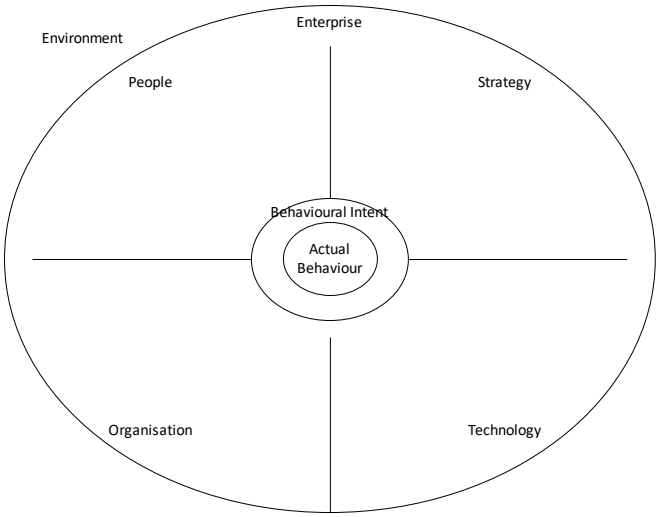
Figure 2.1 presents our analytical framework that relates the STOPE model with the behavioural intent and actual security behaviour of the enterprise. It suggests that the behaviour is a result of the state of affairs and changes in the strategy, technology, organisation, and people of the enterprise situated in its environment.

The strategy dimension includes the definition of security policies used to specify how employees should behave to prevent, detect, and respond to security incidents (Cram et al., 2017). Such policies are considered the foundational element of managing security (Glaspie and Karwowski 2017). They specify roles, responsibilities, and guidelines for acceptable use of information systems and the response to security incidents to minimize the enterprise's risks. The policies influence the organisation's information security culture and define the employees' expected behaviour.

The technology dimension concerns the hardware and software used to defend the enterprise against security threats. Several checklists that have been proposed to achieve comprehensive coverage as evaluate the defence (Dhillon and Backhouse, 2001). These checklists offer overviews of conceivable controls as countermeasures to secure information systems and prevent incidents. Priorities for cost-efficient protection can be set with a suitable risk analysis of data and systems.

Figure 2.1

STOPE dimensions (Bakry, 2003) applied for structuring the analysis of information security in the enterprise



The organisation dimension reflects the structure and culture of the enterprise. According to Schein (Schein 1985), culture is *"a pattern of shared basic assumptions that the [enterprise] learned as it solved its problems of external adaptation and internal integration, that has worked well enough to be considered valid and, therefore, to be taught to new members as the correct way you perceive, think, and feel in relation to those problems*." The concept of culture has also been applied to information security (Mahfuth et al., 2017). According to Ross and

Masters (Ross and Masters, 2011), security culture is a "*pattern of behaviours, beliefs, assumptions, attitudes, and ways of doing things that promotes security*." 18 frameworks have been proposed for describing or managing an enterprise's information security culture (Mahfuth et al., 2017). Some of these frameworks cover human factors with training and education for employees and other factors external to the organisation that influence the organisation's security culture.

Management support is an important factor in cultivating a security culture. (Glaspie and Karwowski, 2017; Soomro et al., 2016). An environment supportive for security must be cultivated with adequate budget, technology, and human capital. Management is responsible for organisational decision-making, including the development of information security policies and guidelines. The policies must be regularly reviewed to keep them updated on policies as technology advances. Management is also responsible for overseeing human resources and their awareness and compliance training. Management also must ensure that the security function of the enterprise and the information and IT infrastructure remain aligned with business objectives and security goals.

The people dimension concerns the individual employees of the enterprise. People are the essential asset of an enterprise but are viewed as one of the biggest potential threats to the company's security (Alotaibi et al., 2016). Since they are responsible for many security breaches, they must be given as much attention as technical issues. The employees' security awareness and behaviour have thus been one of the research hotspots in information security research (Lebek et al., 2013; Lebek et al., 2014).

Compliance with information security policy is one of the areas of major challenges in the people dimension. The employees' personality traits influence the employees' policy compliance and, consequently, the meeting of the organisation's security objectives. Information security must be promoted through dissemination, training, and enforcement of policies to prevent non-compliance with policies due to unawareness and the resulting malicious and negligent behaviour. The organisational goals and security policy are expected to be communicated clearly and consistently to the employees. The clarity of policies and usability of controls must be monitored to keep the cost of compliance small, prevent a false sense of security, and ensure that the employees can maintain good job performance.

The training of employees and the consequent awareness and knowledge of information security for a thriving security culture (Glaspie and Karwowski, 2017). Knowledge about policies, roles, and responsibilities helps employees develop a positive attitude towards security and avoid errors that can be a liability to security. Training needs to be up to date with current technology and threats, be understandable by connecting to the terminology and habits of the employees and being of benefit to the targeted employees. The training must be established across the organisation and information security knowledge sharing and collaboration facilitated. The training should be experiential; employees who have experienced a cyber threat are likely to take protective actions. Especially for organisations under specific regulatory authority, training should be recurring and keep up with changes in business processes, standards, and regulations.

Most security policies contain information about penalties for non-compliance and rewards for compliance to reinforce the employees' beliefs about the benefit of compliance and the cost of non-compliance (Glaspie and Karwowski, 2017). Deterrence against negative employee behaviour ranges from remediation to termination of employment. Self-imposed needs, such as social acceptance and approval, and the will to act for a common cause are moral beliefs and social pressures that are used as incentives for compliance.

The organisation and people dimensions are intertwined. On the one hand, the employees' attitude towards compliance affects the information security culture in the enterprise because they are perceived by their colleagues. On the other hand, shared security knowledge and collaboration effects compliance (Glaspie and Karwowski, 2017). Workgroup norms drive individual attitudes. Involving users in the development of security practices can influence the perceived ease of use and usefulness of these practices, hence improve security intentions. Changes in the work situation can, then again, can change security compliance.

The environment dimension concerns external factors that affect the enterprise and how it approaches information security. Security policies may be mandated by regulatory authorities (Glaspie and Karwowski, 2017) and are influenced by standards and regulations (Cram et al., 2017). Much research has also been devoted to cyber-situational awareness, allowing enterprises to perceive and analyse threats in the environment and respond adequately (Franke and Brynielsson, 2014).

2.2.2 Factors influencing information security

Several theories have been considered and used to explain the factors that influence the information security culture and the individual's information security behaviour. These theories were then used as a basis for proposing methods supporting management in assessing and improving information security in their enterprise.

A meta-model has been proposed by Lebek et al. to unify researched theories used for explaining security-related behaviour in the enterprise (Lebek et al., 2014). The meta-model gives an overview of the factors that contribute significantly to employees' security intentions (BI) and, eventually, behaviour (AB). Of primary importance were the behavioural and learning theories. The behavioural theories included the theory of reasoned action (TRA), theory of planned behaviour (TPB), general deterrence theory (GDT), and protection motivation theory (PMT). The learning theories included the social cognitive theory (SCT), social learning theory (SLT), and constructivism. These theories proposed influences on the employees' behavioural intent by considering a security control's usefulness and ease of use (PU, PEDU), the employee's threat appraisal (TA), coping appraisal (CA), and subjective norms (SN), and sanctions communicated by management (S).

Sommestad et al. had performed a meta-review of the research that evaluated the impact of such factors on compliance (Sommestad et al., 2014). According to their study, the most researched factors were subjective norms (SN) and self-efficacy (PBC) used in TRA/TPB and perceived severity of sanctions (PSOS) proposed by GDT. They concluded that many variables

influence employee compliance. However, the strength and interplay of these variables are largely unknown.

Karlsson et al. provide an overview of theories that can be used to explain the information security culture in the enterprise (Karlsson et al., 2015). Important theories include Schein's culture model, Robbin's three-tier organisational behaviour, and Bridges's individual transition process from organisational sciences, Locke's goal-setting theory and Flower's conscious competence learning model from psychology, and Nonaka's modes of knowledge creation from knowledge management. Several factors have been found to influence the security culture in the enterprise (Hassan et al., 2015). They are cultural differences, security awareness, security behaviour, top management commitment, trust, information sharing, security knowledge, security policy, and belief. The use of this knowledge can help to cultivate an information security culture or reinforce it in the organisation.

Several research studies have attempted to identify the diverse human and organisational reasons for compliance with security policy (Alotaibi et al., 2016; Kraemer et al., 2009). Several organisational factors influence employee compliance behaviour: awareness and training, information quality, persuasion, rewards, sanctions (deterrence), and computer monitoring. At the same time, several human factors influence compliance behaviour: perception and situational awareness of security threats, personalities such as prudence and vigilance, habits, freedom in the use of applications and devices, gender, and job satisfaction.

Accordingly, an individual's intention to comply has been proposed to result from a combination of extrinsic and intrinsic motivational factors (Deci and Ryan, 1985; Padayachee, 2012). Compliance behaviour can range from amotivation to passive compliance to active personal commitment. Extrinsic factors can be used to trigger internalisation, the process of developing increasingly intrinsic motivation. Although an individual may be unmotivated initially, he/she may be influenced through extrinsic motivation to become increasingly innate to eventually becoming self-motivated to act (Deci and Ryan, 1985; Padayachee, 2012).

Amotivation (Ryan and Deci, 2000) refers to a state of lacking an intention to act. Amotivation results from not valuing an activity, e.g., due to disobedience or low self-control, or not feeling competent. Amotivation may result from bad *security usability* (Padayachee, 2012). Good security usability would lead to self-efficacy (the perceived ability to develop and use relevant skills) and response efficacy (appropriate benefits generated with the activity), minimise response cost and put the locus of control on the individual.

Extrinsic motivation (Ryan and Deci, 2000) refers to performing an activity because it leads to an expected outcome. Extrinsic factors are the social climate, working conditions, deterrent controls and monitoring, and the individual's awareness of them. Extrinsic motivation is based on external regulation, a will to maintain self-esteem (introjection), identification with regulation, or full assimilation of the regulation (integration).

External regulation (Ryan and Deci, 2000) is imposed with deterrent controls and rewards. According to the general deterrence theory of motivation (GDT), the certainty and swiftness of detecting non-compliance and punishment affect an individual's intention to comply

(Padayachee, 2012). Sanctions may also be informal in the form of self-disapproval like embarrassment or shame, social disapproval like fear of sanctions from peers, and internalisation or moral commitment with regards to legal norms. Positively influencing the individual may be rewards offered for compliant behaviour.

Introjection (Ryan and Deci, 2000) is more internalised than external regulation. Introjection is imposed by building on people's will to avoid anxiety and maintain their ego within the organisation's social climate, hence building on the social climate the employee is confronted with.

Identification (Ryan and Deci, 2000) is more internalised than introjection. Identification occurs when an individual has understood the personal importance of a behaviour. Such understanding can develop through the awareness of policies as well as knowledge of standards and procedures concerning information security. Identification represents here a commitment of the individual with the enterprise.

Integration (Ryan and Deci, 2000) has been explained with the protection motivation theory (PMT). Integration refers thereby to the individual autonomously appraising both personally relevant threats (threat appraisal) and the effectiveness of coping responses for removing these threats (coping appraisal).

Intrinsic motivation (Ryan and Deci, 2000) refers to performing an activity because it is inherently interesting or enjoyable. Such motivation results from the individual's personality, habits, and skills. Intrinsic motivation is most successful in high-quality learning and depends on the individual's competence and good habits, etiquette, and ethical values.

2.2.3 Cultivating and assessing information security

The concept of *information security effectiveness* has been proposed to characterise the desired state of information security in an enterprise (Knapp et al., 2007). Security effectiveness means that the enterprise knows the threats it is exposed to, understands its vulnerabilities, has established defences with suitable tools, and has established security attitudes and behaviour among its employees. Effective information security allows successful defence against cyber threats.

An important role in managing information security in the enterprise is the chief information security officer (CISO) (Ashenden and Sasse, 2013). The CISO defines security goals and helps the organisation to achieve them. According to (Knapp et al., 2007), top management support is an overarching factor influencing security effectiveness in an organisation. Such support influences user training, security culture, policy relevance, and policy enforcement.

Six management practices have been proposed to guide organisations in assessing and implementing information security (Alshaikh et al., 2014). Security policy management provides the organisation with regulation. Security risk management is to identify, analyse, and minimise risk proactively. Security incident response management is the complementary reactive set of activities that aim at responding to security incidents and minimising their impact. Security education, training, and awareness (SETA) enables and encourages employees to comply with security policies and procedures. Technical management concerns

the selection, installation, configuration, and documentation of security controls such as firewalls. Intra-organisation liaison management concerns the communication, collaboration, and coordination necessary to align organisational priorities, the budget and resource allocation with the organisation's management, and the cultivation of a security culture involving every employee.

An important aspect of SETA is the communication of security risks so that they are perceived trustworthy and lead to appropriate actions. Effective SETA should change knowledge and attitudes, modify risk-relevant behaviour, and facilitate cooperative decision-making (Nurse et al., 2011). Good risk communication should consider the content, framing, and presentation of the message for a given communication goal, the source and channel used to deliver the message, and the role and characteristics of the message receiver. Hence, a critical success factor for impacting information security is management's understanding of the principles of psychology and experience in marketing campaigns (Lacey, 2010).

Several frameworks have been proposed for cultivating the security culture in the enterprise. For example, Da Viega and Eloff (Da Viega and Eloff, 2010) proposed implementing security components in the organisation, including security policies and program management, and influencing the employees' security behaviour. Employee awareness, countering laissez-faire attitude, finding enough resources to bring about change, and training of employees are challenges that need to be addressed to successfully cultivate a security culture (Karlsson et al., 2015).

Topa and Karyda proposed a unified framework that allows security managers to influence employees' security behaviour (Topa and Karyda 2015). Their framework suggests encouraging compliance of individuals, establishing a security culture in the organisation, and enhancing security usability. Encouragement of *individual compliance* includes actions to foster threat awareness, response self-efficacy, security habits, and response efficacy in combination with sanctions and rewards. The establishment of a security culture includes the provision of enough resources for security compliance, making policies understood, e.g., by co-developing them with the employees, and strong management support for good behaviour expected and exemplified by colleagues and superiors. Enhancement of security usability concerns the user-friendliness and performance of the security systems and the employees' capabilities of using them.

There have been several proposals of methods to assess information security in the enterprise (AlHogail and Mirza, 2014; Okere et al., 2012). According to Okere et al., the security culture should be assessed based on artefacts, espoused values, shared tacit assumptions, and information security culture (Okere et al., 2012). Sherif et al. offer an overview of factors that should be used for assessing an organisation's security culture as well as employee security awareness and behaviour that are necessary to cultivate a security culture (Sherif et al., 2015). Several questionnaire-based approaches have been proposed that capture such factors (Schlienger and Teufel 2005; Da Veiga et al., 2007; Spruit and Röling, 2014).

2.2.4 Applicability for SMEs

The here given overview of work on information security in the enterprise indicated a comprehensive systematic review that covers many theories, frameworks, and models. However, the research was agnostic to the size of the enterprise and based on assumptions that may be valid for large enterprises but not small ones. Well-visible, for example, is the assumption that management can establish information security policies and communicate them systematically to the employees, e.g., with a SETA programme. Most SMEs lack such expert knowledge, however, and struggle to follow these recommendations.

Some research has been performed to compare such diverse contexts. Omidosu and Ophoff showed that security behaviour differs between the organisational and home contexts (Omidosu and Ophoff, 2016). In the *organisational context*, awareness training is formal, guidelines are established and monitored, non-compliance is being punished, the safety climate is strong, and computing resources are used with proper access control. In addition to a stable psychological relationship between the employee and the organisation, employees are relieved of in-depth security thinking with IT support readily available, the IT function performing risk assessment, and the IT function deploys and enforces security measures such as the use of antivirus and firewalls. In the *home context*, individuals that give security little importance practice security voluntarily by being guided by perceived fear instead of being monitored and exposed to sanctions. Security behaviour requires competence that the individuals acquire through self-learning and use for deciding about and implementing security controls without the guidance or assistance of IT support. This environment is particularly vulnerable to attacks like social engineering and phishing or to individuals ignoring or deactivating automated security measures when accessing information. A possible reason for these differences is the changing locus of control (Padayachee, 2012) from the highly expert IT and management environment in the organisation to the individual end-user in the home context.

Today, there is no consolidated understanding of the SMEs' characteristics, their information security challenges, and influential factors that can be used to cultivate and assess information security in SMEs. Especially small enterprises may share many of the characteristics of the home context and lack characteristics that are present in large organisations. Advice based on the current state of art thus risks being ineffective or meeting too limited self-efficacy, hence not being feasible to help protect SMEs against cyber threats.

2.3 RESEARCH METHOD

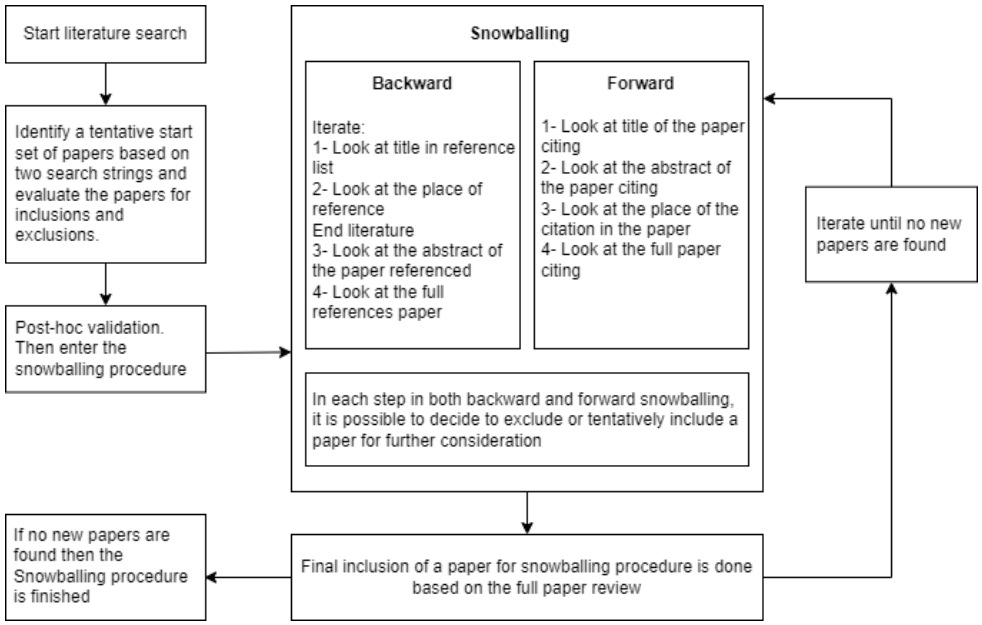
The research was designed to be a systematic review following the guidelines provided by Wohlin (2014). We used the snowballing (SB) strategy to find relevant literature on adherence to good information security practices in SMEs (Figure 2.2). Ahmad et al. (2017) assert that SB is less likely to miss relevant papers even with different terminology than database search. Wohlin (2014) states that there is a good possibility of finding a seminal and highly cited paper in the snowballing method. Furthermore, in SB, we do not have different database search challenges, such as database selection, research string construction, working with different database interfaces, and search limitations regarding different terminologies and synonyms.

The research objectives include identifying theories and theoretical factors that have been used in the context of SMEs' information security adherence, studying and synthesising the state of empirical validation of theoretical relationships, and determining SMEs' specific characteristics and main adherence goals.

To select the studies, we decided to review not only those papers that applied theories or theoretical constructs in SMEs but also papers that considered the company sizes as a control variable and highlighted the effect of size on their results. Moreover, we included peer-reviewed conference proceedings and journal papers written in English to accumulate reliable information, and technical reports, unpublished papers, duplicated studies, book chapters, non-peer-reviewed publications, and papers without available full text were excluded. To the best of our knowledge, this study is the first literature review in this context, and it covers the relevant papers until the end of June 2020.

Figure 2.2.

Snowballing procedure (based on Wohlin, 2014)



Included papers should fulfil one of the main following criteria:

- Applying theories (or theoretical constructs) for studying adherence to good information security practices in SMEs,

OR

- Studying theories or theoretical constructs in the context of information security in general. However, they consider and compare multiple organisational sizes. So, the company size should be measured as a control variable, and its effect should be reflected in the results.

In accordance with the mentioned criteria, the following publications are excluded:

1. those papers that do not address SMEs' information security practices,

2. those papers that only discuss applied theories or models in the context of information security without considering company size variable,
3. those papers that do not study theoretical constructs.

Based on Wohlin (2016), formulating research questions is the first step in snowballing search. Section 3.1 presents research questions and relevant motivations. The next step is identifying the start set. Start set papers are those papers that are applied for snowballing research and are included in the final systematic literature review (Wohlin, 2014). All papers in the start set have been fully studied by the first author and examined by the third author before snowballing (a post-hoc validation suggested by Nurdiani et al., 2016). Our approach to finding the start set papers is explained in section 3.2. Both backward and forward snowballing iterations and included papers are discussed in section 3.3. Data extraction and the quality appraisal are explained in sections 3.4 and 3.5, respectively.

2.3.1 Research questions

To understanding SMEs' characteristics and the effective theoretical factors that influence SMEs' adherence to good information security behaviours, the following research questions are formulated, Table 2.1.

Table 2.1

Research questions for the systematic literature review

ID	Research question	Motivation
RQ1	What theories are in use to explain adherence to good information security practices?	The main contribution of the RQ1 is to recognise theories from different disciplines that have been studied in the context of SMEs' information security adherence to good practices.
RQ1.1	What are the goals of adherence that can be explained with these theories?	This research question wants to identify and consolidate the main goals of the inclusions.
RQ1.2	What is the state of empirical validation of these theories for explaining adherence?	This research question contributes to exploring and synthesising the state of empirical support of the studied theories.
RQ2	How do the characteristics of small and medium-sized enterprises affect the adherence to information security?	By answering this research question, we identify the specific characteristics in SMEs which can affect adherence to information security practices.

2.3.2 Start set identification

Since all identified papers in SB depend on papers in the start set, constructing a suitable start set is an important task (Badampudi et al., 2015). To find the start set papers and avoid missing relevant studies, we first created two search strings based on the main keywords in our research questions. Then we selected Scopus as the reference database to identify tentative papers. Scopus is easy to use, includes papers from various publishers, and provides us with the possibility of a multidisciplinary search. According to (Wohlin, 2014), any scientific database (e.g., Google Scholar) can be used for searching tentative start set papers.

Since we intended to include papers studying SMEs and papers considering organisational size as a control variable, two search strings were formulated, and then two clusters of tentative papers were created. During the study of tentative papers from the first search string, we

realised that there are papers that study theoretical factors while the theory(s) are hidden or not explicitly explained in the title or abstract. Therefore, to avoid missing relevant papers, the term "((theor*))" has been removed from the first search string, and the search has been repeated. The new search string was assessed, verified, and the search was also conducted by the second author to improve the reliability of the procedure. For the first search string, all papers and for the second search string, only highly cited tentative papers (based on the Wohlin (2014) recommendation) were reviewed. Then the titles and abstracts were reviewed to screen and select the start set papers. This information is available in Scopus. Next, if the title and abstract of a paper were not clear enough for inclusion or exclusion decision, introduction and conclusion also were studied. Finally, the whole tentative papers were studied with respect to the inclusion and exclusion criteria and snowballing guidelines. Then final decisions were made in a researchers' meeting between the first and third authors (Figure 2.3). The following search strings were applied in Scopus:

A) TITLE-ABS-KEY ((("information security" OR "information system security" OR "cyber security" OR "cyber crime" OR "cyber attack" OR "cybersecurity" OR "data theft")) AND ((sme* OR "small and medium"))) AND (LIMIT-TO (SRCTYPE, "p") OR LIMIT-TO (SRCTYPE, "j")) AND (LIMIT-TO (LANGUAGE, "English"))

B) TITLE-ABS-KEY ((("information security" OR "information system security" OR "cyber security" OR "cyber crime" OR "cyber attack" OR "cybersecurity" OR "data theft")) AND ((theor*)) AND (("adherence" OR "compliance"))) AND (LIMIT-TO (SRCTYPE, "p") OR LIMIT-TO (SRCTYPE, "j")) AND (LIMIT-TO (LANGUAGE, "English"))

By doing the initial search, the number of results for the first search string was (303), and for the second one was (327). The search strings were formulated in more detail to reduce noise in the review. The number of tentatively selected papers for the first search string was 17 (papers 1-17, cluster A), and for the second was 11 (papers 18-28, cluster B). Therefore, 28 tentative papers were included in our start set for a more in-depth review, Appendix B.

The next step was the selection of the actual start set papers. In the tentative list, candidate 3 was the new extension of candidate 4. So, candidate 4 was excluded. Candidate 5 was an extension of candidates 6, 7, 8, and 9. Although these candidates explain a framework focusing on external and internal influences on SME information security culture, none of them applied a theory. In turn, candidates 5, 6, 7, 8, and 9 were excluded. Candidates 18 and 20 considered different demographic characteristics such as annual revenue, the number of employees, or the number of computers; however, no explicit results presented the effect of organisational size on security policy compliance. So, candidates 18 and 20 were also excluded. Candidate 23 was excluded after a discussion between the first and second authors. Candidates 22, 24, 25, 26, and 28 were excluded since none of them have considered the role of organisational size in their analysis.

Then, according to the Snowballing guidelines (Badampudi et al., 2015), all selected candidates 1, 2, 3, 10, 11, 12, 13, 14, 15, 16, and 17 from cluster A and candidates 19, 21, and

27 from cluster B were reviewed to remove papers that have common authors or refer to each other. Therefore, candidates 16, 17, 19, and 21 were removed (these papers later have been included through backward and forward SB) from the actual start set. The start set papers are denoted P1-P10 and presented in Table 2.3.

Finally, according to the exclusion and inclusion criteria, the third author performed a post-hoc validation. This validation was done to improve the reliability of the procedure and assess the quality and relevance of the primary studies included by the first author. As part of the post-hoc validation, the Kappa coefficient was calculated to determine the extent of agreements between the first and third authors. We had a Kappa coefficient of 0.607 (≈ 0.61). A Kappa coefficient between 0.61 – 0.80 is interpreted as a substantial agreement (Landis and Koch, 1977; Nurdiani et al., 2016). However, the disagreements occurred due to the quality of a few publication outlets. The disagreements were resolved through a discussion between the first and third authors, and we adopted an inclusive approach.

Figure 2.3

Process of inclusion/exclusion of start set papers

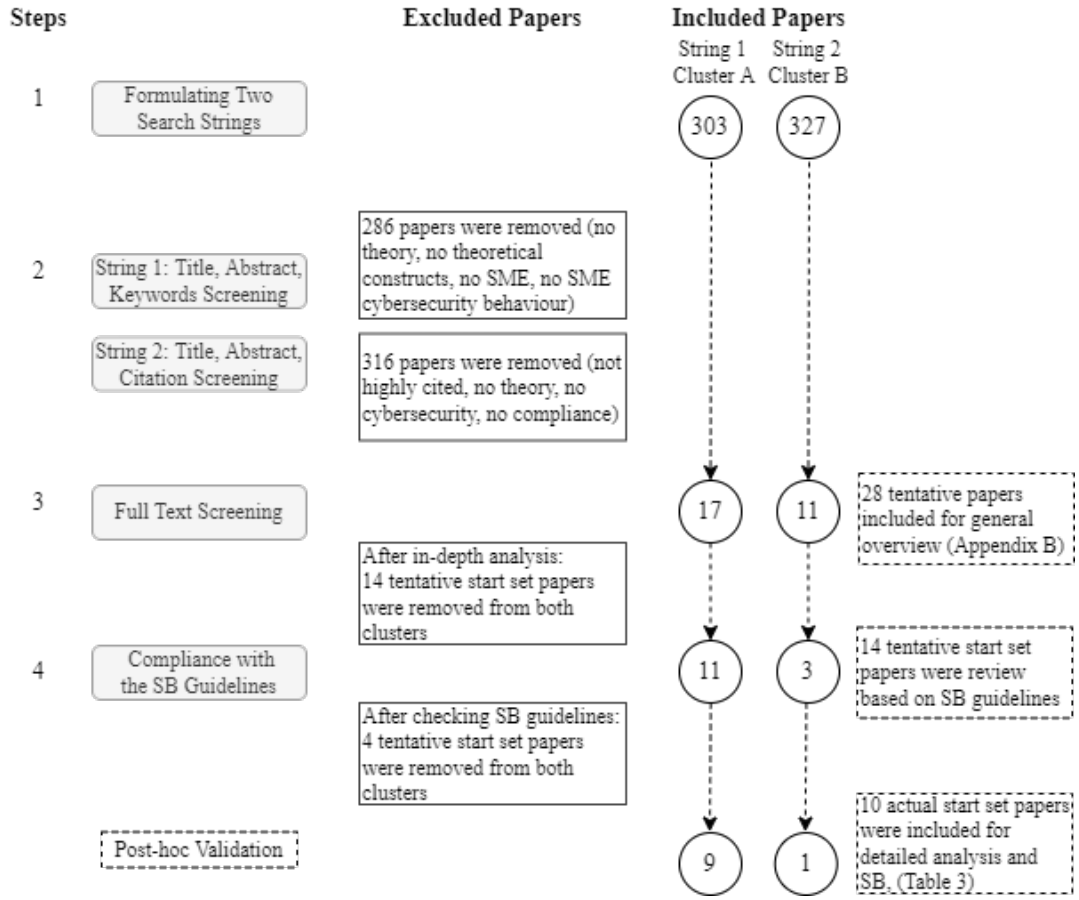


Table 2.2 demonstrates our compliance with the snowballing guidelines for identifying a suitable start set (Wohlin, 2014; Badampudi et al., 2015).

Table 2.2

The snowballing guidelines (Badampudi et al., 2015)

Guideline	Compliance
"The papers in start set should not refer each other."	The papers in the start set are not referring to each other.
"The number of papers must be reasonable. Focused (specific) research areas require fewer papers than broader research area."	Our research covers the topics about information security adherence in SMEs. Since we have two search strings for two clusters, we believe that the papers in the start set were of a good size, i.e., ten papers.
"The start set should cover several different publishers, years and authors."	The papers in the start set do not have a common author, and they cover publications between 2003 and mid-2020.
"The start set ought to be formulated from keywords in the research questions."	The search strings were formulated based on the keywords in four research questions. We considered the synonyms of terms to cover studies that applied different terminologies.

2.3.3 Snowballing iterations

The backward snowballing (BSB) and forward snowballing (FSB) were conducted based on the start set (P1-P10). According to (Wohlin, 2014), papers that did not fulfil the basic criteria (language and publication type) and already reviewed papers were excluded. Then the papers' abstracts were studied. If the information was not enough, the place citing the paper was examined. Finally, if this was not enough, other parts of the papers were reviewed until a definitive decision could be taken based on the inclusion and exclusion criteria. The BSB was conducted by screening the reference list of included papers, and the FSB was done by screening papers that cited the inclusions in Scopus.

- Iteration 1

For the BSB, 579 papers were evaluated:

(P1 → 40, P2 → 60, P3 → 49, P4 → 55, P5 → 23, P6 → 55, P7 → 24, P8 → 55, P9 → 130, P10 → 88)
and five new papers, candidates P11 (from P3), P12 (from P6), P13 (from P1), P14 (from P2), and P15 (from P8), were included; Table 2.3.

For the FSB, 334 papers were evaluated:
(P1 → 2, P2 → 5, P3 → 21, P4 → 280, P5 → 17, P6 → 5, P7 → 2, P8 → 2, P9 → 0, P10 → 0)

and six new papers, candidates P16 (from P4), P17 (from P3), P18 (from P4), P19 (from P4), P20 (from P4), and P21 (from P4), were included; Table 2.3.

- Iteration 2

Based on 11 identified papers in the first iteration (P11-P21), the second iteration of BSB and FSB was conducted.

For the BSB, 774 papers were examined:
(P11 → 45, P12 → 45, P13 → 117, P14 → 71, P15 → 56, P16 → 138, P17 → 52, P18 → 21, P19 → 63, P20 → 131, P21 → 35)

and no new papers were identified and included.

For the FSB, 1465 papers were examined:
(P11 → 175, P12 → 0, P13 → 826, P14 → 422, P15 → 10, P16 → 1, P17 → 3, P18 → 2, P19 → 1, P20 → 19, P21 → 6)

and four new papers, candidates P22 (from P13), P23 (from P13), P24 (from P13), and P25 (from P14), were included; Table 2.3.

- Iteration 3

Based on four identified papers in the second iteration (P22-P25), the third iteration of BSB and FSB was conducted. In this iteration, 123 papers were examined (P22 → 15, P23 → 25, P24 → 31, P25 → 52) for the BSB, and 87 papers were examined (P22 → 60, P23 → 2, P24 → 1, P25 → 24) for the FSB. However, no new papers were identified and included. Therefore, SB was stopped. Figure 2.4 illustrates the backward and forward SB iterations.

Finally, all inclusions were reviewed and confirmed by the second author.

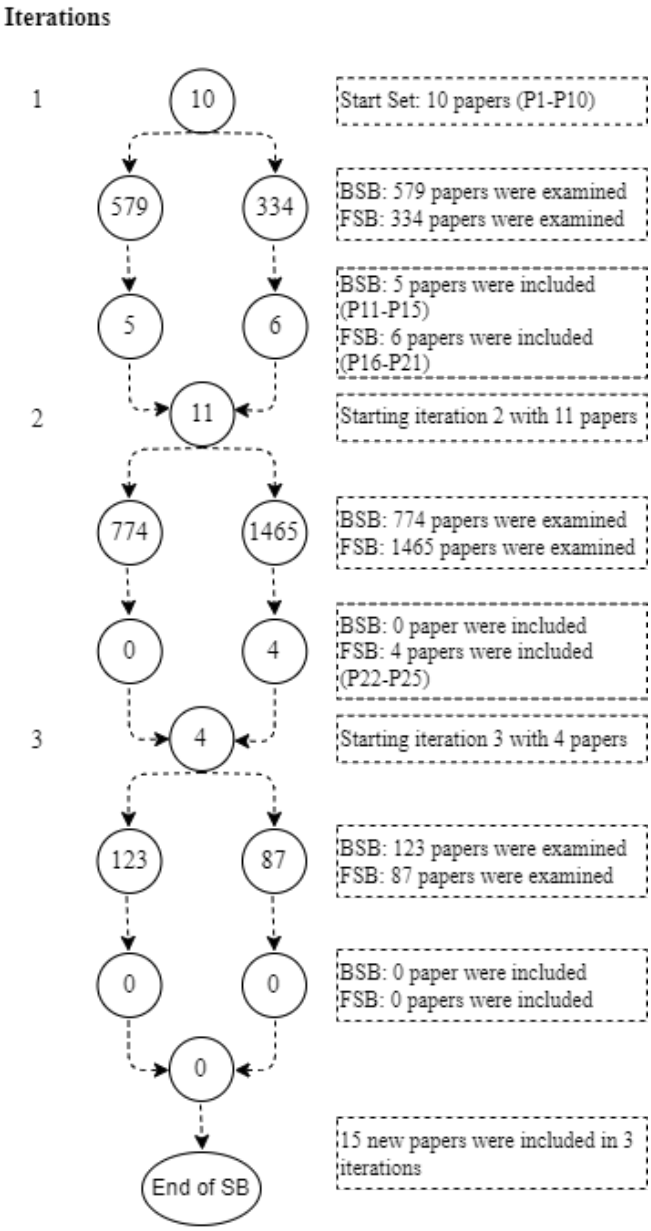
Table 2.3

Overview of 25 included papers (the reference list of the included papers is present in Appendix A)

ID	Author and Year	Focus type	Inclusion step
P1	Zec and Kajtazi, 2015	SME specific	Start set
P2	Browne et al., 2015	SME specific	Start set
P3	Gundu & Flowerday, 2013	SME specific	Start set
P4	Kankanhalli, 2003	Org. size	Start set
P5	Kaur & Mustafa, 2013	SME specific	Start set
P6	Renaud & Weir, 2016	SME specific	Start set
P7	Brunner et al., 2018	SME specific	Start set
P8	Sadok et al., 2020	SME specific	Start set
P9	Aigbefo et al., 2020	SME specific	Start set
P10	Solomon & Brown,2020	Org. size	Start set
P11	Lee1 & Larsen, 2009	SME specific	Iteration 1
P12	Njenga & Jordaan, 2016	SME specific	Iteration 1
P13	Bulgurcu et al., 2010	Org. size	Iteration 1
P14	Herath & Rao, 2009	Org. size	Iteration 1
P15	Renaud, 2016	SME specific	Iteration 1
P16	Barlette & Jaouen, 2019	SME specific	Iteration 1
P17	Gundu, 2019	SME specific	Iteration 1
P18	Beebe & Rao, 2009	Org. size	Iteration 1
P19	Barlette, 2015	SME specific	Iteration 1
P20	Barton, 2016	SME specific	Iteration 1
P21	Chen & Benusa, 2017	SME specific	Iteration 1
P22	Guo & Yuan, 2012	Org. size	Iteration 2
P23	Shih et al., 2016	SME specific	Iteration 2
P24	Clapper & Richmond, 2016	SME specific	Iteration 2
P25	Parsons et al., 2015	Org. size	Iteration 2

Figure 2.4

Backward and forward snowballing iterations



2.3.4 Data extraction

Data extraction was performed based on our research questions (section 3.1). The first author conducted data extraction for all 25 papers, and the results were presented to the second author for validation. The following data has been extracted:

1. Meta-data. Title, publication year, and publication source.
2. Studied theory. The theories have been applied for studying adherence to information security behaviours.
3. Studied theoretical constructs.
4. The goal of adherence.
5. Empirical support for relationships of the theories.
6. Empirical validation methods.

7. SME characteristics or organisational size impacts.
8. Context and focus. Some studies focused on employees, and some of them focused on management.

2.3.5 Quality appraisal

The quality appraisal is critical for the interpretation of findings and weighting the importance of studies when results are being synthesised (Kitchenham and Charters, 2007). After the post-hoc validation with the third author, we decided to have an inclusive strategy and include literature not only from high-impact journals but also include from lower-tier conferences. We are aware that the selection of high-rank journal and conference publications is recommended (Brocke et al., 2009; Kitchenham et al., 2009). However, we chose the inclusive strategy due to 1) information security research has largely neglected the SME context (Heidt et al., 2019), so the number of SME studies is limited, and 2) some papers (from lower-tier publishers) studied theories that we believe are necessary to support further research in SME information security improvement. So, we did not exclude any study based on the quality of the publication outlet.

For the quality assessment of the studies, we focused on the research reports. We answered five quality assessment questions (based on Kitchenham and Charters, 2007) for each study during the data extraction, Table 2.4. By Q1, we assessed if the aims of the studies were clearly described. By Q2, we assessed if the studies provided enough information and relevant references about the applied theoretical basis for adherence. By Q3, we assessed whether different research process steps were properly documented to increase reliability. By Q4, we assessed if an explicit report of the context of intervention was delivered and if the empirical result could be generalised. By Q5, we assessed if the research findings were properly reported and discussed.

Table 2.4

Quality appraisal

ID	Quality appraisal question	Yes	Partially	No
Q1	Are the aims of research clearly stated?	25	0	0
Q2	Are the theories and constructs clearly described?	22	3	0
Q3	Is the research process adequately documented?	23	2	0
Q4	Are the contexts and data sources clearly explained?	14	7	4
Q5	Are the research findings clearly explained and discussed?	20	4	1

2.4 RESULTS

This section elaborates on extracted data from a total of 25 studies that discuss the applied theories for adherence to information security with respect to SMEs' characteristics or organisational size.

The distribution of the studies demonstrates that 68% of studies (17 papers) were published after 2015. Figure 2.5 gives the chronological overview of the studies' distribution.

Figure 2.6 shows the distribution of the applied theories, i.e., from psychology, economics, sociology, information systems, and criminology. 18 theories were found in the studies, which

shows a considerable diversity, and some papers adopted a combination of several theories. As can be seen, Protection Motivation Theory (PMT) is the most adopted theory, appearing in 28% of the studies, followed by General Deterrence Theory (GDT) in 24% and Theory of Planned behaviour (TPB) in 20% of the studies. It should be noticed that some studies (P1, P4, P6, P15) did not indicate the adoption of a theory; however, they used some theoretical constructs to study information security behaviours. Studied theories are further explained in section 5.1.

Studies considered guidelines and policies as essential statements of security practices in pursuit of preventing organisations' information and technology resources from security threats. However, since the simple existence of policies does not automatically translate into desirable behaviours (Bulgurcu et al., 2010), many theories and models have been adopted to explain the influence of social, organisational, and psychological factors on individuals' motivation for compliance with security policies, warding off illegitimate behaviours, and awareness of security policies. We found that seeking approaches to promote policy compliance for the adoption of good security behaviours (52%) and management security practices (32%) are discussed in the majority of the studies. Figure 2.7 shows the adherence goals to bridge the gaps in information security practices.

The included papers were classified based on the state of empirical validation or evaluation and applied research methods. One paper (P2) did not report validation results, and some papers applied several methods. As can be seen in Figure 2.8, survey (60%) constitutes the most commonly used research methods. This is followed by interview (24%), and case study (12%).

We applied two search strings and included not only SME-specific studies but also those papers that evaluated the impact of organisational size (control variable) on information security adherence. As shown in Table 2.5, four out of seven studies indicated the significant effect of organisation size on information security activities.

Table 2.5

The impact of organisation size on information security practices

Organisation size impact	Paper ID	Key points
Yes	P4	Smaller companies often invest less in deterrent efforts compared to large companies.
	P10	Organisational size was significantly relevant to compliance behaviour. Therefore, older and larger organisations should have established cultures and employees intuitively understand the behavioural rules.
	P18	Organisational size affects the balance of implementation of controls. Technical controls are the priority specially in small organisations.
	P25	Organisational information security culture and information security decision making tend to improve as the size increases.
No	P13	organisation size has no signification effect on an employee's intention to comply with the information security policy.
	P14	Organisation size (the number of employees) has no significant effect on employee policy compliance intention.
	P22	Organisation size has no effect on the intentions to security policy violations.

Figure 2.5
Distribution of the studies by year of publication

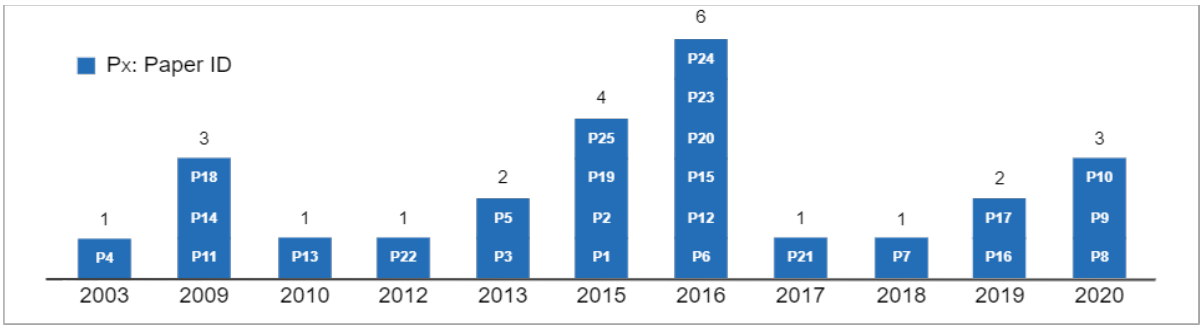


Figure 2.6
Distribution of the applied theories

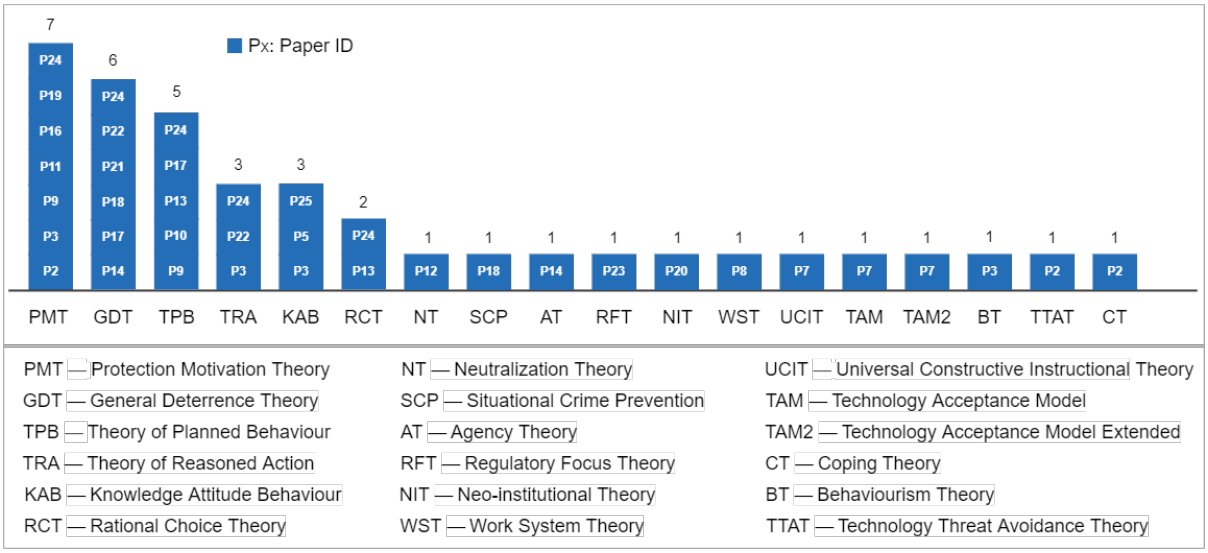


Figure 2.7
Distribution of the studies by goals of adherence

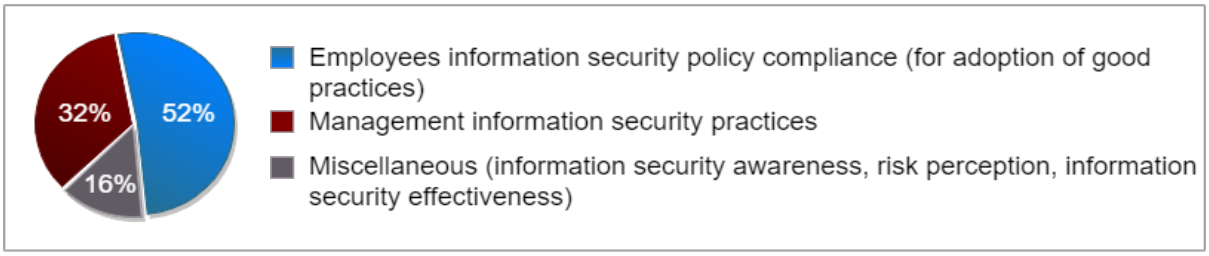
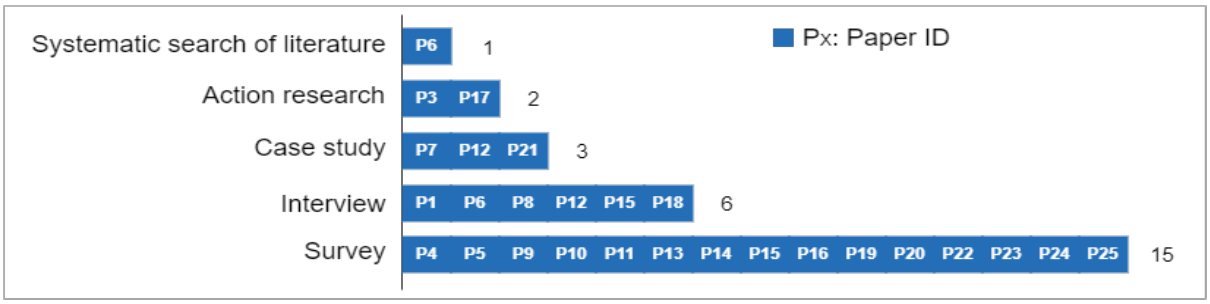


Figure 2.8
Distribution of the studies based on research methods



2.5 ANALYSIS

This section presents the synthesis of the extracted data from 25 studies to answer the research questions. First, we offer a summary of the studied theories. Then, we elaborate on the main goals of adherence. Then, we provide an overview of the empirical validation of the theories. Finally, we detail studied SME characteristics and their effects on information security adherence.

