Association for Information Systems

AIS Electronic Library (AISeL)

AMCIS 2022 Proceedings

SIG SEC - Information Security and Privacy

Aug 10th, 12:00 AM

Self-endorsed Cybersecurity Capability Improvement for SMEs

Samuel A. Fricker
Fachhochschule Nordwestschweiz FHNW, samuel.fricker@fhnw.ch

Alireza Shojaifar
Utrecht University, alirezashfar@gmail.com

Follow this and additional works at: https://aisel.aisnet.org/amcis2022

Recommended Citation

Fricker, Samuel A. and Shojaifar, Alireza, "Self-endorsed Cybersecurity Capability Improvement for SMEs" (2022). *AMCIS 2022 Proceedings*. 27.
https://aisel.aisnet.org/amcis2022/sig_sec/sig_sec/27

This material is brought to you by the Americas Conference on Information Systems (AMCIS) at AIS Electronic Library (AISeL). It has been accepted for inclusion in AMCIS 2022 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.

Self-endorsed Cybersecurity Capability Improvement for SMEs

Completed Research

Samuel A. Fricker
Fachhochschule Nordwestschweiz FHNW,
Switzerland; Blekinge Institute of
Technology, Sweden
samuel.fricker@fhnw.ch

Alireza Shojaifar
Fachhochschule Nordwestschweiz FHNW,
Switzerland; Utrecht University,
Netherlands
alirezashfar@gmail.com

Abstract

Low cybersecurity awareness and the lack of good practices have led to a growing number of cyber-attacks 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 behavior and guide them to carry out the security improvement on their own. The paper describes the theoretical framework for modeling self-determination and explains how the adoption of cybersecurity recommendations can be internalized 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.

Keywords

Cybersecurity awareness and capability, Small medium-sized enterprises, SME, self-endorsed behavior.

Introduction

Cybersecurity has received much attention during the recent years. Data and systems have become critical assets in most organizations, 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 organization 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 prioritize 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 a. 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 summarized 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 study 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 study 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 summarizes important lessons that we have learned from the application of the CYSEC method during piloting with SMEs. The paper ends with a conclusion.

Self-Determination Theory

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 organizational 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 behavior are awareness and training, information quality, persuasion, rewards, sanctions (deterrence), and computer monitoring. Also, several human factors influence the compliance behavior: 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 1). The organization can influence the employee (extrinsic motivation) and trigger internalization, the process of developing increasingly self-determined behavior (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), minimize 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 organization. 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).

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

Table 1. Continuum of motivations with suitable nudges for amplifying desired behavior, based on self-determination theory (Padayachee 2012).

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 internalization or moral commitment with regards to legal norms. Positively influencing the individual may be rewards offered for compliant behavior.

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

Identification is more internalized than introjection. Identification occurs when an individual has understood the personal importance of a behavior. 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.

Nudges that Amplify Good Behavior

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 behavior and be persistent to the extent that the behavioral 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 behavior to be adopted. *Relatedness* to a person who acts as a role model for the behavior can reinforce self-motivation and even offer a template of how to adopt the behavior (Shojaifar et al., 2020).

Both intrinsic and extrinsic motivation leads to the adoption and internalization of new behavior. However, the more intrinsic the motivation is, the more effective and sustainable the adoption of the behavior 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 2 shows, for the continuum from intrinsic motivation to amotivation, how behavior may be influenced. Any method for helping users to achieve goals should operationalize these factors in the method's design (Shojaifar et al., 2020).

Motivation	**How Desired Behavior is Influenced**
Intrinsic motivation: a person with interested and joy in a desired behavior 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 behaviors 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 behaviors and values, new behavior is internalized 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 behavior. **C)** Regulation through identification can only be achieved if autonomy of choice is provided. **D)** To integrate a regulation, the rules' meaning must be synthesized 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 2. Factors for influencing desired behavior, based on SDT (Deci and Ryan 1985)

The table points to the important SDT constructs that should be operationalized 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 behavior, 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).

Automated Coaching of Cybersecurity Improvements

The improvement of cybersecurity of SMEs depends on communicating cybersecurity knowledge from experts to these SMEs. Table 3 characterizes 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.

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.