2.5.1 Applied theories for explaining adherence (RQ1)

The purpose of this research question was to identify the applied theories used to study information security adherence. Here we describe three highly applied theories. We summarised the key points of the theories in Table 2.6.

Protection Motivation Theory (PMT). Rippetoe and Rogers (1987) describe how protection motivation theory can explain the effects of threatening health information on attitude and behaviour change. In their study, individuals are informed about the severity and probability of the threat; however, people can prevent the threat if they have the right perception of the threat and have a suitable adaptive response. Rogers (1983) explains that the theory can be used in any situation concerning threats.

Rogers (1983) states that three components of a fear appeal (the magnitude of noxiousness, the conditional probability, and response efficacy), independently and in combination, influence attitude change and begin the coping process. According to PMT, the focus is on the cognitive processes and protective motivation instead of fear as an emotion that indirectly impacts attitude and behaviour change. Attitude change is a function of protective motivation. The amount of protective motivation stems from two cognitive appraisal processes (threat appraisal and coping appraisal) about the noxiousness and likelihood of a threat and the effectiveness of a recommended coping response. The outcome of these processes can specify if an individual is motivated to perform a protective behaviour or not. Threat appraisal and coping appraisal motivate people to have an adaptive response to a threat (Rippetoe and Rogers, 1987).

According to Rogers (1983), any source of information about a threat can initiate two mentioned cognitive processes. This information can be received from the environment (verbal persuasion or observational learning) or intrapersonal sources (personality variables or antecedent experiences). Then the cognitive processes based on their components appraise either maladaptive or adaptive responses. The probability of these responses can be increased or decreased based on variables. For the threat appraisal process, intrinsic and extrinsic rewards can increase the likelihood of maladaptive response, whereas severity and vulnerability of the threat can decrease. For the coping appraisal process, response efficacy and self-efficacy beliefs can increase the probability of adaptive response, and response costs (any expense, difficulty, or complexity) can decrease. Further, Rogers (1983) indicates that the best way to measure protection motivation is by measuring behavioural intention.

PMT is one of the widely applied theories in information security. Herath and Rao (2009) [P14] indicate that the concepts of fear appeals are pertinent and applicable in the context of

information security. They state that two constructs (response efficacy and self-efficacy) directly impact employees' compliance intention. Lee and Larsen's (2009) [P11] study proposes and validates a theoretical model by adopting PMT to identify factors affecting the adoption of protective applications in SMEs.

General Deterrence Theory (GDT). Straub (1990), with respect to Blumstein et al. (1978), states that GDT is a criminological theory based on the idea that disincentives or sanctions against committing a deviant behaviour can deter others from committing criminal behaviour. They emphasise that individuals respond to effective policy and the appropriate punishment. Straub and Welke (1998) indicate that this theory studies antisocial personalities and explains how to dissuade potential abusers or offenders from doing antisocial acts. Straub (1990) explains that disincentives are defined by two constructs: the certainty of sanction and the severity of sanctions. The certainty of sanctions is concerned with the risk of punishment, and severity explains that the penalties for violation are severe. Cheng et al. (2013) state that individuals' behaviour to some degree is based on rational decisions, and disincentives can influence them. They indicate that certainty means "an individual believes that his or her criminal behaviour will be detected" and severity means that "it will be harshly punished."

Akers (1990) states that deterrence theory assumes that individual behaviours are based on "rational decisions." He explains that when the deterrence doctrine is expanded to cover further variables such as both rewards and punishment, it moves to become the rational choice theory.

Many papers applied GDT to explain individuals' policy compliance behaviours. Straub and Welke (1998) assert that GDT has been used successfully in the context of the information system, and active and visible policies can significantly discourage potential computer violators. Herath and Rao (2009) [P14] consider the effects of certainty and severity on employees' intention to comply with security policies. They indicate that certainty of punishment ("existence and visibility of detection mechanism") is more crucial than severity. Kankanhalli et al. (2003) [P4] demonstrate the relation between deterrent efforts on information security effectiveness. However, they emphasise that SMEs were found to engage in fewer deterrent efforts than larger organisations.

Theory of Planned Behaviour (TPB). Ajzen (1991) proposes TPB as an extension of the theory of reasoned action (TRA) by adding perceived behavioural control (PBC) to cover TRA limitations about individuals' behaviour with incomplete volitional control. Perceived behavioural control is defined as "people's perception of the ease or difficulty of performing the behaviour of interest." Mathieson (1991) explains that PBC is a function of control beliefs and perceived facilitation. Control belief represents a perception of the availability of skills, resources, and opportunities, and perceived facilitation is an assessment of the importance of the resources to have the outcomes.

Table 2.6

Summary of applied theories (P1, P4, P6, P15 did not explicitly state a theory; however, their models applied some theoretical constructs of PMT or GDT)*

Theory	Reference for this paper	Main Constructs	Application	Frequency	Main Domain
Protection motivation theory (PMT)	Rogers (1983)	• Response-efficacy • Self-efficacy • Response-cost • Severity • Vulnerability	P2, P3, P9, P11, P16, P19, P24 P6*, P15*	7	Psychology
General deterrence theory (GDT)	Straub (1990)	• Certainty of punishment • Severity of punishment	P1*, P4*, P14, P17, P18, P21, P22, P24	6	Criminology
Theory of planned behaviour (TPB)	Ajzen (1991)	• Attitude • Perceived behavioural control • Subjective norms • Intention	P9, P10, P13, P17, P24	5	Psychology
Theory of reasoned action (TRA)	Fishbein and Ajzen (1975)	• Attitude • Subjective norms • Intention	P3, P22, P24	3	Psychology
Knowledge attitude behaviour model (KAB)	Schneider and Cheslock (2003)	• Knowledge • attitude • behaviour	P3, P5, P25	3	Health
Rational choice theory (RCT)	McCarthy (2002)	• Cost/ punishment • Benefit/ rewards	P13, P24	2	Criminology
Neutralization theory (NT)	Siponen and Vance, 2010	• Neutralization	P12	1	Criminology
Situational crime prevention (SCP)	Clarke (1980)	• Situational crime prevention techniques	P18	1	Criminology
Agency theory (AT)	Eisenhardt (1989)	• Principal • Agent • Monitoring • Opportunism	P14	1	Economics, Organisation
Regulatory focus theory (RFT)	Higgins (1998)	• Promotion focus • Prevention focus	P23	1	Psychology
Neo-institutional theory (NIT)	DiMaggio and Powell (1983)	• Coercive • Mimetic • Normative	P20	1	Sociology, management
Work system theory (WST)	Bostrom and Heinen (1977)	• Work system	P8	1	Organisation, management
Universal constructive instructional theory (UCIT)	Puhakainen (2006)	• Knowledge functions • Learning components, • Possibilities/constraints	P7	1	Learning
Technology acceptance model (TAM)	Davis (1985)	• Perceived usefulness • Perceived ease of use • Attitude • Intention	P7	1	Information systems
Technology acceptance model - extended (TAM2)	Venkatesh and Davis (2000)	• Perceived usefulness • Perceived ease of use • Attitude • Intention • Subjective norms	P7	1	Information systems

Coping theory (CT)	Lazarus (1993)	• Emotion focus • Problem focus	P2	1	Psychology
Behaviourism theory (BT)	Ertmer and Newby (1993)	• Stimuli • Response	P3	1	Psychology, learning
Technology threat avoidance theory (TTAT)	Liang and Xue (2009)	• Risk tolerance • Social influence • Emotion-focused coping • Problem-focused coping • Response-efficacy • Self-efficacy • Response-cost • Severity • Vulnerability	P2	1	Psychology, information systems

According to TPB, the intention is the central construct to catch the motivational factors. Three constructs can predict intentions to perform behaviours: attitudes, subjective norms, and perceived behavioural control. Individuals' behavioural beliefs and outcome evaluations indicate the attitude, normative beliefs and motivation for behaviour based on significant others indicate subjective norms, and control beliefs and perceived facilitation indicate PBC (Mathieson, 1991). Moreover, TPB explains that background factors such as demographics, experience, and knowledge can indirectly impact behaviour by influencing behavioural, normative, and control beliefs.

In the context of information security policy compliance, Bulgurcu et al. (2010) [P13] adopt the main constructs of the TPB as antecedents of an employee's intention to comply, and Clapper and Richmond (2016) [P24] apply the theory to explain an SME employee's intention to comply with data security standard.

2.5.2 The goals of adherence (RQ1.1)

This research question aims to identify the main goals of adherence that are explained with the applied theories. Three goal categories are identified. The two primary goals of the majority of studies are employees' information security policy compliance to adopt good behaviours and management information security practices. The third category encompasses the other goals, including information security awareness, employees risk perception, and security effectiveness. Table 2.7 demonstrates an overview of the adherence goals and applied theories.

Information security policy compliance to adopt good practices. Many of the inspected publications in this study applied theories or theoretical models to identify what drives employees' compliance, examine employees' behavioural intention, and propose solutions to promote policy compliance behaviour. An emerging research stream focus on the human aspects of information security to identify the factors that lead to policy compliance behaviour (Bulgurcu et al., 2010) [P13]. Information security policy is "a statement of the roles and responsibilities of the employees to safeguard the information and technology resources of their organisations" (Bulgurcu et al., 2010). Identifying factors that impact employees' compliance with the roles and responsibilities stipulated in information security policies is central to

defining where organisations should focus when planning employees' compliance improvement (Bulgurcu et al., 2010).

Management information security practices. The results show that supporting management information security behaviours is one of the adherence goals of the selected studies. We consider all managerial activities associated with CEOs, executives, managers, and IT professionals' management in this category of goals. Top management support has a significant impact on the implementation of information security effectiveness. Specifically, top managers are the primary decision-makers in small businesses to identify and support preventive measures (Kankanhalli et al., 2003 [P4]; Njenga and Jordaan, 2016 [P12]). They may participate in both protective and supportive behaviours (Barlette and Jaouen, 2019) [P16]. Therefore, understanding how to support SME managers' in making decisions and identifying the factors that influence their intention to adopt information security solutions is important for many studies (e.g., Lee and Larsen, 2009 [P11]; Barlette and Jaouen, 2019 [P16]).

Miscellaneous goals. Three goals were identified: effectiveness of information security, awareness, and risk perception. Kankanhalli et al. (2003) [P4] examined the relationships between three organisational factors (organisational size, top management support, industry type) and security measures, and relationships between security measures (deterrent efforts, preventive efforts, deterrent severity) and information security effectiveness. The study showed the impact of organisational factors on security measures. Moreover, greater deterrent efforts and preventive measures enhance information security effectiveness. Kaur and Mustafa (2013) [P5] examined the effects of knowledge, attitude, and behaviour on awareness of three elements of information security (confidentiality, integrity, and availability). Their results showed no significant relationship between knowledge and information security awareness, while attitude and behaviour significantly correlate with awareness. Renaud and Weir (2016) [p6] and Renaud (2016) [p15] particularly focus on SME employees' risk perceptions. The studies discussed three levels of individual processing of the threat appeals: minor risk, medium risk, and significant risk. Accordingly, the papers categorise individuals' willingness to implement security measures into three categories: lax about security, caring about security, and concerned about security.

2.5.3 The state of empirical validation of the theories (RQ1.2)

Because many of the applied theories have been borrowed from contexts other than information systems, this research question aimed to investigate to what extent the theories have been empirically validated in information security adherence. In order to answer this question, we synthesised the state of empirical validation of all the studied theories in Table 2.8. The studies have empirically shown the applicability of 16 (out of 18) theories for explaining information security adherence. Also, the studies provided empirical support for most of the theoretical relationships of the constructs. Moreover, as shown in Table 2.7 and Table 2.8, many studies used more than one theory or a combination of several constructs from different theories due to one theory did not fit properly to the data.

Table 2.7

Overview of the adherence goals and applied theories in the selected studies

Goal	Paper	Applied Theory	Other Constructs	Example of Application
Information security policy compliance to adopt good practices	P2	CT, PMT, TTAT	Awareness, Social influence	Why IT threat avoidance and IT security adoption need to be viewed in conjunction with each other
	P3	TRA, PMT, BT, KAB		How subjective norm, threat-appraisal, and coping-appraisal impact policy compliance intention
	P8	WST		Why policies that highlight information security are often disconnected from actual work activities
	P9	TPB, PMT	Habit, Hardiness	How hardiness and habit can explain employee security behaviour intention
	P10	TPB		What is the role of perceived behavioural control in employee information security compliance behaviour
	P13	TPB, RCT	Awareness	How the benefit of compliance and cost of noncompliance impact employee intention to comply
	P14	AT, GDT	Social pressure, Perceived effectiveness	Employee perceived effectiveness of their actions impact security policy compliance intentions
	P17	GDT, TPB		How punishment and reward may motivate information security policy compliance
	P21	GDT	Social pressure, knowledge, self-efficacy, awareness, knowledge	Cost of compliance and cost of policy violation contribute to healthcare organisations' intention to comply with information security policies
	P22	GDT, TRA		How do multilevel sanctions prevent information security violations
	P23	RFT		What motivational mechanism impact compliance
	P24	TRA, TPB, PMT, RCT, DT	Knowledge	Self-efficacy influences a small business's intention to comply
	P25	KAB	Rewards and punishments	How improving security culture may influence policy compliance
Management information security practices	P1	*not mentioned*	Shame, Guilt	IT professionals may fail to report their mistakes to the management. SMEs need to employ IT professionals that show higher levels of guilt-proneness
	P7	TAM, TAM2, UCIT		SMEs require dedicated training that sustainably raises employee awareness for day-to-day business activities
	P11	PMT	Social influence, Situation behavioural control	How self-efficacy may impact SME executives' security solution adoption
	P12	NT		Owners of SMEs may rationalize their deviant behaviour
	P16	PMT	Social influence	How perceived vulnerability may impact CEOs information security actions
	P18	SCP, GDT		According to CISOs, information security

				strategies are still predominantly preventive
	P19	PMT		How coping appraisal may impact SME CEOs' intention to implement information security measures
	P20	NIT		How external pressures encourage senior managers to involve in information security
Miscellaneous (Information security effectiveness, awareness, risk perception)	P4	*not mentioned*	Deterrent efforts, Deterrent severity	How deterrent effort impact the effectiveness of information security.
	P5	KAB		How knowledge, attitude, and behaviour may impact information security awareness in an SME.
	P6	*not mentioned*	Threat appraisal, Coping appraisal	How do SMEs take the risk of cyberattack
	P15	*not mentioned*	Threat appraisal, Coping appraisal	SMEs may positively assess their coping appraisal; however, they could still decide not to take action

Table 2.8

Overview of empirical validation of the theories (P2 applied CT and TTAT theories; however, did not report validation)*

Theory	Construct	Association	Interpretation
Protection motivation theory (PMT)	• Response-efficacy (coping appraisal)	+	• Threat and coping appraisal support compliance intention (P3)
	• Self-efficacy (coping appraisal)	no effect	• Threat appraisal has no effect on employees' intention (P9)
	• Response-cost (coping appraisal)	+	• Threat and coping appraisal significantly impact executives' adoption intention (P11)
	• Severity (threat appraisal)	+	• Employees perceived effectiveness of their security behaviour positively impacts intention to compliance (P14)
	• Vulnerability (threat appraisal)	+	• All constructs support CEOs' supportive actions (P16)
		+	• All constructs (except severity) support CEOs' protective actions (P16)
		+	• Vulnerability and coping appraisal support behavioural intention (P19)
		no effect	• Severity has no effect on behavioural intention (P19)
		no effect	• Neither the cost of compliance nor the cost of noncompliance support intention to comply (P24)
		+	• Self-efficacy, perceived cost of the breach, and vulnerability support intention to comply (P24)
General deterrence theory (GDT)	• Certainty of punishment	-	• Severity of punishment has a significant negative effect on intention of information security compliance (P14)
	• Severity of punishment	+	• Certainty of detection has a positive impact on intention of information security policies compliance (P14)
		+	• Deterrence measures (certainty and

			severity) can assist in reducing the risk of employees' policy violation (P17)
		+	• Deterrence strategies have impact on improving organisations' information security (P18)
		+	• GDT supports policy adherence intention (P21)
		+	• Personal self-sanctions and workgroup sanctions have significant deterrent effects on employee security policy violations (P22)
		no effect	• Organisational sanctions have no significant impact when self and workgroup sanctions are considered (P22)
		-	• Workgroup sanctions have a significant negative impact on employee intentions to violate security policies (P22)
		+	• Organisational sanctions perceived by employees have a positive impact on perceived workgroup sanctions (P22)
		no effect	• Cost of non-compliance has no effect on the owner' intention to comply (P24)
Theory of planned behaviour (TPB)	• Attitude • Perceived behavioural • control • Subjective norms • Intention	+	• Subjective norm and attitude show a slight influence on the intention to comply with information security (P9)
		+	• Hardiness and habit have a significant effect on employee security behaviour intention (P9)
		+	• TPB explains employee policy compliance by organisational culture and information security culture (P10)
		+	• Attitude, normative beliefs, and self-efficacy have a significant influence on intention to comply (P13)
		+	• TPB explains infosec policy compliance (P17)
		+	• TPB explains employee policy compliance intention (P24)
Theory of reasoned action (TRA)	• Attitude • Subjective norms • Intention	+	• Subjective norms and attitudes have an impact on compliance intention (P3)
		+	• Subjective norms influence employee's information security compliance intention (P14)
		+	• Social pressure impacts individuals' intention to comply (P21)
		-	• Workgroup sanctions have a significant negative impact on employee intentions to violate security policies (P22)
		+	• Normative beliefs are positively associated with intention to comply (P24)
Knowledge attitude behaviour model (KAB)	• Knowledge • attitude • behaviour	+	• An increase in knowledge makes a positive change in attitude and information security behaviour (P3)
		+	• Attitude and behaviour have a significant influence on information security awareness (P5)
		no effect	• Knowledge has no significant impact on information security awareness (P5)
		+	• Attitude and behaviour have a significant

			relationship to confidentiality (P5)
		+	• Knowledge of legislation supports an organisation's intention to comply (P21)
		+	• General knowledge of IT security supports awareness and policy compliance intention (P24)
		+	• Information security culture has a positive correlation with knowledge of policy (P25)
		+	• Information security culture has a positive correlation with attitude towards policy (P25)
		+	• Information security culture has a positive correlation with behaviour (P25)
Rational choice theory (RCT)	• Cost/ punishment • Benefit/ rewards	+	• Beliefs of compliance benefit, compliance cost, and noncompliance cost have a significant influence on employee's attitude toward compliance (P13)
		+	• Information security awareness positively affects attitude, the benefit of compliance, cost of compliance, and cost of noncompliance beliefs (P13)
		no effect	• Findings show that perceived cost of compliance, cost of a breach, and the benefit of compliance have no effect on small business's intention to comply (P24)
		+	• Organisations with high consequence penalties are more likely to have better organisational information security culture (P25)
		+	• High consequence penalties influence better knowledge of policies (P25)
		no effect	• Severe penalties will not necessarily impact on better information security decisions (P25)
		-	• Organisations without rewards are more likely to have better information security decisions (P25)
Neutralization theory (NT)	• Neutralization	-	• The neutralization approach served as antecedents to information security risks in small businesses (P12)
Situational crime prevention (SCP)	• Situational crime prevention techniques	+	• Anticipated benefit, the perceived effort required, and the perceived risk of being caught are three primary decision influences that impact cyber offenders' decision-making (P18)
Agency theory (AT)	• Principal • Agent • Monitoring • Opportunism	+	• Agency theory explained the principal-agent relationship for information security policy compliance (P14)
Regulatory focus theory (RFT)	• Promotion focus • Prevention focus	no effect	• Promotion-approach and promotion-avoidance mechanisms are ineffective for motivating policy compliance when employees are unaware of the security policy (P23)
		+	• Prevention-approach and prevention-avoidance support compliance intention even employees are unaware of the

			security policy (P23)
		+	• Promotion-approach is more effective than promotion-avoidance to frame compliance intention when employees have information security policy awareness (P23)
		+	• Prevention-approach is more effective than prevention-avoidance to frame compliance intention no matter if employees are aware or not of security policy (P23)
Neo-institutional theory (NIT)	• Coercive • Mimetic • Normative	+	• Senior management beliefs about information security influence their participation in information security practices (P20)
		+	• Senior management information security belief impacts security assimilation in organisations (P20)
		+	• Mimetic influences improve senior management participation by increasing their belief in information security (P20)
		no effect	• Normative and coercive influences have an insignificant impact on either senior management belief or participation (P20)
Work system theory (WST)	• Work system	+	• A work system perspective may explain and provide a coherent form of effective information security practices in a real-world working context (P8)
Universal constructive instructional theory (UCIT)	• Knowledge functions • Learning components, • Possibilities/constraints	+	• UCIT provides a framework to design a high-quality information security course (P7)
Technology acceptance model (TAM) and (TAM2)	• Perceived usefulness • Perceived ease of use • Attitude • Intention • Subjective norms	+	• TAM and TAM2 provided a rigorous approach to assess and explain the acceptance of an information security tool (P7)
Coping theory (CT)*	• Emotion focus • Problem focus	*not available*	
Behaviourism theory (BT)	• Stimuli • Response	+	• The findings of the study support Behaviourism theory for explaining policy compliance intention (P3)
Technology threat avoidance theory (TTAT)*	• Risk tolerance • Social influence • Emotion-focused coping • Problem-focused coping • Response-efficacy • Self-efficacy • Response-cost • Severity • Vulnerability	*not available*	

2.5.4 The effects of SMEs' characteristics on adherence (RQ2)

The purpose of this research question was to identify which SME characteristics the papers have studied and how these characteristics have influenced information security adherence. We conceptually organised the frequently mentioned SME characteristics around technical skills, knowledge and awareness, financial resources, and organisational features. In the following, we elaborate on the characteristics and their effects on adherence to information security.

Technical skills. One of SMEs' most common characteristics is the lack of technical skills and access to experts to achieve the required skills. According to the selected studies, skill shortage is one of the major constraints that influences the implementation of the recommended security measures for mitigating security threats. The studies indicate that supporting information security skills and connection with experts should take heed to improve adoption of security measures. Renaud and Weir (2016) [P6] with respect to SMEs lack of required skills indicate that "an SME that acknowledges the likelihood of attacks is still at risk of implementing insufficient measures." Clapper and Richmond (2016) [p24] indicate the lack of technical knowledge and resources as barriers to information security compliance in SMEs and demonstrate that communication with experts influences SME awareness-raising. Njenga and Jordaan (2015) [P12] explain that a lack of skills may impact managers' decision-making process. SME CEOs are not sufficiently qualified to handle protective actions, implement new security procedures, and manage technologies in their companies (Barlette and Jaouen, 2019 [P16]; Lee and Larsen, 2009 [P11]).

Knowledge and awareness. The studies have highlighted the lack of knowledge and awareness of information security as one of the SMEs' characteristics that exposes them to information security risks. Zec and Kajtazi's (2015) [P1] findings show that the level of awareness about the information security standards of IT professionals is deficient. SMEs lack understanding and awareness of information security policies (Shih et al., 2016) [P23]. "[SMEs] did not know what actions to take to improve their resilience" (Renaud and Weir, 2016) [P6]. They require information, advice, and better policing (Renaud, 2015) [P15]. Moreover, the lack of knowledge and awareness is strongly linked to security measures' adoption and implementation. Sadok et al. (2020) [P8] believe that SMEs have a weak understanding of implementing and managing effective security controls. Brunner et al. (2018) [P7] emphasise that SMEs require dedicated training that raises employee awareness for sustainable information security operations.

Financial resources. Many researchers point out SMEs' lack of financial resources as an essential constraint for information security adherence and adoption. According to Lee and Larsen (2009) [P11], the IT budget is a key facilitator of the anti-malware software adoption intention for non-IS experts and non-IT intensive SMEs. They explain that SME executives with larger IT budgets are more likely to adopt anti-malware for their organisations. Brunner et al. (2018) [P7] emphasise that SMEs are usually under-resourced for implementing regular training initiatives, and Chen and Benusa (2017) [P21] indicate that due to the lack of IT budget, small healthcare providers cannot afford in-house IT specialists.

Organisational features. Studies indicate certain organisational features that impact information security activities in SMEs. (Barlette and Jaouen, 2019 [P16]; Aigbefo et al., 2020 [P9]) argue that it is unrealistic to replicate the findings from information security studies in large organisations because SME hierarchies are less structured, they do not have access to the same level of resources, and SME CEOs are often the sole decision-makers. SMEs often do not have established cultures (Dojkovski et al., 2010), and information security is not the priority (Browne et al., 2015) [P2]. Moreover, they often invest less in deterrent measures (Kankanhalli et al., 2003 [P4]; Beebe and Rao, 2009 [P18]).

2.6 DISCUSSION

This study has presented the first systematic review of information security adherence in SMEs and offered several contributions. First, this chapter reviewed 18 applied theories and provided new insights into the state of empirical support by identifying and synthesising the validated antecedents of adherence based on theoretical relationships. We also included articles that examined the impact of organisational size on employees' information security behaviours to provide a more comparative and holistic view of information security adherence research. We found that PMT, GDT, and TPB are the most frequently applied theories. This finding is consistent with previous systematic reviews in the information security field. Lebek et al. (2014), in a theory-based literature review, classified 54 theories and illustrated that TPB/TRA, GDT, and PMT are the three dominantly applied behavioural theories. Also, Kuppusamy et al. (2020), in a literature review of information security compliance behaviour identified 19 theories and models that TPB, PMT, and GDT are the widely applied theories. Moreover, we found that the majority of the studies used survey measuring as the research method. According to Lebek et al.'s (2014) study, the quantitative empirical research method is dominant in the examined research field. However, in Lebek et al.'s (2014) study, the experimental research method has been used in 11% of the studies, while this method has not been applied to SME studies. Therefore, we think future research is needed that applies additional research methodologies such as experiments or action research.

Second, this study demonstrated that the majority of prior studies (84%) focused on two goals: information security policy compliance and management information security. It shows that researchers are less prone to focus on other topics, such as the effectiveness of information security communication (Smit et al., 2021), SME awareness-raising, and SMEs' risk perception. However, these topics are important, and studies show that information security communication and risk perception impact CEOs' decision-making, motivation to comply, and effective protection (Renaud and Weir, 2016 [P6]; Barlette and Jaouen, 2019 [P16]). Therefore, future research can focus more on these topics.

Third, this research identified and synthesised the main SME characteristics and constraints that strongly influence information security activities. SMEs' hierarchies are less structured, and they lack technical skills, knowledge and awareness, and financial resources. Research shows that organisational characteristics influence SME information security behaviour (Mijnhardt et al., 2016; Barlette and Jaouen, 2019 [P16]; Heidt et al., 2019; Aigbefo et al., 2020

[P9]). SMEs lag behind larger organisations in adopting protective measures, and they have cognitive and technical limitations (Renaud, 2016 [P15]; Shojaifar et al., 2018; Barlette and Jaouen, 2019 [P16]); however, organisational information security has neglected the SME context (Heidt et al., 2019). According to Toni Allen from British Standards Institute, "SMEs have not historically been the target of cybercrime, but in 2015 something drastically changed." (Smith, 2016). The specific characteristics indicate an immediate need for well-targeted security awareness and training programmes and socio-technical approaches that streamline SME risk management processes (Sadok and Bednar, 2016; Renaud and Weir, 2016 [P6]). ENISA (2020) emphasises the need for the right tools to help SMEs be protected against cyber threats before they happen. Our study demonstrated that one paper (P7) proposed an SME-specific tool for information security management and evaluated the tool's utility. Improving SMEs' knowledge, awareness, and skill is undoubtedly a worthy objective, and cost-effective, lightweight awareness training tools might be a solution. Future studies may build on Brunner et al. (2018) [P7] and examine the utility of new SME-friendly methods and tools.

Fourth, the findings of this article demonstrated that information security literature (e.g., Lebek et al., 2014; Kuppusamy et al., 2020) has empirically studied theories to explain employees' security-related behaviours that have not yet been used for SMEs. We found that many papers studied the influence of punishments and rewards on SME employees' motivation (based on GDT or RCT); however, what is less understood is that motivation has various types and qualities. A study by Deci et al. (1999) demonstrated that all tangible and expected rewards for desirable performance tend to undermine intrinsic motivation. To extend the domain of applied theories for SMEs, self-determination theory (SDT) (Deci and Ryan, 1985; Deci, 1992; Ryan and Deci, 2000) is proposed as a new research focus to study information security adherence.

SDT provides a broader understanding of human motivation and offers additional options that can be applied in the context of SMEs. SDT proposes two basic distinct types of motivation: intrinsic and extrinsic. "Intrinsic motivation refers to doing something because it is inherently interesting, and extrinsic motivation refers to doing something because it leads to a separable outcome." SDT proposes various types of extrinsic motivation that reflect different degrees of autonomy or self-determination (Ryan and Deci, 2000). Further, SDT identifies a set of basic psychological needs: competence, autonomy, and relatedness. Autonomy refers to a desire to participate in activities with a choice of freedom or a sense of volition. Competence refers to individuals' desire to interact effectively with the environment to produce desired outcomes and prevent undesired results. Relatedness reflects a sense of connectedness and belonging to others or a social environment (Deci, 1992; Vallerand, 1997).

SDT has been studied and empirically supported in the information security context (Padayachee, 2012; Menard et al., 2017; Pham et al., 2017). We argue that SME literature would benefit from applying SDT, and future research may draw on this theory and empirically investigate the effect of basic psychological needs on employees' policy compliance.

Although we applied a rigorous approach to select and review the literature, this study has several limitations. One limitation is related to the included studies. A low number of studies

considered SMEs' information security compared to larger companies. To mitigate this issue, we used an inclusive strategy for selection to gain a more comprehensive view of the field and reduce the threat of missing relevant publications. Therefore, the quality of the inclusions may not be the same because some of the studies appeared in lower-tier conference proceedings and journals.

Moreover, this study is limited to English literature, and we also excluded non-peer-reviewed publications (e.g., books). Another limitation is concerned about the applied scientific database for snowballing. We only used Scopus for identifying start sets and forward snowballing. Additionally, this literature review is limited to publications that have been published until June 2020. Nevertheless, this chapter is the first systematic literature review that reviews 18 theories applied to study information security adherence in SMEs and synthesises the empirical validation of the theories. The chapter contributes with the suggestion for important avenues for SMEs' information security future research.

2.7 Conclusion

In this chapter, the researchers presented the first systematic literature review (SLR) that investigates theory-based studies considering information security adherence in small and medium-sized enterprises. We used the snowballing strategy, selected 25 articles published between 2003 and mid-2020, and synthesised the results to answer four research questions.

The results indicated that 18 theories had been studied in the context of SMEs' information security. Protection motivation theory (PMT), general deterrence theory (GDT), and theory of planned behaviour (TPB) are the mainly applied theories to explain adherence. Furthermore, this SLR revealed that the majority of the articles focused on two goals: employees' policy compliance to adopt good practices and management information security practices. Synthesising the state of empirical validation of the theories demonstrated that 16 theories are relevant in explaining adherence in SMEs, and most of the theoretical relationships have been supported (Table 2.8). Moreover, the results indicated that the survey is the dominant research method. In addition, the results showed that SMEs have common characteristics that differentiate them from large organisations and significantly influence information security adherence. The identified characteristics are a) a lack of technical skills; b) a lack of knowledge and awareness; c) a lack of financial resources; and d) organisational features. Although literature emphasised the specific characteristics of SMEs, only one paper studied the design and rigorous evaluation of an SME-specific tool for information security management.

Furthermore, four directions for future research on SME information security adherence are encouraged. First, the SME research stream can extend the domain of applied theories by studying additional theories that have not yet been used or empirically validated for SMEs (e.g., self-determination theory). Future empirical studies may focus on autonomy, competence, and relatedness constructs to validate the impact of motivation on SME employees' information security adherence. Second, the SLR uncovered that surveys and interviews are widely applied research methodologies. Future research requires further attention to additional methods such as experiments or action research. Third, we identified

that the effectiveness of security communication, SME awareness-raising, and SMEs' risk perception are areas that still need further attention. Finally, designing and evaluating SME-specific tools and methods that facilitate information security improvement are promising paths for future study.

Appendix A

SLR References

P1- Zec, M., & Kajtazi, M. (2015). Examining how IT professionals in SMEs take decisions about implementing cyber security strategy. In *ECIME2015-9th European Conference on IS Management and Evaluation: ECIME*, p. 231.

P2- Browne, S., Lang, M., & Golden, W. (2015). Linking Threat Avoidance and Security Adoption: A Theoretical Model for SMEs. In *Bled eConference,* p. 35.

P3- Gundu, T., & Flowerday, S. V. (2013). Ignorance to awareness: Towards an information security awareness process. *SAIEE Africa Research Journal*, 104(2), 69-79.

P4- Kankanhalli, A., Teo, H. H., Tan, B. C., & Wei, K. K. (2003). An integrative study of information systems security effectiveness. *International journal of information management*, 23(2), 139-154.

P5- Kaur, J., & Mustafa, N. (2013). Examining the effects of knowledge, attitude and behaviour on information security awareness: A case on SME. In 2013 *International Conference on Research and Innovation in Information Systems (ICRIIS)*, pp. 286-290. IEEE.

P6- Renaud, K., & Weir, G. R. (2016). Cybersecurity and the Unbearability of Uncertainty. In *2016 Cybersecurity and Cyberforensics Conference (CCC),* pp. 137-143, IEEE.

P7- Brunner, M., Mussmann, A., & Breu, R. (2018). Introduction of a tool-based continuous Information Security Management System: An exploratory case study. In *2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C)*, pp. 483-490, IEEE.

P8- Sadok, M., Alter, S., & Bednar, P. (2020). It is not my job: exploring the disconnect between corporate security policies and actual security practices in SMEs. *Information & Computer Security*, 28(3), 467–483.

P9- Aigbefo, Q. A., Blount, Y., & Marrone, M. (2020). The influence of hardiness and habit on security behaviour intention. *Behaviour & Information Technology*, 1-20.

P10- Solomon, G., & Brown, I. (2020). The influence of organisational culture and information security culture on employee compliance behaviour. *Journal of Enterprise Information* Management, 34(4), 1203-1228.

P11- Lee, Y., & Larsen, K. R. (2009). Threat or coping appraisal: determinants of SMB executives' decision to adopt anti-malware software. *European Journal of Information Systems*, 18(2), 177-187.

P12- Njenga, K., & Jordaan, P. (2016). We want to do it our way: The neutralisation approach to managing information systems security by small businesses. *The African Journal of Information Systems*, 8(1), 3.

P13- Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS quarterly*, 34(3), 523-548.

P14- Herath, T., & Rao, H. R. (2009). Encouraging information security behaviours in organisations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, 47(2), 154-165.

P15- Renaud, K. (2016). How smaller businesses struggle with security advice. *Computer Fraud & Security*, 2016(8), 10-18.

P16- Barlette, Y., & Jaouen, A. (2019). Information security in SMEs: determinants of CEOs' protective and supportive behaviours. *Systemes d'information management*, 24(3), 7-40.

P17- Gundu, T. (2019). Acknowledging and reducing the knowing and doing gap in employee cybersecurity compliance. In *ICCWS 2019 14th International Conference on Cyber Warfare and Security*, pp. 94-102.

P18- Beebe, N. L., & Rao, V. S. (2009). Examination of organisational information security strategy: A pilot study. *AMCIS* 2009 Proceedings.

P19- Barlette, Y., Gundolf, K., & Jaouen, A. (2015). Toward a better understanding of SMB CEOs' information security behaviour: Insights from threat or coping appraisal. *Journal of Intelligence Studies in Business*, 5(1).

P20- Barton, K. A., Tejay, G., Lane, M., & Terrell, S. (2016). Information system security commitment: A study of external influences on senior management. *Computers & Security*, 59, 9-25.

P21- Chen, J. Q., & Benusa, A. (2017). HIPAA security compliance challenges: The case for small healthcare providers. *International Journal of Healthcare Management*, 10(2), 135-146.

P22- Guo, K. H., & Yuan, Y. (2012). The effects of multilevel sanctions on information security violations: A mediating model. *Information & management*, 49(6), 320-326.

P23- Shih, H. P., Guo, X., Lai, K. H., & Cheng, T. C. E. (2016). Taking promotion and prevention mechanisms matter for information systems security policy in Chinese SMEs. In 2016 *2nd International Conference on Information Management (ICIM),* pp. 110-115, IEEE.

P24- Clapper, D., & Richmond, W. (2016). Small Business Compliance with PCI DSS. *Journal of Management Information & Decision Sciences*, 19(1).

P25- Parsons, K. M., Young, E., Butavicius, M. A., McCormac, A., Pattinson, M. R., & Jerram, C. (2015). The influence of organisational information security culture on information security decision making. *Journal of Cognitive Engineering and Decision Making*, 9(2), 117-129.

Appendix B

Table 2.9 demonstrates our tentative start set papers. The first author fully studied all papers and selected ten papers for the actual start set.

Table 2.9

Tentative start set papers

	Authors	Title
1	Zec, Kajtazi (2015)	Examining how IT Professionals in SMEs Take Decisions About Implementing Cyber Security Strategy
2	Browne et al. (2015)	Linking Threat Avoidance and Security Adoption: A Theoretical Model for SMEs
3	Gundu, Flowerday (2013)	Ignorance to Awareness: Towards an Information Security Awareness Process
4	Gundu, Flowerday (2012)	The Enemy Within: A Behavioural Intention Model and an Information Security Awareness Process
5	Dojkovski et al. (2010)	Enabling Information Security Culture: Influences and Challenges for Australian SMEs
6	Dojkovski et al. (2008)	Developing information security culture in small and medium size enterprises: Australian case studies
7	Dojkovski et al. (2007)	Fostering Information Security Culture in Small and Medium Size Enterprises: An Interpretive Study in Australia
8	Dojkovski et al. (2007)	Institutionalising Information Security Culture in Australian SMEs: Framework and Key Issues
9	Dojkovski et al. (2006)	Challenges in Fostering an Information Security Culture in Australian Small and Medium Sized Enterprises
10	Kankanhalli et al. (2003)	An integrative study of information systems security effectiveness
11	Kaur, Mustafa (2013)	Examining the Effects of Knowledge, Attitude and Behaviour on Information Security Awareness: A Case on SME
12	Renaud, Weir (2016)	Cybersecurity and the Unbearability of Uncertainty
13	Brunner et al. (2018)	Introduction of a Tool-based Continuous Information Security Management System: An Exploratory Case Study
14	Sadok et al. (2020)	It is not my job: exploring the disconnect between corporate security policies and actual security practices in SMEs
15	Aigbefo et al. (2020)	The influence of hardiness and habit on security behaviour intention
16	Barlette, Jaouen (2019)	Information security in SMEs: determinants of CEOs' protective and supportive behaviour
17	Gundu (2019)	Acknowledging and Reducing the Knowing and Doing Gap in Employee Cybersecurity Compliance
18	Ifinedo (2012)	Understanding information systems security policy compliance: An integration of the theory of planned behaviour and the protection motivation theory
19	Herath, Rao (2009)	Encouraging information security behaviours in organisations: Role of penalties, pressures and perceived effectiveness
20	Herath, Rao (2009)	Protection motivation and deterrence: a framework for security policy compliance in organisations
21	Bulgurcu et al. (2010)	Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness
22	Hu et al. (2012)	Managing employee compliance with information security policies: The critical role of top management and organisational culture
23	Puhakainen, Siponen (2010)	Improving employees' compliance through information systems security training: an action research study
24	Hong, Furnell (2019)	Motivating Information Security Policy Compliance: Insights from Perceived Organisational Formalization
25	Li et al. (2019)	Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behaviour
26	Kim, Han (2019)	Do employees in a "good" company comply better with information security policy? A corporate social responsibility perspective
27	Solomon, Brown (2020)	The influence of organisational culture and information security culture on employee compliance behaviour
28	Siponen, Vance (2010)	Neutralization: new insights into the problem of employee information systems security policy violations

CHAPTER 3

Designing for Motivation in Cybersecurity

Low cybersecurity awareness and the lack of good practices have led to a growing number of cyberattacks and incidents in small and medium-sized enterprises (SMEs). This study introduces CYSEC, a new lightweight Do-It-Yourself (DIY) approach to communicate cybersecurity awareness training to a large number of SMEs and encourage them to improve their capability continuously. CYSEC is a method and tool that implements the Self-Determination Theory (SDT) to motivate SME end-users to sustainable self-endorsed forms of security behaviour and guide them to carry out the security improvement on their own. The chapter describes the theoretical framework for modelling self-determination and explains how the adoption of cybersecurity recommendations can be internalised step-by-step by an SME by following an iterative process in CYSEC. Finally, significant lessons learned about the use of CYSEC and its intervention in pursuit of cybersecurity adoption in the pilot SMEs are presented.

This chapter is based on the following publication:
Fricker, S. A., & Shojaifar, A. (2022). Self-endorsed Cybersecurity Capability Improvement for SMEs. In *Proceedings of the 28th annual Americas Conference on Information Systems (AMCIS 2022)*, Minneapolis. Association for Information Systems.

3.1 INTRODUCTION

Cybersecurity has received much attention during the recent years. Data and systems have become critical assets in most organisations, and the threat of attack is continuing to grow. The omnipresent threat of cybercrime implies that many companies view security as one of their top concerns (Cearley et al. 2017), and global spending on cybersecurity has increased in 2018 already to $144 billion at a growth rate of 12.4 percent, from the last years (Moore and Keen 2018).

Small and medium-sized enterprises (SMEs) have become an important target for cyberattacks. According to Symantec, SMEs are attacked increasingly frequently, and attacks on them have started to outnumber the attacks on large enterprises (Wood et al. 2016). SMEs are attractive targets because of their large number and low awareness of cyber risks. Of the 25 million SMEs in the European Union (Hope, 2019), many face the same security challenges as larger companies, with the most important worries of employee awareness and management support for cybersecurity (Knapp et al. 2006).

Many SMEs lack cybersecurity capabilities that would protect them effectively against cyber incidents. Ideally, an organisation would coordinate its security, promote awareness of security-related issues, and establish a resilient cybersecurity culture (Furnell et al. 2002). However, SMEs often lack understanding of risks, do not have the necessary security expertise, lack financial resources to buy consultancy or training, and seldom can prioritise cybersecurity over the daily business. Thus, few SMEs have effective procedures, policies, and controls in place to counteract cyber threats (Gupta, Hammond 2005; Spinellis et al. 1999), leaving SMEs vulnerable to attacks from outsiders as well as from insiders with direct access to the company's systems. These SMEs often become aware that they should have mitigated a cyber incident after it has happened, or if their peers or mass media have pointed them to the need of doing so.

SMEs wanting to improve cybersecurity are confronted with the unfortunate choice of using effort-intensive bespoke consultancy offered by experts or improving their capabilities in an ad-hoc fashion. Researchers have criticized the inadequacy of these choices and suggested the creation of theory-driven and empirically grounded approaches that are tailored for SMEs (Siponen et al., 2007). Several theories have been investigated, including the Protection Motivation Theory, the General Deterrence Theory, and the Technology Acceptance Model, to understand the factors that explain whether and how SMEs and their staff adopt cybersecurity capabilities (Browne et al., 2015; Kankanhalli et al., 2003; Padayachee, 2012). These factors have been summarised in the encompassing Self-Determination Theory (Deci and Ryan 1985; Padayachee, 2012), based on which it can be described how SMEs may be nudged to adopting good practice for diverse levels of motivation that range from amotivation to intrinsic motivation (Padayachee, 2012). Studying how awareness-raising approaches can be tied to the motivations of the target audience and presenting the lessons to learn have been recommended (Chipperfield and Furnell, 2010).

This chapter introduces a new, lightweight approach for SMEs to improve their cybersecurity capabilities, CYSEC. CYSEC is a structured method based on the Self-Determination Theory

that allows experts to communicate cybersecurity recommendations and SMEs to self-assess and improve their capabilities in a do-it-yourself (DIY) fashion. CYSEC is supported with a tool offered to the SME and a process that leads to stepwise incremental improvements of cybersecurity capabilities in the SME. In comparison to bespoke consultancy, CYSEC encourages independence and self-determination of the end-user SMEs and allows cybersecurity experts to scale their reach, allowing to impact more SMEs with less efforts.

The chapter is structured as follows. First, it introduces the self-determination theory and describes how, for diverse levels of self-motivation, the adoption of good cybersecurity practices can be encouraged and adherence to these practices managed. It then describes how we have applied the self-determination theory for the design of the CYSEC method, tool, and process allowing DIY cybersecurity capability improvement in an SME. The ensuing section summarises important lessons that we have learned from the application of the CYSEC method during piloting with SMEs. The chapter ends with a conclusion.

3.2 SELF-DETERMINATION THEORY

3.2.1 Modes of compliance and motivation

An individual's intention to comply has been proposed to result from a combination of extrinsic and intrinsic motivational factors, all well explained within the encompassing Self-Determination Theory (SDT) (Deci and Ryan 1985). SDT allows to integrate diverse human and organisational reasons for compliance with security policy (Alotaibi et al. 2016; Kraemer et al. 2009). The factors they (Alotaibi et al. 2016; Kraemer et al. 2009) identified do influence the employees' compliance behaviour are awareness and training, information quality, persuasion, rewards, sanctions (deterrence), and computer monitoring. Also, several human factors influence the compliance behaviour: perception and situational awareness of security threats, personalities such as prudence and vigilance, habits, freedom in the use of applications and devices, gender, and job satisfaction.

According to SDT (Deci and Ryan, 1985; Padayachee, 2012), employees' motivation to comply range from amotivation to passive compliance to active personal commitment (Table 3.1). The organisation can influence the employee (extrinsic motivation) and trigger internalisation, the process of developing increasingly self-determined behaviour (intrinsic motivation). Although an individual may be unmotivated initially, s/he may be influenced through extrinsic motivation to become increasingly innate to eventually becoming self-motivated to act.

Amotivation refers to a state of lacking an intention to act. Amotivation results from not valuing an activity or not feeling competent. Amotivation may result from disobedience or bad security usability (Padayachee, 2012). Good security usability would lead to self-efficacy (the perceived ability to develop and use relevant skills) and response efficacy (appropriate benefits generated with the activity), minimise response cost, and put the locus of control on the individual.

Extrinsic motivation means to perform an activity because it leads to an outcome that is expected by the organisation. Extrinsic factors are the social climate, working conditions, deterrent controls and monitoring, and the employee's awareness of them. Extrinsic motivation is based on reward and punishment (external regulation), a will to maintain self-esteem (introjection), acceptance of regulation (identification), or full assimilation of the regulation (integration).

Table 3.1

Continuum of motivations with suitable nudges for amplifying desired behaviour, based on self-determination theory (Padayachee, 2012).

Amotivation	**Extrinsic Motivation**				**Intrinsic Motivation**
	External Regulation	Introjection	Identification	Integration	
					
Handle apathy, resistance, opportunism, and incompetence.	Enforce behaviour with rewards and deterrent controls	Encourage behaviour with relatedness and feedback	Agree to behaviour with awareness and commitment	Adapt with behaviour with threat and coping appraisal	Feed interest, commitment, etiquette, and competence.

External regulation is imposed with deterrent controls and rewards. According to the general deterrence theory of motivation (GDT), the certainty and swiftness of detecting non-compliance and punishment affect an individual's intention to comply (Padayachee, 2012). Sanctions may also be informal in the form of self-disapproval like embarrassment or shame, social disapproval like fear of sanctions from peers, and internalisation or moral commitment with regards to legal norms. Positively influencing the individual may be rewards offered for compliant behaviour.

Introjection is more internalised than external regulation. Introjection imposed by building on people's will to avoid anxiety and maintain their ego within the organisation's social climate, hence building on the social climate the employee is confronted with.

Identification is more internalised than introjection. Identification occurs when an individual has understood the personal importance of a behaviour. Such understanding can develop through the awareness of policies as well as knowledge of standards and procedures concerning cybersecurity. Identification represents here a commitment of the individual with the enterprise.

Integration has been explained with the protection motivation theory (PMT). Integration refers thereby to the individual autonomously appraising both personally relevant threats (threat appraisal) and the effectiveness of coping responses for removing these threats (coping appraisal).

Intrinsic motivation refers to performing an activity because it is inherently interesting or enjoyable. Such motivation results from an individual's personality, habits, and skills. Intrinsic

motivation is most successful in high-quality learning and depends on the individual's competence and good habits, etiquette, and ethical values.

3.2.2 Nudges that Amplify Good Behaviour

Self-motivation is about goal orientation, energy, and persistence – all related to producing results. If a goal is perceived as necessary, the concerned person will start adapting his or her behaviour and be persistent to the extent that the behavioural change will sustain. According to SDT (Deci and Ryan, 1985; Padayachee, 2012), a person will be self-motivated if these psychological needs have been satisfied: competence, autonomy, and relatedness. A lack of perceived competence will lead the person to give up. Autonomy is important as the free choice determines how convinced the person is about the behaviour to be adopted. Relatedness to a person who acts as a role model for the behaviour can reinforce self-motivation and even offer a template of how to adopt the behaviour (Shojaifar et al., 2020).

Both intrinsic and extrinsic motivation leads to the adoption and internalisation of new behavior. However, the more intrinsic the motivation is, the more effective and sustainable the adoption of the behaviour is. For each type of motivation, several forces influence how people are moved to act. People can feel motivated because they value an activity, e.g., by an abiding interest. People with such intrinsic motivation have interest, excitement, and confidence, which manifests as enhanced performance, persistence, and creativity. People under external pressure, e.g., with a bribe, fear of being surveyed, or other external influence, risk being unwilling and unmotivated. Still, people can be externally motivated by a stimulating personal commitment to excel and offering role models recognition. Table 3.2 shows, for the continuum from intrinsic motivation to amotivation, how behaviour may be influenced. Any method for helping users to achieve goals should operationalise these factors in the method's design (Shojaifar et al., 2020).

The table points to the important SDT constructs that should be operationalised by a coaching method and suggests hypotheses that can be used for evaluating whether the method supports the effectiveness of the cybersecurity knowledge communication for SMEs. The constructs concern attributes of the method user and of the method environment with which the user interacts. The method user's attributes are interest in the desired behaviour, competence, and autonomy. The method environment's attributes are relatedness, belonging, and connectedness offered to the user, pressure imposed through rewards, threats, and deadlines, and knowledge provided for helping the user to develop self-efficacy, and choice offered for fostering autonomy of the user (Shojaifar et al., 2020).

3.3 Automated Coaching of Cybersecurity Improvements

The improvement of cybersecurity of SMEs depends on communicating cybersecurity knowledge from experts to these SMEs. Table 3.3 characterises these roles of the cybersecurity ecosystem. In addition to these roles, we introduce the new role of the knowledge broker. The knowledge broker coordinates the knowledge communication to SMEs and helps them to become secure by raising awareness of threats and controls and by facilitating improvements. The broker identifies experts, gathers cybersecurity knowledge of relevance for SMEs, and creates channels for communicating that knowledge to the SMEs. To serve the large number

of SMEs, while considering the scarcity of experts, automation is required to scale such communication.

Table 3.2

Factors for influencing desired behaviour, based on SDT (Deci and Ryan, 1985)

Motivation	How Desired Behaviour is Influenced
Intrinsic motivation: a person with interested and joy in a desired behaviour tends to seek out novelty and challenges, to explore, learn, and exercise one's capacities even in the absence of specific rewards.	Autonomy of choice, perceived competence or self-efficacy, and a caring environment with optimal challenges and feedback of how the person's actions lead to the outcomes enhance intrinsic motivation and performance (Deci and Ryan, 1985). Extrinsic rewards, threats, deadlines, pressured evaluations, and imposed goals diminish intrinsic motivation.
Extrinsic motivation: continuum from coercion to stimulating intrinsic motivation: **A) External regulation** is associated with control or alienation, and actions are perceived imposed by external regulators **B) Introjected regulation** is not accepted as the one's own, but behaviours are performed to maintain a feeling of worth, e.g., to avoid guilt or anxiety or attain pride **C) Regulation through identification** conscious valuing of rules such that the action is accepted or owned as personally important **D) Integrated regulations** are fully assimilated to the self as a result of evaluation and bringing the regulations into congruence with one's other values and needs	With prescribed behaviours and values, new behaviour is internalised with meaningful rationales, autonomy, and relatedness (Deci and Ryan, 1985). **A)** External regulation is achieved with salient rewards or threats. **B)** Introjected regulation is achieved with the provision of belonging and connectedness, e.g., by having significant others to whom people feel attached or related prompt, model, endorse, or value the desired behaviour. **C)** Regulation through identification can only be achieved if autonomy of choice is provided. **D)** To integrate a regulation, the rules' meaning must be synthesised with respect to the person's goals and values with great autonomy in the sense of choice, volition, and freedom from excessive external pressure.
Amotivation: lacking intention to act due to coercion, leading to failed goal achievement.	Amotivation results from not valuing an activity, not feeling competent to do it, or not expecting the activity to yield a desired outcome.

Table 3.3

Roles in the cybersecurity ecosystem for SMEs

SMEs	Cybersecurity Experts
The SMEs are the entities deserving protection. An SME may be decomposed into the roles of management expected to define goals and policies, the employees whose behaviour influences the SME's security, and the CISO[1] who coordinates incident response and security improvement. SMEs appear in a large number; in the EU, they represent more than 99% of the enterprises (Hope, 2019).	The cybersecurity experts are those how have the knowledge and capacity to handle incidents, protect an organisation's data, ICT infrastructure, and product and service offerings, and define policies giving rise to good security cultures, respectively train people in good security behaviour. They appear in a number significantly smaller than the total number of SMEs.

[1] One step in improving security in an SME is to determine the SME's Chief Information Security Officer.

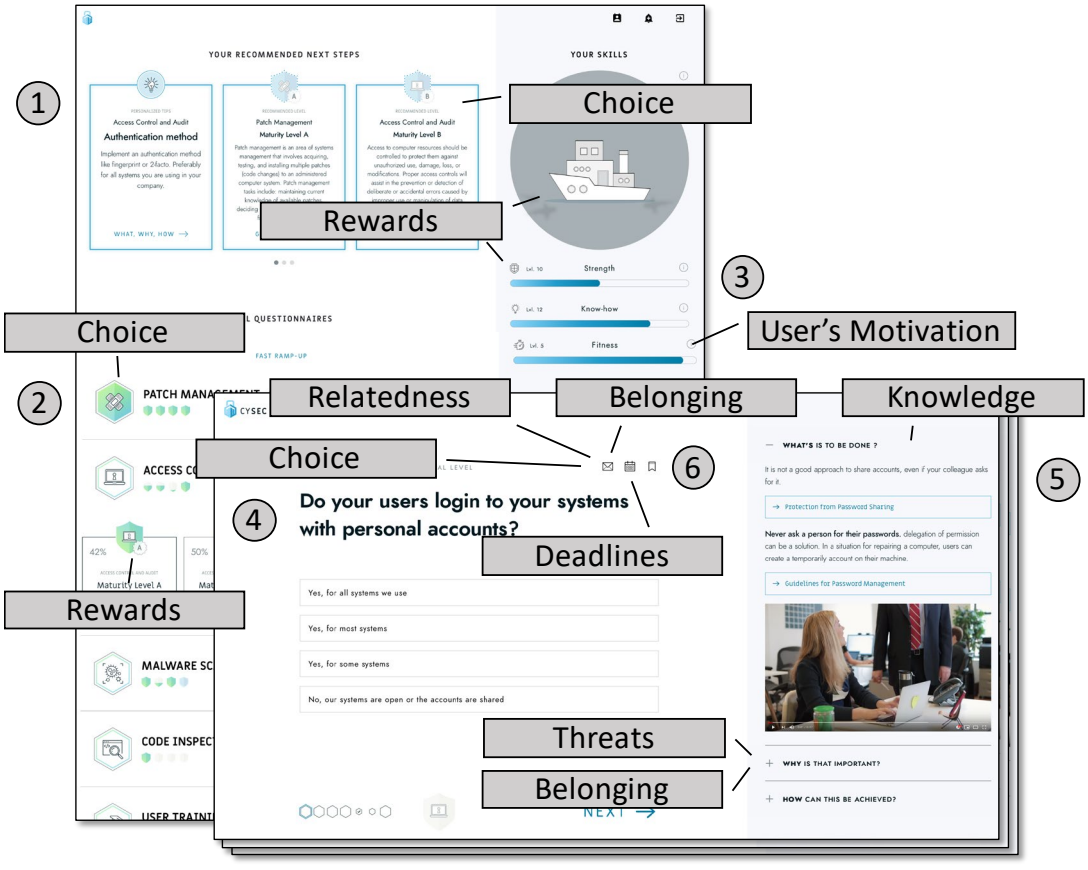
To successfully communicate cybersecurity knowledge, the knowledge broker must solve several challenges. Cybersecurity knowledge is broad in scope, and its relevance depends a lot on the context in which it is applied. For that reason, knowledge brokerage must filter the relevant knowledge for a given SME and present it in a way accessible by the SME. Hence, to ensure the fitness of the provided cybersecurity knowledge, tailoring is needed with filters based on the specific characteristic of the SME.

It is the customers, the customer projects, and the employees that are the business priority for most SMEs and not cybersecurity improvements. For that reason, nudges for motivating SMEs need to be carefully deployed and offered along each SME's journey of hardening its security. Knowledge brokerage can offload some of the communication between cybersecurity experts and SMEs and scale some of the improvement work, but still requires the presence of the cybersecurity community. The here presented approach requires the community to reflect cybersecurity practice, innovate solutions for protection against evolving threats. It also requires openness for setting standards and establishing a climate conductive to cybersecurity useful for SMEs, and recognition of achievements, respectively social feedback to reward good behaviour and establish appropriate norms.

3.3.1 Offering Relatedness, Appraisal, Knowledge, and Choice in a Coaching Tool

Figure 3.1

Main user interfaces of CYSEC and mapping of its features to SDT constructs



CYSEC is a method and tool allowing SMEs' Chief Information Security officers (CISO) to improve cybersecurity in a do-it-yourself fashion. The method guides the CISO in following Deming's plan-do-check-act (PDCA) (Deming, 1952) cycles of selecting sensible security themes, implementing the recommended practice, checking progress, and adapting based on lessons learned. The tool offers memory allowing the CISO to continue the PDCA work where he left off. The tool also includes SDT design elements to offer motivation for effective results and sustainability of the progress (Shojaifar et al., 2020).

Table 3.4

Implementation of Nudges

Nudge	**Locus**	**Function**
Relatedness	Dashboard: recommendations	Self-adaptation of recommendations to SME profile and improvement progress.
	Dashboard: progress summary	Continuous feedback about progress and motivation.
	Work area: steps	Self-adaptation of recommended next improvements
	Offline	Personal workshops with SMEs for reflecting about improvement experience.
Belonging, and Connectedness (Relatedness)	Work area: action cockpit	Fostering of personal communication between CISO and employees.
	Offline	Personal workshops with SMEs for reflecting about improvement experience.
Rewards, threats, and deadlines (Competence, Autonomy)	Dashboard: progress summary	Feedback about the defense strength built and knowledge acquired in the company, and persistence in working on cybersecurity ("fitness").
	Work area: expert knowledge	Information about importance of improvements, e.g., by referring to cyber risks that should be mitigated.
	Work area: action cockpit	Setting of calendar entries and mailing reminders to employees.
Knowledge (Competence)	Dashboard: access to capability areas	Access to knowledge and recommendations for building cybersecurity in the SME.
	Work area: expert knowledge	Presentation of knowledge and recommendations for building cybersecurity in the SME.
Choice (Autonomy)	Dashboard: recommendations	Presentation of the three top recommendations, offering choice about the next important improvements.
	Dashboard: access to capability areas	Presentation of capability areas, offering choice about type of cybersecurity to build.
	Work area: action cockpit	Choice of deferring improvements with a calendar entry or bookmark and of involving employees by e-mail.

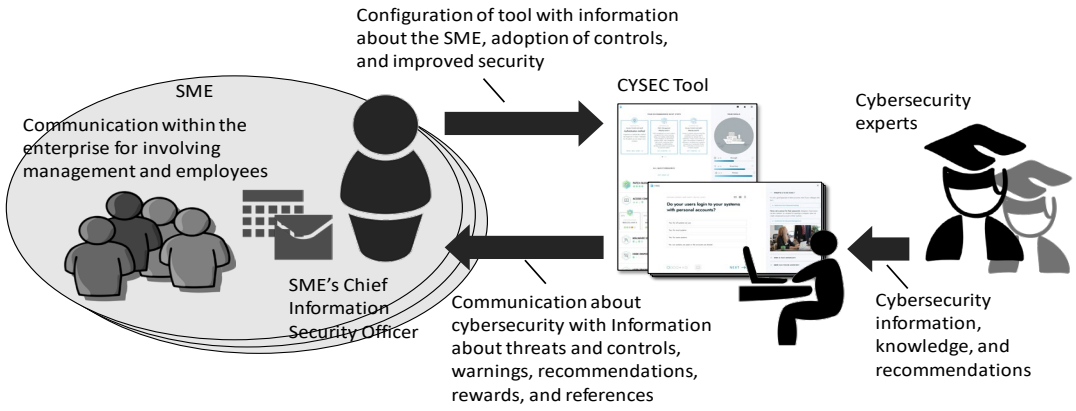
Figure 3.1 shows the two main interfaces of the CYSEC tool offered to the user. A dashboard shows the features (1) recommendations for next improvements, (2) access to capability areas for PDCA work, (3) summary information about the company progress. Once the PDCA work for a given capability area is started, e.g., by choosing a recommendation or a capability area, the user enters the work area that offer the features (4) self-assessment, (5) access to expert knowledge, and (6) action cockpit for creating calendar entries, mails, and reminders (Shojaifar et al., 2020). Table 3.4 describes how CYSEC operationalises SDT.

3.3.2 Knowledge Communication and Improvement Process

To act as a knowledge broker, the CYSEC tool has been positioned between the cybersecurity experts who provide expertise and the SMEs who use it for improving their security. Figure 3.2 gives an overview of the roles and information flows. Here, we describe an SME's improvement process that is enabled by the CYSEC tool, the approach allowing expert knowledge to be integrated into the tool, and the role of the community to establish a culture for securing SMEs in a sustainable manner.

Figure 3.2

Roles and flows of information and knowledge for improving cybersecurity



3.3.3 Enabling Self-determined Cybersecurity Improvement in the SME

The CYSEC tool encourages its users to continuously improve their cybersecurity incrementally step-by-step by following an iterative process of plan-do-check-act (PDCA) (Deming, 1952) improvement cycles. PDCA is established for decades already for structuring improvements in an organisation.

Plan stands for the setting of an objective for an improvement cycle. CYSEC guides this planning with recommendations that are adapted to the profile of the enterprise and its progress in being secure. Initially, the tool user is recommended to configure the organisation in the tool, among others with information about the CISO, workforce, infrastructure, and type of business. This information is then used to recommend improvements that fast lead to all-over-the-board protection. Once such protection is achieved, recommendations for specialty needs of the SME get prioritised. While the CYSEC tool offers recommendations, it is always the CISO who is in control about which recommendation to adopt first and which ones to postpone.

Do stands for implementing suitable actions to achieve the objective set for the improvement cycle. CYSEC uses a question-answer approach allowing the CISO to self-assess his enterprise and receive feedback acknowledging achievements and guiding how to improve his organisation. The knowledge is communicated in the form of what should be done, why the action is important, and how the action can be realised with suitable tools and services suggested as controls and employee training. For new topics, the CISO can access training modules that allow him to understand the topic and apply the controls.

Check stands for analysing the outcomes of the actions with respect to the objective set for the improvement cycle. Checking can mean to verify if the concerned controls are running as intended, interact with employees to verify awareness, and reflect if the security objective has been achieved.

Act stands for reinforcing an improvement by analysing the overall improvement progress, causes for inefficiencies, gaps, or other difficulties, and institutionalising good practice. Inefficiencies could lead to abandoning one type of control and replacing it with a more user-friendly one. Gaps could lead to specialised improvements beyond what CYSEC was recommending. Institutionalising could mean to define when to follow-up and revisit the security objective of the current PDCA cycle.

3.3.4 Communicating Cybersecurity Expertise with CYSEC

The capability area recommended first to a new user is *company configuration*. It provides the user with the ability to characterise the company, define common roles like the CISO, Data Protection Officer, and Cyber Security Incident Response Team (CSIRT), declare compliance needs like for the General Data Protection Regulation (GDPR), and document the SME's business model as well as the ICT infrastructure used to run the business. The questions and provided knowledge are prepared in a way to raise awareness of organisational aspects of cybersecurity and guide the users in establishing the appropriate cybersecurity organisation. Also, the configurations are reused for tailoring any other capability area and ensure the pertinence and relevance of the questions.

The currently available capability areas for fast-track improvements are malware scans, patch management, access control, backup, and user training. These areas were chosen because they address basic information security goals for any SME. If implemented adequately together, offer a good basic level of security.

CYSEC is flexible and allows programmers to add any other capability area that security experts consider relevant for SMEs. In the context of our project, network controls, intrusion prevention with Honeypots, and security engineering for software and hardware products like IoT are presented because of their relevance. Other specialist areas are expected to relate to the protection of personal or confidential data processed by SMEs and algorithms trained for applications of artificial intelligence offered or used by SMEs. The already included capability areas can be used as templates for how to present the new areas in an accessible way to SMEs for capability improvement.

3.4 LESSONS-LEARNED FROM SMES' DO-IT-YOURSELF IMPROVEMENT

Twelve SMEs (project partners) utilised CYSEC. The participating SMEs formed a variety of companies with different levels of expertise in cybersecurity. They had experience in IT, and all of them implemented some security controls, including password management, basic approaches for privacy protection, firewalls, two-factor authentication, cloud security features, and anti-virus installation. These SMEs utilised CYSEC during the piloting period. We conceptually organised the results of the studies around two themes: the impact of CYSEC on SMEs and the improvement needs for CYSEC. There are the lessons we have learned within each, supported by significant quotes from the users. The lessons learned present the synthesised findings from the evaluation studies (by applying the qualitative method) at the end of the project.

3.4.1 The impact of CYSEC

CYSEC impacted cybersecurity activities and the decision-making process in the SMEs by providing users with a holistic view of the essential cybersecurity capabilities, threats, and countermeasures.

Lesson 1: Giving a holistic view of security threats through a self-assessment approach motivates users to plan a new security improvement or reassess their current policy.

CYSEC informed the SMEs about the security controls based on a list of capabilities. Those SMEs that were aware of the threats but were not actively thinking of them were motivated to plan for practice.

"I can say we implemented training after using CYSEC because it is almost in the plan but using CYSEC boosts us to implement these training."

"We were aware of most of them [threats and controls], but not actively thinking of them; however, after it [CYSEC], we decided and have planned to improve the process of password recycling and the process of backups."

"CYSEC clarifies and reinforces the improvement in processes, technical issues, and people."

"CYSEC is useful to review and check if everything is OK or not, a complete review of cybersecurity issues. We used your tool to review our policy."

The tool increased awareness for those SMEs that have been unaware of some threats and vulnerabilities.

"It gives you comprehensive information in a holistic way. Now we know about software automated patching."

"After using CYSEC, we organised small meetings discussing the problems, and there is a person in charge of managing it and monitoring the plans."

Lesson 2: CYSEC is a tool that an SME can use to start learning cybersecurity and onboard new employees.

Some SME CEOs indicated that CYSEC has an impact on adopting preventive cybersecurity behaviours for those employees that get started in security or for the new employees. It can

facilitate gaining knowledge with the quick training and a view of all threats that may be obscured at the beginning.

"We have a lot of online features, when you start a company, you should be aware of all security threats and controls, and we must have CYSEC at the beginning of a start-up."

"CYSEC is most useful for the new members of the company. It gives quick training and view of all threats; we let them do the CYSEC assessment, and we see their results."

3.4.2 Improvement of CYSEC

This theme is about how users experienced the tool usage and their attitudes about the impact of CYSEC. Moreover, what requirements should be considered to improve the security communication effectiveness.

Lesson 3: Providing knowledge according to the SMEs' expertise is critical in awareness-raising.

The SMEs had a diversity of security expertise. CYSEC had a positive awareness-raising impact on SMEs that were not cybersecurity experts. However, the tool demonstrated no awareness-raising impact on cybersecurity expert SMEs since they required advanced knowledge (e.g., trusted Boot and hardware encryption). CYSEC needs to provide more targeted content to support communication effectiveness.

"We did not do patch management and backups correctly and regularly. Also, we were not aware of checking and monitoring antimalware policies."

"After using it, we realised that all controls are important, and there is no control that we can ignore."

"We have high-level security skills. CYSEC is more useful for us if you add more advanced security controls. For instance, hardware encryption."

Lesson 4: Fitting the training content to the SME business model influences perceived effectiveness.

The SMEs had different business models and requirements. Having access to customised (not general information) and SME-specific content that is consonant with SME requirements and characteristics are crucial. Security expert SMEs needed more fresh security information, e.g., about compromised websites. Besides the content of the training material, CYSEC needs to support different languages to facilitate learning for the users who do not know English very well.

"[training content] is often too generic. It should be customisable, giving specific suggestions based on our infrastructure."

"Translate coaches in different languages, because most SMEs have difficulty in using English and learn in English. It is necessary to have it in different languages."

"Having a list of the latest threats and security vulnerabilities. The most recent things to keep us update to be interesting for us."

Lesson 5: Taking hands-on solutions for those SMEs that are not experts is crucial.

For those SMEs that were not cybersecurity experts, access to practical solutions (e.g., available products, available patches, training courses) compatible with their immediate needs was necessary.

"The tool should provide some specific solutions and prioritisation. The tool should give most important suggestions, and an action plan for the next six months."

"We need to know how to solve the problems (not only presenting the problems). We do not know how to improve compliance or monitor changes in individuals' behaviours. We need access to patches, training courses, and personalising security products."

3.5 CONCLUSION

This study presented CYSEC, a do-it-yourself (DIY) cybersecurity assessment and capability improvement method and tool for small medium-sized enterprises (SMEs), and the key lessons learned from the usage of the CYSEC in pilot SMEs. We explained how the CYSEC method guides SMEs through plan-do-check-act cycles and personalised recommendations. We demonstrated how CYSEC implemented Self-Determination Theory to support effective security communication with SMEs for motivating sustainable self-endorsed forms of security behaviour. Based on the findings, we have learned that supporting relevant knowledge and skills according to the SMEs' security requirements is necessary to reinforce self-endorsed capability improvement. Further, CYSEC, with a holistic view of security threats and practices, motivated SMEs for planning, provided them with a comprehensive understanding, and supported them in reassessing security topics. Also, the tool was helpful in onboarding SMEs' new employees by providing immediate knowledge and quick assessment. Nevertheless, it should be noted that a tool for knowledge communication cannot replace interaction with peers in a community. Future research may build upon the lessons learned to study how we can support effective communication between security experts and SMEs. Further, CYSEC needs to be more aligned to global standards, e.g., ISO 27001. Future research needs to study how CYSEC may impact the adoption of security standards in SMEs.

CHAPTER 4

Automating Cybersecurity Communication

Cybersecurity is essential for the protection of companies against cyber threats. Traditionally, cybersecurity experts assess and improve a company's capabilities. However, many small and medium-sized businesses (SMBs) consider such services not to be affordable. We explore an alternative do-it-yourself (DIY) approach to bringing cybersecurity to SMBs. Our method and tool, CYSEC, implements the Self-Determination Theory (SDT) to guide and motivate SMBs to adopt good cybersecurity practices. CYSEC uses assessment questions and recommendations to communicate cybersecurity knowledge to the end-user SMBs and encourage self-motivated change. In this chapter, the operationalisation of SDT in CYSEC is presented, and the results of a multi-case study are shown that offer insight into how SMBs adopted cybersecurity practices with CYSEC. Effective automated cybersecurity communication depended on the SMB's hands-on skills, tools adaptedness, and the users' willingness to document confidential information. The SMBs wanted to learn in simple, incremental steps, allowing them to understand what they do. An SMB's motivation to improve security depended on the fitness of assessment questions and recommendations with the SMB's business model and IT infrastructure. The results of this study indicate that automated counselling can help many SMBs in security adoption.

This chapter is based on a shortened instance of the following publication:
Shojaifar, A., Fricker, S. A., & Gwerder, M. (2020). Automating the Communication of Cybersecurity Knowledge: Multi-Case Study. In *IFIP World Conference on Information Security Education (WISE),* pp. 110-124. Springer, Cham.

4.1 INTRODUCTION

Small and medium-sized businesses (SMBs) as the foundation of the EU's economy (Muller et al., 2017) are the weakest spot for cyberattacks (Ntouskas et al., 2012; Caldwell, 2015). SMBs have specific characteristics, and these characteristics separate them from large companies and make them highly vulnerable to security attacks (Gupta and Hammond, 2005; Goucher, 2011; Kurpjuhn, 2015; Mijnhardt et al., 2016). The lack of financial resources, expertise, written formal security policies, and also the common wrong attitude towards security and risks are some of these characteristics. Previous studies considered these characteristics and their influences on SMBs' resilience to security threats (Furnell et al., 2002; Ntouskas et al., 2012; Valli et al., 2014; Brunner et al., 2017).

Ntouskas et al. (2012) present a self-management security method which provides a consultancy environment for SMBs. Brunner et al. (2017) focus on the level of automation in information security management and describe a continuous, risk-driven, and context-aware information security management system. Their framework is applicable to SMBs (Brunner et al., 2017). Furnell et al. (2002) present a self-paced, flexible, and personalised security training software tool. The tool provides employees with the ability to learn some security countermeasures and desired behaviours.

In our experience of working with SMBs that were active in the IT industry, we found out that access to knowledge is not enough for motivating the SMBs to adopt appropriate behaviour. The SMBs need to understand the severity of threats and the impacts on their businesses. Moreover, providing hands-on skills that are consonant with the SMBs' capability motivates them to have security practices. We have not found any approach that considers the SMBs' motivation in the adoption of cybersecurity through self-assessment, learning, and improvement. Technical security measures form a large part of information security research (Dhillon and Torkzadeh, 2006). Cybersecurity is more effective if the attention goes beyond the technical protecting means to the users, social, and organisational environment (Dhillon and Torkzadeh, 2006; Pahnila et al., 2007; Cranor, 2008). Human errors are the main cause of security failures (Cranor, 2008) and promoting users' self-efficacy, and knowledge in information security can enhance organisation security (Rhee et al., 2009).

CYSEC is a self-paced SMB-specific training and assessment method that automates elements of a counselling dialogue (Shojaifar et al., 2018) between a security expert and employees in the SMB to ward off cyber threats. The interaction and dialogue between employees and security experts bridge the gap between them and makes the information security measures more effective (Albrechtsen and Hovden, 2009). Since users' resistance to accepting security tools and advice is one of the main problems for information security (West, 2008), the dialogue in CYSEC is based on theoretical foundations of motivation and the effects of employees' psychological needs on cybersecurity adoption. Persuasion is more effective than rational training strategies when the level of commitment to change is low (Hayes, 2002).

The current study focuses on CYSEC evaluation to see whether the CYSEC is useful and effective as a method of communicating cybersecurity expertise for enabling DIY cybersecurity assessment and capability improvement for SMBs. The study purpose was

approached by using an observation strategy based on the think-aloud protocol. While the previous literature mainly studies individuals' security behaviour through several interviews (Albrechtsen and Hovden, 2009; Menard et al., 2017; Pham et al., 2017), the empirical findings of this study are based on observing actual usage of the tool to determine those factors which facilitate or control users' behaviour. The data was qualitatively analysed based on our theoretical model derived from Self-determination Theory (SDT) (Ryan and Deci, 2000; Deci and Ryan, 2008). Our results demonstrate that SDT can explain motivational factors for effective counselling communication, and these factors influence users' behaviour to adopt cybersecurity recommendations. Unmet psychological needs may hamper users' adoption of cybersecurity behaviours. We observed that the automated dialogue is more effective when the method offers adapted behaviour, users' self-efficacy improvement, and SMBs' confidentiality issues together.

The remainder of the chapter is structured as follows. Section 2 presents the theoretical background. Section 3 describes the CYSEC method. Section 4 describes the design of the study. Section 5 presents the process of data collection in SMBs. Section 6 analyses the results and answers the research questions. Section 7 discusses the significance of the results and the threats to validity. Section 8 summarises and concludes.

4.2 Theoretical Background

Cybersecurity studies draw on a variety of theories from different disciplines (Menard et al., 2017; Pham et al., 2017). Self-Determination Theory (SDT) (Ryan and Deci, 2000) provides a rigorous theoretical framework for studying motivation and has been considered in cybersecurity (Menard et al., 2017; Pham et al., 2017). SDT describes and explains people's psychology of being self-motivated for adopting personal behaviours (Ryan and Deci, 2000). SDT was developed and evaluated with extensive research that resulted in an in-depth understanding of the conditions under which people will develop towards being a self-motivated in pursuing what they and their community consider as being desirable. The results of the research help managers and coaches to bring meaningful norms of behaviour into use and support the concerned people in adopting the conduct.

Self-motivation concerns goal-orientation, energy, and persistence – all related to producing results. If a goal is perceived to be important, the concerned person will start adapting his or her behaviour and be persistent to the extent that the behavioural change will sustain. According to SDT, a person will be self-motivated if these psychological needs have been satisfied: competence, autonomy, and relatedness. A lack of perceived competence, or self-efficacy, will lead the person to give up. Autonomy is important as the free choice determines how convinced the person is about the behaviour to be adopted. Relatedness to a person who acts as a role model for the behaviour can reinforce the self-motivation and even offer a template of how to adopt the behaviour.

Both intrinsic and extrinsic motivation leads to the adoption and internalisation of new behaviour. However, the more intrinsic the motivation is, the more effective and sustainable the adoption of the behaviour is. For each type of motivation, several forces influence how

people are moved to act. People can feel motivated because they value an activity, e.g., by an abiding interest. People with such intrinsic motivation have interest, excitement, and confidence, which manifests as enhanced performance, persistence, and creativity. People under external coercion, e.g., with a bribe, fear of being surveilled, or other external pressure, are risking to be unwilling and unmotivated. Still, people can be externally motivated by a stimulating personal commitment to excel and offering role models' recognition. We demonstrated the continuum of motivation and how behaviour may be influenced in Chapter 3 (see Table 3.2). Any method for helping users to achieve goals should operationalise these factors in the method's design.

Table 3.2 (in Chapter 3) is pointing to the important SDT constructs that should be operationalised by a coaching method. It suggests hypotheses that can be used for evaluating whether the method supports the effectiveness of the cybersecurity knowledge communication for SMBs. The constructs concern attributes of the method user and environment with which the user interacts. The method user's attributes characterise the user's desired behaviour, self-efficacy, and autonomy. The method environment's attributes are relatedness, belonging, and connectedness offered to the user, pressure imposed through rewards, threats, and deadlines, the knowledge provided for helping the user to develop self-efficacy, and choice offered for fostering autonomy of the user.

4.3 CYSEC, A DIY CYBERSECURITY IMPROVEMENT METHOD

CYSEC is a method and tool allowing SMBs' Chief Information Security Officer (CISO) to improve cybersecurity in a do-it-yourself fashion. The method guides the CISO in following Deming's plan-do-check-act (PDCA) (Deming, 1952) cycles of selecting sensible security themes, implementing a recommended practice, checking progress, and adapting based on lessons-learned. The tool offers memory allowing the CISO to continue the PDCA work where he left off. The tool also includes design elements based on SDT that aim at offering motivation for effective results and sustainability of the improvements.

The content has been organised into five cybersecurity themes (Patch Management, Access Control and Audit, Malware Scans, User Training, Backup). These themes allow fast ramp-up of security capabilities with minimal effort and large impact on SMBs.

Recommendations are generated based on users' answers to the self-assessment questionnaires for maturity improvement (Ozkan and Spruit, 2018). For the first time, new users will see one recommendation to fill out the company coach. As an adaptation rule, the answers to the company coach affect the questions asked in the other coaches. After completing the company coach, several coaches will be active in the dashboard. The available capabilities are defined and prioritised based on the cybersecurity expert's propositions (third author). When a user selects one coach, s(he) has access to the self-assessment questions and relevant capability training content. Providing the content was based on the research into the training material (Gardner and Thomas, 2014), technical reports provided by Symantec and Ponemon, and meeting with experts. Technical reports provide updated cybersecurity solutions and statistics. At the end of each coach, users see summary information and are redirected to the

dashboard. In the dashboard, they see the progress information, achieved scores, and new recommendations for cybersecurity practices and selection of the next coach(es).

The main features and interfaces of CYSEC have been presented in Chapter 3 (see Figure 3.1, Table 3.4). In the rest of this chapter, we explain the formative evaluation of CYSEC.

4.4 STUDY DESIGN

The study aimed at evaluating whether CYSEC is useful and effective as a method of communicating cybersecurity expertise for enabling DIY cybersecurity assessment and capability improvement for SMBs. To achieve this aim, we designed a deductive multi-case study and used observation as the main method for data collection (Yin, 2009). Case studies are common in information systems research and cybersecurity (Pham et al., 2017).

For planning the case study, a study protocol was developed and sent to the participating SMBs. Before conducting the case studies, a pilot workshop was performed for a start-up project that involved the second and third researchers and a developer. The pilot allowed to identify and resolve initial problems in the study design. The selection of the cases was based on the availability of the SMBs. It has been done in two steps. At first, data collection was based on four SMBs, and during the study (project lifetime), two more SMBs were included. Based on Yin (2009), when using a multiple-case design, the number of case replications is essential instead of sampling logic, and the model of generalisation is analytic generalisation when we have a developed theory as a template. The selected SMBs have security resources, working in the software industry, and their CISOs have a level of expertise in security. The CISOs' behaviour was the unit of analysis. Table 4.1 presents our SMBs' demographics. Based on the EU Commission definition, companies with < 50 employees and annual turnover ≤ €10 million are small, and those with < 250 employees and annual turnover ≤ €50 million medium.

Table 4.1

SMBs Demographics

ID	Step	Size	Offices	Maturity (Some controls implemented)	Structure
1	1	Medium	3	Access control., network controls, backup, encryption	CEO, security team, employees
2	1	Medium	3	Password mgmt., patch mgmt., encryption, (training) security best practices for developers	CEO, security team, employees
3	1	Small	2	Password mgmt., Code inspection	CEO, security team, employees
4	1	Small	1	Access control, patch mgmt.,	Professors, manager, Security team, users
5	2	Small	1	Using a firewall, Access control	CEO, manager, employees
6	2	Small	1	Password mgmt.,	CEO, managers, developers

4.4.1 Research Questions and Case Selection

The following two research questions were analysed. RQ1 related the communication method to the user's motivation and adoption of cybersecurity recommendations. RQ2 reflects users' evaluations of the method and tool after the actual usage.

RQ1[2]*: How do the CYSEC dashboard and work area features influence the effectiveness of communicating cybersecurity to motivate users' adoption of desired behaviour?* To improve SMBs' cybersecurity capability, they need to adopt good cybersecurity practices. Since CYSEC provides security experts' recommendations and training content, we are studying SMBs' cybersecurity adoption through CYSEC communication. The factors of the study are based on the SDT constructs and CYSEC features (see Chapter 3). We evaluate the effectiveness of communication by observing users' behaviour, attention, comprehension, and theoretical cause-effect relationships (Yin, 2009). *RQ2*[3]*: Do the SMB human end-users perceive CYSEC to be acceptable and useful as a tool assisting DIY cybersecurity assessment and improvement?* Tool acceptance and perceived usefulness are significant for us since a problem for information security is the users' resistance to accepting security tools (West, 2008). Therefore, in RQ2, we want to have the users' attitude.

4.4.2 Workshop Design and Meeting with Companies

Each workshop started with an explanation of the study, steps, and relevant objectives. To collecting honest responses (Bennett and Robinson, 2000), the researcher emphasised that the collected data would be applied anonymously for academic purposes and then obtained the subjects' consent. During the workshops, the researcher took notes about how the subjects interacted with the tool and asked them to "think aloud" (Runeson et al., 2012) and explain their expectation. The workshops had four parts and four tasks for the CISO in the SMB. In part 1, the CISOs characterised their companies. In part 2, and to understand the main user's capabilities, the CISOs answered three questions about their level of education, experience in cybersecurity, and their roles. The responses to the questions were used to confirm the suitability of the selected case for the study. In part 3, the user applied the CYSEC. In part 4, the observation was supplemented with a post-observation quantitative questionnaire (Table 4.2). The result section presents the process of the workshops.

4.5 RESULTS

In this section, we present the process of data collection in the 1-day workshops.

Company 1: two people (CISO) participated in the workshop, which took 26 minutes. This workshop took a short time since the users only provided their feedback at the end of the workshop. The researcher had the lowest degree of interaction in this workshop. It seems they were familiar with the topics and questions, so they refer to the training content only two or three times.

[2] Modified in Chapter 1
[3] Modified in Chapter 1

Company 2: Two people from a team of cybersecurity participated. The workshop took one hour and forty-three minutes. The users referred to the training content several times when they were not able to understand the actual goal of the questions. The users stated that the training content for some questions is not completely correct.

Company 3: Only one person (CISO) participated. The workshop took two hours and thirty-five minutes. The user explained that their SMB had not managed any cybersecurity training courses and security awareness issues are usually sent to the employees by email. During the workshop, the user experienced several system time-outs. So, the user required to log in several times. This issue was due to a bug in the tool, and it distracted the user's attention to some extent. So, the researcher needed to interact with the user. For this SMB, confidentiality issues were very critical.

Company 4: A team of seven IT specialist participated. The workshop took two hours and a half. The users went through the coaches the same as the first workshop. The distinctive feature of this workshop was the discussion about each question between participants to find suitable answers based on the company's requirements. The users applied training content too much to understand the questions. For this SMB dynamic, and reliable training material was significant.

Company 5: Only one person (CISO) participated. The workshop took thirty-four minutes. The user stated that their SMB has no chain of management. In this workshop, the user emphasised that some of the questions have no suitable options for the answer.

Company 6: Two people from a team of cybersecurity participated. The workshop took forty minutes. People in the workshop had a language problem, and they used Google translate to understand the content. So, the researcher needed to interact with the users. The users went through some of the coaches.

In all workshops, the mechanism of the tool usage was almost the same and the users referred to the training content mostly when they had a problem to understand questions. The meaning of some of the questions was not clear for the CISOs. Also, all of them required a summary and recommendation after finishing each coach.

4.6 ANALYSIS

For answering the research questions, we explain the researcher's observations of the tool usage based on SDT-specific features of the CYSEC, which indicated in Chapter 3.

4.6.1 Factors Influencing Cybersecurity Communication (RQ1)

According to the workshop results, the CYSEC dashboard and work area features affected the users' motivation for the adoption of desired behaviour. These features together can facilitate security management and intra-organisational connection between the CISO and the employees and support self-efficacy and capability improvement in the SMBs. The participating SMBs learned about cybersecurity and adopted practices and controls when the immediate perceived learning experience was good.

Available Expert Knowledge (CYSEC Work Area). As suggested by SDT, we have observed that improving self-efficacy had a positive impact on the users' self-motivation. The

immediate relevance of the training material provided by the CYSEC tool affected the subjects' decision to study the training material. Still, even though the participants did not have any systematic cybersecurity course so far, none of them read the full knowledge texts provided by CYSEC. Instead, the subjects studied training material when they did not understand a question or wanted to know more about a topic to select suitable answers.

Company 4: "*We need practical instructions and steps to help us solve our issues and not general ideas.*"

Company 2: "*some materials are not relevant to the right topics/questions.*"

When responding to some of the questions, they referred to the training content occasionally and only to find a specific issue. For instance, to explore how they can measure the strength of password based on a tool.

Perceived reliability, expert support, clarity, and local language support of the content were important in the sense that the lack of these quality attributes hindered participants from accepting training input.

Company 4: "*Parts of the content are not clear enough for us, and some materials (statistics) are not reliable since they are not covering many security experts and SMBs' opinions.*"

Company 2: "*Training content needs to present the severity of threats clearly.*"

Company 2: "*Since the coaches are in English, it might be possible for some SMBs to be unwilling to apply the tool.*"

Company 6: "*Can you please tell me what actually you mean [even after using Google translate for the training content].*"

The quotes here can demonstrate the users' awareness and attention to the training content with respect to the effectiveness of the communication.

Assessment Questions for Next Step Improvement (CYSEC Work Area). As suggested by SDT, choice supported autonomy and self-motivation. However, the options should always be relevant and adapted to the IT infrastructure and operations of the company. The participants looked for questions that fit their interest and perceived needs. If they could not find such questions, they explained their needs by referring to their company's characteristics (assets). Moreover, they wanted the coach to adapt the questions to the SMB's characteristics specified with preceding answers.

Company 3: "*here, the tool should provide a lot of questions to cover different operating systems.*"

Also, the users wanted each question to be answerable with options for the response that explained the situation precisely. The researcher observed that the users did not answer some questions or selected an imprecise option due to lack of suitable choices.

Company 2 about the question "Do your users use any other authentication method, such as fingerprint or 2-factor authentication, to control access to your sensitive systems:" "*for some systems yes, for some systems and users no. I cannot answer properly, so I select the answer [Yes, for some systems]*."

Company 5: "*I need an option between yes and no*."

The quality of the questions also influenced the efficiency of the users. Some of the questions were perceived to be confusing. When being confronted with such questions, the participants looked for training content, searched the Internet for the topic, or asked the researcher for clarification.

Company 4: "*some of the questions are confusing and not clear enough for us.*"

Company 2: "*I could not understand if the question is related to servers or employees' computers.*"

The quotes here can demonstrate the users' comprehension and their ability to answer the assessment questions. Their behaviours and comments refer to the effectiveness of communication.

Action Cockpit (CYSEC Work Area). As suggested by SDT, we have observed that respect of the belonging within the organisation is important. While the CISOs answered most training and awareness questions, they communicated with their colleagues to find the answer for some of the questions. The CISO in Company 2 made a call to answer some questions. When he could not find his colleague, he highlighted the question for future consideration. Also, in Company 4, the IT specialist had a discussion to find the best answers for some questions based on their company requirements.

Recommendations (CYSEC Dashboard). As suggested by SDT, self-efficacy and relatedness had a positive impact on users' autonomous motivation. All SMBs wanted to receive feedback after finishing a coach and recommendations for next improvements.

Company 1: "*we need a summary and recommendation after each coach*."

Access to Capability Areas (CYSEC Dashboard). As suggested by SDT, choices support users' autonomy and motivation. Still, a recommended order was appreciated by the SMBs, even though the order must not be enforced. Some of the participants selected capability areas based on reflected priorities or requirements.

Company 2 on which capability do you want to select to answer? "*No preference [for the capabilities]. we can answer based on the list*."

Other participants followed different orders, and one looked for a specific capability area that was not available in the list of capability areas.

Progress Summary (CYSEC Dashboard). None of the participants was intrinsically motivated; SDT's model of introjected regulation was best explaining the participants' adoption behaviour. The participants wanted feedback about their performance, and it was important that the feedback was credible. The gamification elements of showing progress impacted the users' motivation. All the participated CISOs in this study wanted to have a simple summary which indicated their company's progress.

4.6.2 Acceptance and Usefulness of CYSEC (RQ2)

The answer to RQ2 is based on the supplementary data collected at the end of each study about the users' attitudes. Users evaluated the usefulness of the tool by responding to a five-

level Likert scale questions about the tool usefulness (low [L], rather low [RL], medium [M], rather high [RH], high [H]) and justified their evaluation. The follow-up questionnaire (Table 4.2) aimed at understanding users' attitudes about tool acceptance and usefulness. However, the short survey and small number of SMBs were not statistically significant for analysis.

Company 1: "*CYSEC is easy to use and useful*."

Company 2: "*the severity of the threats should be more visible in the training content*." Also, Company 2 stated "*CYSEC needed to be evaluated by our employees.*"

Company 3: "*I have not referred too much to the training content, so I prefer not to evaluate the second question.*" Moreover, this company explained that "*the confidentiality issues and the lack of some relevant questions in the specific topics influence our evaluation.*"

Company 4: "*although CYSEC is easy to use, the instructions in the training content are not easy to implement and practical for us*."

Company 5: "*CYSEC provides lots of training material in one place. However, the gamification elements of showing progress need to be more transparent*."

Company 6: "*the logic behind the questions needs to be improved to better support adaptation*."

CYSEC usefulness was perceived to be high by Company 1, Company 4 and Company 6, rather high by Company 2 and Company 5, and medium by Company 3. The lowest rank (medium [M]) chosen by Company 3 put a strong emphasis on a) confidentiality before and during the study and b) the lack of relevant questions in specific advanced topics. This result indicates that a tool like CYSEC that is based on self-assessment and tailored training modules was accepted as a do-it-yourself approach allowing SMBs to manage most capabilities.

Table 4.2

Questionnaire for the workshops' part 4.

Part 4 Questionnaire	**ID 1**	**ID 2**	**ID 3**	**ID 4**	**ID5**	**ID6**
Have you been aware of these threats/vulnerabilities? (Content)	RH	RH	H	RH	RH	H
How do you evaluate the quality of the information in the training content?	RH	RH	-	RH	RH	H
Does the training content send a clear message about the threat severity or your vulnerability?	RH	M	M	RH	RH	RH
Are the instructions of the training content doable?	H	RH	M	M	H	H
How easy is applying CYSEC (easy to use)?	RH	-	M	H	H	H
How useful is applying CYSEC to improve your security awareness and capability?	H	RH	M	H	RH	H

4.7 DISCUSSION

We have presented an approach for allowing SMBs to improve their cybersecurity in a DIY fashion. This result allows moving from a bespoke, consultancy-centred advisory to an automated model of communicating cybersecurity knowledge that is scalable yet individualised, hence allows to serve many SMBs with little effort. Our approach implements the self-determination theory (Ryan and Deci, 2000), which describes the motivation for achieving outcomes and the factors influencing such motivation. SDT is not the only relevant theory, however. Protection motivation theory (Menard et al., 2017) is one of the widely used theories and would offer an alternative for method and tool design, allowing us to focus on motivating the users to protect their assets and company. We have chosen to implement SDT first as, in our understanding, the improvement of cybersecurity also concerns the creation of new capabilities in the organisation: installing and configuring tools, establishing policies, and training employees beyond just protecting an asset.

In a multi-case study, we offered insights on the actual use of our designed method and tool in real-world SMB settings. Such validation goes beyond just evaluating intentions as in (Menard et al., 2017) or theoretical relationship as in the common survey-based studies. The presented work is the first step towards operationalising SDT and using it to achieve an impact on practice. As a result, we have discovered issues for future research that would not have been discovered otherwise. The findings of the study suggest that one challenge of motivating and supporting SMBs is the choice of knowledge that is being communicated. The wrong knowledge, extraneous security awareness details, or knowledge gaps reduce motivation and influence the adoption of security recommendations. Also, we discovered a potential barrier that should be addressed by future research: confidentiality. While SDT emphasises relatedness, we observed resistance to documenting and sharing security-related information both within and among companies. Alleviating confidentiality worries is crucial for improving the method's success.

Following Yin (2009), our study has the following threats to validity. **Construct validity**: are the operational measures for the concepts being studied correct? Our choice of constructs is based on SDT that we implemented in the CYSEC tool (Chapter 3) and discussed with the study participants. We described how we had implemented the constructs and offered a chain of evidence between the answers to the research questions and the data collected in the workshops. To ensure that the results reflect not only our subjective impressions, we did member checking.

Internal validity: can the cause-effect relationships in SDT be distinguished from bogus relationships? We used pattern matching and explanation-building for addressing internal validity threats. We identified relevant observations and feedback collected in the workshops and evaluated which ones spoke for a relationship, respectively against, resulting in the reported analysis. We also asked for what could have influenced the assessment, for example, whether the participants had cybersecurity training before the workshop to rule out the influence of such expertise. A longitudinal study, e.g., based on follow-up surveys, could be a

research strategy for evaluating whether and how the SMBs change their practices with extended use of the CYSEC tool.

External validity: can the study be generalised? The participating SMBs were diverse but still had similarities: all were active in the digitisation, had a CISO without deep expertise in cybersecurity but several years of experience, and did not provide any training to their employees. Since they had some knowledge in cybersecurity, they were able to answer the questions without continually referring to the training content and succeeded to implement some security controls. However, this study has not covered a) SMBs with considerable expertise in the cybersecurity b) SMBs that hardly use IT, and c) SMBs without any budget and personnel for cybersecurity. The study results may change for such SMBs because of different knowledge needs and relevance of assessment questions and improvement recommendations.

Reliability: can the study be replicated with the same results? We developed and piloted a case study protocol that we applied in the main study. The protocol ensured that the operational steps were clear, and that each SMB had enough time to use the tool without distraction. All the steps were traced in a case study database. To strengthen the chain of evidence, we presented our findings to the participating SMBs' subjects and cybersecurity experts in a formal meeting for correction (member checking).

4.8 CONCLUSION

The chapter has evaluated the actual usage of the CYSEC, a do-it-yourself (DIY) security assessment and improvement method for small and medium-sized businesses (SMBs), through an explanatory multi-case study. This study followed a deductive approach and tested constructs drawn on the Self-Determination Theory to evaluate the impact of the method on the effectiveness of cybersecurity communication to the SMBs. We applied observation and feedback questionnaires for data collection.

The results support the influence of the following features on communication effectiveness and users' motivation: expert knowledge, self-adaptating assessment question, action cockpit for connectedness in SMBs, self-adaptating recommendations, provided capability areas, and progress summary. They empower SMBs to adopt and adhere to cybersecurity. The content, including questionnaires and recommendations, need to be presented in an easy-to-understand manner to improve users' competency. The assessment questionnaires and recommendations need to adapt to each specific SMB to increase autonomy. Also, for users' acceptance and adherence, CYSEC needs to consider the company confidentiality seriously. Users are emotionally connected to the SMBs' data do not want to share their information, especially about vulnerabilities, with the tool or third parties outside the SMB. Thus, confidentiality, trust, and relatedness may influence security communication and tool acceptance positively.

CHAPTER **5**

Confidentiality Concerns for Security Information Sharing

Small and medium-sized enterprises (SME) are considered an essential part of the EU economy; however, highly vulnerable to cyberattacks. SMEs have specific characteristics which separate them from large companies and influence their adoption of good cybersecurity practices. To mitigate the SMEs' cybersecurity adoption issues and raise their awareness of cyber threats, we have designed a self-paced security assessment and capability improvement method, CYSEC. CYSEC is a security awareness and training method that utilises self-reporting questionnaires to collect companies' information about cybersecurity awareness, practices, and vulnerabilities to generate automated recommendations for counselling. However, confidentiality concerns about cybersecurity information have an impact on companies' willingness to share their information. Security information sharing decreases the risk of incidents and increases users' self-efficacy in security awareness programs. This chapter presents the results of semi-structured interviews with seven chief information security officers (CISOs) of SMEs to evaluate the impact of online consent communication on motivation for information sharing. The results were analysed in respect of the Self-Determination Theory (SDT). The findings demonstrate that online consent with multiple options for indicating a suitable level of agreement improved motivation for information sharing. This allows many SMEs to participate in security information sharing activities and supports security experts to have a better overview of common vulnerabilities.

This chapter is based on the following publication:
Shojaifar, A., & Fricker, S. A. (2020). SMEs' Confidentiality Concerns for Security Information Sharing. In *International Symposium on Human Aspects of Information Security and Assurance (HAISA)*, pp. 289-299. Springer, Cham.

5.1 INTRODUCTION

Small and medium-sized enterprises (SMEs) have a considerable diversity and form the backbone of the EU's economy (Muller et al., 2017). However, although they need to deal with a similar level of cybersecurity risk as large companies, information security is not always a priority (Kurpjuhn, 2015; Osborn, 2015). Moreover, the lack of written security policy, financial resources, and security expertise are other operational constraints and make SMEs more vulnerable (Furnell et al., 2002; Gupta and Hammond, 2005). To effectively understand information security policy and foster an information security culture, providing appropriate training and awareness tools specifically for small enterprises is necessary (Furnell et al., 2002).

Training and awareness programs are the most commonly suggested approaches in the literature for security policy compliance, and they can alleviate employees' limited knowledge of cybersecurity (Puhakainen and Siponen, 2010). Systematic training programs are a good means of facilitating continuous information security communication in organisations. Information security training should apply content and approaches that enable and motivate learners to systematic cognitive processing of information they receive in training (Puhakainen and Siponen, 2010).

CYSEC is a self-paced SME-specific training and awareness method that provides training by automating the elements of information security communication between employees and a security expert (Shojaifar et al., 2018). Since there is a resistance to changing cybersecurity behaviour and adopting security tools by employees (West, 2008), the method implements the motivational constructs—namely, the needs for autonomy, competence, and relatedness—in the self-determination theory (SDT) (Deci and Ryan, 1985; Ryan and Deci, 2000) to motivate learners to adopt advice. CYSEC provides training, recommendations, and relevant hands-on skills based on SMEs' answers to the self-assessment questions to enable them to become more self-determined.

Security information sharing is a challenge for companies, and they are reluctant to share their information and report their incidents (Geer et al., 2003; Robinson and Disley, 2010; Choo, 2011). Fear of negative publicity and competitive disadvantage, believing that the chance of a successful prosecution is not high, believing that the cyber incident was not severe enough to be reported, and a lack of motivation and trust are some of the major hindrances to information sharing activities (Geer et al., 2003; Choo, 2011). However, security information sharing is a significant measure to reduce the risks of similar incidents and develop a better understanding of the risks facing a community (Geer et al., 2003; Bedrijfsrevisoren et al., 2015). The European Network and Information Security Agency (ENISA) (Bedrijfsrevisoren et al., 2015) explains that the nature of cyber incidents and attacks is borderless. To support the management of threats and vulnerabilities in the community of cybersecurity, the exchange of data and cross-border cooperation is necessary (Bedrijfsrevisoren et al., 2015). Bedrijfsrevisoren et al. indicate that trust is the critical element in enhancing security information sharing. Therefore, the actual usage of CYSEC requires further investigation.

The current study aims to evaluate the impact of online consent communicating on SME's chief information security officers (CISOs) motivation for security information sharing. Taking approaches that motivate users to adopt security recommendations can support the effectiveness of cybersecurity communication (Cranor 2008). The semi-structured interview method was selected for data collection about behavioural motivation. The data was qualitatively analysed based on a proposed theoretical model by Yoon and Rolland (2012) for explaining knowledge-sharing behaviours in virtual communities. The model studies the effect of basic psychological needs in SDT (autonomy, competence, and relatedness) and two antecedents of the basic needs: familiarity and anonymity. Familiarity refers to an individual's understanding of the environment and increases the trust of other people (Gefen, 2000). Anonymity refers to the inability of others to identify an individual or for others to identify one's self (Christopherson, 2007) and may influence individuals' knowledge sharing behaviour in a virtual community (Yoon and Rolland, 2012).

Our study results indicate that SDT and two antecedents (familiarity and anonymity) account for motivation for security information-sharing behaviour, and online consent has a positive impact on CISOs' motivation. The online consent increased users' trust and provided value for SMEs to make choices and decisions about the suitable level of relatedness for sharing information.

The remainder of the chapter is organised as follows. Section 2 presents the research background, the theoretical model, and the research prototype. Section 3 describes the design of our study. Section 4 presents the analysis approach and the answer to the research question. Section 5 discusses the significance of the results and the threats to validity. Section 6 summarises and concludes.

5.2 Research Background

Security information sharing has been identified to increase end-users' self-efficacy in security awareness programs (Rhee et al., 2009; Robinson and Disley, 2010). Security information sharing means *"the exchange of network and information security-related information such as risks, vulnerabilities, threats, internal security issues, and good practice"* (Bedrijfsrevisoren et al., 2015). Security information should be shared to understand the risks facing the community and any related significant information infrastructure and reduce the risk of incidents.

Confidentiality concerns and the lack of incentives prevent companies to share security information (Geer et al., 2003; Robinson and Disley, 2010). Geer et al. (2003) state *"individual companies might have some rudimentary understanding of their own information security health, but we have no aggregate basis for public policy because organisations do not share their data."* The companies' confidentiality concerns include worries about reputation, losing customers, fears of misuse of the information, and strong emotional relatedness to the organisational data. These concerns exist even if security information is anonymised.

Trust influences a user's willingness to share knowledge (Chang and Chuang, 2011; Yoon and Rolland, 2012) and security information (Bedrijfsrevisoren et al., 2015). Hosmer (1995)

defines trust as *"the expectation by one person, group, or firm of ethically justifiable behaviour on the part of the other person, group, or firm in a joint endeavour or economic exchange."* Some arrangements could mitigate confidentiality concerns relevant to trust issues. The arrangements include to (1) give control of information to the company which shared it, (2) agree about how to use and protect shared information, (3) preserve data anonymity, and (4) develop standard terms for communicating information (Robinson and Disley, 2010). Deci et al. (1989) explain that also autonomy support, including the offering of choice and relevant information, impacts trust.

The Self-Determination Theory (SDT) has been proposed as a theoretical framework to study humans' motivational dynamics and consequent behaviours (Deci et al., 1989; Ryan and Deci, 2000; Deci and Ryan, 1985). People have different levels and orientations of motivation. Self-determination in SDT is defined as: *"the capacity to choose and to have those choices, rather than reinforcement contingencies, drives, or any other forces or pressures, to be the determinants of one's actions. But self-determination is more than capacity. It is also a need."* Deci and Ryan (1985) have hypothesised a basic, innate aptitude to be self-determining that leads humans and organisations to engage in desirable behaviours.

SDT assumes that the satisfaction of humans' basic psychological needs – autonomy, competence, and relatedness – leads to self-motivation and positive outcomes (Vallerand, 1997). Autonomy refers to a desire to engage in activities with a choice of freedom. Competence implies that individuals have a desire to interact effectively with the environment for producing desired outcomes and preventing undesired events. Relatedness reflects a sense of belongingness and connectedness to others or a social environment.

To explain knowledge-sharing behaviours, Yoon and Rolland (2012) extended SDT with two antecedents, familiarity and anonymity. Familiarity refers to an individual's understanding of an environment based on the prior experience and learning of the what, who, how, and when of what is happening (Gefen, 2000). Familiarity may improve perceived competence, the feeling of relatedness (Yoon and Rolland, 2012). Anonymity refers to the inability of others to identify a person or for others to identify one's self (Christopherson, 2007). It can reduce social barriers and allow group members to contribute their opinions (Yoon and Rolland, 2012). Anonymity may impact on autonomy and the feeling of relatedness. Figure 5.1 shows the complete model.

We applied Yoon and Rolland's (2012) model to study the impact of motivational factors in online consent on the information-sharing activities of CISOs. We asked SMEs to use self-assessment questionnaires to collect security information and share it with a community of security experts and other SMEs. The consent provides choices and the opportunity for CISOs to exert control over information sharing. Through the choices, CISOs can define their relatedness to the tool and the community. Each choice gives information and explains how and where the shared information will be used to increase users' familiarity with the data usage environment. The consent emphasises that the shared information will be used anonymously.

The consent form included three choices based on three levels of relatedness and agreement. (1) disagreement to share security information. (2) agreement to automated processing of

security information for recommendations of cybersecurity improvements in their company. (3) agreement to share security information for cybersecurity research. The form includes the choice of anonymity. It supports familiarity by elaborating on the usage of security information to reduce the complexity for new users and enhance the users' competence. Figure 5.2 shows the consent form.

Figure 5.1

Research model (Yoon and Rolland (2012))

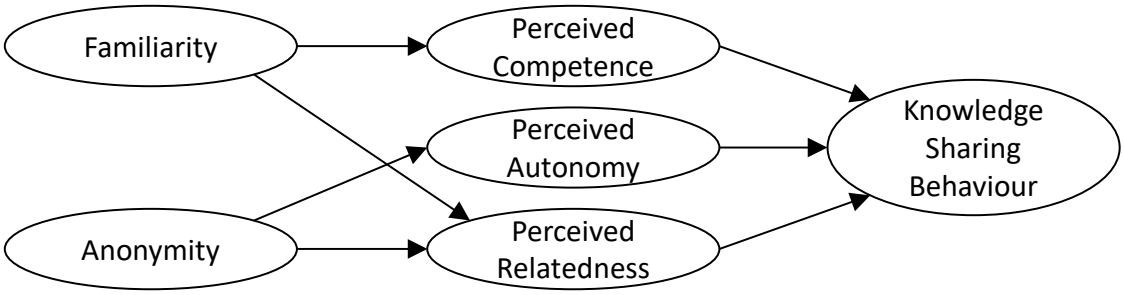
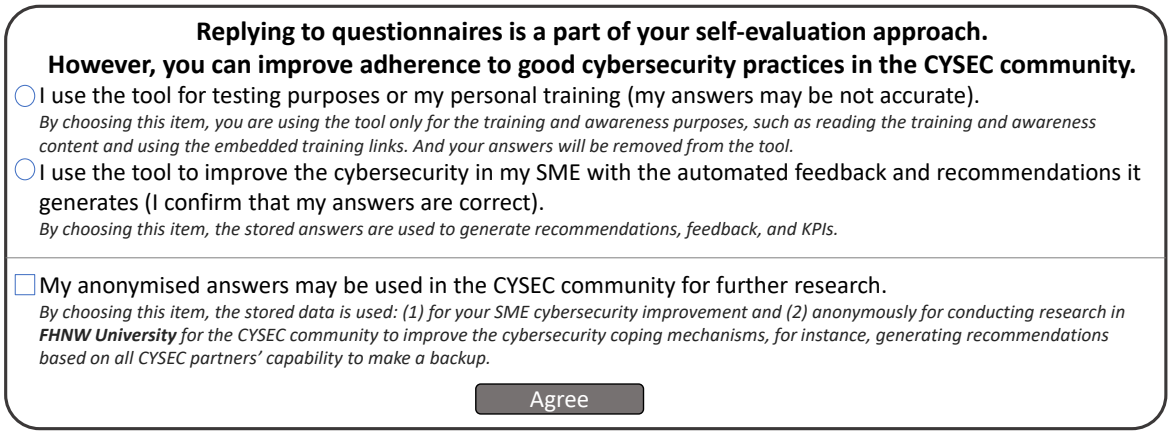


Figure 5.2

Screenshot of the Online Consent Prototype



5.3 METHOD

This study aims at finding out the impact of online consent communicating on SME's CISOs motivation for sensitive information sharing behaviour. Semi-structured interviews (Yin, 2009) were applied to conduct the empirical part of this study. The interview is one of the most frequently used methods and the most significant sources of data in empirical studies in software engineering. Interviews provide researchers with important insights into the quality and usability of artefacts since much of the knowledge that is of interest is only available in the minds of users (Runeson et al., 2012). The same method (interview with CISOs, and key informants who are Network and Information Security experts) has already been used in the context of cybersecurity (Beebe and Rao, 2009) and security information sharing (Robinson and Disley, 2010).

A theoretical model based on SDT (Figure 5.1) was chosen to analyse the CISOs' information-sharing motivation and whether online consent can motivate them. When we have

a developed theory as a template, the model of generalisation is the analytic generalisation (Yin, 2009). The study seeks answers to this research question: *Do the choice of anonymity and the elaboration of how shared information will be used motivate CISOs of SMEs to share security information?* Security information sharing is a necessary measure in the context of cybersecurity (Gal-Or and Chose, 2005; Bedrijfsrevisoren et al., 2015) and for SMEs (Birkás and Bourgue, 2013; Lewis et al., 2014). We are studying how motivational constructs, controlling over data through choices, online agreement, and familiarity with the usage of shared information, can impact information-sharing behaviour. Recorded interviews were analysed based on content analysis (interviewees' argumentations) and theoretical cause-effect relationships (Yin, 2009).

At first, a pilot study, including three interviews with three SMEs' CISOs (project partners), has been conducted—the pilot study allowed to identify and resolve initial problems in the interview questions and the online consent design. The selection of the subjects was based on the availability of the SMEs. There were twelve SMEs (four project partners and eight open call partners), and seven of them participated in the interviews. The participating SMEs came from five EU countries, and all were active in the IT industry. All of them implemented some security controls, including password management, basic approaches for privacy protection, using firewalls, two-factor authentication, cloud security features, and anti-virus installation. One person from each SME was interviewed. The people interviewed were chosen because they all were CISOs or senior managers, and all have been involved in cybersecurity tasks within their companies. All were college graduates and had several years of experience in security. One of the interviewed people was a cybersecurity expert and provided a more in-depth perspective on the importance of security information sharing, the necessity for an agreement, and anonymity. Table 5.1 presents the SMEs' demographics. In the European Union, companies are considered to be SMEs if they have fewer than 250 employees and an annual turnover of less than € 50 million (European Commission).

Table 5.1

SMEs' Demographics

ID	Org. size	Offices	Maturity	Structure
1	Small	2	Some controls implemented	CEO, security team, employees
2	Small	1	Some controls implemented	Professors, manager, security team, users
3	Medium	3	Some controls implemented	CEO, security team, employees
4	Small	2	Some controls implemented	CEO, security manager, employees, behavioural scientist
5	Small	2	Some controls implemented	CEO, employees
6	Small	1	Some controls implemented	CEO, employees
7	Small	2	Some controls implemented	CEO, security team, employees

Interviews were conducted face-to-face when possible. For four SMEs, a request for the online interview has been sent. All interviewees had the possibility to find a suitable time. In the online interviews, the screen of the interviewer's computer was shared, and the interviewees were able to see and read the content and had enough time to think about the answers. All the interviews were conducted without distraction. Each interview started with an explanation of the study. Then we presented each interviewee with a screenshot of the online consent and asked them about their understanding of it. All interviewees understood the idea and content. To collecting honest responses, the researcher emphasised that the collected data would be applied anonymously for academic purposes and then obtained the subjects' consent. In the end, a summary of the key findings and answers presented to the interviewees. All interviews were recorded and transcribed.

5.4 Analysis of the Interview Results

For answering the research question, we studied the impact of anonymity choice and elaboration of data use on SME CISOs' motivation for security information sharing. The interview transcripts showed that both design elements of the online consent form affected the CISOs' motivation for security information sharing. They supported relatedness, autonomy, and competence, and enhanced the CISOs' trust perception. The study participants were motivated to share security information when they perceived that they had control of the communication, and the information was securely stored.

Security Information Sharing Behaviour. Through the interviews, it became clear that the agreement form encouraged the CISOs' information sharing with the tool. ID7 emphasised that the agreement was not only useful but also legally necessary. ID3 and ID7 stated that the agreement positively affected their trust.

ID3: "*it has a positive effect on trust because it shows that you take care of the data process and make it clear*."

ID7: "*the online consent impacts on trust and shows me that there are thoughts, conditions, and efforts to provide different options and approaches for disclosure*."

ID1: "*with this agreement, I feel safer*."

Role of Autonomy Through Choice. The analysis of the study participants' arguments showed that the autonomy offered by the choice of sharing security information influenced their information-sharing intention.

ID7: "*providing options show me that these people know what they are asking for and give you options*."

All interviewees recognised the importance of security information sharing for receiving better advice; however, some of them selected the third choice (sharing information for research).

ID1: "*I may change my answer later*."

ID7: "*I need to check with my boss. Do I still have the ability to edit my selection? I can decide and let you use the answers, but until the end of the duration of the project*."

The respondents were asked whether they wanted to add a new option to the online consent, but no new option was suggested.

Role of Familiarity Through Elaboration of Security Information Use. Improving the CISOs' familiarity with how security information would be used positively affected competence and relatedness. All except ID6 wanted to have a clear description of how their information would be used.

ID6 stated: "*the text is clear and understandable, and it improves my awareness*."

ID1, ID3, ID4, and ID7 emphasised that the agreement has not provided sufficient information. When asked why,

ID1 stated: "*I do not know how my company information is stored; also, it should be stated if we can change our answer later*."

ID3: "*I assumed that after generating recommendations, the data should be destroyed*."

ID7: "*it should be clearly stated if the data will be used in the future and after the project*." ID4 also wanted to know more about the security information recipient "FHNW" indicated on the consent form. The interviewees were also asked to state if they wanted to know how the information is processed. Most interviewees stated that their organisations only wanted to have the results of the analysis, i.e., the tool's recommendations.

ID2: "*I do not care how and when my data will be used for the research. I just want to have the results.*"

ID5 and ID6 wanted to know, however, how their information would be processed.

The content of the agreement was perceived to be confusing for some of the subjects. Some of the interviewees suggested modifications to the content.

ID2: "*the second option should be rephrased: [try to answer the questionnaires to the best of your knowledge to help us give you more accurate recommendations]*." "*Options should be re-arranged: Options #2 and #3 should be separated from option #1*." "*Option #3 should be rephrased, something like [if you allow us to collect your answer, we will be able to improve the tool, provide you better analysis, and better help you in the future. (Yes or No)]?*"

ID4: "*rephrasing can clarify the message because I do not know if I select option #1, I will receive a recommendation*."

ID7: "*I think giving an option to SMEs that indicates my answer may or may not be accurate can demote the whole*."

Role of Anonymity Through Security Information Anonymisation. Anonymising the security information could influence perceived relatedness and autonomy and, in turn, encourage security information sharing. The analysis of the interviewees' arguments showed that all believed that anonymity would reduce the risks of sharing information. They felt more secure when the tool support anonymity.

ID2: "*if my data is anonymised, I don't care how my data will be used*."

ID1: "*anonymised data sharing shows that it is safe*."

ID7: "*I presume that when you put stress on anonymity in the third option, it can imply that the second option is not anonymised. I assume that even for other usages (KPI, recommendations), SMEs should not be recognisable*."

The interviewees would not share security information that would expose details about their organisation, hence would break their anonymity.

ID3: "*consent cannot change my opinion; I am not answering the textbox questions*."

ID7: "*I know that Yes/No or multi-choice questions can be used for the statistical analysis; however, any question that refers more to deterministic answers, I don't want to answer*."

5.5 Discussion

5.5.1 Security Information Sharing

Security information sharing is widely acknowledged (Geer et al., 2003; Robinson and Disley, 2010; Bedrijfsrevisoren et al., 2015); however, confidentiality worries, lack of incentives, and lack of trust lead the companies to avoid sharing information and reporting vulnerabilities (Geer et al., 2003; Robinson and Disley, 2010). To motivating companies to share their security information, attention to arrangements such as giving control of information to the company which shared information, having an agreement, and preserving data anonymity is necessary (Robinson and Disley, 2010).

In this chapter, based on a theoretical model for knowledge-sharing behaviour in virtual communities (Yoon and Rolland, 2012), we have evaluated the impact of online consent communicating on SME CISOs' motivation for information sharing. The model (Yoon and Rolland, 2012) extended the self-determination theory and included two antecedents (familiarity and anonymity) on basic psychological needs (perceived autonomy, perceived competence, and perceived relatedness). Yoon and Rolland's (2012) study indicates that perceived autonomy does not influence knowledge-sharing behaviours in virtual communities since a virtual community is a voluntary environment that is not controlled by anyone else. However, our findings show that in the context of security information sharing, users' perception of controlling over information sharing increased their motivation, and providing choices enabled users to have selective permission controls. This finding is consistent with the previous study (Robinson and Disley, 2010). Moreover, Yoon and Rolland's (2012) study shows that anonymity has a negative impact on knowledge-sharing activities since the anonymity in a virtual community can be used to attack the opinions of other people, and "*in a highly anonymous environment, individuals may think about other people's reactions to their opinion*." In our study, users emphasised that preserving anonymity is essential. Although our study is based only on qualitative findings and a small sample, we can explain the anonymity based on the perception of altruism (Chang and Chuang, 2011) and the risk of information misuse (Lewis et al., 2014).

In CYSEC, the self-assessment questionnaires are used to collect security information (including cybersecurity awareness, practices, and vulnerabilities) and share with a community

of security experts and other SMEs. The results demonstrated that online consent with the choice of anonymity and the elaboration of how shared information is used motivated CISOs of the SMEs to share their information. Also, we discovered that CISOs would not share security information that would expose details. For future research, the other legal and economic incentives (Gal-Or and Chose, 2005) should be considered, and not only CISOs opinions but also employees' viewpoints should be studied.

5.5.2 Study Limitation

This study has some limitations. One criterion influencing the sufficiency of the interviews was saturation. The saturation point is reached when no new information is gathered, or the subjects' viewpoints are repeated (Runeson et al., 2012). Due to the small sample size, we could not reliably validate saturation and implement a statistical analysis in our study. The study is based on seven interviewed persons from seven SMEs that were active in the IT industry, which limits generalisability. Further research with a larger sample and a diversity of SMEs could reveal more robust results and provide more insights into the influence of the industry type on the SME engagement in security information sharing. Second, since the study is based on the CISOs' and senior managers' viewpoints of security information sharing, our study lacks the view of SME employees. To have a wider perspective, we need the views of SME employees.

5.6 Conclusion

The chapter has evaluated the impact of online consent communicating on motivating CISOs of SMEs for security information sharing. This study followed a deductive approach and tested constructs drawn on the Self-Determination Theory (SDT) as well as two antecedents of SDT constructs (familiarity and anonymity) to evaluate the impact of the online consent on the security information sharing motivation. We applied semi-structured interviews with seven CISOs from seven SMEs for data collection. The study results indicate that online consent increased CISOs' trust and had a positive impact on security information sharing intention. The consent supports familiarity with the environment through the elaboration of security information usage. Moreover, online consent considers the role of anonymity and autonomy through security information anonymisation and the choice of sharing information.

CHAPTER 6

Empirical Study of a Self-paced Cybersecurity Tool

This chapter aims to present the evaluation of a self-paced tool, CyberSecurity Coach (CYSEC), and discuss the adoption of CYSEC for cybersecurity capability improvement in small and medium-sized enterprises (SMEs). Cybersecurity is increasingly a concern for SMEs. Previous literature has explored the role of tools for awareness-raising. However, few studies validated the effectiveness and usefulness of cybersecurity tools for SMEs in real-world practices. This study is built on a qualitative approach to investigating how CYSEC is utilised in SMEs to support awareness-raising and capability improvement. CYSEC was placed in operation in 12 SMEs. We first conducted a survey study and then nine structured interviews with chief executive officers (CEOs) and chief information security officers (CISO). The results emphasise that SMEs are heterogeneous. Thus, one cybersecurity solution may not suit all SMEs. The findings specify that the tool's adoption varied quite widely. Four factors are primary determinants influencing the adoption of CYSEC: personalisation features, CEOs' or CISOs' awareness level, CEOs' or CISOs' cybersecurity and IT knowledge and skill, and connection to cybersecurity expertise. This empirical study provides new insights into how a self-paced tool has been used in SMEs. This study advances the understanding of cybersecurity activities in SMEs by studying the adoption of CYSEC. Moreover, this study proposes significant dimensions for future research.

This chapter is based on the following publication:
Shojaifar, A., & Fricker, S. A. (2023). Design and Evaluation of a Self-paced Cybersecurity Tool. *Information & Computer Security,* 31(2), 244-262.

6.1 INTRODUCTION

Small and medium-sized enterprises (SMEs) are companies with fewer than 250 employees and an annual turnover of less than € 50 million (European Commission, 2003). SMEs play a significant role in national economic growth and prosperity (OECD, 2017). They represent 99% of all businesses in the EU (European Commission, 2019).

Many SMEs are unaware of cybersecurity's importance, and the lack of adoption of solutions is a real risk (European Digital SME, 2020). Studies argue that the lack of expertise and resources prevents SMEs from adopting cybersecurity solutions (Kabanda et al., 2018; European Digital SME, 2020; Aigbefo et al., 2022). However, like larger organisations, the risk of malicious threats and cyberattacks for SMEs has become significant (Kurpjuhn, 2015; Alahmari and Duncan, 2020). Toni Allen from the British Standards Institute explains that "SMEs have not historically been the target of cybercrime, but in 2015 something drastically changed." (Smith, 2016). The recent reports confirm the increase in reported cyberattacks against SMEs due to the absence of defences (Ponemon Institute, 2019; Lloyd, 2020).

Abundant studies have confirmed the influence of awareness training programs on cybersecurity behaviour (Puhakainen and Siponen, 2010; Bulgurcu et al., 2010; ENISA, 2017; Haeussinger and Kranz, 2017) and for SMEs (Gundu and Flowerday, 2013; Kabanda et al., 2018; Wong et al., 2022). Such training is valuable for developing a cybersecurity culture in SMEs (Dojkovski et al., 2010).

Self-assessment tools (Ponsard et al., 2019) are solutions that can facilitate awareness-raising and capability improvement in SMEs. ENISA (2020) highlights a need for the right tools to help SMEs be protected against cyber threats before they happen. However, few studies rigorously evaluated the application of cybersecurity tools and their impacts on appropriate behaviour in SMEs.

This chapter focuses on the evaluation of our method and tool (CYSEC). CYSEC automates elements of a counselling dialogue between cybersecurity experts and CEOs or Chief information security officers (CISO) in SMEs. We provide a synthesised view of the factors emphasised by CEOs or CISOs after using CYSEC in real environments for two months. Security research should focus on actual behaviour as the practical phenomenon of interest rather than intention (Crossler et al., 2014). The findings clarify how the tool met the needs and expectations and why it was successful or unsuccessful in awareness-raising and capability improvement.

The study purpose was approached by conducting structured interviews with CEOs or CISOs. We selected CEOs or CISOs because many studies have demonstrated the vital role of management in achieving effective cybersecurity in SMEs (Lee and Larsen, 2009; Njenga and Jordaan, 2016; Barlette and Jaouen, 2019). For instance, Lee and Larsen (2009) showed that SME executives could adequately assess their companies' collective capabilities to adopt cybersecurity solutions.

The qualitative inductive thematic analysis demonstrates that SMEs are very heterogeneous with diverse characteristics, business needs, and capabilities. Therefore, one cybersecurity

approach may not suit all SMEs. This finding is aligned with prior works (Wilson and Hash, 2003; Garg et al., 2012; Tsohou et al., 2012; Caldwell, 2016; Renaud, 2016;). However, very few studies have considered the importance of diversity in cybersecurity for SMEs (Lee and Larsen, 2009; European Digital SME, 2020).

The adoption of CYSEC varied quite widely. We found four factors that affected the tool's adoption: a) the tool's personalisation features; b) CEOs' or CISOs' cybersecurity awareness level; c) CEOs' or CISOs' cybersecurity and IT knowledge and skill level; and d) connection to cybersecurity expertise. Considering these factors can assist in designing effective tools for SMEs. We argue that the findings can offer a significant contribution to the field and potential directions for future research. The evaluation of the effectiveness of cybersecurity tools for SMEs has not received adequate attention. Also, prior research specifies a literature gap in the evaluation of awareness training programs (Muronga et al., 2019).

The remainder of this study is organised as follows. Section 2 presents an introduction to cybersecurity awareness and the CYSEC method; section 3 outlines the applied research methods; section 4 explains our findings; in section 5, the findings are discussed, and future research avenues are proposed. Finally, section 6 summarises and concludes.

6.2 CYBERSECURITY AWARENESS

According to the NIST (Wilson and Hash, 2003):

> "*Awareness is not training. The purpose of awareness presentations is simply to focus attention on security. Awareness presentations are intended to allow individuals to recognise IT security concerns and respond accordingly. In awareness activities, the learner is a recipient of information, whereas the learner in a training environment has a more active role. Awareness relies on reaching broad audiences with attractive packaging techniques*."

Given this definition, raising awareness of cyber threats and changing behaviour for best practices are the aims of implementing awareness training programs (Bada et al., 2015; Muronga et al., 2019). The definition also highlights the importance of communication techniques for reaching broad audiences (Beyer et al., 2015; ENISA, 2017).

A cybersecurity awareness program (called user awareness training) is a building block of a mature security program (Gardner and Thomas, 2014). It affects employees' motivation for compliance behaviour (Bulgurcu et al., 2010) and organisations' security culture (Furnell and Clarke, 2005). Bada et al. (2015) argue that the primary purpose of awareness programs is to persuade individuals to adopt the offered knowledge.

Existing literature identifies various antecedents that impact employee cybersecurity awareness. Haeussinger and Kranz (2017) identify three classes of antecedents: institutional, individual, and socio-environmental. Further, they indicate that future research should investigate the awareness levels of different target groups. Lebek et al. (2014) identify many behavioural constructs, mainly from social psychology and criminology. Further, they indicate that future studies must focus on additional factors instead of measuring core construct relationships.

Studies propose various methods and factors for delivering and communicating cybersecurity awareness content. Haeussinger and Kranz (2017) identify methods such as e-learning, online game-based training, discussion, checklist, e-tutorial, media richness, and phishing mail exercises. Wilson and Hash (2003) indicate that web-based communication is the most popular technique for distributed environments and may allow better individual interaction. They emphasise the importance of ease of use, scalability, accountability, and a broad base of industry support as the features of an effective communication method. Gundu and Flowerday (2013) argue that implementing online learning methods significantly reduces the costs of running awareness campaigns. Bada et al. (2015) explain that the material of an effective awareness training program is interesting, engaging, targeted, current, and simple enough to be followed by recipients.

Prior research has highlighted discrepancies between SMEs and large organisations. SMEs engage in fewer deterrent efforts than larger organisations (Kankanhalli et al., 2003). In SMEs, constraints of low formalisation and the strong influence of individual leadership characteristics influence IT security decisions (Heidt et al., 2019). Therefore, it may be unrealistic for SMEs to replicate and implement solutions studied for large organisations (Aigbefo et al., 2022).

ENISA (2020) emphasises the need for the right tools to help SMEs be protected against cyber threats before they happen. A range of tools has been developed to support SMEs. Brunner et al. (2018) introduce ADAMANT as an SME-friendly tool that supports continuous risk-driven and context-aware information security management. Furnell et al. (2002) describe a tool that suits small organisations and enables employees to acquire the desired training in specific cybersecurity areas at their own pace. Ponsard et al. (2019) present several cybersecurity tools and self-assessment questionnaires for SMEs. For instance, the Cyber Essentials framework in the UK (HM Government UK, 2014) provides basic countermeasures, advice, and self-assessment tool (UK Gov., 2018) to protect SMEs from cyberattacks.

Although Ponsard et al.'s (2019) study helps to know more about SME-specific tools and methods, the evidence of the evaluation and the use and usefulness of the solutions are missing. Addressing the lack of understanding about cybersecurity adoption in SMEs is important since the literature demonstrates a lack of adoption of protective technologies in SMEs (Lewis et al., 2014; Renaud and Weir, 2016; European Digital SME, 2020). Evaluating a designed IS artefact and publishing the outcomes are essential (Hevner et al., 2004; Peffers et al., 2008). Qualitative assessment is needed to understand the interaction of people, organisations, and technology for theory development or problem-solving (Hevner et al., 2004; Klein and Meyers, 1999). Moreover, qualitative studies may add value to the training and awareness research field due to the dominance of quantitative work (Lebek et al., 2014). Hence, this study investigates the qualitative evaluation of our tool to see why and why not it was successful in SMEs. The remainder of this section describes our method and tool.

6.2.1 CYSEC tool for SME cybersecurity awareness and capability improvement

This section outlines our self-paced method and tool, CyberSecurity Coach (CYSEC). CYSEC is designed to allow users easy access to cybersecurity topics and provides Do It

Yourself (DIY) step-by-step instructions for cybersecurity implementation and continuous progress.

CYSEC has two main interfaces (Capability Improvement Dashboard and Capability Work Area), each with several components.

The Capability Improvement Dashboard shows an overview of the available capability areas, recommendations, and the summary section. Capability areas are thematic blocks consisting of stepwise questions and training content. We introduced a concept named coach. It is a capability area with relevant recommendations and gamification elements. CYSEC has six capability areas (coaches): Company, Patch Management, Access Control and Audit, Malware Scans, User Training, and Backup. The CYSEC design supports adding more capability areas according to the SME's needs. CYSEC offers memory allowing the users to continue working with capability areas or changing their answers to the questions at any time. Recommendations are generated according to the users' answers to the self-assessment questionnaires. They specify the next steps by offering a tool for installation, a cybersecurity behaviour, or a self-assessment question. Finally, the summary section demonstrates the user's progress status and latest achievements. According to the progress in the capability areas, gamification elements (e.g., badges and scores) will be updated. Figure 6.1 (a, b, c) illustrates screenshots of the dashboard features.

The Capability Work Area encompasses self-assessment questionnaires (Ozkan and Spruit, 2018; Parsons et al., 2017), embedded training content, and a summary page. The questionnaires and training content together provide users with the ability to learn about cybersecurity topics and assist them in implementing controls in a DIY manner. Each question introduces a new threat, vulnerability, or concept and provides several choices of answers presenting the implementation degree. The order of the questions is from an easy to advanced capability pattern, and users' responses impact the adaptation of questions. Training content offers users various materials, including videos, links to training resources or tools and relevant advice. Training content was developed based on the available scientific and technical resources (e.g., Symantec, ENISA, and Ponemon's reports). Finally, at the end of each capability area, a summary page is shown, and users have the option to start a new capability area or get back to the dashboard. The screenshots (d, e, f) in Figure 6.1 illustrate the capability work area.

For a new user, according to Figure 6.1, first (a) the recommendation to the Company capability area is presented. The user's answers to the company questionnaire impact the adaptation of the questions in the other capability areas. By answering the company capability questions, (b) new recommendations and (c) new capability areas will be active to the user. Information in the dashboard helps the user check the progress and objectives, interact with the employees, and decide the next step based on lessons learned and recommendations.

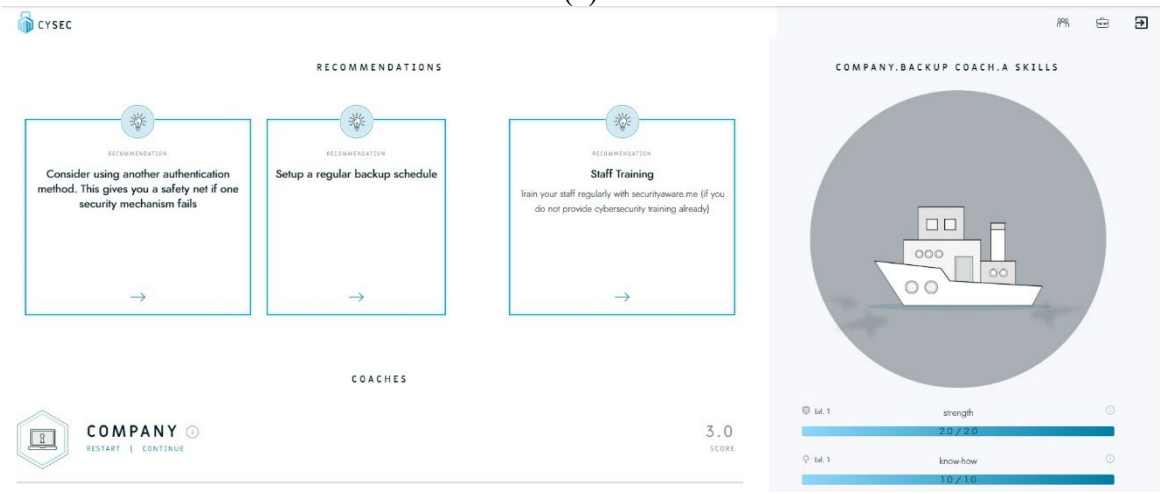
CYSEC bridges the gap between experts and users and supports a DIY capability improvement journey by managing and automating elements of a counselling dialogue between cybersecurity experts and SMEs' CEOs or CISOs. Self-assessment questionnaires have been used in several SMEs' cybersecurity improvement processes (Ponsard et al., 2019); however,

the CYSEC method encourages cybersecurity practices in SMEs by providing the ability to learn and implement controls in a stepwise approach.

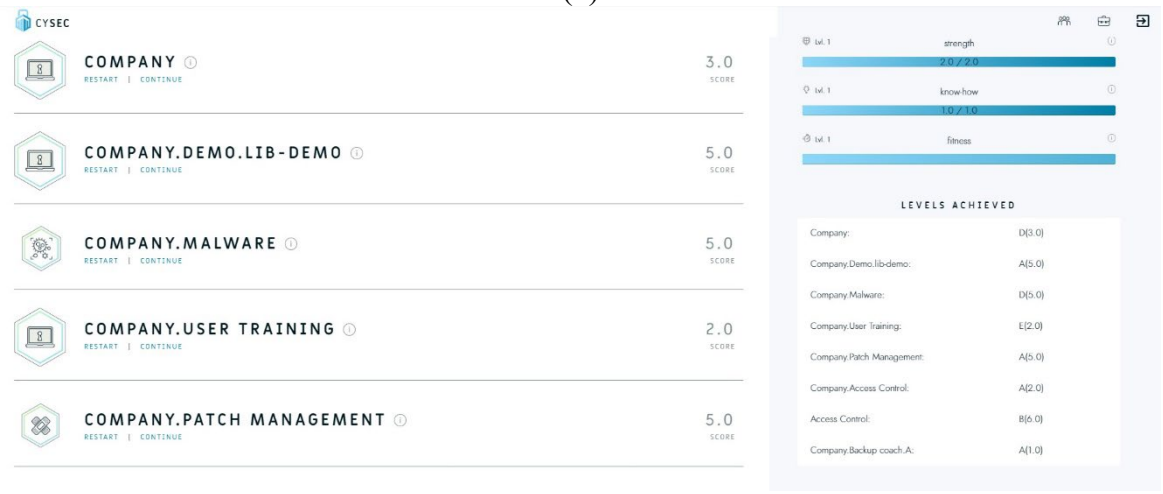
Figure 6.1

CYSEC tool screenshots

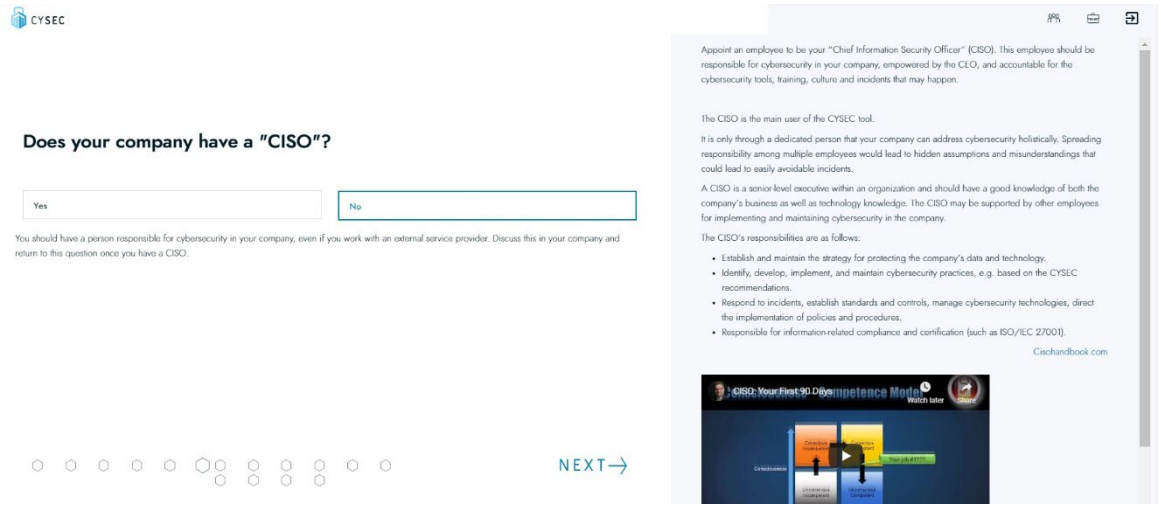
(a)



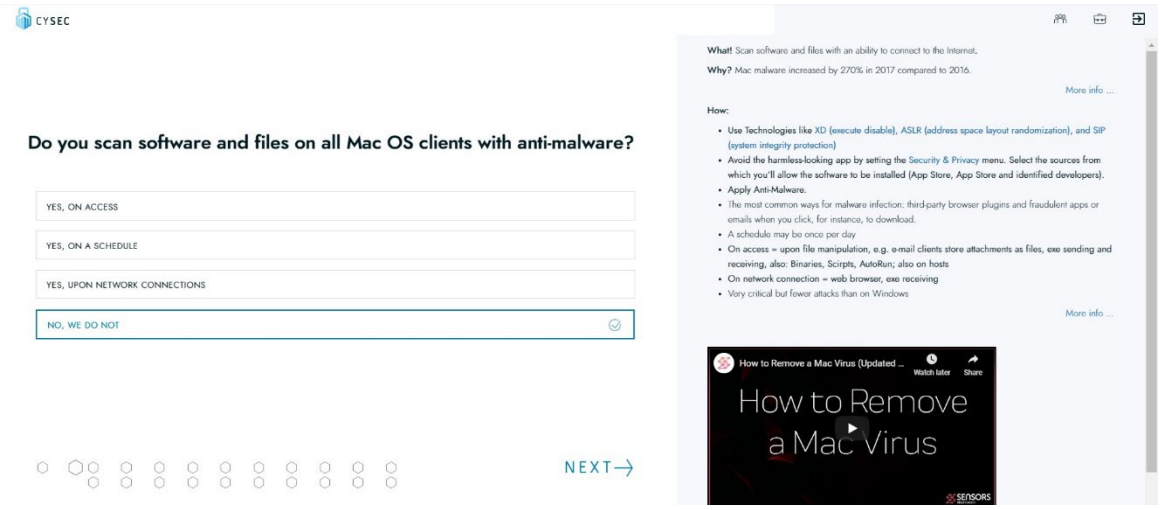
(b)



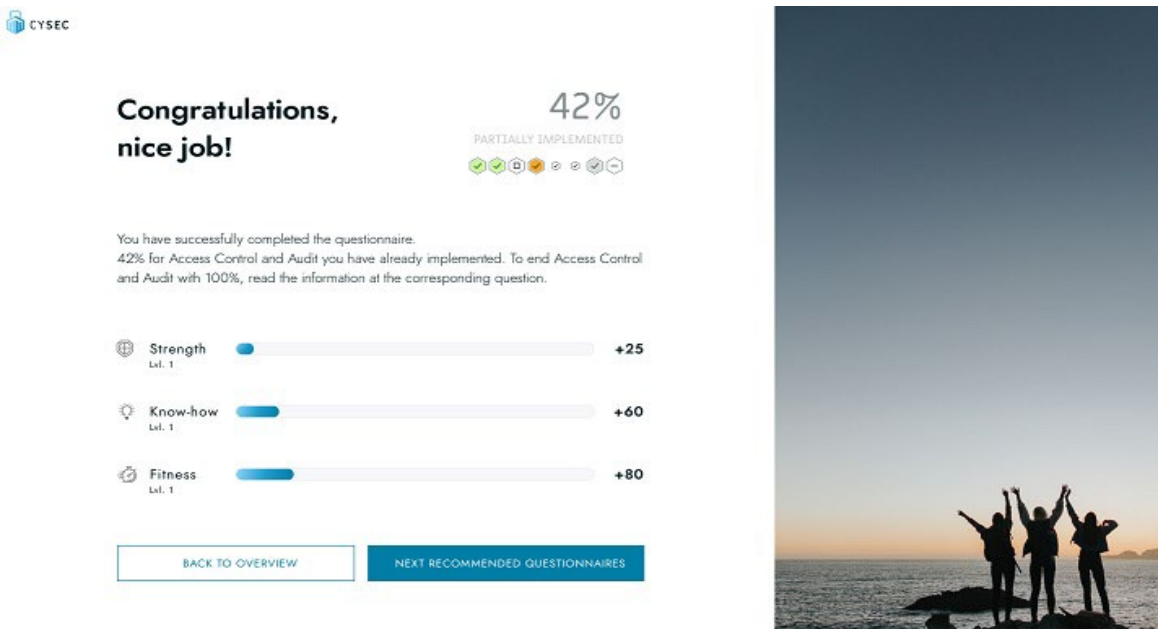
(c)


CYSEC
Does your company have a "CISO"?
Yes
No
You should have a person responsible for cybersecurity in your company, even if you work with an external service provider. Discuss this in your company and return to this question once you have a CISO.
NEXT
Appoint an employee to be your "Chief Information Security Officer" (CISO). This employee should be responsible for cybersecurity in your company, empowered by the CEO, and accountable for the cybersecurity tools, training, culture and incidents that may happen.
The CISO is the main user of the CYSEC tool.
It is only through a dedicated person that your company can address cybersecurity holistically. Spreading responsibility among multiple employees would lead to hidden assumptions and misunderstandings that could lead to easily avoidable incidents.
A CISO is a senior-level executive within an organization and should have a good knowledge of both the company's business as well as technology knowledge. The CISO may be supported by other employees for implementing and maintaining cybersecurity in the company.
The CISO's responsibilities are as follows:
Establish and maintain the strategy for protecting the company's data and technology.
Identify, develop, implement, and maintain cybersecurity practices, e.g. based on the CYSEC recommendations.
Respond to incidents, establish standards and controls, manage cybersecurity technologies, direct the implementation of policies and procedures.
Responsible for information-related compliance and certification (such as ISO/IEC 27001).
Cisohandbook.com
CISO: Your First 90 Days
Watch later
Share

(d)


CYSEC
Do you scan software and files on all Mac OS clients with anti-malware?
YES, ON ACCESS
YES, ON A SCHEDULE
YES, UPON NETWORK CONNECTIONS
NO, WE DO NOT
NEXT
What! Scan software and files with an ability to connect to the Internet.
Why? Mac malware increased by 270% in 2017 compared to 2016.
More info ...
How:
Use Technologies like XD (execute disable), ASLR (address space layout randomization), and SIP (system integrity protection)
Avoid the harmless-looking app by setting the Security & Privacy menu. Select the sources from which you'll allow the software to be installed (App Store, App Store and identified developers).
Apply Anti-Malware.
The most common ways for malware infection: third-party browser plugins and fraudulent apps or emails when you click, for instance, to download.
A schedule may be once per day
On access = upon file manipulation, e.g. e-mail clients store attachments as files, exe sending and receiving, also: Binaries, Scripts, AutoRun; also on hosts
On network connection = web browser, exe receiving
Very critical but fewer attacks than on Windows
More info ...
How to Remove a Mac Virus (Updated ...
Watch later
Share
How to Remove a Mac Virus
SENSORS

(e)


CYSEC
Congratulations, nice job!
42%
PARTIALLY IMPLEMENTED
You have successfully completed the questionnaire.
42% for Access Control and Audit you have already implemented. To end Access Control and Audit with 100%, read the information at the corresponding question.
Strength
Lvl. 1
+25
Know-how
Lvl. 1
+60
Fitness
Lvl. 1
+80
BACK TO OVERVIEW
NEXT RECOMMENDED QUESTIONNAIRES

(f)

6.3 RESEARCH METHOD

We intend to study and discuss the influence of CYSEC on awareness and capability improvement in SMEs from the perspective of CISOs and CEOs. We adopted a qualitative approach to acquire an in-depth and contextualised understanding of how the users in different SMEs apply the tool. A qualitative study is a more helpful alternative to determine richer insights with a small number of subjects (Lee, 2003). The findings helped us identify four factors that need to be considered in designing a viable self-paced tool for SMEs.

Before collecting data, a cloud version of the tool has been available for two months to 12 participating SMEs in this study. During this period, all the subjects used the tool in their companies and were in contact with the researcher about the tool's features, technical problems, and general questions. The study sample size is relatively small; thus, hard statistical indexes are not of particular importance in the study (Jarvinen, 2001; Tryfonas et al., 2001). Accordingly, interpretive research and empirical evaluation are deemed to be appropriate (Klein and Myers, 1999; Tryfonas et al., 2001).

We aim to answer the main question[4]: *Why did CYSEC either result in the intended use and usefulness of the tool for cybersecurity competence improvement or fail?* One problem with cybersecurity is the users' resistance to accepting tools (West, 2008). Identifying the vital factors that may impact the effectiveness of awareness improvement solutions is essential to support sustained engagement in practices (Bada et al., 2015). The research question wants to surface those influential factors that affect the adoption of CYSEC in SMEs.

The research applied a two-phase data collection process: first, a survey and then structured interviews. In the first phase, eight SMEs were involved, and all of them were small companies. A questionnaire about the features and content of the tools was sent to the subjects, e.g. "Which parts of the training content (video, text, integrated training links) are practical?" During the analysis of the survey results, it became evident that due to data deficiencies, we would not be able to carefully examine some issues. Findings from the first phase of the study helped to develop a matured interview instrument for the second phase.

In the second phase, nine structured interviews were conducted. The sample size indicated the need for data of high quality and validity (Walsham, 1995; Tryfonas et al., 2001). Therefore, personal contact with interviewees was performed to enhance the source's validity, and the second author also joined the first four interview meetings as an observer. After the interviews, the first and second authors checked the quality and validity of the data and planned for the next interviews. The interview questions were phrased based on the information security awareness topics (Bulgurcu et al., 2010). We avoided asking questions leading the interviewees' positive or negative opinions about the tool. We developed a structured instrument to guide the interviews and collect rich data. The purpose of this phase of the data collection was threefold: firstly, understanding what the subjects knew before and after using the tool about security threats, vulnerabilities, responsibilities, and countermeasures; secondly, identifying the impact of the tool on actual practices in each company; and thirdly, determining

[4] Modified in Chapter 1

the perceived benefit of the tool, what countermeasures are either relevant or irrelevant to the companies and what security controls are required but not included in the tool.

Interview is one of the most frequently used methods and the most significant sources of data in empirical studies in software engineering (Runeson et al., 2012). The same qualitative method has already been used in the context of cybersecurity (Albrechtsen and Hovden, 2009; Pham et al., 2017; Heidt et al., 2019).

The study sample consisted of different kinds of SMEs, differentiating in size, business interests, cybersecurity maturity, implemented measures, and information security policy availability. Two of them were cybersecurity providers, and three had clear written security policies. The participating SMEs came from six EU countries, and all except two SMEs were active in the IT industry. In terms of the people interviewed, in each SME, we interviewed one person. We had a purposeful sampling [Stratified, Typical case, Critical case (Miles and Huberman, 1994)], and all the interviewees were CISOs or senior managers with cybersecurity responsibilities, and all have been involved in security tasks within their companies. Also, all of them had IT skills to use the tool. Prior research emphasised the significant roles of top management in commitment to effective cybersecurity in SMEs (Kankanhalli et al., 2003; Lee and Larsen, 2009; Barlette and Jaouen, 2019). Two of the interviewed people were cybersecurity experts. One interviewee had limited basic knowledge of cybersecurity. Therefore, we had a diversity of interviewees with different cybersecurity knowledge levels to compare the subjects and develop a holistic view. Details about the interviewees and SMEs are given in Table 6.1.

The interviews lasted for about 40 minutes to one hour. Each interview started with explaining the study objectives and presentation of a table including the defined threats, vulnerabilities, and security controls introduced in CYSEC. The aim was to give an overview of the awareness topics and assist the interviewee's memories to provide rich data. Each interviewee was assigned a pseudonym. In order to collect honest responses and allay the concerns of the interviewees about the confidential information, the researcher emphasised that the collected data would be applied anonymously for academic purposes. Then the subjects' consent was obtained. In the end, a summary of the key findings and answers were presented to the interviewees.

All interviews were recorded and transcribed, and like the previous studies (Stobert and Biddle, 2014; Kabanda et al., 2018), we performed an inductive thematic analysis. Thematic analysis is a method for identifying, analysing, and reporting themes or patterns within collected data (Patton, 1990; Braun and Clarke, 2006).

The qualitative analysis process started by repeatedly reading the transcripts to find the patterns throughout the data. The first step outlined the initial codes, selected quotes, and their meaning. The second step was based on the existing codes and iterating on them. This step involved finding the relationships between the codes, expanding, modifying, and clustering the identified code based on their evident similarities. Finally, the last step identified the significant concepts and themes connected to several specific quotations to confirm the validity and show the themes' ideas. In this phase, an internal review was done, and codes, identified themes, and

selected quotes were presented to the second author to validate the themes' accuracy and reliability. For further verification, the researcher presented the themes in a workshop with experts.

Table 6.1

Profile of the interviewees' organisations

ID	Size	Offices	SME structure	Service	Interviewee cybersecurity experience	Interviewee role
ID1	Small	1	Professors, manager, Security team, users (university-hosted start-up)	Education and training	Non-expert	CEO
ID2	Medium	3	CEO, security team, employees	IoT, Network, Sensor	CISO	Security support staff
ID3	Medium	3	CEO, security team, employees	Online Voting	CISO	Security support staff
ID4	Small	2	CEO, security team, employees	Energy value-added services	CISO	Security support staff
ID5	Small	3	CEO, project managers, security team, employees	IT and security solution provider	Expert	Technical Manager
ID6	Small	2	CEO, chief medical officer, legal counsellor, head engineer, support engineers, community manager, behavioural scientist, designer	Health care	Non-expert	CEO
ID7	Small	1	Horizontal structure	IT service provider	Non-expert	CEO
ID8	Small	1	CEO, employees	IT service provider	Expert	CEO
ID9	Small	1	CEO, employees	Security consulting	Expert	Security Consultant

6.4 RESEARCH FINDINGS

This section presents the results of the inductive thematic analysis and answers the research question. The emergent themes indicate how CYSEC has been used in SMEs and what factors influenced its usefulness. The concepts used in the study were derived from the interviewees' comments and reasoning.

SMEs demonstrated a wide diversity of capabilities and needs that affected the adoption or lack of adoption of CYSEC. Our findings indicated that the following factors must be considered to answer the research question: the tool's personalisation features; CEOs' or CISOs' cybersecurity awareness level; CEOs' or CISOs' cybersecurity and IT knowledge and

skill; and connection to cybersecurity expertise. CYSEC partially supported personalisation, cybersecurity awareness, knowledge and skill improvement, and connection to cybersecurity expertise. CYSEC has not been fully successful. The tool would need to be completed with the missing critical factors to be successful.

6.4.1 Personalisation

The primary emergent theme was personalisation. The SMEs had heterogeneous infrastructure and cybersecurity needs. Personalisation of the CYSEC capabilities, awareness training material, and features tends to affect the tool and recommendations' adoption. All the interviewees with various levels of expertise valued personalisation. ID1 commented:

The questions [in the self-assessment questionnaires] are not arranged properly. Why do we need to answer questions about scanning all servers while we do not have windows servers? […] we need access to patches and personalised security products.

This was further supported by the other interviewees:

ID3: increase the usefulness of the tool: provide a follow-up checklist for all the security controls we can apply.

ID4: prepare personalised coaches for our company. We have not implemented all the introduced controls because of our infrastructure.

ID5: I do not see any irrelevant control in general; I think some of them do not apply to our company. They are valid, but we are a small company and do not have, for example, a data protection officer.

ID8: divide the tool into two personalised sub-tools, useful for expert and non-expert users.

Further, several interviewees requested new coaches according to their security needs. For instance, ID4 indicated:

Some of our employees are working remotely after the pandemic [COVID-19]. We need cybersecurity coaches about remote working and the usage of VPNs.

ID6: if CYSEC extended with a coach that focuses on managing the service delivery of third-party cloud providers, then it would be more useful for our company.

The results show that the diversity of CYSEC training material, including text, videos, and links for further studies, supported personalisation. While some interviewees explained that the text was more appreciative as an easy and fast way to understand the first idea of the content, others indicated that videos were the most practical elements to convey the content better and were more emphatic and pleasant.

Therefore, the tool must accommodate diverse business interests, vulnerabilities, and needs. General cybersecurity content per se cannot properly work for SMEs. Providing targeted mitigations is likely to improve the adoption of CYSEC.

6.4.2 CEOs or CISOs cybersecurity awareness level

The findings reveal that the interviewees have different perceptions of cybersecurity, severity, and vulnerability of threats. Therefore, they have different attitudes and approaches

to cybersecurity practices. The study participants from ID5, ID8, and ID9 indicated that they have a cybersecurity policy in place and put a high value on security practices. Also, cybersecurity is part of their routines. They have a comprehensive view of controls. They know cybersecurity will become obsolete, so they have a long-term attitude to review and update their training for employees. For example, ID5 noted:

It [CYSEC] gives quick training and a view of all threats to the new members; we let them know and do the CYSEC assessment. We see their results, and we update them.

ID8 revealed that they review their policy two or three times a year in an internal meeting to change, for instance, the rules to integrate the new cybersecurity updates to their existing policy.

We used your tool to review our policy. I do not think there was any impact on our awareness. We used the tool as a list to review cybersecurity topics. To be most useful, consider the completeness of the tool.

For some study participants, cybersecurity is still in its infancy, and they looked at awareness topics as secondary issues. ID6 noted:

We, as an SME have many things to do. We need to have reminders and capabilities but in a non-distracting way.

Some SMEs have a policy in some focus areas partially written, and some do not have any policy in place. ID1, ID2, and ID6 reported that after using CYSEC, they plan to participate in training courses, implement some security controls, or prepare for regular backup or patch management. ID1 noted:

After CYSEC, we organised small meetings to discuss the problems, and now there is a person in charge of managing it.

ID1, ID6, and ID7 asked for clear goals, an action plan to achieve the goals in specific focus areas and hands-on solutions. ID7 commented:

The tool should give the most important prioritised suggestions and an action plan for the next six months.

Moreover, interviewee ID1 revealed that they had a wrong perception of their cybersecurity status, and CYSEC encouraged them to ponder their vulnerabilities. ID1 noted:

[before CYSEC] we thought we were secure, and now we know we are still not in a secure situation. Now we realise the risk of ignoring the implementation of security controls.

Therefore, considering target groups' awareness levels and attitudes and providing pertinent content for each group is inclined to promote the adoption of CYSEC.

6.4.3 CEOs' / CISOs' cybersecurity and IT knowledge and skill level

Study participants had various levels of competence in IT and cybersecurity and therefore indicated different knowledge and skill needs. ID3 suggested that CYSEC should prepare training for more advanced cybersecurity controls (e.g., trusted boot, hardware encryption).

ID5: They [CYSEC content] are basic awareness and training for our company. We knew all of them. It [CYSEC] can be useful for the new members of the company. Having a list of the latest threats and security vulnerabilities, the most recent things, keeping us updated to be interesting for our company, for instance: to know a new list of password leaks or a list of compromised websites to be sure about our passwords, to change our password, to have it as soon as it is going to be published, and some examples of attacks.

While the new employees of the companies can use CYSEC, this type of SME needs updated and newest cybersecurity material.

Conversely, study participants ID1, ID2, ID4, ID6, and ID7 demonstrated a lack of knowledge and skill in cybersecurity. They mostly focused on the introduced topics in CYSEC instead of asking for the latest threats. The interviewees wanted to have a repository of current knowledge and practical solutions. While CYSEC impacted awareness-raising, it did not adequately supply these SMEs with practical cybersecurity skills. For example, ID1 noted:

It [CYSEC] has a high impact, and we have realised security threats and controls. Now we know the risk of ignoring the implementation of security controls. I understand the threats and efforts to deal with the threats. However, we are at zero. We need to know how to solve the problems and not only present the problems. There should be a list of products that we can use.

Furthermore, the researcher found that those with a low level of computer literacy or non-ICT individuals had a significant problem applying CYSEC and realising the value of cybersecurity practices.

CYSEC helped us to realise how cybersecurity competence might differ among SMEs. Therefore, identifying required knowledge and skill sets congruent with SME's competence supports the meaningfulness of the solution and is inclined to promote the adoption of CYSEC.

6.4.4 Connection to cybersecurity expertise

The findings reveal that SMEs may have various connections to exchange knowledge or manage cybersecurity activities. Their connections influenced the way they utilised CYSEC and recommendations. For example, while ID8 have cybersecurity capability, they are connected to other experts in their community. ID8 noted:

We are working in our association, and we learn from other companies' experiences. We can suggest [CYSEC recommendations] to other companies in our association. Also, our servers are protected by our providers.

ID2, ID3, and ID4 have CISOs to manage cybersecurity activities and support employee-related tasks. ID2 noted:

It [CYSEC] provides quick wins, checking how many of the controls have been implemented that can be shown to upper management.

Furthermore, ID6 revealed that the company had delegated some cybersecurity activities to third parties. Therefore, many of the recommendations were immaterial to them.

ID6: It [the training content] was not applicable to us, the hardware that we use for the services is managed by third parties, and they also set up the network. We need a coach about cloud services for training the employees.

Conversely, ID1 and ID7 had no connection to third parties, associations, or internal and external cybersecurity experts. They needed various sources of knowledge, hands-on skills, and connections to relevant associations and experts. ID1 noted:

We do not have a security team department. If you do not have a CISO, CYSEC should offer training classes and certification. We need delivery of services.

The results reveal that supporting connections to experts, associations, and computer emergency response teams (CERT) to receive updates, gain and transfer knowledge is significant across all types of SMEs and influences CYSEC use and usefulness.

The main factors of the analysis are summarised in Table 6.2.

Table 6.2

Analysis findings

Analysis themes	**Findings**	**CYSEC degree of implementation**
The tool's personalised features	• Various types of awareness training material (video, text, further study links) supported users' needs. • The self-assessment approach was not properly aligned with diverse business interests and needs.	To some extent implemented
CEOs or CISOs cybersecurity awareness level	• The holistic view of threats and vulnerabilities supported users with a long-term attitude to review their policies for updates. • The holistic view of threats and vulnerabilities supported users with a short-term attitude to realise the significance of implementing all relevant security controls and adopting security practices; however, the tool did not support a prioritised action plan for the next steps.	To some extent implemented
CEOs or CISOs cybersecurity and IT knowledge and skill level	• For expert users, the tool did not prepare material for advanced security controls or new changes in the threat landscape. Therefore, the tool has no impact on their awareness-raising or skill improvement. • For users lacking cybersecurity awareness and knowledge, the tool supported awareness-raising but did not sufficiently provide hands-on solutions for skill development.	To a small extent implemented
Connection to cybersecurity expertise	• For SMEs with access to external or internal CISOs, the tool did not support a new connection to SME associations and CERTs to receive updates, exchange knowledge, or fill the gaps given its business model. • For SMEs without external or internal CISOs, the tool supported a connection to cybersecurity experts (CYSEC team) to gain the required knowledge and skill for implementing security controls.	To some extent implemented

6.5 DISCUSSION

Our results demonstrated that CYSEC was adopted in different ways, and due to SME heterogeneity one intervention method may not suit all. We recognised the impact of four factors on the adoption of CYSEC:

a) personalisation features;
b) awareness levels of CEOs or CISOs;
c) cybersecurity and IT knowledge and skill levels of CEOs or CISOs; and
d) connection to cybersecurity expertise for gaining or exchanging knowledge.

We found that the impact of the tool was in different ways. Some SMEs used the tool to introduce awareness topics to new employees and assess the state of cybersecurity within their companies, in line with (D'Arcy and Hovav, 2007). In some SMEs, the tool changed CEOs' attitudes toward the threats by providing a holistic view of potential vulnerabilities and ever-present cybersecurity threats, in line with Albrechtsen (2007) and Caldwell (2016). In some SMEs, the tool offered common insight into cybersecurity, collective thoughts, and intra-organisational knowledge-sharing, in line with Hagen and Albrechtsen (2009). Furthermore, in line with Bulgurcu et al. (2010) and Puhakainen and Siponen (2010), CYSEC stimulated some CEOs to plan further training. However, the findings are in contrast with the previous study by Lee et al. (2004) that indicated information security awareness solutions have no vital effect on employees' behaviour.

Personalisation features. CYSEC, to some extent, implemented personalisation features. The findings indicate the importance of personalised controls and self-assessment questionnaires in the adoption of CYSEC. It can help SMEs identify the value of the recommendations regarding their business models and goals. Previous research has shown that CEOs and employees usually have a good understanding of the company's assets and processes. Linking cybersecurity best practices to this understanding increases awareness and motivation and helps develop a security culture in line with the business context (Amankwa et al., 2015; Beyer et al., 2015; Sadok et al., 2020).

CEOs' / CISOs' cybersecurity awareness level. CYSEC, to some extent, supported different awareness levels. The findings reveal that the users may have different awareness levels and, thus, attitudes towards cybersecurity activities. Some users had long-term attitudes and needed to know the changes in the threat landscape and IT technologies to update their policies and protection. However, some users had short-term attitudes or even false beliefs about their true threat exposure. They considered cybersecurity activities as a secondary object. Consistent with Heidt et al. (2019) and Wong et al. (2022), awareness is closely linked to SME managers' general attitudes. Individuals' cognitive beliefs and attitudes significantly impact cybersecurity practices' intention (Bulgurcu et al., 2010). CYSEC provided a holistic view to support SME diversity. Offering more rounded and holistic awareness training content that addresses all aspects of an employee's online life motivates them to practice (Caldwell, 2016).

CEOs' / CISOs' cybersecurity and IT knowledge and skill level. CYSEC, to a small extent, supported relevant cybersecurity and IT knowledge and skill. Our results indicate that CYSEC needs to support CEOs and CISOs according to their degrees of competence or self-efficacy in

IT and cybersecurity. Self-efficacy is a motivational construct that influences individuals' initial choice of engagement. It can be changed due to learning and feedback (Gist and Mitchell, 1992). Puhakainen and Siponen (2010) explain that awareness training content should be relevant and fit the recipient's cognitive level to motivate them to engage. It is vital to notice the cybersecurity level of target audiences to ensure the success of a cybersecurity program (ENISA, 2017). CEOs are willing to adopt tools based on their self-efficacy in cybersecurity (Lee and Larsen, 2009) and self-efficacy in IT (Kirsch and Boss, 2007).

Connection to cybersecurity expertise. CYSEC, to some extent, supported connection to cybersecurity expertise. The findings provide evidence of the importance of the connection to cybersecurity experts and SME associations with such expertise. This connection can ease SMEs' persuasion to disseminate information in their associations or receive updates from CERTs to make timely decisions. Further, SMEs often lack the necessary cybersecurity skills to implement procedures for mitigating risks (Njenga and Jordaan, 2016; Renaud, 2016). Also, the lack of IT expertise hinders tools' adoption (Lee and Larsen, 2009). Therefore, connections to experts provide them with hands-on training for protective measures (Dupuis et al., 2019).

Understanding the diversity of SMEs helps develop thoughtful approaches. Untargeted content and unrealistic demands reduce the effectiveness of cybersecurity communication and, consequently, employees' motivation to take an active role in protecting the company's information assets (Beyer et al., 2015). This study demonstrates how SME heterogeneity may influence the adoption of CYSEC. SME heterogeneity has been noticed in other fields of research (Hagen et al., 2012). Few studies have also considered SME diversity and classified them in cybersecurity. Lee and Larsen (2009) demonstrate that SME types (non-IT intensive, IT-intensive) and CEO expertise influence anti-malware adoption. The European Digital SME (2020) discusses the importance of SME types (digital enablers, digitally based, digitally dependent, and start-ups) in the adoption of cybersecurity standards. Future research may be built on the European Digital SME (2020) work to seek appropriate solutions for each type of SME.

This research has some limitations. The main concern with the findings is generalisability due to the small sample size, a typical limitation of qualitative studies (Karjalainen et al., 2013; Lee and Baskerville, 2003). The nature of this study is exploratory, and the qualitative approach helped us get a more nuanced understanding of the SMEs' diverse cybersecurity needs. Future research would further validate the identified factor using a quantitative approach, questionnaire surveys to perhaps 1,000 participants, and confirms generalisability. Future studies may also consider the diversity of SMEs that may exist within an industry to propose more tailored solutions.

Moreover, our data were collected in SMEs located in Europe. Literature indicates that cultural characteristics may influence cybersecurity learning preferences that lead to distinct cybersecurity behaviours in different countries (Karjalainen et al., 2013). Future research would be appealing to consider cultural issues in similar SMEs outside Europe, for instance, in developing countries (Kabanda et al., 2018). Another limitation of the study is the short-term distance between CYSEC availability in the SMEs and the interviews, almost two months. So,

the findings demonstrate the short-term effects. Cybersecurity is an ongoing activity; further study is needed to have a longitudinal design, even beyond one year of the tool exposure, to study the long-term impacts of the tool. Nevertheless, this research makes an empirical contribution to the few studies investigating the impacts of a self-paced tool on cybersecurity behaviour and awareness-raising in SMEs.

6.6 Conclusion

Facilitating proactive cybersecurity development and raising awareness are the most challenging issues for many SMEs. Self-paced tools can support awareness-raising and cybersecurity capability development in many SMEs. In this study, we had close contact with 12 SMEs to evaluate our self-paced tool, CYSEC. Our qualitative approach allowed us to gain a deeper understanding of SMEs' diversity and the effectiveness of CYSEC in real-world practices. We first conducted a survey study and then nine structured interviews with SME CEOs or CISOs.

Our findings highlighted the heterogeneity of SMEs (i.e., various needs, capabilities, and vulnerabilities). The personalisation features influenced the adoption of CYSEC. Since the SMEs had various information and communication technology infrastructures and business models. Further, CEOs' or CISOs' awareness level, IT and cybersecurity knowledge, and skills affected the tool usage. CYSEC provided a holistic view of threats, vulnerabilities, and cybersecurity mitigations to support various levels of awareness. The tool had an awareness-raising impact on users with short-term attitudes or even false beliefs about their true threat exposure. However, these users required more practical solutions. For users with a high level of awareness who wanted to know about the new changes in the threat landscape, CYSEC did not support awareness and knowledge improvement. Also, the findings endorsed the role of connection to experts and SME associations. This connection is inclined to facilitate gaining and exchanging information to implement measures.

Our future work will investigate SME heterogeneity. We intend to differentiate SME needs and vulnerabilities. We believe that well-targeted awareness training content can support the effectiveness of CYSEC.

CHAPTER 7

A Classification of Organisations

Cybersecurity is increasingly a concern for small and medium-sized enterprises (SMEs), and there exist many awareness training programs and tools for them. The literature mainly studies SMEs as a unitary type of company and provides one-size-fits-all recommendations and solutions. However, SMEs are not homogeneous. They are diverse with different vulnerabilities, cybersecurity needs, and competencies. Few studies considered such differences in standards and certificates for security tools adoption and cybersecurity tailoring for these SMEs. This study proposes a classification framework with an outline of cybersecurity improvement needs for each class. The framework suggests five SME types based on their characteristics and specific security needs: cybersecurity abandoned SME, unskilled SME, expert-connected SME, capable SME, and cybersecurity provider SME. In addition to describing the five classes, the study explains the framework's usage in sampled SMEs. The framework proposes solutions for each class to approach cybersecurity awareness and competence more consistent with SME needs.

This chapter is based on the following publication:
Shojaifar, A., & Järvinen, H. (2021). Classifying SMEs for Approaching Cybersecurity Competence and Awareness. In *The 16th International Conference on Availability, Reliability and Security* (pp. 1-7).

7.1 INTRODUCTION

Small and medium-sized enterprises (SMEs) are perceived to have the weakest defences against cyberattacks (Caldwell, 2015; Renaud, 2016). Many SMEs are often unaware of cybersecurity's significance, and the lack of adoption of precautions is a real risk (Renaud, 2016; European Digital SME, 2020).

Diverse solutions proposed to provide training for awareness and cybersecurity capability improvement for SMEs. A vast amount of security advice is available (Renaud, 2016). ENISA developed training for raising awareness (ENISA, 2010). Other work described information security maturity assessments (Mijnhardt et al., 2016; Cholez and Girard, 2014), self-paced tools for training awareness improvement (Furnell et al., 2002; Ponsard et al., 2019; Shojaifar et al., 2020), and information security management approaches (Ntouskas et al., 2011; Brunner et al., 2017). However, a report from Pnemon Institute (Keeper and Ponemon, 2019) shows an increase in sophisticated cyberattack against SMEs. A recent report from Hiscox (Lloyd, 2020) demonstrates a sharp increase in reported cyberattacks among SMEs across UK, Europe, and the US. Many SMEs still lack awareness or do not adopt any of these solutions. One of the reasons for the lack of adoption may be that each of these approaches may fit some SMEs but not others.

SMEs are heterogeneous exhibit diverse cybersecurity needs, perceptions, and capabilities (Chua et al., 2009; Muller et al., 2017). For example, SMEs might have different Information System (IS) expertise, various cybersecurity self-efficacy, and diverse appreciation of cybersecurity threats (Gupta and Hammond, 2005; Lee and Larsen, 2009; Renaud and Weir, 2016; European Digital SME, 2020). This diversity indicates that there is no one-size-fits-all. Consistency of security information with the target group's profile, including demographic factors, is imperative for delivering security content (Garg et al., 2012; Renaud, 2016; Caldwell, 2016; ENISA, 2017; European Digital SME, 2020). For example, the cybersecurity level of target audiences is vital to ensuring a cybersecurity program's success (ENISA, 2017). However, few studies have considered SMEs' differences and how to communicate and approach cybersecurity in a tailored manner (Lee and Larsen, 2009; Renaud and Weir, 2016; European Digital SME, 2020). Study (European Digital SME, 2020) focuses only on cybersecurity standards and certification schemes adoption. Study (Lee and Larsen, 2009) considers only two SME types, and (Renaud and Weir, 2016) only studies individuals' risk perceptions and security management practices.

This study aims at addressing the heterogeneity problem with a classification framework. It distinguishes between categories of SMEs based on their characteristics. The characteristics include SME staff IT knowledge, cybersecurity offering, cybersecurity expertise in SME, awareness of threats and the importance of protection, awareness of good practices, and awareness of the dynamic essence of cybersecurity.

Classification framework is of vital importance since it reduces the complexity of approaching cybersecurity improvement by identifying security improvement needs for each class. The framework indicates that each type of SME needs a specific approach to be well protected. Therefore, instead of providing inefficient general recommendations and training

content, cybersecurity communications effectively target each SME class. The study identified five types of SMEs, including cybersecurity provider, capable, expert-connected, unskilled, and abandoned SMEs. We argue that the classification can offer a significant contribution to the SME cybersecurity literature because SME classification has not yet been adequately served.

The remainder of this chapter is organised as follows. Section 2 presents the background of the research. Section 3 outlines the classification framework for approaching cybersecurity improvement. Section 4 explains the use of the framework in sampled SMEs. Section 5 discusses the significance of the framework and future research avenues. Section 6 summarises and concludes.

7.2 Research Background

Classification is significant since it decreases the complexity of working with various entities with different features and reduces the amount of information we need to store (Rosch, 1999; Smith and Medin, 2013). Defining concepts is important since "*if we perceived each entity as unique, we would be overwhelmed by the sheer diversity of what we experience and unable to remember more than a minute fraction of what we encounter*" (Smith and Medin, 2013). Based on Smith and Medin (2013), concepts allow us to go beyond the information given. When we assign an entity to a class on the basis of its perceptible attributes, we can infer some of its non-perceptible attributes. Category knowledge helps to make inferences about the presence of unobserved or unobservable features (Rosch, 1999; Rehder and Burnett, 2005).

Rosch (1999) proposes two fundamental principles for classification: cognitive economy and perceived world structure. The cognitive economy refers to category systems' functions and indicates that category systems need to "*provide maximum information with the least cognitive effort.*" Perceived world structure refers to the structure of the information so provided and indicates that "*the perceived world comes as structured information rather than as arbitrary or unpredictable attributes*." Therefore, "*maximum information with least cognitive effort is achieved if categories map the perceived world structure as closely as possible*."

Prior research considered SME classes in business and the characteristics in which SMEs differ widely from one another. Chua et al. (2009) indicate that the characteristics of SME owner-managers, the aspects of the firm and its employees, and the characteristics of the environment in which they operate impact SME heterogeneity. Hagen et al. (2012) provide evidence and introduce four distinct SME profiles and strategic business patterns.

Digital SME Alliance (2020) highlights the importance of the analysis of different types of SMEs' cybersecurity requirements and consequently adapting the measures for effective cybersecurity adoption. Furthermore, the study based on Interim Report (2019) confirms the impact of industry type and firm size on cybersecurity adoption. They identify four types of SMEs and their role in the digital ecosystem to tailor security standards:

- Digital enablers are SMEs that are active in developing and providing cybersecurity solutions.

- Digitally based are SMEs that cybersecurity is not the core of their business; however, they highly depend on digital and security solutions from the first category to ensure their business continuity.
- Digitally dependent are end-user SMEs that form the largest category of SMEs. They use regular ICT for running their businesses, and they need to access easily understandable and practical solutions.
- Start-ups are SMEs that security has a low priority since they are busy with the functional development of their business models. They need to understand the importance of security compliances and be motivated to adopt security standards.

Lee and Larsen (2009) consider anti-malware software adoption in SMEs through a survey study. Their study indicates two types of SMEs (IT-intensive industries, non-IT intensive industries) and two types of SME executives (IS experts, non-IS experts). The study emphasises that vendor support, including the presence of designated technicians, easy access to technical assistance, 24 × 7 services, and periodic training, is a key facilitator in persuading executives to adopt security solutions. While the study explains the impact of industry type on adoption decision, it does not indicate a significant effect of the firm size on the adoption intention and actual adoption. Moreover, the study based on Protection Motivation Theory (PMT) (Rogers, 1983) explains that SME executives' IS self-efficacy strongly influences cybersecurity adoption decisions.

Self-efficacy and outcome expectancies demonstrate individuals' perception of capabilities and capacities to perform specific required tasks successfully (Bandura, 1977). Self-efficacy is a motivational construct that influences individuals' initial choice of activities, goals, task engagement, and affective reactions to tasks. Moreover, it is a dynamic construct that can be changed due to learning, experience, and feedback (Gist and Mitchell, 1992).

Information system (IS) research has considered self-efficacy as a fundamental determinant of IS usage (Davis, 1989). Organisational supports, including top management encouragement, impact employees' self-efficacy and IS usage (Igbaria and Iivari 1995). Furthermore, since efficacy beliefs are situationally specific (Bandura, 1982; Davis, 1989), others have considered cybersecurity self-efficacy and used instruments to measure cybersecurity efficacy and skills (e.g., Bulgurcu et al., 2010). Competence in cybersecurity can be explained based on self-efficacy (Bulgurcu et al., 2010).

Collective self-efficacy focuses on employees' aggregated capabilities instead of individual-focused and assessed by organisational representatives (Bandura et al., 1999; Lee and Larsen, 2009). SME executives or top managers are identified as individuals who can adequately assess their companies' collective self-efficacy. Also, their self-efficacy impact cybersecurity adoption in SMEs (Lee and Larsen, 2009).

Bulgurcu et al. (2010) indicate that providing organisational security awareness is an important factor in persuading employees to adopt security technologies and practices. They distinguish two types of awareness: general security awareness and information security policy

(ISP) awareness. General security awareness is defined as an overall understanding of security threats, their consequences, and the importance of precautions. In addition, ISP awareness is defined as understanding the requirements prescribed in the policies and the aims of those requirements. Both types of awareness can be considered for SMEs.

Although the classification of SMEs is needed to tailor cybersecurity solutions, little attention has been given to it. Lee and Larsen (2009) consider the importance of self-efficacy and expertise; however, categorising SMEs into IT-intensive and non-IT-intensive and the executives to expert and non-expert seems insufficient. Digital SME Alliance (2020) classifies SMEs to better adapt standards and certification schemes to the needs of SMEs in short to medium-term; however, the study explains that for the long-term goal, a mix of raising awareness and providing practical solutions is needed.

We now move to the classification framework to draw out approaching cybersecurity awareness-raising and capability improvement in various types of SMEs.

7.3 SME Cybersecurity Competence Classification – a Framework with Improvement Needs

This section proposes a classification framework of five SME types and indicates cybersecurity improvement needs for each class (Table 7.1). The framework resulted from the paper design author experience with SMEs of six EU countries over several years on two projects. Iterative design security solutions for SMEs, using the design science research methodology (Hevner et al., 2004), provided us the opportunity to learn more about SMEs and their differences. The concepts (classes) were defined to reflect maximum information about the SME characteristics and cybersecurity competence with the least cognitive effort to distinguish between the classes.

The following factors have been considered in the classification. The factors provide a minimal set, mutually independent to reflect competence and awareness in SMEs.

- SME with cybersecurity offering (CSO). The SME can be a cybersecurity provider company.
- Staff and CEO with cybersecurity expertise or in active contact with a cybersecurity expert (CSEA). The SME may have sufficient proficiency in cybersecurity or have internal/external CISO that support cybersecurity activities in the company or have no security expertise and connection to a security expert.
- Staff and CEO with in-depth IT user Expertise (ITE). The SME staff can have sufficient IT expertise or receive technical support from available resources.
- Staff and CEO with awareness about cyber threats and the importance of protection (CSTA). This factor reflects the SME staff's general perception of cybersecurity risks and the importance of implementing countermeasures.
- Staff and CEO with awareness of SME-expected good cybersecurity practice (CSGP). This factor reflects SME staff and CEO's understanding of the importance of guidelines

and policies and the availability of a written policy in the company. The SME may have an explicit security guideline or policy statement in place according to the SME security requirements, or partially written for some focus areas, or no clear policy or guideline statement.

- CEO or CISO with awareness of the dynamic character of cybersecurity (CSAD). The SME approaches in cybersecurity can differ. If they realise that cybersecurity becomes obsolete, they may have a long-term attitude to plan updated training and review their policies. If they look at the awareness topics as secondary issues, they try to adopt security solutions to gain a security level. If they have no clear perception of potential threats and vulnerabilities, they are reluctant to adopt cybersecurity solutions.

According to the SME types, the approach of cybersecurity improvement needs to be adapted. Thus, the training awareness content or hands-on solutions would be more meaningful for SMEs. Five proposed classes are:

Cybersecurity Abandoned SMEs. In this type, SMEs have no cybersecurity policy or guideline. Along with a lack of security competence, IT skill shortages seem to constrain cybersecurity activities. They have no resource allocation or connection to cybersecurity resources. They have no clear perception of security threats; consequently, they do not see the need for security measures or commitment to cybersecurity practices. Providing extrinsic motivation to adopt security solutions and change incorrect beliefs about its true threat exposure is a significant need for this class.

Moreover, they need access to basic security and IT knowledge, hands-on skills, and training content to improve their capabilities. Further, connection to trusted security experts and peers for communication seems necessary. It can facilitate security controls implementation and knowledge transfer.

Cybersecurity Unskilled SMEs. In this type, SMEs have a partially written cybersecurity policy for some focus areas. They are aware of some security threats and vulnerabilities; however, they do not have a holistic view. They have a lack of cybersecurity skills. They are not connected to experts, third parties, or associations to exchange knowledge and develop their employees' skills, and therefore they lack the competence to manage cybersecurity measures. They realise the importance of cybersecurity measures and are willing to comply with security policies. Thus, access to hands-on security skills, training content, and cybersecurity experts can lead them to improve their capabilities and adopt security solutions.

Cybersecurity Expert-connected SMEs. This type of SME has a partially written policy for some focus areas. They are connected and dependent on trusted third parties or have a CISO to manage their cybersecurity measures. They are aware of the importance of cybersecurity, and they have a connection to gain knowledge and skills. The employees are not adequately skilled in cybersecurity; in turn, access to specific capabilities and training based on their business model can fill the cybersecurity gaps for protecting the SME.

Table 7.1

SME Cybersecurity Competence Classification

SME Cybersecurity Classes	**CSO**	**CSEA**	**ITE**	**CSTA**	**CSGP**	**CSAD**	**Cybersecurity Improvement Needs**
Abandoned SMEs [a]	None	None	None	None	None	None	CS motivation, IT knowledge, CS knowledge, CS connection
Unskilled SMEs [b]	None	None	Yes	Partially	Partially	Adoption of CS Practices	CS training, CS guidance, CS connection
Expert-connected SMEs [c]	None	Internal /external CISO	Yes	Yes	Partially	Adoption of CS Practices	CS completion
Capable SMEs [d]	None	Expert	Yes	Yes	Yes	Continuous Improvement	CS news CS evolution
Provider SMEs [e]	Yes	Expert	Yes	Yes	Yes	Continuous Improvement	CS news CS evolution

CSO = SME with Cybersecurity Offering; **CSEA** = staff, and CEO with cybersecurity expertise or in active contact with a cybersecurity expert; **ITE** = staff, and CEO with in-depth IT user Expertise; **CSTA** = staff and CEO with awareness about cyber threats and the importance of protection; **CSGP** = staff and CEO with awareness of SME-expected good cybersecurity practice; **CSAD** = CEO or Chief information security officer (CISO) aware about the dynamic character of cybersecurity

[a] **Abandoned SMEs:**

CS motivation: motivate the SME to adopt cybersecurity to overcome false beliefs about its true threat exposure,
IT knowledge: teach the SME's staff basic IT knowledge, including how to install, configure, and de-install software on devices,
CS knowledge: raise awareness about the most important cyber threats for the SME and recommendations for protection,
CS connection: connect the SME with a cybersecurity expert and peers that are improving their cybersecurity.

[b] **Unskilled SMEs:**

CS training: offer training to employees,
CS guidance: offer step-by-step instructions for implementing and maintaining SME-specific controls,
CS connection: connect the SME with a cybersecurity expert and peers that are improving their cybersecurity.

[c] **Expert-connected SMEs:**

CS completion: fill the gaps for protecting the SME given its business model.

[d, e] **Capable SMEs and Provider SMEs:**

CS news: maintain awareness about incidents and changes in the threat landscape,
CS evolution: adapt the protection to changes in the threat landscape, CS and IT technologies, and the SME's business model.

Cybersecurity Capable SMEs. This type of SME has a cybersecurity culture and a written security policy fully aligned with what cybersecurity must be done, the same as the cybersecurity provider SMEs (the next class). However, the key differentiator between this type and security provider SMEs is their business model. They have expertise and proficiency in IT and cybersecurity. Access to the updated and newest cybersecurity and IT technologies material to adapt their protection approaches holds useful for this type. Also, access to cybersecurity news helps them maintain awareness about incidents and changes in the threat landscape.

Cybersecurity Provider SMEs. They provide security solutions for others. This type of SME has a cybersecurity culture and a written security policy the same as the capable SMEs (the previous class). They are aware that threats are ever-changing, so they regularly review their policy and updates their rules. Moreover, they have a plan to update their training for employees. Thus, this type best demonstrates having a proactive attitude about cybersecurity activities. The same as cybersecurity-capable SMEs, their paramount cybersecurity need is access to the newest cybersecurity and IT technologies material and news (e.g., new policies, compromised websites).

7.4 The Use of the Framework

This section presents the early validation of the framework to provide evidence on the use and usefulness of the solution. The results are based on the first author qualitative study, interview, with five sampled SMEs (project partners). The participating SMEs have different sizes (micro, small, and medium) and are active in various industries. The selection of the subjects was based on their availability and their cybersecurity competence and experience level. This is an exemplar section to illustrate one example for each class of SME. This approach has been confirmed by (Wieringa et al., 2006).

SME-1 is a micro-enterprise active in hair and beauty. The subject demonstrated no expertise in IT and cybersecurity. She was unaware of how a phishing attack can impact her business and her customers' data. Moreover, she did not know whom she should contact when an incident happens. Interestingly, she explained that:

"I rank rather high my company security level."

Further, she did not indicate any specific security need. It seems she does not have a correct perception of cybersecurity threats.

According to the framework, the SME executive has the lowest level of self-efficacy; abandoned SME. Therefore, basic training for security awareness, cybersecurity motivation for implementing relevant security control, and supporting a connection to security and IT experts seem necessary.

SME-2 is a small company active in the IT industry. The subject was willing to improve the SME's cybersecurity, and the company has a partially written policy for password management. However, the subject was unable to manage security measures and find relevant resources. The subject noted:

"We do not have a security team department. If you do not have a CISO, [you need] offers [for] training classes and certification. We need delivery of services." Furthermore, the subject stated: *"We need to know how to solve the problems and not only presenting the problems."*

According to the framework, it is an unskilled cybersecurity SME. Access to hands-on resources, training courses, and cybersecurity experts seems necessary.

SME-3 is a micro health care company. The subject indicated specific training awareness requirements based on the company business model. He further explained that:

"[general training content] is not applicable to us, the hardware that we use for the services is managed by third parties, and they also set up the network. We need training content about cloud services for training the employees."

According to the framework, it is a cybersecurity expert-connected SME. A third party is responsible for managing their cybersecurity measures. Although the SME staff are aware of potential security threats, they do not have enough cybersecurity competence according to their business model. Access to specific training awareness content congruent with their business model seems useful.

SME-4 is a medium-sized company active in electronic voting technologies. The company has a security department as well as a written policy. The subject noted that:

"Access to material for more advanced security controls such as trusted boot or hardware encryption or a list of the latest threats and vulnerabilities is useful [for us]."

According to the framework, it is a cybersecurity capable SME. Access to the latest updates and advanced security controls seems useful.

SME-5 is a small company active in cybersecurity. The company provides security solutions and advice to other firms. The company has a written policy in place and puts a high value on review and update security measures. The subject indicated that:

"We review our policy two or three times a year. Having the most recent updates and news are useful to review."

According to the framework, it is a cybersecurity provider SME. The company staff has great cybersecurity competence, and the same as the cybersecurity-capable SMEs, access to the latest updates in cybersecurity and IT seems useful.

7.5 Discussion

The contribution of this study is proposing an SME classification framework and indicating cybersecurity improvement needs for each SME type. The framework can reduce the complexity of SME heterogeneity and the lack of security adoption, leading to targeting more effective cybersecurity competence and awareness.

Commonly studies distinguish between SMEs based on the number of employees (European Commission; Beheshti, 2004; Gupta and Hammond, 2005). However, it is not enough to approach effective cybersecurity in SMEs. In line with (Lee and Larsen, 2009; European

Digital SME, 2020), this study demonstrates that classification helps enrich the understanding of SME types to communicate and keep them engaged effectively. The classification approach is in contrast with the idea of CYSFAM (Ozkan et al., 2021) that proposes a maturity model for generic organisations. Moreover, compared to (Lee and Larsen, 2009; European Digital SME, 2020) (which identify four and two types of SMEs, respectively), this study indicates five types of SMEs with no counterpart for the cybersecurity capable SMEs.

The proposed framework is not a maturity model, and it does not convey that one class is more secure or vulnerable than the others. Instead, it is a taxonomy of distinct SME types and indicates that each type exhibits different needs to be secured. The idea can be similar to personas (Ki-Aries and Faily, 2017) that provide a taxonomy within the design stage to understand archetypes of business users and goals. Therefore, the framework does not signify that there is a progression from one class to another one. While there are predictable reasons for movement between classes, there is no necessary sequence between the SME classes. For instance, an unskilled SME can hire an internal CISO, or an abandoned SME may establish a connection to a security provider SME and, consequently, move to the expert-connected class.

SMEs are heavily restricted with the available funding for cybersecurity purposes (Fielder et al., 2016); however, cybersecurity projects and service providers are approaching security in SMEs by developing cost-effective and lightweight solutions. The framework can help these service providers understand the level of cybersecurity expertise and good practices of SMEs in the different categories. Even more importantly, it shows the need to reach out to the potential end-users of their solutions with a messaging that focuses on the improvement needs of each category. The improvement needs of each category vary greatly, and there is little overlap. This means that a cybersecurity service provider must choose between the target audiences or markets it prioritises when it comes to communications, messaging, and even offering services and tools. For example, the European Horizon 2020 project Geiger (Geiger Consortium, 2020) could specialise first in one of the categories and focus on capturing its interest with the communications highlighting its specific improvement needs, and then extend the services and communications to reach the rest of the groups.

In the context of GEIGER, the key contents of communications targeted to the different categories could be:

- Abandoned SMEs: raising awareness of the existence and importance of addressing cybersecurity threats, teaching basic IT skills and how to evaluate risks, recommendations, and connecting with experts and tool providers.
- Unskilled SMEs: offering beginner or intermediate level training packages and connecting with experts (“Digital Security Defenders”) who can provide concrete support in implementing the given recommendations.
- Expert-connected SMEs: connecting with experts who can assist in detecting the remaining weak areas and in establishing robust good practices for daily operations and continuous improvement.

- Capable SMEs and provider SMEs: highlighting the features of the offered tool that allow for continuous monitoring of and adaptation to the threat landscape and novel tools and technologies.

To raise the chosen target audience's interest and convince them, messaging highlighting their improvement needs should be consistently implemented throughout all channels. Consistent security messages affect SMEs' threat appraisal (Renaud, 2016) and motivate them to implement necessary but straightforward precautions (Lee and Larsen. 2009; Dojkovski et al., 2010; Renaud, 2016). For example, if choosing to focus on the abandoned SMEs category, the essential contents of the landing page of the GEIGER solution could include a catchy and concrete story of a peer SME who discovered their cybersecurity risks and started improving them with the help of GEIGER. Also, a short questionnaire to evaluate their current risks. CEOs in abandoned SMEs may have incorrect perceptions of their security level and potential risks. So, they might be demotivated to adopt cybersecurity solutions. Julisch argues that SMEs may argue "nobody would want to attack us" (Julisch, 2013). Beliefs and perceptions affect users' intention of cybersecurity activities (Bulgurcu et al., 2010). Furthermore, GEIGER could support abandoned SMEs' IT skills. They lack the technical IT expertise, affecting the GEIGER solution adoption. The lack of IT and computer self-efficacy impacts security solution adoption (Kirsch and Boss, 2007; Kabanda et al., 2018), and in SMEs is a significant inhibitor (Lee and Larsen, 2009).

As the businesses in the categories of abandoned and unskilled SMEs have low awareness of cybersecurity issues, it is likely to be most efficient to reach out to them through non-cybersecurity-related channels that they already follow for professional or personal purposes. For example, trade or association newsletters and publications or presence at industry events, as well as direct contacts through their trusted service providers (such as accountants) or peer SMEs. The three other categories could, in addition, be reached through channels and events linked to cybersecurity.

This chapter proposed a framework and exemplar section to apply it based on one sampled SME for each category. The avenue for future research is to empirically validate the framework across a broader sample of SMEs using, for instance, a survey-based quantitative approach studying the diversity of the SMEs in categories and elaborate their needs in more detail. Further, future work needs to entail more metrics for SME classification, for instance, concerning privacy needs, if SMEs that need to process personal information have active contact with Data Protection Officer (DPO). However, this study takes its place among the very few studies in SMEs' classification for cybersecurity improvement.

7.6 Conclusion

The chapter has proposed a classification framework to better target value-ridden cybersecurity improvement in various types of SMEs. Based on SME characteristics, the framework identified five SME types: cybersecurity abandoned SME, unskilled SME, expert-connected SME, capable SME, and provider SME. Moreover, the framework studied different cybersecurity needs for approaching security improvement in each class.

Further, the study illustrated the use of the framework in the sampled SMEs from different industries. The early validation of the framework demonstrated that the framework could explain the differences between SME types. Moreover, the subjects identified some needs that have been considered in the framework. The security needs constituted a broad diversity. Cybersecurity unskilled and abandoned SMEs needed to connect to security experts and access training awareness material. The expert-connected SME mainly required capabilities to fill specific security gaps, and capable and provider SMEs needed to have updated and newest cybersecurity and IT technologies material.

The framework aims to demonstrate how each class of SME can be effectively communicated and well protected and does not convey that one class is more secure or vulnerable than the others. Therefore, the framework can help cybersecurity service providers in that they can position SMEs in one of the classes in the early face to decide how to communicate and offer services and tools.

CHAPTER 8

Conclusion

This dissertation introduced "Volitional Cybersecurity" (VCS) as a significant contribution to the knowledge (Chapter 1). VCS provides a systematic way to think about adoption and manage long-term adherence to cybersecurity approaches. It assists in demystifying and structuring the aspects of cybersecurity behaviour in heterogeneous contexts that have neither been sufficiently recognised in prior studies nor embedded in cybersecurity solutions. The validation of VCS has been performed in small and medium-sized enterprises or businesses (SMEs/SMBs) context.

This final chapter synthesises the arguments in the dissertation to answer the main research question (MRQ) posed in Chapter 1 (section 1.5) and outlines the activities performed for the construction and validation of VCS. Chapter 8 hopefully places this dissertation well in the ever-changing context of cybersecurity and its impact on volitional behaviour.

MRQ: How can we support volitional forms of behaviour with a self-paced tool to increase the quality of cybersecurity engagement?

The design science research method is used as the primary method for this dissertation to answer MRQ. All chapters and research questions (RQs) are structured around the design science research method's activities (section 1.6, Figure 1.6). In turn, the dissertation brings a chain of chapters and RQs that together tell one story.

First, a systematic literature review was conducted about adherence to information security practices. Chapter 2 presented the proposed theoretical foundations and the extent of empirical evidence that information security adoption and adherence have been validated. Further, the frequently mentioned characteristics of the context (SMEs) were identified. The researcher identified and proposed Self-determination theory (SDT) as the kernel theory of the dissertation in this step. Also, a series of potential directions and themes for future research (incorporated in this dissertation) were specified in this chapter (also see Table 1.1). Chapter 2 demonstrated that most of the applied theories in the context of the research originated from disciplines other than information systems and cybersecurity. Further, motivation is a key concept across many cybersecurity studies focusing on human aspects. However, what is less understood is that motivation can be intrinsic and extrinsic, with various types and qualities. Also, the researcher realised that past works have largely relied on studying theoretical relationships in survey-based studies or evaluating intentions, whereas little research has studied actual cybersecurity behaviours.

According to the findings of Chapter 2, Chapter 3 investigated the design of CYSEC (the main artefact). CYSEC design was grounded in the rigorous theory of motivation (SDT) for the sustainability of volitional self-endorsed behaviour. SDT provided the author with a comprehensive overview of various types of extrinsic motivation that reflected different degrees of self-determination. Thus, the arguments for users' behaviour can be traced back to the SDT constructs. The design included features such as tailored recommendations, embedded awareness training content, and stepwise series of self-assessment questions to facilitate self-endorsed capability improvement and support the quality of cybersecurity engagement.

In Chapters 4 and 6, the researcher explained how CYSEC was demonstrated, and its use and usefulness were rigorously evaluated. Chapter 4 presented the results of the formative evaluation of the CYSEC prototype. The researcher had a deductive approach and applied the explanatory multi-case study (observation strategy) and post-observation questionnaire. This approach provided us with first-hand experience of CYSEC's use and usefulness. The main design improvement needs were identified in this step. Chapter 6 presented the results of the summative evaluation of CYSEC. The researcher had an inductive approach and applied a survey study, structured interviews, and conceptual modelling. This approach gave the researcher an understanding of why and why not CYSEC was successful. The vital factors that affected CYSEC's usefulness and the quality of cybersecurity engagement were recognised in this evaluation.

According to the findings of Chapter 4, Chapter 5 investigated users' confidentiality worries in security-related information sharing. Based on an SDT model for knowledge sharing in virtual communities (Yoon and Rolland, 2012), the researcher designed an online consent prototype to tackle the challenges of lacking motivation and trust. The researcher had a deductive approach to validating the artefact and applied semi-structured interviews. The findings showed that users' perception of control over information sharing influenced motivation for security information sharing.

According to the findings of Chapter 6, Chapter 7 investigated the heterogeneity of the context and its impacts on cybersecurity communication. Therefore, a classification including five concepts to represent five types of SMEs was formulated (Abandoned, Unskilled, Expert-connected, Capable, and Provider), and the exemplars were provided. The researcher identified the improvement needs for each class. Accordingly, what is best for one class of SMEs is not necessarily best for another. Therefore, the classification can reduce communication complexity and support a better quality of cybersecurity engagement.

The rest of this chapter is organised as follows: Section 8.1 delineates the answers to the research questions presented in Chapter 1 (section 1.5). Section 8.2 considers VCS theory and elaborates on its implications. Section 8.3 presents the limitation of this research and proposes avenues for future research. Finally, Section 8.4 describes the reflections on this research.

8.1 Research questions and contributions

This research investigated eight research questions (see Chapter 1, section 1.5) to answer the main research question of the dissertation. In the following, we elaborate on the answers to the questions.

The research elaborated in Chapter 2 answers RQ1, RQ1.1, RQ1.2 and RQ2. A systematic literature review (snowballing strategy; Wohlin (2014)) was conducted to study SMEs' adherence to information security practices.

RQ1 – *What theories are in use to explain adherence to good information security practices?*

Chapter 2 identified 18 theories applied to study adherence to information security practices in SMEs (Figure 2.6). The constructs mainly come from the psychology and criminology

domains. The findings revealed that PMT, GDT, and TPB are the most frequently applied theories. This finding is consistent with previous systematic literature reviews in the information security field. The findings indicated that motivation is a key concept across many cybersecurity studies, and the focus on punishments, rewards, and fear appeals is predominant.

RQ1.1 – *What are the goals of adherence that can be explained with these theories?*

The majority of the inspected publications focused on employees' information security policy compliance to adopt good behaviours and management information security practices. They applied theories or theoretical models to identify what drives employees' compliance, examine employees' behavioural intentions, and propose solutions to promote policy compliance behaviour. Also, understanding how to support SME managers in making decisions and identifying the factors that impact their intention to adopt information security solutions is important for many studies.

RQ1.2 – *What is the state of empirical validation of these theories for explaining adherence?*

Most of the applied theories have been borrowed from domains other than information systems. This research question investigated to what extent the theories have been empirically validated in the information security domain. In order to answer this question, the researcher synthesised the state of empirical validation of all the studied theories. The findings demonstrated that most of the theories had been empirically validated. Also, the studies provided empirical support for most of the theoretical relationships of the constructs.

RQ2 – *How do the characteristics of small and medium-sized enterprises affect the adherence to information security?*

The frequently mentioned SME characteristics were conceptually organised around technical skills, knowledge and awareness, financial resources, and organisational features. The findings show that skill shortage is one of the major constraints that influences the implementation of the recommended security measures for mitigating information security threats. Also, the lack of technical knowledge and resources are barriers to information security compliance. Further, the studies have highlighted the lack of awareness of information security as one of the SMEs' characteristics that exposes them to information security risks. Moreover, many researchers have portrayed SMEs' lack of financial resources as an essential constraint for adherence to information security approaches. Finally, the studies have indicated certain characteristics (e.g., they are less structured, they do not have access to the same level of resources, and CEOs are often the sole decision-makers) that impact information security activities in SMEs.

The work in Chapter 2 contributes to the knowledge with the first literature review on information security adherence in SMEs. Also, it offers the potential directions and needs for future research that have been incorporated into this dissertation (Table 8.1). Further, it demonstrates that the studied theories mainly originated from disciplines other than information systems and cybersecurity. Additionally, the findings reveal that although a wide variety of theories have been considered in the context of SMEs and many studies focused on motivation, SDT has not been applied to SMEs. Therefore, the researcher posed RQ3.

Table 8.1

Potential directions and themes for future research were identified in the literature review (Chapter 2) and then considered in the subsequent chapters.

Theme	Suggestions for future study in information security adherence	Chapter
Behavioural Theory	Self-determination theory of motivation. • Studying different types of motivation (not only punishment / reward) • Studying hypothesised effects of autonomy, competence, and relatedness on employees' compliance, adherence, and adoption	3, 4, 5
Goal of Adherence	Considering the importance of • Effectiveness of information security communication • Risk perception • Awareness-raising	4, 5, 6, 7
Research Methodology	Considering additional research methods • Experiment • **Design science** and action research	2 - 7
Context Heterogeneity	Proposing tailored solutions • Design and evaluation of volitional self-endorsed cybersecurity approaches • Classification of heterogeneous contexts for effective communication	3, 4, 6, 7

The research elaborated in Chapter 3 answers RQ3. Chapter 3 presented the design of CYSEC (the primary artefact) and explained the lessons learned (synthesising the project deliverables findings).

RQ3 – *How is SDT operationalised in a self-paced tool to facilitate end-users' self-endorsed cybersecurity behaviour?*

CYSEC includes SDT design elements to offer relatedness, knowledge, and choice for effective communication and sustainability of the progress. The tool has two main interfaces. A dashboard shows the features:

(a) recommendations for next improvements [relatedness, competence, autonomy],

(b) access to capability areas [autonomy, competence],

(c) summary information about the company's progress [relatedness, competence].

Once the user enters the work area (e.g., by choosing a recommendation or a capability area), it offers the features:

(d) self-assessment questions [autonomy, competence],

(e) access to expert knowledge [competence, relatedness], and

(f) action cockpit for creating calendar entries, mails, and reminders [relatedness, competence, autonomy].

The work in Chapter 3 contributes to the follow-up project with an artefact (CYSEC technology transferred). Also, to our knowledge, this is the first time SDT has been considered for designing cybersecurity self-paced tools. The design knowledge also has been used in the follow-up project. Further, the implementation of the Self-Determination Theory in Chapter 3 guided us towards discovering the impact of the CYSEC dashboard and work area features on

cybersecurity communication effectiveness and users' motivation to adopt desired behaviour. Therefore, RQ4 and RQ5 were posed.

The research elaborated in Chapter 4 answers RQ4 and RQ5. The chapter explained the conducted explanatory multi-case study (observation strategy) and short survey for the formative evaluation of CYSEC.

RQ4 – *How do the available features of cybersecurity tools influence the effectiveness of communicating cybersecurity to motivate users' adoption of desired behaviour?*

RQ4 intends to realise how CYSEC hypothesised features support the effectiveness of cybersecurity knowledge communication for volitional behaviour. The researcher found that the CYSEC dashboard and work area features positively affected users' motivation to adopt desired behaviour. He noticed that the features could facilitate cybersecurity management and connectedness between the CISO and employees. Self-assessment questions, access to expert knowledge, recommendations, and progress summary supported self-endorsed capability improvement in the SMEs. The findings demonstrated that participating SMEs learned about cybersecurity and adopted practices and controls when the immediate perceived learning experience was good. The findings also revealed that perceived reliability, expert support, clarity, and local language support of the content were important in the sense that the lack of these quality attributes hindered some of the participants from accepting training input. Further, the options should always be relevant and adapted to the IT infrastructure and operations of the company.

RQ5 – *Do the SME human end-users perceive CYSEC to be useful as a tool assisting do-it-yourself (DIY) cybersecurity assessment?*

The answer to RQ5 is based on the supplementary data collected at the end of each study (users' attitudes). Users evaluated the usefulness of the tool by responding to five-level Likert scale questions (low, rather low, medium, rather high, high) and justified their evaluation. CYSEC's usefulness was perceived to be rather high and high by all except one SME CISO. This CISO highlighted the importance of confidentiality concerns and the lack of relevant questions (in specific advanced topics) for his evaluation; "medium". This result indicates that a tool like CYSEC based on a self-endorsed method was accepted, allowing SMEs to manage capabilities.

The work in Chapter 4 provided descriptive knowledge about the use and usefulness of the CYSEC prototype. It offered insights into the actual use of the designed method and tool in real-world SME settings. Such validation goes beyond just evaluating intentions or theoretical relationships, as in the common survey-based studies. The researcher also discovered a potential barrier that should be addressed by future research: confidentiality. He observed resistance to documenting and sharing security-related information both within and among companies. Therefore, in the subsequent chapter, the researcher posed RQ6. Additionally, the findings of the study suggested some improvement needs. For instance, one challenge in motivating and supporting users to adopt recommendations is the choice of knowledge being communicated. Therefore, in Chapter 6, the researcher posed RQ7.

The research elaborated in Chapter 5 answers RQ6. The chapter explained the conducted semi-structured interviews to validate the impact of the online consent prototype (the second artefact) on user motivation for security-related information sharing.

RQ6 – *Do the choice of anonymity and the elaboration of how shared information will be used motivate SMEs to share security information?*

To answer RQ6, the researcher designed an online consent prototype. The design of the online consent is grounded in SDT. The prototype allows CISOs to exert control over information sharing. Through the choices, CISOs can define their relatedness to the community. Each choice gives information and explains how and where the shared information will be used to increase users' familiarity with the data usage environment.

The findings endorsed the positive effect of the online consent on user's motivation for security-related information sharing. It supported relatedness, autonomy, and competence, and enhanced the CISOs' trust perception. The study participants were motivated to share security information when they perceived that they had control of the communication, and the information was securely and anonymously stored.

The work in Chapter 5 provided descriptive knowledge about the usefulness of the online consent prototype for security-related information sharing. The major insight revealed from the findings about the importance of supporting security information sharing has been subsequently used in the follow-up project.

The research elaborated in Chapter 6 answers RQ7. The chapter explained the conducted survey study and structured interviews for the summative evaluation of CYSEC.

RQ7 – *What are the reasons that result in the intended use and usefulness of the tool for cybersecurity competence improvement?*

A version of CYSEC was placed in operation in real environments for two months, and then the researcher conducted the summative evaluation. In this period, the users were able to use the final version of CYSEC and answer the survey questions. Afterwards, they participated in the interviews. This approach allowed the researcher to gain a deeper understanding of SMEs' diversity, as well as the effectiveness of CYSEC in real-world practices.

The researcher noticed that SMEs have heterogeneous awareness training needs, and the tool usage varied quite widely. The tool's adoption is influenced by the personalisation features. Furthermore, CEOs' or CISOs' awareness level, IT and cybersecurity knowledge, and skills affected the tool usage. CYSEC had an awareness-raising impact on the users with short-term attitudes or even false beliefs about their true threat exposure. These users also required more practical solutions. However, CYSEC did not support users with a high level of awareness in knowledge and awareness improvement. Also, the findings specified the importance of connection to experts and SME associations. This connection can facilitate gaining and

exchanging information and support SMEs that lack in-house skills to implement protective measures. Table 8.2 summarises the main factors of the analysis.

Table 8.2

Analysis findings

Analysis themes	Findings	Degree of implementation in CYSEC
The tool's personalised features	• Various types of awareness training material (video, text, further study links) supported users' needs. • The self-assessment approach was not properly aligned with diverse business interests and needs.	To some extent implemented
CEOs/CISOs cybersecurity awareness level	• The holistic view of threats and vulnerabilities supported users with a long-term attitude to review their policies for updates. • The holistic view of threats and vulnerabilities supported users with a short-term attitude to realise the significance of implementing all relevant security controls and adopting security practices; however, the tool did not support a prioritised action plan for the next steps.	To some extent implemented
CEOs/CISOs cybersecurity and IT knowledge and skill level	• For expert users, the tool did not prepare material for advanced security controls or new changes in the threat landscape. Therefore, the tool has no impact on their awareness-raising or skill improvement. • For users lacking cybersecurity awareness and knowledge, the tool supported awareness-raising but did not sufficiently provide hands-on solutions for skill development.	To a small extent implemented
Connection to cybersecurity expertise	• For SMEs with access to external or internal CISOs, the tool did not support a new connection to SME associations and CERTs to receive updates, exchange knowledge, or fill the gaps given its business model. • For SMEs without external or internal CISOs, the tool supported a connection to cybersecurity experts (CYSEC team) to gain the required knowledge and skill for implementing security controls.	To some extent implemented

The work in Chapter 6 provided some contributions to the knowledge. With empirical evidence, the findings clarify the vital factors that influenced the use and usefulness of CYSEC. Moreover, consistent with prior literature (Bulgurcu et al., 2010; Wong et al., 2022), Chapter 6 demonstrates the impact of awareness on cybersecurity behaviour. However, in addition to the types of awareness (general cybersecurity awareness and awareness of cybersecurity policy) indicated by the mentioned studies, Chapter 6 demonstrates the impact of a new type, *awareness of the dynamic essence of cybersecurity,* on behaviour. However, the findings contrast with the Lee et al. (2004) work that indicated cybersecurity awareness solutions do not strongly affect employees' behaviour. Further, Chapter 6 findings about SME heterogeneity guided the researcher towards identifying different classes of SMEs to support targeted solutions and reduce communication complexity. Therefore, the researcher posed RQ8.

The research elaborated in Chapter 7 answers RQ8. According to the findings in Chapter 6, the researcher proposed a new classification framework and exemplars to present the early validation of the framework. Further, the framework's concepts were validated in workshops in the follow-up project.

RQ8 – *How can we classify the heterogeneous SME context to reduce the complexity of approaching effective cybersecurity?*

The researcher identified a minimal set of mutually independent factors for the classification:

- cybersecurity offering,
- available cybersecurity expertise or active contact with a cybersecurity expert,
- available in-depth IT Expertise,
- available awareness about cyber threats and the importance of protection,
- available awareness of good cybersecurity practices,
- available awareness of the dynamic essence of cybersecurity.

Based on the identified factors, the researcher classified SMEs and differentiated between their cybersecurity needs. The classification framework proposes five classes:

- *Cybersecurity Abandoned*: These companies have no cybersecurity policy or guideline. IT skills shortages constrain cybersecurity activities along with a lack of cybersecurity competence. They have no resource allocation or connection to cybersecurity resources. They have no clear perception of cybersecurity threats; consequently, they do not see the need for cybersecurity measures.
  Motivating to adopt solutions and change incorrect beliefs about its true threat exposure is a significant need for this class. Moreover, they need access to basic cybersecurity and IT knowledge, hands-on skills, and training content to improve their capabilities, knowledge inadequacies, and understanding. Further, connection to trusted experts and peers for communication is necessary.
- *Cybersecurity Unskilled*: These companies have a partially written cybersecurity policy for some focus areas. They are aware of some cybersecurity threats and vulnerabilities; however, they do not have a holistic view. They lack cybersecurity skills. They are not connected to experts, third parties, or associations to exchange knowledge and develop their employees' skills; hence, they lack the competence to manage cybersecurity measures.
  Since they realise the importance of cybersecurity measures, they are willing to comply with policies. Thus, access to hands-on skills, training content, and cybersecurity experts can lead them to leverage their capabilities to adopt solutions.
- *Cybersecurity Expert-connected*: These companies have a partially written policy for some focus areas. They are connected and dependent on trusted third parties or have an internal CISO to manage their cybersecurity measures. The staff are aware of cybersecurity's importance and have a connection to gain knowledge and skills.
  The employees are not adequately skilled in cybersecurity; in turn, access to specific capabilities and solutions based on the business context can fill the cybersecurity gaps.

- *Cybersecurity Capable*: These companies have a cybersecurity culture and a written cybersecurity policy fully aligned with what cybersecurity must be done, the same as the cybersecurity provider SMEs. They have expertise and proficiency in IT and cybersecurity. However, the key differentiator between this type and cybersecurity provider SMEs is their business model.
  Access to the latest cybersecurity and IT technologies content can assist them in updating their protection measures. Also, access to cybersecurity news helps them maintain awareness about incidents and changes in the threat landscape.
- *Cybersecurity Provider*: These companies provide cybersecurity solutions for others. They have a cybersecurity culture and a written policy, the same as the capable SMEs. The staff know that threats are ever-changing, therefore the CEOs/CISOs regularly review their policy and update their rules. Moreover, they have a plan to update their training for employees.
  Like cybersecurity-capable SMEs, their paramount cybersecurity need is access to the newest cybersecurity and IT technologies material and news.

The work in Chapter 7 contributes to knowledge and the follow-up project with a new view of the SME spectrum. It provides a simplifying tool that helps systematically describe and compare SME cybersecurity needs. Further, the classification framework highlights the diversity of SMEs. It indicates that what is best for one class of SME to improve its cybersecurity capability is not necessarily best for another.

8.2 VOLITIONAL CYBERSECURITY THEORY AND THE IMPLICATIONS

Volitional cybersecurity (VCS) theory is the major outcome of this research. It is structured around the core concept of volitional self-determined cybersecurity behaviour. It is agreeable for a user to understand the rationale and significance behind the behaviour and consequences (e.g., performing or not performing an appropriate cybersecurity behaviour), perform cybersecurity behaviour or choose cybersecurity technologies with free will and have relevant technical capabilities.

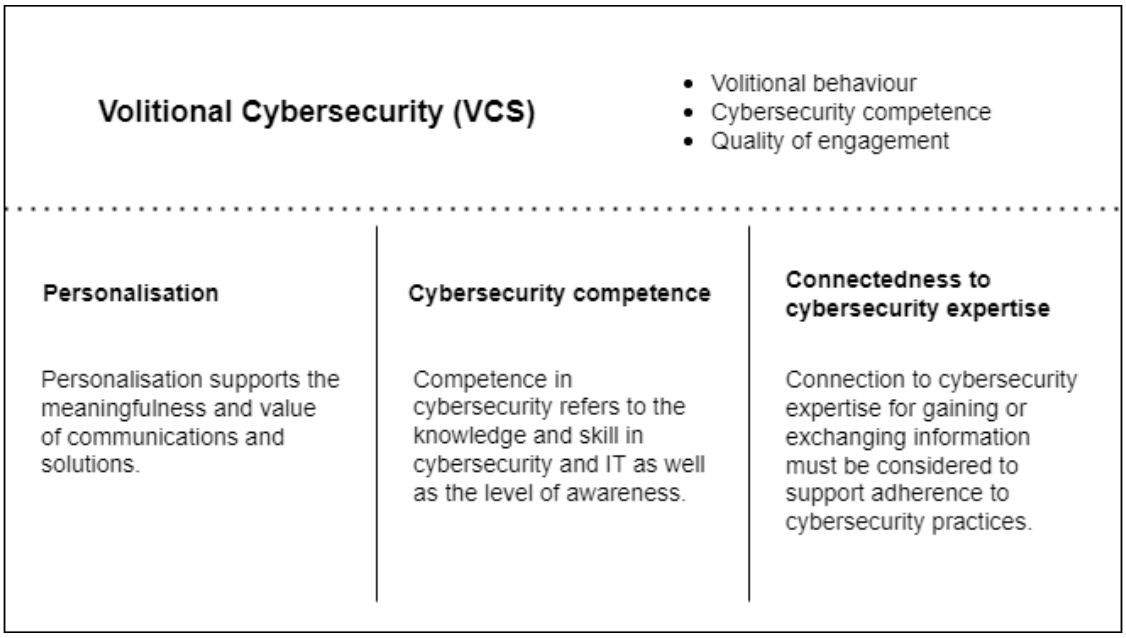
Bélanger et al. (2017) indicate that forcing individuals into information security compliance can lead to undesired behaviours. Similarly, Parsons et al. (2015) explain that severe penalties will not necessarily translate into better information security decisions. They highlight the importance of attitude towards the significance of cybersecurity rules (explaining why a procedure is important) for a better self-reported behaviour.

The volitional active cybersecurity behaviour concept has received scant attention and has never been systematically elaborated in the cybersecurity discipline. Therefore, VCS can be of interest to the discipline. VCS theory suggests that a heterogeneous context can be classified based on the cybersecurity competence of target groups and their distinct requirements. Further, VCS explicates that supporting three factors: A) personalisation, B) cybersecurity competence (defined based on knowledge and skill in IT and cybersecurity as well as awareness), and C) connectedness to cybersecurity expertise affect the adoption of

cybersecurity measures and better quality of cybersecurity engagement across all classes of the context (Figure 8.1).

Figure 8.1

The constructs of the Volitional Cybersecurity theory



The analysis results demonstrated that users wanted to adopt approaches most suited to their daily business activities and needs. Also, the empirical findings showed that users wanted to promote their cybersecurity capabilities. It is essential to entail thinking of cybersecurity competence improvement aligned with the users' competence level. Further, the findings demonstrated that the connection to cybersecurity expertise (for gaining information about ever-changing threats and countermeasures) could foster volitional strivings.

Accordingly, cybersecurity approaches that ignore the personalisation of cybersecurity solutions, the cybersecurity competence of target groups, and the connectedness of recipients to cybersecurity expertise in heterogeneous contexts lead to poorer acceptance of the value or utility of solutions.

VSC generates four implications.

a) Information security policy compliance. VCS has implications for cybersecurity research in heterogeneous contexts. Researchers could use VCS as a lens to view organisational challenges of cybersecurity motivation (Siponen et al., 2014), explore the diversity of needs in a context, and propose personalised and practical policies most suited to daily business routines (Garg et al., 2012; Caldwell, 2016; ENISA, 2017; Haeussinger and Kranz, 2017; Sadok et al., 2020). Motivating employees for policy compliance has received much attention in the literature. It would be essential to examine how an implemented information security policy provides guidelines for supporting volitional information security behaviour (self-endorsement and a feeling of choice vs compliance and experiencing coercion) to promote the quality of information security engagement.

b) Awareness programs. Researchers could also build on VCS to develop effective awareness programs and interventions for cybersecurity behaviour change (Bulgurcu et al., 2010; Bada et al., 2015; Bélanger et al., 2017; Gundu, 2019; Wong et al., 2022). Cybersecurity awareness has been aptly noted as an antecedent for behaviour change (e.g., Bada et al., 2015; Li et al., 2019; Chang and Coppel, 2020). Considering the notion of classification of a target context, incorporating content concerning different types of awareness, and establishing connections to cybersecurity expertise for continued communication provide potential avenues for future research to uncover how to enhance the effectiveness of awareness-raising programs.
c) Cybersecurity tool design. VCS also has implications for cybersecurity tool designers. VCS can be construed as prescriptive knowledge (Gregor and Hevner, 2013) for designing self-paced artefacts. VCS explains why the new self-paced cybersecurity tool needs specific features. Designers may draw upon the findings to design tools and methods that support volitional cybersecurity behaviours. VCS suggests that designers can personalise features concerning users' needs, support continued competence improvement aligned with users' competence level and include functions that connect users with cybersecurity expertise.
d) Cybersecurity communication. VCS has implications for practitioners and service providers to reach out to the potential end-users of their solutions. Awareness messaging and cybersecurity communications must be relevant and tailored to target groups (Renaud, 2016). A cybersecurity service provider must choose between the target audiences or markets it prioritises when it comes to communications, messaging, and even offering services and tools.

8.3 LIMITATIONS AND FUTURE DIRECTIONS

This section briefly discusses the validity and limitations, mitigations and directions for future research.

The data were collected from enterprises located in France, Spain, the UK, Greece, Italy, and Switzerland (a representative sample) since the focus of the research projects (Horizon 2020) was Europe. However, this research was limited geographically to companies in Europe. Literature indicates that cultural characteristics may influence cybersecurity behaviours in different countries (see Karjalainen et al., 2013; Tsohou et al., 2015, Chang and Coppel, 2020; Ameen et al., 2021). Future research would be appealing to consider cultural issues and expand the geographic population, for instance, in developing countries (see Kabanda et al., 2018; Chang and Coppel, 2020) to validate VCS.

The scope of the selected cases was designed for micro-, small- and medium-sized enterprises. Some studies argue that organisational size has an impact on cybersecurity behaviour or policy compliance intention (e.g., Solomon and Brown, 2020; Aigbefo et al., 2022), although some studies do not show the impact of organisational size (e.g., Lee and Larsen, 2009; Guo and Yuan, 2012). More research is needed to study volitional cybersecurity behaviour in large organisations.

Past works have found links between employees' personality traits (e.g., habit and hardiness) and cybersecurity behaviour (e.g., Alohali et al., 2018; Aigbefo et al., 2022). Also, different generations use cybersecurity tools differently. For instance, Alohali et al. (2018) discussed the correlation between the factor of age, personality, and cybersecurity behaviour. Studying the effects of employees' personality traits and the correlation between the age of the employees and cybersecurity tool adoption were excluded from this dissertation.

The author was involved in a sustained connection with 14 organisations for case studies. With these cases, the researcher applied qualitative research approaches to have an in-depth dive to better understand their cybersecurity behaviours and acquire tacit knowledge that was of interest. A qualitative study is a more helpful alternative to determine richer insights with a small sample size (Lee, 2003). To address the concern with the number of cases, the researcher had a purposeful sampling of representative cases (Stratified, Typical, and Critical cases (Miles and Huberman, 1994)). This approach provided a rich diversity of SMEs, differentiating in size, business interests, cybersecurity maturity, IT maturity, awareness level, implemented measures, and information security policy availability. Therefore, the volume of the collected data provided convincing evidence and clear patterns for theory development. Future research could build on the findings of this research by applying alternative research methods (e.g., a questionnaire survey) to validate the theory in a larger number of cases and provide quantitative support.

Although the literature (Karjalainen et al., 2013; Lee and Baskerville, 2003) explains that generalisability (commonly referred to as statistical generalisation, Yin (2009)) is a typical limitation of qualitative studies (due to the small sample size), case studies rely on analytical generalisation Yin (2009). Yin explains that in analytical generalisation, "*a previously developed theory is used as a template to compare the empirical results of the case study. [...] in doing a case study, your goal will be to expand and generalise theories*." Further, he indicates that in the case studies, "*the investigator is striving to generalise a particular set of results to some broader theory.*" Therefore, the mode of generalisation in this dissertation is "*analytical generalisation.*" SDT provided a lens for the researcher, influenced the data collection and analysis and guided him to focus on the activities and features that were crucial to examine. Then, in the inductive theorising approach, the researcher generalised the findings of the qualitative multiple case studies to a new theory (Volitional Cybersecurity) to explain the constructs and relationships.

CYSEC product was placed in operation in real environments for two months. There was a short-term distance between CYSEC availability in the organisations and the final interviews. Therefore, the findings demonstrate the short-term effects. However, cybersecurity is an ongoing activity. Future research is needed to have a longitudinal nature, even beyond one year of the tool exposure, to capture the longitudinal impacts of the tool, whether and how the companies change their practices over time with extended use of the CYSEC tool and perceive its usefulness.

In the following paragraphs, more possible directions for future research are outlined. The future directions are conceptually organised into four categories based on the categories suggested in Table 1.1 presented in Chapter 1.

First, from the theory perspective – while protection motivation theory (PMT) and general deterrence theory (GDT) have dominated information security studies, this study suggests that future research needs to discover new models and theories that can be of help in volitional forms of cybersecurity behaviour. Considering cybersecurity behaviour from the lens of PMT and GDT, although valuable, provides limited insight into active, volitional behaviour. Researchers can investigate a wider range of motivation types. Notably, this dissertation proposed VCS. VCS can be a topic of research on its own. It provides new theoretical insights in the context of cybersecurity behaviour, and future research might examine the hypothesised effects of personalisation, cybersecurity competence, and connectedness to cybersecurity expertise on cybersecurity behaviour change.

Second, from the goal perspective – given the findings that show employees and CEOs can have different types of awareness and that cybersecurity awareness impacts behaviour, awareness-raising is another key area to study in the future. Particularly, Chapter 7 classified SME context and identified associated needs for each class. Future studies can identify what class of SMEs lack what type of awareness, propose tailored awareness-raising interventions and then validate the effectiveness of cybersecurity communication.

Third, from the method perspective – the literature review, consistent with Lebek et al.'s (2014) literature review, demonstrates that previous research has largely relied on surveys or interview studies. Methods such as experiments, action research or design science research have not sufficiently received attention. The experimental method has been used to study, for instance, the impact of fear appeals on cybersecurity behaviour (Boss et al., 2015; Johnston et al., 2015). However, the literature review (Chapter 2) shows that the experimental research method has not been applied to SME studies. Therefore, a future step is to include a broader set of methods.

Fourth, from the context heterogeneity perspective – the findings of this research underscore the importance of attention to the diversity of organisations when approaching awareness-raising programs. Future research could build on the proposed classification and identify a broader set of metrics representing distinctive characteristics of organisations, e.g., concerning privacy issues for organisations that need to process personal information and have active contact with Data Protection Officers.

8.4 Reflections

The following paragraphs outline three research perspectives that are worth rethinking.

Reflections on the interdisciplinary research. Working on a subject that combines the knowledge and views of multiple fields was an immersion in a complex and interesting topic for the author. It was interesting because the projects were conducted in a collaborative context that involved various stakeholders and researchers of several stripes. It was possible to see the

cybersecurity problem from various perspectives and read and discuss topics that were seemingly unrelated to the problem. In turn, the author touched on a variety of topics (e.g., diversity of motivation for cybersecurity activities, organisation structure) to bridge the gaps. However, understanding the fields, reconciling the topics across knowledge domains and writing papers that satisfy reviewers from different disciplines are not easy. The author narrowly focused on the volitional cybersecurity behaviour of the use cases. Thus, he gained a nuanced understanding of the complexity of diverse cybersecurity needs and vulnerabilities (concerning SME heterogeneity) when they were using the innovative tool (CYSEC). Therefore, it was possible to identify new constructs as well as discover some of the discrepancies and classify them to facilitate proactive cybersecurity development.

According to Van Noorden (2015), interdisciplinary research is on the rise and can have broad societal and economic impacts. Cybersecurity is the fusion of several sciences; in turn, conducting interdisciplinary research is of crucial importance. Abundant literature demonstrates the complex essence of cybersecurity threats and the consequences of ever-present cyberattacks. Therefore, the need for appropriate countermeasures is urgent. This research shows that taking into consideration various dimensions (e.g., human motivation, organisation structure, technical skills) to find the appropriate mitigations is necessary.

Reflections on the VCS theory. The interdisciplinary research process and the problem-solving projects led the researcher to develop Volitional Cybersecurity (VCS) theory based on its grounding rigorous foundation, Self-determination Theory (SDT). VCS, like SDT, posits a minimal set of factors (personalisation, cybersecurity competence, and connectedness to cybersecurity expertise) that are necessary for improving and sustaining the quality of cybersecurity engagement regardless of the target groups' setting. Therefore, ignoring these factors can cause a lack of will to adherence to cybersecurity recommendations across all target groups. The author calls them basic cybersecurity needs for supporting appropriate cybersecurity behaviour.

Given that VCS is new, potential avenues for future research remain. It is hoped that VCS inspires other scholars studying cybersecurity behaviours to extend this line of study. The researcher suggests that future studies can identify and examine additional factors (i.e., derived from other kernel theories) that may be relevant to volitional active cybersecurity behaviour. Also, VCS should be validated in distinctly different contexts. It can help us understand much more about adherence to cybersecurity solutions.

Reflections on the heterogeneous context. This study was performed in the context of small and medium-sized enterprises (SMEs). The literature predominantly considers SMEs as a unitary type of company and offers one-size-fits-all advice and solutions. The findings demonstrated that SMEs are heterogeneous (e.g., varied cybersecurity competence, vulnerability, business model) and focusing on organisation size may not sufficiently predict the cybersecurity needs of SMEs. Therefore, we ceased proposing the same solutions for different SMEs. This research surfaced a diversity of cybersecurity needs and vulnerabilities. Understanding this diversity offered the notion of classification and identifying the improvement needs for each class. According to VCS, the *SME Cybersecurity Competence*

Classification and proposing solutions that are integrated with the needs and competence level of each class support a better quality of cybersecurity engagement. Because SMEs represent 99% of all businesses in the EU (European Commission), this classification framework makes a significant contribution to the field and explains why cybersecurity interventions that are effective for one class of SMEs are not necessarily effective for another.

The classification framework represents varied types of SMEs. The concepts and the identified needs have been used in the follow-up project (Geiger, 2020). Also, the framework has been considered in the recent European SME guide on information security controls (European Digital SME, 2022). However, it will also be important to assess the classification across a wide range of SMEs. For instance, researchers may use quantitative methodological approaches to examine the classification and the diversity of SMEs that may exist within an industry.

Bibliography

Ahmad, B., Richardson, I., & Beecham, S. (2017). A systematic literature review of social network systems for older adults. In *International Conference on Product-Focused Software Process Improvement*, 482-496, Springer, Cham.

Aigbefo, Q. A., Blount, Y., & Marrone, M. (2022). The influence of hardiness and habit on security behaviour intention. *Behaviour & Information Technology*, 41(6), 1151-1170, DOI: 10.1080/0144929X.2020.1856928.

Ajzen, I. (1991). The Theory of Planned Behaviour. *Organisational Behaviour and Human Decision Processes*, 50(2), 179-211.

Akers, R. L. (1990). Rational choice, deterrence, and social learning theory in criminology: The path not taken. In *Crime Opportunity Theories*, 299-322. Routledge.

Alahmari, A., & Duncan, B. (2020). Cybersecurity risk management in small and medium-sized enterprises: A systematic review of recent evidence. In *2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*, 1-5. IEEE.

Albrechtsen, E. (2007). A qualitative study of users' view on information security. *Computers & security*, 26(4), 276-289.

Albrechtsen, E., Hovden, J.(2009). The information security digital divide between information security managers and users. *computers & security,* 28(6), 476-490.

AlHogail, A., & Mirza, A. (2014). A proposal of an organisational information security culture framework. In *Proceedings of International Conference on Information, Communication Technology and System (ICTS),* 243-250. IEEE.

Alohali, M., Clarke, N., Li, F., & Furnell, S. (2018). Identifying and predicting the factors affecting end-users' risk-taking behaviour. *Information & Computer Security*, 26(3), 306–326.

Alotaibi, M., Furnell, S., & Clarke, N. (2016). Information security policies: A review of challenges and influencing factors. In *11th International Conference for Internet Technology and Secured Transactions (ICITST)*, 352-358. IEEE.

Alshaikh, M., Ahmad, A., Maynard, S. B., & Chang, S. (2014). Towards a taxonomy of information security management practices in organisations. *ACIS*.

Amankwa, E., Loock, M., & Kritzinger, E. (2015). Enhancing information security education and awareness: Proposed characteristics for a model. In *the Second International Conference on Information Security and Cyber Forensics*, 72-77.

Ameen, N., Tarhini, A., Shah, M. H., Madichie, N., Paul, J., & Choudrie, J. (2021). Keeping customers' data secure: A cross-cultural study of cybersecurity compliance among the Gen-Mobile workforce. *Computers in Human Behaviour*, 114, 106531.

Ashenden, D., & Sasse, A. (2013). CISOs and organisational culture: Their own worst enemy? *Computers & Security*, 39, 396-405.

Assembly of Behavioural and Social Sciences (US). Panel on Research on Deterrent and Incapacitative Effects, Blumstein, A., Cohen, J., & Nagin, D. (1978). Deterrence and

incapacitation: Estimating the effects of criminal sanctions on crime rates (p. 431). Washington, DC: *National Academy of Sciences*.

Bada, M., Sasse, A., & Nurse, JRC. (2015). Cyber security awareness campaigns: Why do they fail to change behaviour?. *International Conference on Cyber Security for Sustainable Society*, 118-31.

Badampudi, D., Wohlin, C., & Petersen, K. (2015). Experiences from using snowballing and database searches in systematic literature studies. In *Proceedings of the 19th International Conference on Evaluation and Assessment in Software Engineering*, 1-10.

Bakry, S. H. (2003). Development of security policies for private networks. *International Journal of Network Management*, 13(3), 203-210.

Ban, L. Y., & Heng, G. M. (1995). Computer security issues in small and medium-sized enterprises. *Singapore Management Review*, 17(1), 15-29.

Bandura, A. (1977). Self-efficacy: toward a unifying theory of behavioural change. *Psychological review*, 84(2), 191-215.

Bandura, A. (1982). Self-efficacy mechanism in human agency. *American psychologist*, 37(2), 122-147.

Bandura, A., Freeman, W. H., & Lightsey, R. (1999). Self-efficacy: The exercise of control. *Journal of Cognitive Psychotherapy*, 13(2), 158-166.

Barki, H., Paré, G., & Sicotte, C. (2008). Linking IT implementation and acceptance via the construct of psychological ownership of information technology. *Journal of Information Technology*, 23(4), 269-280.

Barlette, Y., Gundolf, K., & Jaouen, A. (2015). Toward a better understanding of SMB CEOs' information security behaviour: Insights from threat or coping appraisal. *Journal of Intelligence Studies in Business*, 5(1).

Barlette, Y., & Jaouen, A. (2019). Information security in SMEs: determinants of CEOs' protective and supportive behaviours. *Systemes d'information management*, 24(3), 7-40.

Barton, K. A., Tejay, G., Lane, M., & Terrell, S. (2016). Information system security commitment: A study of external influences on senior management. *Computers & Security*, 59, 9-25.

Beazley. (2019). Breach Briefing. https://www.ncsc.govt.nz/assets/NCSC-Documents/beazley-breach-briefing-2019.pdf.

Bedrijfsrevisoren, D., Muynck, J.D., & Portesi, S. (2015). Cyber security information sharing: An overview of regulatory and non-regulatory approaches. The European Union Agency for Network and Information Security (ENISA).

Beebe, N. L., & Rao, V. S. (2009). Examination of organisational information security strategy: A pilot study. In *Americas Conference on Information Systems (AMCIS),* USA.

Beheshti, H. M. (2004). The impact of IT on SMEs in the United States. *Information management & computer security*, 12(4), 318-327.

B´elanger, F., Collignon, S., Enget, K., & Negangard, E. (2017). Determinants of early conformance with information security policies. *Information and Management*, 54(7), 887–901. https://doi.org/10.1016/j.im.2017.01.003.

Bennett, R.J., Robinson, S.L.(2000). Development of a measure of workplace deviance. *J. Appl. Psychol,* 85(3), 349-360.

Berry, C. T., & Berry, R. L. (2018). An initial assessment of small business risk management approaches for cyber security threats. *International Journal of Business Continuity and Risk Management*, 8(1), 1-10.

Beyer, M., Ahmed, S., Doerlemann, K., Arnell, S., Parkin, S., Sasse, A.M., Passingham, N. (2015). Awareness is only the first step: A framework for progressive engagement of staff in cyber security. techreport, Hewlett Packard Enterprise, available from https://www.slideshare.net/HPBVEx/awareness-is-only-the-first-step.

Birkás, B., & Bourgue, R. (2013). EISAS-european information sharing and alerting system. European Union Agency for Network and Information Security.

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviours. *MIS quarterly*, 39(4), 837-864.

Bostrom, R. P., & Heinen, J. S. (1977). MIS problems and failures: a socio-technical perspective, part II: the application of socio-technical theory. *MIS quarterly*, 11-28.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative research in psychology*, 3(2), 77-101.

Brocke, J. V., Simons, A., Niehaves, B., Niehaves, B., Reimer, K., Plattfaut, R., & Cleven, A. (2009). Reconstructing the giant: On the importance of rigour in documenting the literature search process. *ECIS 2009 Proceedings*.

Browne, S., Lang, M., & Golden, W. (2015). Linking Threat Avoidance and Security Adoption: A Theoretical Model for SMEs. In *Bled eConference*, 35.

Brunner, M., Mussmann, A., & Breu, R. (2018). Introduction of a tool-based continuous Information Security Management System: An exploratory case study. In *IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C),* 483-490, IEEE.

Brunner, M., Sillaber, C., Breu, R.(2017). Towards automation in information security management systems. In *IEEE International Conference on Software Quality, Reliability and Security (QRS)*, Prague, Czech Republic, 160–167. IEEE.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information Security Policy Compliance: an Empirical Study of Rationality-Based Beliefs and Information Security Awareness. *MIS quarterly*, 34(3), 523-548.

Caldwell, T. (2015). Securing small businesses–the weakest link in a supply chain?. *Computer Fraud & Security*, 2015(9), 5-10.

Caldwell, T. (2016). Making security awareness training work. *Computer Fraud & Security*, 2016(6), 8-14.

Carr, M., & Lesniewska, F. (2020). Internet of Things, cybersecurity and governing wicked problems: learning from climate change governance. *International Relations*, 34(3), 391-412.

Cearley, D.W., Burke, B., Searle, S., Walker, M.J. (2017). Top 10 strategic technology trends for 2018. Gartner.

Chang, H. H., & Chuang, S. S. (2011). Social capital and individual motivations on knowledge sharing: Participant involvement as a moderator. *Information & management*, 48(1), 9-18.

Chang, L. Y., & Coppel, N. (2020). Building cyber security awareness in a developing country: lessons from Myanmar. *Computers & Security*, 97, 101959.

Chapman, P. (2020). Are your IT staff ready for the pandemic-driven insider threat?. *Network Security*, 2020(4), 8-11.

Chen, J. Q., & Benusa, A. (2017). HIPAA security compliance challenges: The case for small healthcare providers. *International Journal of Healthcare Management*, 10(2), 135-146.

Cheng, L., Li, Y., Li, W., Holm, E., & Zhai, Q. (2013). Understanding the violation of IS security policy in organisations: An integrated model based on social control and deterrence theory. *Computers & Security*, 39, 447-459.

Chipperfield, C., & Furnell, S. (2010). From security policy to practice: Sending the right messages. *Computer Fraud & Security*, 2010(3), 13-19.

Choi, S., Martins, J. T., & Bernik, I. (2018). Information security: Listening to the perspective of organisational insiders. *Journal of information science*, 44(6), 752-767.

Cholez, H., & Girard, F. (2014). Maturity assessment and process improvement for information security management in small and medium enterprises. *Journal of Software: Evolution and Process*, 26(5), 496-503.

Choo, K.-K.R.(2011). The cyber threat landscape: Challenges and future research directions. *Computers & Security*, 30(8), 719-731.

Christopherson, K.M.(2007). The positive and negative implications of anonymity in Internet social interactions: ‘‘On the Internet, Nobody Knows You’re a Dog’’. *Computers in Human Behaviour*, 23(6), 3038-3056.

Chua, A., Deans, K., & Parker, C. (2009). Exploring the types of SMEs which could use blogs as a marketing tool: a proposed future research agenda. *Australiasian journal of information systems*, 16(1), 117-136.

Clapper, D., & Richmond, W. (2016). Small business compliance with PCI DSS. *Journal of Management Information & Decision Sciences*, 19(1).

Clarke, R. (1980). Situational crime prevention: Theory and practice. Brit. J. Criminology, 20, 136.

Cleary, G., Corpin, M., Cox, O., Lau, H., Nahorney, B., O'Brien, D., O'Gorman, B., Power, J., Wallace, S., Wood, P., Wueest, C. (2018). Internet Security Threat Report. Volume 23, Symantec Corporation.

Corallo, A., Lazoi, M., Lezzi, M., & Luperto, A. (2022). Cybersecurity awareness in the context of the Industrial Internet of Things: A systematic literature review. *Computers in Industry*, 137, 103614.

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. *Technology Innovation Management Review*, 4(10).

Cram, W. A., Proudfoot, J. G., & D'arcy, J. (2017). Organisational information security policies: a review and research framework. *European Journal of Information Systems*, 26(6), 605-641.

Cranor, L. F. (2008). A framework for reasoning about the human in the loop. In *1st Conference on Usability, Psychology and Security*, San Francisco, CA, USA.

Crossler, R.E., Long, J.H., Loraas, T.M., & Trinkle, B.S. (2014). Understanding compliance with bring your own device policies utilizing protection motivation theory: Bridging the intention-behaviour gap. *Journal of Information Systems*, 28(1), 209-226.

Curricula, C. (2017). Curriculum guidelines for post-secondary degree programs in cybersecurity. A Report in the Computing Curricula Series Joint Task Force on Cybersecurity Education. URL: https://www. slideshare. net/MatthewRosenquist/cybersecurity-curricula-guidelines-for-postsecondarydegree-programs. https://www.acm.org/binaries/content/assets/education/curricula-recommendations/csec2017.pdf.

CyberMDX Philips (2020). Perspectives in Healthcare Security. https://info.cybermdx.com/hubfs/Downloadable%20Assets/CyberMDX%20Philips_Perspectives%20in%20Healthcare%20Security%20Report.pdf.

D'Arcy, J. & Hovav, A. (2007). Deterring Internal Information Systems Misuse. *Communications of the ACM*, 50(10), 113-117.

D'Arcy, J., & Hovav, A. (2009). Does one size fit all? Examining the differential effects of IS security countermeasures. *Journal of business ethics*, 89(1), 59-71.

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information systems research*, 20(1), 79-98.

Da Veiga, A., & Eloff, J.H. (2007). An information security governance framework. *Information systems management*, 24(4), 361-372.

Da Veiga, A., Martins, N., & Eloff, J. H. (2007). Information security culture-validation of an assessment instrument. *Southern African Business Review*, 11(1), 147-166.

Davis, F. D. (1985). A technology acceptance model for empirically testing new end-user information systems: Theory and results (Doctoral dissertation, Massachusetts Institute of Technology).

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS quarterly*, 13(3), 319-340.

Daviter, F. (2017). Coping, taming or solving: alternative approaches to the governance of wicked problems. *Policy Studies*, 38(6), 571-588.

Deci, E.L. (1992). The relation of interest to the motivation of behaviour: A self-determination theory perspective. The role of interest in learning and development, 44.

Deci, E.L., Connell, J.P., & Ryan, R.M.(1989). Self-determination in a work organisation. *Journal of Applied Psychology*, 74 (4), 580-590.

Deci, E.L., Koestner, R., & Ryan, R. M. (1999). A meta-analytic review of experiments examining the effects of extrinsic rewards on intrinsic motivation. *Psychological Bulletin*, 125(6), 692-700.

Deci, E. L., Koestner, R., & Ryan, R. M. (2001). Extrinsic rewards and intrinsic motivation in education: Reconsidered once again. *Review of educational research*, 71(1), 1-27.

Deci, E. L., & Ryan, R. M. (1985). The general causality orientations scale: Self-determination in personality. *Journal of research in personality*, 19(2), 109-134.

Deci, E.L., & Ryan, R. M. (1985). Intrinsic motivation and self-determination in human behaviour. New York: Plenum Publishing Co.

Deci, E.L., Ryan, R. M.(2008). Self-determination theory: a macrotheory of human motivation, development, and health. *Can. Psychol*, 49(3), 182-185.

Deci, E. L., & Ryan, R. M. (2000). The "what" and "why" of goal pursuits: Human needs and the self-determination of behaviour. *Psychological inquiry*, 11(4), 227-268.

Deci, E. L., Ryan, R. M., & Williams, G. C. (1996). Need satisfaction and the self-regulation of learning. *Learning and individual differences*, 8(3), 165-183.

Deming, W.E. (1952). Elementary principles of the statistical control of quality: a series of lectures. Tokyo: Nippon Kagaku Gigutsu Remmei: *Japanese Union of Science and Engineering (JUSE)*.

Dhillon, G. (2001). Violation of safeguards by trusted personnel and understanding related information security concerns. *Computers & security*, 20(2), 165-172.

Dhillon, G., & Backhouse, J. (2001). Current directions in IS security research: towards socio-organisational perspectives. *Information systems journal*, 11(2), 127-153.

Dhillon, G., Torkzadeh, G.(2006). Value-focused assessment of information system security in organisations. *Inf. Syst. J.* 16, 293-314.

DiMaggio, P. J., & Powell, W. W. (1983). The iron cage revisited: Institutional isomorphism and collective rationality in organisational fields. *American sociological review*, 147-160.

Dojkovski, S., Lichtenstein, S., & Warren, M. (2010). Enabling information security culture: influences and challenges for Australian SMEs. In *ACIS 2010: Proceedings of the 21st Australasian Conference on Information Systems*.

Donalds, C., & Osei-Bryson, K. M. (2020). Cybersecurity compliance behaviour: Exploring the influences of individual decision style and other antecedents. *International Journal of Information Management*, 51, 102056.

Dupuis, M., Geiger, T., Slayton, M., & Dewing, F. (2019). The Use and Non-Use of Cybersecurity Tools Among Consumers: Do They Want Help?. In *Proceedings of the 20th Annual SIG Conference on Information Technology Education*, 81-86.

Eisenhardt, K. M. (1989). Agency theory: An assessment and review. *Academy of management review*, 14(1), 57-74.

ENISA. 2010. Training material for SMEs. available from: https://www.enisa.europa.eu/publications/archive/training-material-SMEs

ENISA. 2012. Involving Intermediaries in Cyber-security Awareness Raising, 30 Nov. available from: https://www.enisa.europa.eu/publications/involving-intermediaries-in-cyber-security-awareness-raising

ENISA. (2017). Cybersecurity culture in organisations. European Union Agency for Network and Information Systems, available from: https://www.enisa.europa.eu/publications/cyber-security-culture-in-organisations

ENISA. (2020). European SMEs facing increased cyber threats in changing digital landscape. 23 Nov. available from: https://www.enisa.europa.eu/news/enisa-news/european-smes-facing-increased-cyber-threats-in-a-changing-digital-landscape

Ertmer, P. A., & Newby, T. J. (1993). Behaviourism, cognitivism, constructivism: Comparing critical features from an instructional design perspective. *Performance improvement quarterly*, 6(4), 50-72.

European Commission (2003). What is an SME? available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32003H0361.

European Commission (2019). Supporting specialised skills development: big data, Internet of Things and cybersecurity for SMEs. EASME/COSME/2017/007 Interim Report, March 2019. Available from: https://www.digitalsme.eu/digital/uploads/March-2019_Skills-for-SMEs_Interim_Report_final-version.pdf

Fielder, A., Panaousis, E., Malacaria, P., Hankin, C., & Smeraldi, F. (2016). Decision support approaches for cyber security investment. *Decision support systems*, 86, 13-23.

Fishbein, M., & Ajzen, I. (1975). Belief, attitude, intention, and behaviour: An introduction to theory and research. *Philosophy and Rhetoric*, 10(2).

Franke, U., & Brynielsson, J. (2014). Cyber situational awareness–a systematic review of the literature. *Computers & security*, 46, 18-31.

Furnell, S., & Clarke, N. (2005). Organisational security culture: Embedding security awareness, education, and training. *Proceedings of the IFIP TC11 WG*, 11, 67-74.

Furnell, S., & Clarke, N. (2012). Power to the people? The evolving recognition of human aspects of security. *Computers & Security*, 31(8), 983-988.

Furnell, S., Gennatou, M., & Dowland, P.S. (2002). A prototype tool for information security awareness and training. *Logistics Information Management*, 15(5/6), 352-357.

Gal-Or, E., & Chose, A. (2005). The economic incentives for sharing security information. *Information Systems Research*, 16 (2), 186-208.

Gardner, B., Thomas, V. (2014). Building an Information Security Awareness Program: Defending Against Social Engineering and Technical Threats. Elsevier/Syngress, Amsterdam.

Garg, V., Camp, L. J., Connelly, K., & Lorenzen-Huber, L. (2012). Risk communication design: Video vs. text. In *International Symposium on Privacy Enhancing Technologies Symposium*, 279-298. Springer, Berlin, Heidelberg.

Geer, D., Hoo, K. S., & Jaquith, A. (2003). Information security: Why the future belongs to the quants. *IEEE Security & Privacy*, 1(4), 24-32.

Gefen, D.(2000). E-Commerce: the role of familiarity and trust. Omega, 28(6), 725–737.

GEIGER Consortium. (2020). GEIGER Project Website. https://project.cyber-geiger.eu/.

Ghobadian, A., & Gallear, D. N. (1996). Total quality management in SMEs. Omega, 24(1), 83-106.

Gist, M. E., & Mitchell, T. R. (1992). Self-efficacy: A theoretical analysis of its determinants and malleability. *Academy of Management review*, 17(2), 183-211.

Glaspie, H. W., & Karwowski, W. (2017). Human factors in information security culture: A literature review. In *International Conference on Applied Human Factors and Ergonomics*, 269-280. Springer, Cham.

Goucher, W.(2011). Do SMEs have the right attitude to security? *Computer Fraud & Security*, 2011(7), 18-20.

Gregor, S., & Hevner, A. R. (2013). Positioning and presenting design science research for maximum impact. *MIS quarterly*, 337-355.

Gundu, T. (2019). Acknowledging and reducing the knowing and doing gap in employee cybersecurity complaince. In *ICCWS 14th International Conference on Cyber Warfare and Security*, 94-102.

Gundu, T., & Flowerday, S. V. (2012). The enemy within: A behavioural intention model and an information security awareness process. In *2012 Information Security for South Africa*, 1-8. IEEE.

Gundu, T., & Flowerday, S.V. (2013). Ignorance to awareness: towards an information security awareness process. *South African Institute of Electrical Engineering*, 104(2), 69-79.

Guo, K. H., & Yuan, Y. (2012). The effects of multilevel sanctions on information security violations: A mediating model. *Information & management*, 49(6), 320-326.

Gupta, A., & Hammond, R. (2005). Information systems security issues and decisions for small businesses: an empirical examination. *Information Management & Computer Security*, 13(4), 297-310. https://doi.org/10.1108/09685220510614425

Haeussinger, F., & Kranz, J. (2017). Antecedents of Employees' Information Security Awareness – Review, Synthesis, and Directions for Future Research. In *European Conference on Information Systems*, 1-20.

Hagen, B., Zucchella, A., Cerchiello, P., & De Giovanni, N. (2012). International strategy and performance—Clustering strategic types of SMEs. *International Business Review*, *21*(3), 369-382.

Hagen, J.M., & Albrechtsen, E. (2009). Effects on employees' information security abilities by e-learning. Information Management & Computer Security, 17(5), 338-407.

Han, B., Wu, Y. A., & Windsor, J. (2014). User's adoption of free third-party security apps. *Journal of Computer Information Systems*, 54(3), 77-86.

Hassan, N. H., Ismail, Z., & Maarop, N. (2015). Information Security Culture: A systematic literature review. *Proceedings of the 5th International Conference on Computing and Informatics*, (205), 456–463. https://doi.org/10.4018/IJCWT.2015040103

Hayes, J.(2002). The Theory and Practice of Change Management. Palgrave, New York.

Heidt, M., Gerlach, J. P., & Buxmann, P. (2019). Investigating the security divide between SME and large companies: How SME characteristics influence organisational IT security investments. *Information Systems Frontiers*, 21(6), 1285-1305.

Herath, T., & Rao, H. R. (2009). Encouraging information security behaviours in organisations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, 47(2), 154-165.

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems*, 18(2), 106-125.

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS quarterly*, 28(1), 75-105.

Higgins, E. T. (1998). Promotion and prevention: Regulatory focus as a motivational principle. *In Advances in experimental social psychology*, 30, 1-46. Academic Press.

HM Government, UK. (2014). Cyber Essentials Scheme: Requirements for basic technical protection from cyber-attacks. June 2014. Guidance, Business and management.

Hong, Y., & Furnell, S. (2022). Motivating information security policy compliance: Insights from perceived organisational formalization. *Journal of Computer Information Systems*, 62(1), 19-28.

Hope, K. (2019). Annual Report on European SMEs 2018/2019. European Commission. DOI:10.2826/500457.

Hosmer, L. T. (1995). Trust: The connecting link between organisational theory and philosophical ethics. *Academy of management Review*, 20(2), 379-403.

Huang, R., Zmud, R.W. & Price, L.R. (2010). Influencing the effectiveness of IT governance practices through steering committees and communication policies. *European Journal of Information Systems*, 19(3), 288-302.

Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information & Management*, 51(1), 69-79.

Igbaria, M., & Iivari, J. (1995). The effects of self-efficacy on computer usage. *Omega*, 23(6), 587-605.

Jarvinen, P.H. (2001). Research questions guiding selection of an appropriate research method. *Proceedings of the 8th Information Security Management and Small Systems Security Conference*, Las Vegas, September 27-28.

Johnston, A. C., Warkentin, M., & Siponen, M. (2015). An enhanced fear appeal rhetorical framework. *MIS quarterly*, 39(1), 113-134.

Julisch, K. (2013). Understanding and overcoming cyber security anti-patterns. *Computer Networks*, 57(10), 2206-2211.

Kabanda, S., Tanner, M., & Kent, C. (2018). Exploring SME cybersecurity practices in developing countries. *Journal of Organisational Computing and Electronic Commerce*, 28(3), 269-282.

Kankanhalli, A., Teo, H. H., Tan, B. C., & Wei, K. K. (2003). An integrative study of information systems security effectiveness. *International journal of information management*, 23(2), 139-154.

Kapur, M., Bahl, M., Tutieja, A., Gupta, S., Gupta, A. (2015). Cybercrime Survey Report 2015. KPMG in India.

Karjalainen, M., Siponen, M., Puhakainen, P. and Sarker, S. (2013). One size does not fit all: different cultures require different information systems security interventions. *PACIS 2013 Proceedings*, Jeju Island, 98.

Karlsson, F., Åström, J., & Karlsson, M. (2015). Information security culture: state-of-the-art review between 2000 and 2013. *Information & Computer Security*, 23(3), 246–285.

Kaur, J., & Mustafa, N. (2013). Examining the effects of knowledge, attitude and behaviour on information security awareness: A case on SME. In *International Conference on Research and Innovation in Information Systems (ICRIIS)*, 286-290. IEEE.

Keeper & Ponemon. (2019). Global State of Cybersecurity in Small and Medium-Sized Businesses. Exclusive Research Report, available from: https://start.keeper.io/2019-ponemon-report.

Ki-Aries, D., & Faily, S. (2017). Persona-centred information security awareness. *Computers & Security*, 70, 663-674.

Kirsch, L., & Boss, S. (2007). The last line of defense: motivating employees to follow corporate security guidelines. *In Proceedings of the 28th International Conference on Information Systems (ICIS)*, 103.

Kitchenham, B., Brereton, O. P., Budgen, D., Turner, M., Bailey, J., & Linkman, S. (2009). Systematic literature reviews in software engineering–a systematic literature review. *Information and software technology*, 51(1), 7-15.

Kitchenham, B., & Charters, S. (2007). Guidelines for performing systematic literature reviews in software engineering. *Technical Report EBSE-2007-01*, Keele University.

Klein, H.K. and Myers, M.D. (1999). A set of principles for conducting and evaluating interpretive field studies in information systems. *MIS quarterly*, 23(1),67-93.

Knapp, K.J., Marshall, T.E., Rainer, R.K., & Ford, F.N. (2007). Information security: management's effect on culture and policy. *Information Management & Computer Security*, 14(1), 24-36.

Knapp, K.J., Marshall, T.E., Rainer, R.K., Morrow, D.W. (2006). The top information security issues facing organisations: What can government do to help. *Network security*, 1, 327.

Kraemer, S., Carayon, P., & Clem, J. (2009). Human and organisational factors in computer and information security: Pathways to vulnerabilities. *Computers & security*, 28(7), 509-520.

Kuppusamy, P., Samy, G. N., Maarop, N., Magalingam, P., Kamaruddin, N., Shanmugam, B., & Perumal, S. (2020). Systematic literature review of information security compliance behaviour theories. *Journal of physics: conference series*, 1551(1), p. 012005. IOP Publishing.

Kurpjuhn, T. (2015). The SME security challenge. *Computer Fraud & Security*, 2015(3), 5-7.

Lacey, D. (2010). Understanding and transforming organisational security culture. *Information Management & Computer Security*, 18(1), 4-13.

Lallie, H. S., Shepherd, L. A., Nurse, J. R., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & Security*, 105, 102248.

Landis, J.R., Koch, G.G. (1977). The measurement of observer agreement for categorical data. *Biometrics*, 33, 159–174.

Lange, T., Ottens, M., & Taylor, A. (2000). SMEs and barriers to skills development: a Scottish perspective. *Journal of European industrial training*, 24(1), 5-11.

Lazarus, R. S. (1993). Coping theory and research: Past, present, and future. *Psychosomatic Medicine*, 55, 2324-2347.

Lebek, B., Uffen, J., Breitner, M. H., Neumann, M., & Hohler, B. (2013). Employees' information security awareness and behaviour: A literature review. In *46th Hawaii International Conference on System Sciences*, 2978-2987. IEEE.

Lebek, B., Uffen, J., Neumann, M., Hohler, B., Breitner, M. H. (2014). Information security awareness and behaviour: a theory-based literature review. *Management Research Review*, 37(12),1049-1092.

Lee, A.S. and Baskerville, R.L. (2003). Generalising generalisability in information systems research. *Information systems research*, 14(3), 221-243.

Lee, S.M., Lee, S.G., & Yoo, S. (2004). An integrative model of computer abuse based on social control and general deterrence theories. *Information & Management*, 41(6), 707-718.

Lee, Y. (2003). The technology acceptance model: past, present and future. *Communication of the Association of Information Systems*, 12(50), 752-780.

Lee, Y., & Larsen, K. R. (2009). Threat or coping appraisal: determinants of SMB executives' decision to adopt anti-malware software. *European Journal of Information Systems*, 18(2), 177-187. https://doi.org/10.1057/ejis.2009.11

Lewis, R., Louvieris, P., Abbott, P., Clewley, N., & Jones, K. (2014). Cybersecurity information sharing: A framework for sustainable information security management in UK SME supply chains. In *proceedings of the European Conference on Information Systems (ECIS)*.

Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behaviour. *International Journal of Information Management*, 45, 13-24.

Li, L., Xu, L., He, W., Chen, Y., & Chen, H. (2016). Cyber security awareness and its impact on employee's behaviour. In *International Conference on Research and Practical Issues of Enterprise Information Systems*, 103-111. Springer, Cham.

Liang, H., & Xue, Y. (2009). Avoidance of information technology threats: A theoretical perspective. *MIS quarterly*, 33(1), 71-90.

Lloyd, G. (2020). Expert view: five steps to cyber-safety. SME Guidance for Business Growth. May 6, available from: https://www.smeweb.com/2020/05/06/expert-view-five-steps-to-cyber-safety/

LogMeIn (2020). Psychology of passwords. Available from: https://lp-cdn.lastpass.com/lporcamedia/document-library/lastpass/pdf/en/LastPass-B2C-Assets-Ebook.pdf.

Lopes, I., & Oliveira, P. (2014). Understanding information security culture: a survey in small and medium sized enterprises. In *New Perspectives in Information Systems and Technologies*, Volume 1, 277-286. Springer, Cham.

Mahfuth, A., Yussof, S., Baker, A. A., & Ali, N. A. (2017). A systematic literature review: Information security culture. In *International Conference on Research and Innovation in Information Systems (ICRIIS)*, 1-6, IEEE.

Malone, E. F., & Malone, M. J. (2013). The "wicked problem" of cybersecurity policy: analysis of United States and Canadian policy response. *Canadian Foreign Policy Journal*, 19(2), 158-177.

Malwarebytes (2020). Enduring from home, COVID-19's impact on business security. Santa Clara, USA; https://www.malwarebytes.com/resources/files/2020/08/malwarebytes_enduringfromhome_report_final.pdf.

Manso, C. G., Rekleitis, E., Papazafeiropoulos, F., & Maritsas, V. (2015). Information security and privacy standards for SMEs. European Union Agency for Network and Information Security (ENISA). https://doi.org/10.2824/829076

Mathieson, K. (1991). Predicting user intentions: comparing the technology acceptance model with the theory of planned behaviour. *Information systems research*, 2(3), 173-191.

McCarthy, B. (2002). New economics of sociological criminology. *Annual Review of Sociology*, 28(1), 417-442.

Menard, P., Bott, G. J., & Crossler, R. E. (2017). User motivations in protecting information security: Protection motivation theory versus self-determination theory. *Journal of Management Information Systems*, 34(4), 1203-1230.

Mijnhardt, F., Baars, T., & Spruit, M. (2016). Organisational characteristics influencing SME information security maturity. *Journal of Computer Information Systems*, 56(2), 106-115. https://doi.org/10.1080/08874417.2016.1117369

Miles, M., & Huberman, M. (1994). Qualitative data analysis: An expanded sourcebook. (2nd ed.). *Thousand Oaks*, CA: Sage.

Moore, S., Keen, E. (2018). Gartner Forecasts Worldwide Information Security Spending to Exceed $124 Billion in 2019. Gartner Press Release, Sydney, Australia.

Morgan, S. (2020). Cyberwarfare In The C-Suite. Cybercrime Magazine, 13 Nov., https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/.

Muller, P., Julius, J., Herr, D., Koch, L., Peycheva, V., & McKiernan, S.(2017). Annual report on European SMEs 2016/2017: Focus on self-employment. European Commission.

Muronga, K., Herselman, M., Botha, A., & Da Veiga, A. (2019). An analysis of assessment approaches and maturity scales used for evaluation of information security and cybersecurity user awareness and training programs: A scoping review. In *Conference on Next Generation Computing Applications (NextComp)*, 1-6.

Ni, S., Qian, Q., & Zhang, R. (2018). Malware identification using visualization images and deep learning. *Computers & Security*, 77, 871-885.

NIST. (1996). An Introduction to Computer Security: The NIST Handbook. Special Publication 800-12. National Institute of Standards and Technology, Technology Administration. U.S. Department of Commerce.

Njenga, K. & Jordaan, P. (2016). We want to do it our way: The neutralisation approach to managing information systems security by small businesses. *The African Journal of Information Systems*, 8(1), 42-63.

Ntouskas, T., Papanikas, D., & Polemi, N. (2012). A collaborative system offering security management services for SMEs/mEs. In Georgiadis, C.K., Jahankhani, H., Pimenidis, E., Bashroush, R., Al-Nemrat, A. (eds.) *e-Democracy/ICGS3* -2011. LNICSSITE, 99, 220–228. Springer, Heidelberg. https://doi.org/10.1007/978-3-642-33448-1_30

Nurdiani, I., Börstler, J., & Fricker, S. A. (2016). The impacts of agile and lean practices on project constraints: A tertiary study. *Journal of Systems and Software*, 119, 162-183.

Nurse, J. R., Creese, S., Goldsmith, M., & Lamberts, K. (2011). Trustworthy and effective communication of cybersecurity risks: A review. In *1st Workshop on Socio-Technical Aspects in Security and Trust (STAST)*, 60-68, IEEE.

OECD (2017). Enhancing the contributions of SMEs in a global and digitalised economy. Paris 7-8 June 2017, available from: https://www.oecd.org/industry/C-MIN-2017-8-EN.pdf

Okere, I., Van Niekerk, J., & Carroll, M. (2012). Assessing information security culture: A critical analysis of current approaches. In *Information Security for South Africa*, 1-8, IEEE.

Omidosu, J., & Ophoff, J. (2016). A theory-based review of information security behaviour in the organisation and home context. In *International Conference on Advances in Computing and Communication Engineering (ICACCE)*, 225-231, IEEE.

Osborn, E. (2015). Business versus technology: Sources of the perceived lack of cyber security in SMEs. In *the 1st Int. Conference on Cyber Security for Sustainable Society*.

Ozkan, B.Y. & Spruit, M. (2018). A questionnaire model for cybersecurity maturity assessment of critical infrastructures. In *International Workshop on Information and Operational Technology Security Systems*, 49-60. Springer, Cham, https://doi.org/10.1007/978-3-030-12085-6_5.

Ozkan, B.Y., van Lingen, S., & Spruit, M. (2021). The Cybersecurity Focus Area Maturity (CYSFAM) Model. *Journal of Cybersecurity and Privacy*, 1(1), 119-139. https://doi.org/10.3390/jcp1010007

Padayachee, K. (2012). Taxonomy of compliant information security behaviour. *Computers & Security*, 31(5), 673–680. https://doi.org/10.1016/j.cose.2012.04.004.

Pahnila, S., Siponen, M., Mahmood, A. (2007). Employees' behaviour towards IS security policy compliance. In *40th Annual Hawaii International Conference on System Sciences (HICSS 2007)*, Hawaii, USA, 156-166. IEEE.

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., & Zwaans, T. (2017). The human aspects of information security questionnaire (HAIS-Q): two further validation studies. *Computers & Security*, 66, 40-51.

Parsons, K. M., Young, E., Butavicius, M. A., McCormac, A., Pattinson, M. R., & Jerram, C. (2015). The influence of organisational information security culture on information security decision making. *Journal of Cognitive Engineering and Decision Making*, 9(2), 117-129.

Patton, M.Q. (1990). Qualitative evaluation and research methods. SAGE Publications, inc.

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of management information systems*, 24(3), 45-78.

Pham, H. C., Pham, D. D., Brennan, L., & Richardson, J. (2017). Information security and people: A conundrum for compliance. *Australasian Journal of Information Systems*, 21, 1-16.

Ponemon Institute (2018). Cost of a Data Breach Study: Global Overview. Benchmark Research Report, Ponemon Institute.

Ponsard, C., Grandclaudon, J., & Bal, S. (2019). Survey and Lessons Learned on Raising SME Awareness about Cybersecurity. In *5th Int. Conf. on Information Systems Security and Privacy (ICISSP)*, 558-563, Prague.

PricewaterhouseCoopers LLP (UK). (2010). Information security breaches survey 2010. available from: https://pwc.blogs.com/files/isbs-2010-report-final.pdf.

Puhakainen, P., Petri Puhakainen, C. D., & Ahonen, R. (2006). Design theory for information security awareness. Faculty of Science, University of Oulu, Finland.

Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: an action research study. *MIS Q.* 34(4), 757-778.

Rehder, B., & Burnett, R. C. (2005). Feature inference and the causal structure of categories. *Cognitive psychology*, 50(3), 264-314.

Renaud, K. (2016). How smaller businesses struggle with security advice. *Computer Fraud and Security*, 2016(8), 10-18.

Renaud, K., & Ophoff, J. (2021). A cyber situational awareness model to predict the implementation of cyber security controls and precautions by SMEs. *Organisational Cybersecurity Journal: Practice, Process and People*.

Renaud, K., Von Solms, B., & Von Solms, R. (2019). How does intellectual capital align with cyber security?. *Journal of Intellectual Capital*.

Renaud, K., & Weir, G. R. (2016). Cybersecurity and the Unbearability of Uncertainty. In *2016 Cybersecurity and Cyberforensics Conference (CCC)*, 137-143, IEEE. https://doi.org/10.1109/CCC.2016.29

Rhee, H., Kim, C. and Ryu, Y. (2009). Self-efficacy in information security: its influence on end users' information security practice behaviour. *Computers & Security*, 28(8), 816-826.

Rippetoe, P. A., & Rogers, R. W. (1987). Effects of components of protection motivation theory on adaptive and maladaptive coping with a health threat. *Journal of personality and social psychology*, 52(3), 596.

Robinson, N., & Disley, E. (2010). Incentives and Challenges for Information Sharing in the Context of Network and Information Security. European Network and Information Security Agency (ENISA).

Rogers, R. (1983). Cognitive and physiological processes in fear-based attitude change: A revised theory of protection motivation. In C. J & R. Petty (Eds.), Social psychophysiology: A sourcebook,153-176. New York: Guilford Press.

Rosch, E. (1999). Principles of categorisation, Concepts: core readings, 189. https://doi.org/10.1016/B978-1-4832-1446-7.50028-5.

Ross, S., & Masters, R. (2011). Creating a Culture of Security, ISACA, available from: www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Creating-a-Culture-of-Security.aspx.

Runeson, P., Höst, M., Rainer, A., Regnell, B.(2012). Case Study Research in Software Engineering: Guidelines and Examples. Wiley, Hoboken.

Ryan, R. M., & Deci, E. L. (2000). Intrinsic and extrinsic motivations: Classic definitions and new directions. *Contemporary educational psychology*, 25(1), 54-67.

Ryan, R. M., & Deci, E. L.(2000). Self-determination theory and the facilitation of intrinsic motivation, social development, and well-being. *American Psychologist*, 55(1), 68-78.

Sadok, M., Alter, S., & Bednar, P. (2020). It is not my job: exploring the disconnect between corporate security policies and actual security practices in SMEs. *Information & Computer Security*, 28(3), 467-483.

Sadok, M., & Bednar, P. M. (2016). Information Security Management in SMEs: Beyond the IT Challenges. In *HAISA*, 209-219.

Safa, N. S., Von Solms, R., & Futcher, L. (2016). Human aspects of information security in organisations. *Computer Fraud & Security*, 2016(2), 15-18.

Schlienger, T., & Teufel, S. (2005). Tool supported management of information security culture. In *IFIP International Information Security Conference*, 65-77. Springer, Boston, MA.

Schneider, B., & Cheslock, N. (2003). Measuring results: gaining insight on behaviour change strategies and evaluation methods for environmental education, museum, health, and social marketing programs. San Francisco, CA: CoEvolution Institute.

Sherif, E., Furnell, S., & Clarke, N. (2015). Awareness, behaviour and culture: The ABC in cultivating security compliance. In *10th International Conference for Internet Technology and Secured Transactions (ICITST)*, 90- 94, IEEE.

Shih, H. P., Guo, X., Lai, K. H., & Cheng, T. C. E. (2016). Taking promotion and prevention mechanisms matter for information systems security policy in Chinese SMEs. In *2nd International Conference on Information Management (ICIM)*, 110-115. IEEE.

Shojaifar, A., Fricker, S., & Gwerder, M. (2018). Elicitation of SME requirements for cybersecurity solutions by studying adherence to recommendations. In *REFSQ*.

Shojaifar, A., Fricker, S., & Gwerder, M. (2020). Automating the Communication of Cybersecurity Knowledge: Multi-Case Study. In *IFIP World Conference on Information Security Education*, 110-124, Springer, Cham. https://doi.org/10.1007/978-3-030-59291-2_8

Sieger, J. (2021). Cyberspace, the 21st century battleground. FRANCE 24, 13 Sep; https://www.france24.com/en/tv-shows/tech-24/20210913-cyberspace-the-21st-century-battleground.

Siponen, M., Mahmood, M.A., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information and Management*, 51(2), 217–224. https://doi.org/10.1016/j.im.2013.08.006.

Siponen, M., & Pahnila, S. (2010). Compliance with Information Security Policies: An Empirical Investigation. *Computer*, 43(2), 64-71.

Siponen, M., Pahnila, S., & Mahmood, A. (2007). Employees' adherence to information security policies: an empirical study. In *IFIP International Information Security Conference*, 133-144, Springer, Boston, MA.

Siponen, M., & Vance, A. (2010). Neutralization: New insights into the problem of employee information systems security policy violations. *MIS quarterly*, 34(3), 487-502.

Smith, E. E., & Medin, D. L. (2013). Categories and concepts. In Categories and Concepts. Harvard University Press.

Smith, M. (2016). Huge Rise in Hacker Attacks as Cyber-Criminals Target Small Businesses. The Guardian, 8 Feb; https://www.theguardian.com/small-business-network/2016/feb/08/huge-rise-hack-attacks-cyber-criminals-target-small-businesses.

Smit, T., van Haastrecht, M., & Spruit, M. (2021). The effect of countermeasure readability on security intentions. *Journal of Cybersecurity and Privacy*, 1(4), 675-704.

Solomon, G., & Brown, I. (2020). The influence of organisational culture and information security culture on employee compliance behaviour. *Journal of Enterprise Information Management*, 34(4), 1203-1228.

Sommestad, T., Hallberg, J., Lundholm, K., & Bengtsson, J. (2014). Variables influencing information security policy compliance: A systematic review of quantitative studies. *Information Management & Computer Security,* 22(1), 42-75.

Sommestad, T., Karlzén, H., & Hallberg, J. (2015). The sufficiency of the theory of planned behaviour for explaining information security policy compliance. *Information & Computer Security*.

Song, J. (2016). Why Hackers Want to Attack Your Small Business. Tech.co, 13 Jan. https://tech.co/news/hackers-want-attack-small-business-2016-01.

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management*, 36(2), 215-225.

Spinellis, D., Kokolakis, S., & Gritzalis, S. (1999). Security requirements, risks and recommendations for small enterprise and home-office environments. *Information Management & Computer Security*, 7(3), 121-128.

Spruit, M., & Röling, M. (2014). ISFAM: the information security focus area maturity model. *ECIS*.

Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviours. *Computers & security*, 24(2), 124-133.

Stobert, E., & Biddle, R. (2014). The password life cycle: user behaviour in managing passwords. In *10th Symposium on Usable Privacy and Security (SOUPS), USENIX*, 243-255.

Straub, D.W. (1990). Effective IS security: An empirical study. *Information systems research*, 1(3), 255-276.

Straub, D.W., & Welke, R. J. (1998). Coping with systems risk: Security planning models for management decision making. *MIS quarterly*, 22(4), 441-469.

Sultan, N. A. (2011). Reaching for the "cloud": How SMEs can manage. *International journal of information management*, 31(3), 272-278.

The European Digital SME Alliance. (2022). SME Guide on Information Security Controls. Available from: https://www.digitalsme.eu/new-sme-guide-on-information-security-controls/.

The European Digital SME Alliance. (2020). The EU Cybersecurity Act and the Role of Standards for SMEs, Technical Report. Brussels.

Thomson, K., & Van Niekerk, J. (2012). Combating information security apathy by encouraging prosocial organisational behaviour. *Information Management & Computer Security*.

Topa, I., & Karyda, M. (2015). Identifying factors that influence employees' security behaviour for enhancing ISP compliance. In *International Conference on Trust and Privacy in Digital Business*, 169-179. Springer, Cham.

Tryfonas, T., Kiountouzis, E., & Poulymenakou, A. (2001). Embedding security practices in contemporary information systems development approaches. *Information Management & Computer Security*, 9(4), 183-197.

Tsohou, A., Karyda, M., & Kokolakis, S. (2015). Analyzing the role of cognitive and cultural biases in the internalisation of information security policies: Recommendations for information security awareness programs. *Computers & security*, 52, 128-141.

Tsohou, A., Karyda, M., Kokolakis, S., Kiountouzis, E. (2012). Analysing trajectories of information security awareness. *Information Technology & People*, 25(3), 327-352.

UK Gov. (2018), Cyber essentials self-assessment, https: //www.cyberessentials.ie/self-assessment.

Vallerand, R. J. (1997). Toward a hierarchical model of intrinsic and extrinsic motivation. *Advances in experimental social psychology*, 29, 271-360.

Valli, C., Martinus, I.C., Johnstone, M.N.(2014). Small to Medium Enterprise Cyber Security Awareness: an initial survey of Western Australian Business.

Van Haastrecht, M., Sarhan, I., Shojaifar, A., Baumgartner, L., Mallouli, W., & Spruit, M. (2021). A Threat-Based Cybersecurity Risk Assessment Approach Addressing SME Needs. In *The 16th International Conference on Availability, Reliability and Security*, 1-12.

Van Noorden, R. (2015). Interdisciplinary research by the numbers. *Nature*, 525(7569), 306-307.

Venkatesh, V., & Davis, F. D. (2000). A theoretical extension of the technology acceptance model: Four longitudinal field studies. *Management science*, 46(2), 186-204.

Verizon (2021). Learn to protect your organisation from cyberthreats. Data Breach Investigations Report; https://www.verizon.com/business/resources/reports/dbir/.

Walsham, G. (1995). Interpretive case studies in IS research: nature and method. *European Journal of information systems*, 4(2), 74-81.

Warren, M. J. (2002). Security practice: survey evidence from three countries. *Logistics Information Management*, 15(5/6), 347-351.

Weber, E. P., & Khademian, A. M. (2008). Wicked problems, knowledge challenges, and collaborative capacity builders in network settings. *Public administration review*, 68(2), 334-349.

West, R. (2008). The psychology of security. Communications of the ACM, 51(4), 34-40.

Wieringa, R. (2009). Design science as nested problem solving. In *Proceedings of the 4th international conference on design science research in information systems and technology*, 1-12.

Wieringa, R. J., & Heerkens, J. M. (2006). The methodological soundness of requirements engineering papers: a conceptual framework and two case studies. *Requirements engineering*, 11(4), 295-307.

Wieringa, R., Maiden, N., Mead, N., & Rolland, C. (2006). Requirements engineering paper classification and evaluation criteria: a proposal and a discussion. *Requirements engineering*, 11(1), 102-107.

Wiley, A., McCormac, A., & Calic, D. (2020). More than the individual: Examining the relationship between culture and Information Security Awareness. *Computers & Security*, 88, 101640.

Wilson, M. and Hash, J. (2003). Building an Information Technology Security Awareness and Training Program. Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD, Available from: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=151287.

Wohlin, C. (2014). Guidelines for snowballing in systematic literature studies and a replication in software engineering. In *Proceedings of the 18th international conference on evaluation and assessment in software engineering*, 1-10.

Wohlin, C. (2016). Second-generation systematic literature studies using snowballing. In *Proceedings of the 20th International Conference on Evaluation and Assessment in Software Engineering*, 1-6.

Wong, L. W., Lee, V. H., Tan, G. W. H., Ooi, K. B., & Sohal, A. (2022). The role of cybersecurity and policy awareness in shifting employee compliance attitudes: Building supply chain capabilities. *International Journal of Information Management*, 66, 102520.

Wood, P., Nahorney, B., Chandrasekar, K., Wallace, S., Haley, K., Davis, M., Rankin, S. (2016). Internet Security Threat Report. Symantec Corporation, Volume 21.

Yin, R.K.(2009). Case Study Research: Design and Methods, 4th edn. Sage, Thousand Oaks.

Yoon, C., & Rolland, E. (2012). Knowledge-sharing in virtual communities: familiarity, anonymity and self-determination theory. *Behaviour & Info Tech,* 31(11), 1133-1143.

Zec, M., & Kajtazi, M. (2015). Examining how IT professionals in SMEs take decisions about implementing cyber security strategy. In *ECIME 2015- 9th European Conference on IS Management and Evaluation: ECIME*, 231.

Publication List

Included in the dissertation

Shojaifar, A., Fricker, S., Spruit, M. (2023) (submitted). Adherence to Information Security Practices in Small and Medium-Sized Enterprises. (Under revision for journal publication)

Fricker, S., Shojaifar, A. (2022). Self-endorsed Cybersecurity Capability Improvement for SMEs. In Proceedings of the 28th annual Americas Conference on Information Systems (AMCIS 2022), Minneapolis. Association for Information Systems.

Shojaifar, A., Fricker, S., & Gwerder, M. (2020). Automating the Communication of Cybersecurity Knowledge: Multi-Case Study. In IFIP World Conference on Information Security Education (pp. 110-124). Springer, Cham.

Shojaifar, A., & Fricker, S. (2020). SMEs' Confidentiality Concerns for Security Information Sharing. In International Symposium on Human Aspects of Information Security and Assurance (pp. 289-299). Springer, Cham.

Shojaifar, A., & Fricker, S. A. (2023). Design and Evaluation of a Self-paced Cybersecurity Tool. Information & Computer Security, 31(2), 244-262.

Shojaifar, A., & Järvinen, H. (2021). Classifying SMEs for Approaching Cybersecurity Competence and Awareness. In The 16th International Conference on Availability, Reliability and Security (pp. 1-7).

Other publications (not included)

van Haastrecht, M., Sarhan, I., Shojaifar, A., Baumgartner, L., Mallouli, W., & Spruit, M. (2021). A threat-based cybersecurity risk assessment approach addressing SME needs. In The 16th International Conference on Availability, Reliability and Security (pp. 1-12).

Shojaifar, A., Fricker, S. and Gwerder, M. (2018). Elicitation of SME requirements for cybersecurity solutions by studying adherence to recommendations. In REFSQ.

Shojaifar, A. (2019). SMEs confidentiality issues and adoption of good cybersecurity practices. IFIP Summer School on Privacy and Identity Management. arXiv preprint arXiv:2007.08201.

Summary

This dissertation introduces the “Volitional Cybersecurity” (VCS) theory as a systematic way to think about adoption and manage long-term adherence to cybersecurity approaches. The validation of VCS has been performed in small- and medium-sized enterprises or businesses (SMEs/SMBs) context. The focus on volitional activities promotes theoretical viewpoints. Also, it aids in demystifying the aspects of cybersecurity behaviour in heterogeneous contexts that have neither been systematically elaborated in prior studies nor embedded in cybersecurity solutions.

Abundant literature demonstrates a lack of adoption of manifold cybersecurity remediations. It is still not adequately clear how to select and compose cybersecurity approaches into solutions for meeting the needs of many diverse cybersecurity-adopting organisations. Moreover, the studied theories in this context mainly originated from disciplines other than information systems and cybersecurity. The constructs were developed based on data, for instance, in psychology or criminology, that seem not to fit properly for the cybersecurity context. Consequently, discovering new methods and theories that can be of help in active and volitional forms of cybersecurity behaviour in diverse contexts may be conducive to a better quality of cybersecurity engagement. This leads to the main research question of this dissertation:

How can we support volitional forms of behaviour with a self-paced tool to increase the quality of cybersecurity engagement?

The main contribution of this dissertation is the VCS theory. VCS is a cybersecurity-focused theory structured around the core concept of volitional cybersecurity behaviour. It suggests that a context can be classified based on the cybersecurity competence of target groups and their distinct requirements. This classification diminishes the complexity of the context and is predictive of improvement needs for each class. Further, the theory explicates that supporting three factors: A) personalisation, B) cybersecurity competence, and C) connectedness to cybersecurity expertise affect the adoption of cybersecurity measures and better quality of cybersecurity engagement across all classes of the context. Therefore, approaches that ignore the personalisation of cybersecurity solutions, the cybersecurity competence of target groups, and the connectedness of recipients to cybersecurity expertise may lead to poorer acceptance of the value or utility of solutions. Subsequently, it can cause a lack of motivation for adopting cybersecurity solutions and adherence to best practices.

We used the design science research method as the primary method for the construction and utility evaluation of our artefacts (CYSEC and the online consent prototype). This method shaped the chain of chapters in this dissertation structured around the design science research method’s activities. During this research process, we had a sustained connection with 14 SMEs and one SME association from France, Spain, UK, Greece, Italy, and Switzerland. Also, we investigated the qualitative methods. The qualitative research equipped the researcher with a strong means for acquiring tacit knowledge that was of interest and was only available in the minds of CEOs and chief information security officers (CISOs). Therefore, it was possible to identify new constructs, discover some discrepancies, and classify them to facilitate proactive cybersecurity development.

The research process had three consecutive iterations. In iteration 1, we first conducted a systematic literature review to find the current state of the knowledge, gaps, and potential directions for future research. The researcher identified and proposed Self-determination theory (SDT) as the kernel theory in this step. The design of CYSEC was grounded in SDT. To our knowledge, this is the first time SDT has been used for designing cybersecurity self-paced tools. Then we demonstrated the CYSEC prototype in the context of use and conducted the formative evaluation. The researcher had a deductive approach in this step and applied the explanatory multi-case study (observation strategy) and short survey. The formative evaluation provided strong evidence of the efficacy and usefulness of CYSEC, and specific improvement needs. In iteration 2, we designed (based on SDT) and validated an online consent prototype to tackle the challenges of lacking motivation and trust for security information sharing with CYSEC. The researcher applied semi-structured interviews in this step. The findings showed that users' perception of control over information sharing influences their motivation for security information sharing. In Iteration 3, we improved the CYSEC design and added new features according to the feedback in the formative evaluation. A version of CYSEC was placed in operation in real environments for two months, and then we conducted the summative evaluation. In this step, the researcher had an inductive approach and applied a survey study, structured interviews, and conceptual modelling. The study yielded lessons learned about the impacts of CYSEC and the influential factors that affected its usefulness and the quality of cybersecurity engagement. Also, the findings revealed three types of cybersecurity awareness: awareness about cyber threats and the importance of protection, awareness of best cybersecurity practices, and awareness about the dynamic character of cybersecurity. Further, the researcher proposed SME Cybersecurity Competence Classification to reduce communication complexity for approaching awareness and capability improvement.

VCS generates various implications. It has implications for cybersecurity research in heterogeneous contexts to transcend the common cybersecurity compliance approaches. Building on VCS, researchers could develop interventions looking for volitional cybersecurity behaviour change. Also, it provides knowledge that can be useful in the design of self-paced cybersecurity tools. VCS explains why the new self-paced cybersecurity tool needs specific features. The findings of this dissertation have been subsequently applied to the follow-up project design. Further, it has implications for practitioners and service providers to reach out to the potential end-users of their solutions.

Samenvatting

Dit proefschrift introduceert de theorie van “Vrijwillige Cybersecurity” (“Volitional Cybersecurity”; VCS) als een systematische manier om na te denken over de adoptie en het beheer van de langdurige naleving van cybersecurity benaderingen. De validatie van VCS is uitgevoerd in de context van kleine en middelgrote bedrijven (MKB’s). De focus op zelfbepaalde vrijwillige activiteiten bevordert theoretische standpunten. Ook helpt het bij het demystificeren van de aspecten van cybersecuritygedrag in heterogene contexten die niet systematisch zijn uitgewerkt in eerdere studies of ingebed in cybersecurityoplossingen.

Uit de overvloedige literatuur blijkt een gebrek aan adoptie van uiteenlopende cybersecurityoplossingen. Het is nog steeds niet voldoende duidelijk hoe cybersecurity benaderingen moeten worden geselecteerd en ontworpen tot oplossingen die voldoen aan de behoeften van de vele uiteenlopende organisaties die cybersecurity toepassen. Bovendien zijn de bestudeerde theorieën in dit verband hoofdzakelijk afkomstig uit andere disciplines dan informatiesystemen en cybersecurity. De constructen werden ontwikkeld op basis van gegevens, uit bijvoorbeeld de psychologie of de criminologie, die niet goed passen in de cybersecurity context. Bijgevolg kan het ontdekken van nieuwe methoden en theorieën die van nut kunnen zijn bij actieve en vrijwillige vormen van cybersecurity gedrag in diverse contexten bevorderlijk zijn voor een betere kwaliteit van cybersecurity betrokkenheid. Dit leidt tot de belangrijkste onderzoeksvraag van dit proefschrift:

Hoe kunnen we vrijwillig gedrag ondersteunen met een tool op eigen tempo om de betrokkenheid bij cybersecurity te verhogen?

De belangrijkste bijdrage van dit proefschrift is de VCS-theorie. VCS is een op cybersecurity gerichte theorie die is opgebouwd rond het kernconcept van vrijwillig cybersecurity gedrag. Het suggereert dat een context kan worden ingedeeld op basis van de cybersecurity competentie van doelgroepen en hun specifieke vereisten. Deze classificatie vermindert de complexiteit van de context en helpt de verbeteringsbehoeften voor elke klasse te voorspellen. Verder verklaart de theorie dat het ondersteunen van de drie factoren: A) personalisatie, B) cybersecurity competentie, en C) verbondenheid met cybersecurity expertise, van invloed zijn op de adoptie van cybersecurity maatregelen en een betere kwaliteit van cybersecurity betrokkendheid in alle klassen van de context. Daarom kunnen benaderingen die voorbijgaan aan de personalisering van cybersecurity oplossingen, de cybersecurity competentie van doelgroepen, en de verbondenheid van de eindgebruikers met cybersecurity deskundigheid leiden tot een verminderde acceptatie van de waarde of het nut van oplossingen. Vervolgens kan dit leiden tot een gebrek aan motivatie om cybersecurity oplossingen in te voeren en de beste praktijken na te leven.

We gebruikten de design science onderzoeksmethode als primaire methode voor de constructie en gebruiksevaluatie van onze artefacten (CYSEC en het online toestemmingsprototype). Deze methode vormde de keten van hoofdstukken in dit proefschrift, gestructureerd rondom de activiteiten van de design science onderzoeksmethode. Tijdens dit onderzoeksproces hadden we een duurzame relatie met 14 MKB organisaties en één MKB-vereniging uit Frankrijk, Spanje, het VK, Griekenland, Italië en Zwitserland. Ook onderzochten wij middels kwalitatieve methoden. Het kwalitatieve onderzoek verschafte de onderzoeker een sterk middel om de rijke maar veelal impliciete kennis te verkrijgen uit de hoofden van CEO’s

en CISO's. Daardoor werd het mogelijk om nieuwe constructen te identificeren, enkele discrepanties te ontdekken en deze te classificeren, teneinde een proactieve ontwikkeling op het gebied van cybersecurity te vereenvoudigen.

Het onderzoeksproces kende drie opeenvolgende iteraties. In iteratie 1 voerden we eerst een systematische literatuurstudie uit om de huidige stand van de kennis, lacunes en potentiële richtingen voor toekomstig onderzoek te vinden. De onderzoeker identificeerde en stelde de zelfbeschikkingstheorie ('Self-determination Theory'; SDT) voor als de kerntheorie in deze stap. Het ontwerp van CYSEC was gebaseerd op SDT. Voor zover wij weten, is dit de eerste keer dat SDT is gebruikt voor het ontwerpen van zelfhulpmiddelen voor cybersecurity. Vervolgens hebben we het prototype van CYSEC gedemonstreerd in de gebruikscontext en een formatieve evaluatie uitgevoerd. De onderzoeker hanteerde in deze stap een deductieve benadering en paste de verklarende meervoudige case-study (observatiestrategie) en een korte enquête toe. De formatieve evaluatie leverde sterk bewijs voor de werkzaamheid en het nut van CYSEC, en specifieke verbeteringsbehoeften. In iteratie 2 hebben we (op basis van SDT) een online toestemmingsprototype ontworpen en gevalideerd om de uitdagingen van het gebrek aan motivatie en vertrouwen voor het delen van beveiligingsinformatie met CYSEC te adresseren. De onderzoeker paste hierbij semi-gestructureerde interviews toe. Uit de bevindingen bleek dat de perceptie van de gebruikers, met betrekking tot controle over het delen van informatie, van invloed is op hun motivatie voor het delen van beveiligingsinformatie. In Iteratie 3 hebben we het ontwerp van CYSEC verbeterd en nieuwe functies toegevoegd op basis van de feedback in de formatieve evaluatie. Een cloudversie van CYSEC werd gedurende twee maanden in praktijkomgevingen in gebruik genomen en vervolgens voerden wij de summatieve evaluatie uit. In deze stap hanteerde de onderzoeker een inductieve aanpak en paste hij een enquêtestudie, gestructureerde interviews en conceptuele modellering toe. De studie leverde lessen op over de effecten van CYSEC en de invloedrijke factoren die het nut en de kwaliteit van de betrokkenheid bij cybersecurity beïnvloeden. Ook bleek dat er drie soorten cybersecurity bewustzijn bestaan: bewustzijn van cyberdreigingen en het belang van bescherming, bewustzijn van de beste cybersecurity praktijken, en bewustzijn van het dynamische karakter van cybersecurity. Verder stelde de onderzoeker een nieuw classificatiekader voor om de complexiteit van de communicatie voor de aanpak van bewustwording en bekwaamheidsverbetering te verminderen.

VCS genereert meerdere implicaties. Zo heeft het implicaties voor cybersecurity onderzoek in heterogene contexten om de gebruikelijke cybersecurity nalevingsbenaderingen te overstijgen. Op basis van VCS zouden onderzoekers interventies kunnen ontwikkelen die gericht zijn op vrijwillige gedragsverandering op het gebied van cybersecurity. Ook levert het kennis op die nuttig kan zijn bij het ontwerp van zelfstudie-gedreven cybersecurity instrumenten, bijvoorbeeld om te verklaren waarom een nieuw zelfstudie-gedreven cybersecurity instrument specifieke kenmerken nodig heeft. De bevindingen van dit proefschrift zijn vervolgens toegepast op het ontwerp van het vervolgproject. Verder heeft het implicaties voor praktijkmensen en dienstverleners om de potentiële eindgebruikers van hun oplossingen beter te kunnen bereiken.

Curriculum Vitae

Alireza Shojaifar was born in Tehran, Iran, in 1981. He has completed his bachelor's and master's degrees in Iran and Sweden, respectively, in Software Engineering. Then, he started his PhD in October 2017 at the University of Applied Sciences and Arts Northwestern Switzerland School of Engineering and the University of Utrecht, Information and Computing Sciences department. He worked on two research and innovation (Horizon 2020) cybersecurity projects (SMESEC, GEIGER). He also assisted as a volunteer in the IFIP Summer School on Privacy and Identity Management and the 28th IEEE International Requirements Engineering Conference. His article on SME classification was taken up by the European Digital SME Alliance. He proposed Volitional Cybersecurity Theory, a systematic way to think about adoption and manage long-term adherence to cybersecurity approaches. In December 2022, Alireza started his career in the Dutch finance industry, focusing on research on awareness-raising and cybersecurity behaviour change.

SIKS Dissertation Series

2016

01 Syed Saiden Abbas (RUN), Recognition of Shapes by Humans and Machines
02 Michiel Christiaan Meulendijk (UU), Optimizing medication reviews through decision support: prescribing a better pill to swallow
03 Maya Sappelli (RUN), Knowledge Work in Context: User Centered Knowledge Worker Support
04 Laurens Rietveld (VU), Publishing and Consuming Linked Data
05 Evgeny Sherkhonov (UVA), Expanded Acyclic Queries: Containment and an Application in Explaining Missing Answers
06 Michel Wilson (TUD), Robust scheduling in an uncertain environment
07 Jeroen de Man (VU), Measuring and modeling negative emotions for virtual training
08 Matje van de Camp (TiU), A Link to the Past: Constructing Historical Social Networks from Unstructured Data
09 Archana Nottamkandath (VU), Trusting Crowdsourced Information on Cultural Artefacts
10 George Karafotias (VUA), Parameter Control for Evolutionary Algorithms
11 Anne Schuth (UVA), Search Engines that Learn from Their Users
12 Max Knobbout (UU), Logics for Modelling and Verifying Normative Multi-Agent Systems
13 Nana Baah Gyan (VU), The Web, Speech Technologies and Rural Development in West Africa - An ICT4D Approach
14 Ravi Khadka (UU), Revisiting Legacy Software System Modernization
15 Steffen Michels (RUN), Hybrid Probabilistic Logics - Theoretical Aspects, Algorithms and Experiments
16 Guangliang Li (UVA), Socially Intelligent Autonomous Agents that Learn from Human Reward
17 Berend Weel (VU), Towards Embodied Evolution of Robot Organisms
18 Albert Meroño Peñuela (VU), Refining Statistical Data on the Web
19 Julia Efremova (Tu/e), Mining Social Structures from Genealogical Data
20 Daan Odijk (UVA), Context & Semantics in News & Web Search
21 Alejandro Moreno Célleri (UT), From Traditional to Interactive Playspaces: Automatic Analysis of Player Behavior in the Interactive Tag Playground
22 Grace Lewis (VU), Software Architecture Strategies for Cyber-Foraging Systems
23 Fei Cai (UVA), Query Auto Completion in Information Retrieval
24 Brend Wanders (UT), Repurposing and Probabilistic Integration of Data; An Iterative and data model inde pendent approach
25 Julia Kiseleva (TU/e), Using Contextual Information to Understand Searching and Browsing Behavior
26 Dilhan Thilakarathne (VU), In or Out of Control: Exploring Computational Models to Study the Role of Human Awareness and Control in Behavioural Choices, with Applications in Aviation and Energy Management Domains
27 Wen Li (TUD), Understanding Geo-spatial Information on Social Media
28 Mingxin Zhang (TUD), Large-scale Agent-based Social Simulation - A study on epidemic prediction and control
29 Nicolas Höning (TUD), Peak reduction in decentralised electricity systems - Markets and prices for flexible planning
30 Ruud Mattheij (UvT), The Eyes Have It
31 Mohammad Khelghati (UT), Deep web content monitoring
32 Eelco Vriezekolk (UT), Assessing Telecommunication Service Availability Risks for Crisis Organisations
33 Peter Bloem (UVA), Single Sample Statistics, exercises in learning from just one example
34 Dennis Schunselaar (TUE), Configurable Process Trees: Elicitation, Analysis, and Enactment
35 Zhaochun Ren (UVA), Monitoring Social Media: Summarization, Classification and Recommendation
36 Daphne Karreman (UT), Beyond R2D2: The design of nonverbal interaction behaviour optimized for robot-specific morphologies
37 Giovanni Sileno (UvA), Aligning Law and Action - a conceptual and computational inquiry
38 Andrea Minuto (UT), Materials that Matter - Smart Materials meet Art & Interaction Design
39 Merijn Bruijnes (UT), Believable Suspect Agents; Response and Interpersonal Style Selection for an Artificial Suspect

	40	Christian Detweiler (TUD), Accounting for Values in Design
	41	Thomas King (TUD), Governing Governance: A Formal Framework for Analysing Institutional Design and Enactment Governance
	42	Spyros Martzoukos (UVA), Combinatorial and Compositional Aspects of Bilingual Aligned Corpora
	43	Saskia Koldijk (RUN), Context-Aware Support for Stress Self-Management: From Theory to Practice
	44	Thibault Sellam (UVA), Automatic Assistants for Database Exploration
	45	Bram van de Laar (UT), Experiencing Brain-Computer Interface Control
	46	Jorge Gallego Perez (UT), Robots to Make you Happy
	47	Christina Weber (UL), Real-time foresight - Preparedness for dynamic innovation networks
	48	Tanja Buttler (TUD), Collecting Lessons Learned
	49	Gleb Polevoy (TUD), Participation and Interaction in Projects. A Game-Theoretic Analysis
	50	Yan Wang (UVT), The Bridge of Dreams: Towards a Method for Operational Performance Alignment in IT-enabled Service Supply Chains
2017	01	Jan-Jaap Oerlemans (UL), Investigating Cybercrime
	02	Sjoerd Timmer (UU), Designing and Understanding Forensic Bayesian Networks using Argumentation
	03	Daniël Harold Telgen (UU), Grid Manufacturing; A Cyber-Physical Approach with Autonomous Products and Reconfigurable Manufacturing Machines
	04	Mrunal Gawade (CWI), Multi-core Parallelism in a Column-store
	05	Mahdieh Shadi (UVA), Collaboration Behaviour
	06	Damir Vandic (EUR), Intelligent Information Systems for Web Product Search
	07	Roel Bertens (UU), Insight in Information: from Abstract to Anomaly
	08	Rob Konijn (VU) , Detecting Interesting Differences:Data Mining in Health Insurance Data using Outlier Detection and Subgroup Discovery
	09	Dong Nguyen (UT), Text as Social and Cultural Data: A Computational Perspective on Variation in Text
	10	Robby van Delden (UT), (Steering) Interactive Play Behaviour
	11	Florian Kunneman (RUN), Modelling patterns of time and emotion in Twitter #anticipointment
	12	Sander Leemans (TUE), Robust Process Mining with Guarantees
	13	Gijs Huisman (UT), Social Touch Technology - Extending the reach of social touch through haptic technology
	14	Shoshannah Tekofsky (UvT), You Are Who You Play You Are: Modelling Player Traits from Video Game Behaviour
	15	Peter Berck (RUN), Memory-Based Text Correction
	16	Aleksandr Chuklin (UVA), Understanding and Modeling Users of Modern Search Engines
	17	Daniel Dimov (UL), Crowdsourced Online Dispute Resolution
	18	Ridho Reinanda (UVA), Entity Associations for Search
	19	Jeroen Vuurens (UT), Proximity of Terms, Texts and Semantic Vectors in Information Retrieval
	20	Mohammadbashir Sedighi (TUD), Fostering Engagement in Knowledge Sharing: The Role of Perceived Benefits, Costs and Visibility
	21	Jeroen Linssen (UT), Meta Matters in Interactive Storytelling and Serious Gaming (A Play on Worlds)
	22	Sara Magliacane (VU), Logics for causal inference under uncertainty
	23	David Graus (UVA), Entities of Interest — Discovery in Digital Traces
	24	Chang Wang (TUD), Use of Affordances for Efficient Robot Learning
	25	Veruska Zamborlini (VU), Knowledge Representation for Clinical Guidelines, with applications to Multimorbidity Analysis and Literature Search
	26	Merel Jung (UT), Socially intelligent robots that understand and respond to human touch
	27	Michiel Joosse (UT), Investigating Positioning and Gaze Behaviors of Social Robots: People's Preferences, Perceptions and Behaviours
	28	John Klein (VU), Architecture Practices for Complex Contexts
	29	Adel Alhuraibi (UvT), From IT-BusinessStrategic Alignment to Performance: A Moderated Mediation Model of Social Innovation, and Enterprise Governance of IT
	30	Wilma Latuny (UvT), The Power of Facial Expressions
	31	Ben Ruijl (UL), Advances in computational methods for QFT calculations
	32	Thaer Samar (RUN), Access to and Retrievability of Content in Web Archives

	33	Brigit van Loggem (OU), Towards a Design Rationale for Software Documentation: A Model of Computer-Mediated Activity
	34	Maren Scheffel (OU), The Evaluation Framework for Learning Analytics
	35	Martine de Vos (VU), Interpreting natural science spreadsheets
	36	Yuanhao Guo (UL), Shape Analysis for Phenotype Characterisation from High-throughput Imaging
	37	Alejandro Montes Garcia (TUE), WiBAF: A Within Browser Adaptation Framework that Enables Control over Privacy
	38	Alex Kayal (TUD), Normative Social Applications
	39	Sara Ahmadi (RUN), Exploiting properties of the human auditory system and compressive sensing methods to increase noise robustness in ASR
	40	Altaf Hussain Abro (VUA), Steer your Mind: Computational Exploration of Human Control in Relation to Emotions, Desires and Social Support For applications in human-aware support systems
	41	Adnan Manzoor (VUA), Minding a Healthy Lifestyle: An Exploration of Mental Processes and a Smart Environment to Provide Support for a Healthy Lifestyle
	42	Elena Sokolova (RUN), Causal discovery from mixed and missing data with applications on ADHD datasets
	43	Maaike de Boer (RUN), Semantic Mapping in Video Retrieval
	44	Garm Lucassen (UU), Understanding User Stories - Computational Linguistics in Agile Requirements Engineering
	45	Bas Testerink (UU), Decentralized Runtime Norm Enforcement
	46	Jan Schneider (OU), Sensor-based Learning Support
	47	Jie Yang (TUD), Crowd Knowledge Creation Acceleration
	48	Angel Suarez (OU), Collaborative inquiry-based learning
2018	01	Han van der Aa (VUA), Comparing and Aligning Process Representations
	02	Felix Mannhardt (TUE), Multi-perspective Process Mining
	03	Steven Bosems (UT), Causal Models For Well-Being: Knowledge Modeling, Model-Driven Development of Context-Aware Applications, and Behavior Prediction
	04	Jordan Janeiro (TUD), Flexible Coordination Support for Diagnosis Teams in Data-Centric Engineering Tasks
	05	Hugo Huurdeman (UVA), Supporting the Complex Dynamics of the Information Seeking Process
	06	Dan Ionita (UT), Model-Driven Information Security Risk Assessment of Socio-Technical Systems
	07	Jieting Luo (UU), A formal account of opportunism in multi-agent systems
	08	Rick Smetsers (RUN), Advances in Model Learning for Software Systems
	09	Xu Xie (TUD), Data Assimilation in Discrete Event Simulations
	10	Julienka Mollee (VUA), Moving forward: supporting physical activity behavior change through intelligent technology
	11	Mahdi Sargolzaei (UVA), Enabling Framework for Service-oriented Collaborative Networks
	12	Xixi Lu (TUE), Using behavioral context in process mining
	13	Seyed Amin Tabatabaei (VUA), Computing a Sustainable Future
	14	Bart Joosten (UVT), Detecting Social Signals with Spatiotemporal Gabor Filters
	15	Naser Davarzani (UM), Biomarker discovery in heart failure
	16	Jaebok Kim (UT), Automatic recognition of engagement and emotion in a group of children
	17	Jianpeng Zhang (TUE), On Graph Sample Clustering
	18	Henriette Nakad (UL), De Notaris en Private Rechtspraak
	19	Minh Duc Pham (VUA), Emergent relational schemas for RDF
	20	Manxia Liu (RUN), Time and Bayesian Networks
	21	Aad Slootmaker (OUN), EMERGO: a generic platform for authoring and playing scenario-based serious games
	22	Eric Fernandes de Mello Araujo (VUA), Contagious: Modeling the Spread of Behaviours, Perceptions and Emotions in Social Networks
	23	Kim Schouten (EUR), Semantics-driven Aspect-Based Sentiment Analysis
	24	Jered Vroon (UT), Responsive Social Positioning Behaviour for Semi-Autonomous Telepresence Robots
	25	Riste Gligorov (VUA), Serious Games in Audio-Visual Collections
	26	Roelof Anne Jelle de Vries (UT),Theory-Based and Tailor-Made: Motivational Messages for Behavior Change Technology

	27	Maikel Leemans (TUE), Hierarchical Process Mining for Scalable Software Analysis
	28	Christian Willemse (UT), Social Touch Technologies: How they feel and how they make you feel
	29	Yu Gu (UVT), Emotion Recognition from Mandarin Speech
	30	Wouter Beek, The "K" in "semantic web" stands for "knowledge": scaling semantics to the web
2019	01	Rob van Eijk (UL),Web privacy measurement in real-time bidding systems. A graph-based approach to RTB system classification
	02	Emmanuelle Beauxis Aussalet (CWI, UU), Statistics and Visualizations for Assessing Class Size Uncertainty
	03	Eduardo Gonzalez Lopez de Murillas (TUE), Process Mining on Databases: Extracting Event Data from Real Life Data Sources
	04	Ridho Rahmadi (RUN), Finding stable causal structures from clinical data
	05	Sebastiaan van Zelst (TUE), Process Mining with Streaming Data
	06	Chris Dijkshoorn (VU), Nichesourcing for Improving Access to Linked Cultural Heritage Datasets
	07	Soude Fazeli (TUD), Recommender Systems in Social Learning Platforms
	08	Frits de Nijs (TUD), Resource-constrained Multi-agent Markov Decision Processes
	09	Fahimeh Alizadeh Moghaddam (UVA), Self-adaptation for energy efficiency in software systems
	10	Qing Chuan Ye (EUR), Multi-objective Optimization Methods for Allocation and Prediction
	11	Yue Zhao (TUD), Learning Analytics Technology to Understand Learner Behavioral Engagement in MOOCs
	12	Jacqueline Heinerman (VU), Better Together
	13	Guanliang Chen (TUD), MOOC Analytics: Learner Modeling and Content Generation
	14	Daniel Davis (TUD), Large-Scale Learning Analytics: Modeling Learner Behavior & Improving Learning Outcomes in Massive Open Online Courses
	15	Erwin Walraven (TUD), Planning under Uncertainty in Constrained and Partially Observable Environments
	16	Guangming Li (TUE), Process Mining based on Object-Centric Behavioral Constraint (OCBC) Models
	17	Ali Hurriyetoglu (RUN),Extracting actionable information from microtexts
	18	Gerard Wagenaar (UU), Artefacts in Agile Team Communication
	19	Vincent Koeman (TUD), Tools for Developing Cognitive Agents
	20	Chide Groenouwe (UU), Fostering technically augmented human collective intelligence
	21	Cong Liu (TUE), Software Data Analytics: Architectural Model Discovery and Design Pattern Detection
	22	Martin van den Berg (VU),Improving IT Decisions with Enterprise Architecture
	23	Qin Liu (TUD), Intelligent Control Systems: Learning, Interpreting, Verification
	24	Anca Dumitrache (VU), Truth in Disagreement - Crowdsourcing Labeled Data for Natural Language Processing
	25	Emiel van Miltenburg (VU), Pragmatic factors in (automatic) image description
	26	Prince Singh (UT), An Integration Platform for Synchromodal Transport
	27	Alessandra Antonaci (OUN), The Gamification Design Process applied to (Massive) Open Online Courses
	28	Esther Kuindersma (UL), Cleared for take-off: Game-based learning to prepare airline pilots for critical situations
	29	Daniel Formolo (VU), Using virtual agents for simulation and training of social skills in safety-critical circumstances
	30	Vahid Yazdanpanah (UT), Multiagent Industrial Symbiosis Systems
	31	Milan Jelisavcic (VU), Alive and Kicking: Baby Steps in Robotics
	32	Chiara Sironi (UM), Monte-Carlo Tree Search for Artificial General Intelligence in Games
	33	Anil Yaman (TUE), Evolution of Biologically Inspired Learning in Artificial Neural Networks
	34	Negar Ahmadi (TUE), EEG Microstate and Functional Brain Network Features for Classification of Epilepsy and PNES
	35	Lisa Facey-Shaw (OUN), Gamification with digital badges in learning programming
	36	Kevin Ackermans (OUN), Designing Video-Enhanced Rubrics to Master Complex Skills
	37	Jian Fang (TUD), Database Acceleration on FPGAs
	38	Akos Kadar (OUN), Learning visually grounded and multilingual representations
	01	Armon Toubman (UL), Calculated Moves: Generating Air Combat Behaviour

2020
02 Marcos de Paula Bueno (UL), Unraveling Temporal Processes using Probabilistic Graphical Models
03 Mostafa Deghani (UvA), Learning with Imperfect Supervision for Language Understanding
04 Maarten van Gompel (RUN), Context as Linguistic Bridges
05 Yulong Pei (TUE), On local and global structure mining
06 Preethu Rose Anish (UT), Stimulation Architectural Thinking during Requirements Elicitation - An Approach and Tool Support
07 Wim van der Vegt (OUN), Towards a software architecture for reusable game components
08 Ali Mirsoleimani (UL),Structured Parallel Programming for Monte Carlo Tree Search
09 Myriam Traub (UU), Measuring Tool Bias and Improving Data Quality for Digital Humanities Research
10 Alifah Syamsiyah (TUE), In-database Preprocessing for Process Mining
11 Sepideh Mesbah (TUD), Semantic-Enhanced Training Data AugmentationMethods for Long-Tail Entity Recognition Models
12 Ward van Breda (VU), Predictive Modeling in E-Mental Health: Exploring Applicability in Personalised Depression Treatment
13 Marco Virgolin (CWI), Design and Application of Gene-pool Optimal Mixing Evolutionary Algorithms for Genetic Programming
14 Mark Raasveldt (CWI/UL), Integrating Analytics with Relational Databases
15 Konstantinos Georgiadis (OUN), Smart CAT: Machine Learning for Configurable Assessments in Serious Games
16 Ilona Wilmont (RUN), Cognitive Aspects of Conceptual Modelling
17 Daniele Di Mitri (OUN), The Multimodal Tutor: Adaptive Feedback from Multimodal Experiences
18 Georgios Methenitis (TUD), Agent Interactions & Mechanisms in Markets with Uncertainties: Electricity Markets in Renewable Energy Systems
19 Guido van Capelleveen (UT), Industrial Symbiosis Recommender Systems
20 Albert Hankel (VU), Embedding Green ICT Maturity in Organisations
21 Karine da Silva Miras de Araujo (VU), Where is the robot?: Life as it could be
22 Maryam Masoud Khamis (RUN), Understanding complex systems implementation through a modeling approach: the case of e-government in Zanzibar
23 Rianne Conijn (UT), The Keys to Writing: A writing analytics approach to studying writing processes using keystroke logging
24 Lenin da Nobrega Medeiros (VUA/RUN), How are you feeling, human? Towards emotionally supportive chatbots
25 Xin Du (TUE), The Uncertainty in Exceptional Model Mining
26 Krzysztof Leszek Sadowski (UU), GAMBIT: Genetic Algorithm for Model-Based mixed-Integer opTimization
27 Ekaterina Muravyeva (TUD), Personal data and informed consent in an educational context
28 Bibeg Limbu (TUD), Multimodal interaction for deliberate practice: Training complex skills with augmented reality
29 Ioan Gabriel Bucur (RUN), Being Bayesian about Causal Inference
30 Bob Zadok Blok (UL), Creatief, Creatieve, Creatiefst
31 Gongjin Lan (VU), Learning better – From Baby to Better
32 Jason Rhuggenaath (TUE), Revenue management in online markets: pricing and online advertising
33 Rick Gilsing (TUE), Supporting service-dominant business model evaluation in the context of business model innovation
34 Anna Bon (MU), Intervention or Collaboration? Redesigning Information and Communication Technologies for Development
35 Siamak Farshidi (UU), Multi-Criteria Decision-Making in Software Production

2021
01 Francisco Xavier Dos Santos Fonseca (TUD),Location-based Games for Social Interaction in Public Space
02 Rijk Mercuur (TUD), Simulating Human Routines:Integrating Social Practice Theory in Agent-Based Models
03 Seyyed Hadi Hashemi (UVA), Modeling Users Interacting with Smart Devices
04 Ioana Jivet (OU), The Dashboard That Loved Me: Designing adaptive learning analytics for self-regulated learning
05 Davide Dell'Anna (UU), Data-Driven Supervision of Autonomous Systems
06 Daniel Davison (UT), "Hey robot, what do you think?" How children learn with a social robot

07 Armel Lefebvre (UU), Research data management for openscience
08 Nardie Fanchamps (OU), The Influence of Sense-Reason-Act Programming on Computational Thinking
09 Cristina Zaga (UT), The Design of Robothings. Non-Anthropomorphic and Non-Verbal Robots to Promote Children's Collaboration Through Play
10 Quinten Meertens (UvA), Misclassification Bias in Statistical Learning
11 Anne van Rossum (UL), Nonparametric Bayesian Methods in Robotic Vision
12 Lei Pi (UL), External Knowledge Absorption in Chinese SMEs
13 Bob R. Schadenberg (UT), Robots for Autistic Children: Understanding and Facilitating Predictability for Engagement in Learning
14 Negin Samaeemofrad (UL), Business Incubators: The Impact of TheirSupport
15 Onat Ege Adali (TU/e), Transformation of Value Propositions into Resource Re-Configurations through the Business Services Paradigm
16 Esam A. H. Ghaleb (UM), Bimodal emotion recognition from audio-visual cues
17 Dario Dotti (UM), Human Behaviour Understanding from motion and bodily cues using deep neural networks
18 Remi Wieten (UU), Bridging the Gap Between Informal Sense-Making Tools and Formal Systems - Facilitating the Construction of Bayesian Networks and Argumentation Frameworks
19 Roberto Verdecchia (VU), Architectural Technical Debt: Identification andManagement
20 Masoud Mansoury (TU/e), Understanding and Mitigating Multi-Sided Exposure Bias in Recommender Systems
21 Pedro Thiago Timbó Holanda (CWI), Progressive Indexes
22 Sihang Qiu (TUD), Conversational Crowdsourcing
23 Hugo Manuel Proença (LIACS), Robust rules for prediction and description
24 Kaijie Zhu (TUE), On Efficient Temporal Subgraph Query Processing
25 Eoin Martino Grua (VUA), The Future of E-Health is Mobile: Combining AI and Self-Adaptation to Create Adaptive E-Health Mobile Applications
26 Benno Kruit (CWI & VUA), Reading the Grid: Extending Knowledge Bases from Human-readable Tables
27 Jelte van Waterschoot (UT), Personalised and Personal Conversations: Designing Agents Who Want to Connect With You
28 Christoph Selig (UL), Understanding the Heterogeneity of Corporate Entrepreneurship Programs

2022
01 Judith van Stegeren (UT), Flavor text generation for role-playing video games
02 Paulo da Costa (TU/e), Data-driven Prognostics and Logistics Optimisation: A Deep Learning Journey
03 Ali el Hassouni (VUA), A Model A Day Keeps The Doctor Away: Reinforcement Learning For Personalised Healthcare
04 Ünal Aksu (UU), A Cross-Organisational Process Mining Framework
05 Shiwei Liu (TU/e), Sparse Neural Network Training with In-Time Over-Parameterisation
06 Reza Refaei Afshar (TU/e), Machine Learning for Ad Publishers in Real Time Bidding
07 Sambit Praharaj (OU), Measuring the Unmeasurable? Towards Automatic Co-located Collaboration Analytics
08 Maikel L. van Eck (TU/e), Process Mining for Smart Product Design
09 Oana Andreea Inel (VUA), Understanding Events: A Diversity-driven Human-Machine Approach
10 Felipe Moraes Gomes (TUD), Examining the Effectiveness of Collaborative Search Engines
11 Mirjam de Haas (UT), Staying engaged in child-robot interaction, a quantitative approach to studying preschoolers' engagement with robots and tasks during second-language tutoring
12 Guanyi Chen (UU), Computational Generation of Chinese NounPhrases
13 Xander Wilcke (VUA), Machine Learning on Multimodal Knowledge Graphs: Opportunities, Challenges, and Methods for Learning on Real-World Heterogeneous and Spatially-Oriented Knowledge
14 Michiel Overeem (UU), Evolution of Low-Code Platforms
15 Jelmer Jan Koorn (UU), Work in Process: Unearthing Meaning using Process Mining
16 Pieter Gijsbers (TU/e), Systems for AutoML Research
17 Laura van der Lubbe (VUA), Empowering vulnerable people with serious games and gamification
18 Paris Mavromoustakos Blom (TiU), Player Affect Modelling and Video Game Personalisation
19 Bilge Yigit Ozkan (UU), Cybersecurity Maturity Assessment and Standardisation

	20	Fakhra Jabeen (VUA), Dark Side of the Digital World - Computational Analysis of Negative Human Behaviours on Social Media
	21	Seethu Mariyam Christopher (UM), Intelligent Toys for Physical and Cognitive Assessments
	22	Alexandra Sierra Rativa (TiU), Virtual Character Design and its potential to foster Empathy, Immersion, and Collaboration Skills in Video Games and Virtual Reality Simulations
	23	Ilir Kola (TUD), Enabling Social Situation Awareness in Support Agents
	24	Samaneh Heidari (UU), Agents with Social Norms and Values - A framework for agent based social simulations with social norms and personal values
	25	Anna L.D. Latour (LU), Optimal decision-making under constraints and uncertainty
	26	Anne Dirkson (LU), Knowledge Discovery from Patient Forums: Gaining novel medical insights from patient experiences
	27	Christos Athanasiadis (UM), Emotion-aware cross-modal domain adaptation in video sequences
	28	Onuralp Ulusoy (UU), Privacy in Collaborative Systems
	29	Jan Kolkmeier (UT-EEMCS), From Head Transform to Mind Transplant: Social Interactions in Mixed Reality
	30	Dean De Leo (CWI), Analysis of Dynamic Graphs on Sparse Arrays
	31	Konstantinos Traganos (TU/e), Tackling Complexity in Smart Manufacturing with Advanced Manufacturing Process Management
	32	Cezara Pastrav (UU), Social simulation for socio-ecological systems
	33	Brinn Hekkelman (CWI/TUD), Fair Mechanisms for Smart Grid Congestion Management
	34	Nimat Ullah (VUA), Mind Your Behaviour: Computational Modelling of Emotion & Desire Regulation for Behaviour Change
	35	Mike E.U. Ligthart (VU), Shaping the Child-Robot Relationship: Interaction Design Patterns for a Sustainable Interaction
2023	01	Bojan Simoski (VUA), Untangling the Puzzle of Digital Health Interventions
	02	Mariana Rachel Dias da Silva (TiU), Grounded or in flight? What our bodies can tell us about the whereabouts of our thoughts
	03	Shabnam Najafian (TU Delft), User Modeling for Privacy-preserving Explanations in Group Recommendations
	04	Gineke Wiggers (Leiden University), The Relevance of Impact: bibliometric-enhanced legal information retrieval
	05	P.A. (Anton) Bouter (CWI), Optimal Mixing Evolutionary Algorithms for Large-Scale Real-Valued Optimization Including Real-World Medical Applications
	06	António Pereira Barata (Leiden University), Reliable and Fair Machine Learning for Risk Assessment
	07	Tianjin Huang (TU/e), The Roles of Adversarial Examples on Trustworthiness of Deep Learning
	08	Lu Yin (TU/e), Knowledge Elicitation using Psychometric Learning
	09	Xu Wang (VUA), Scientific Dataset Recommendation with Semantic Techniques
	10	Dennis J.N.J. Soemers (UM), Learning State-Action Features for General Game Playing
	11	Fawad Taj (VUA), Towards Motivating Machines: Computational Modeling of the Mechanism of Actions for Effective Digital Health Behavior Change Applications
	12	Tessel Bogaard (VUA), Using Metadata to Understand Search Behavior in Digital Libraries
	13	Injy Sarhan (UU), Open Information Extraction for Knowledge Representation
	14	Selma Čaušević (TU Delft), Energy resilience through self-organization
	15	Alvaro Henrique Chaim Correia (TU/e), Insights on Learning Tractable Probabilistic Graphical Models
	16	Peter Blomsma (TiU), Building Embodied Conversational Agents: Observations on human nonverbal behaviour as a resource for the development of artificial characters
	17	Meike Nauta (UT), Explainable AI and Interpretable Computer Vision – From Oversight to Insight
	18	Gustavo Penha (TU Delft), Designing and Diagnosing Models for Conversational Search and Recommendation
	19	George Aalbers (TiU), Digital Traces of the Mind: Using Smartphones to Capture Signals of Well-Being in Individuals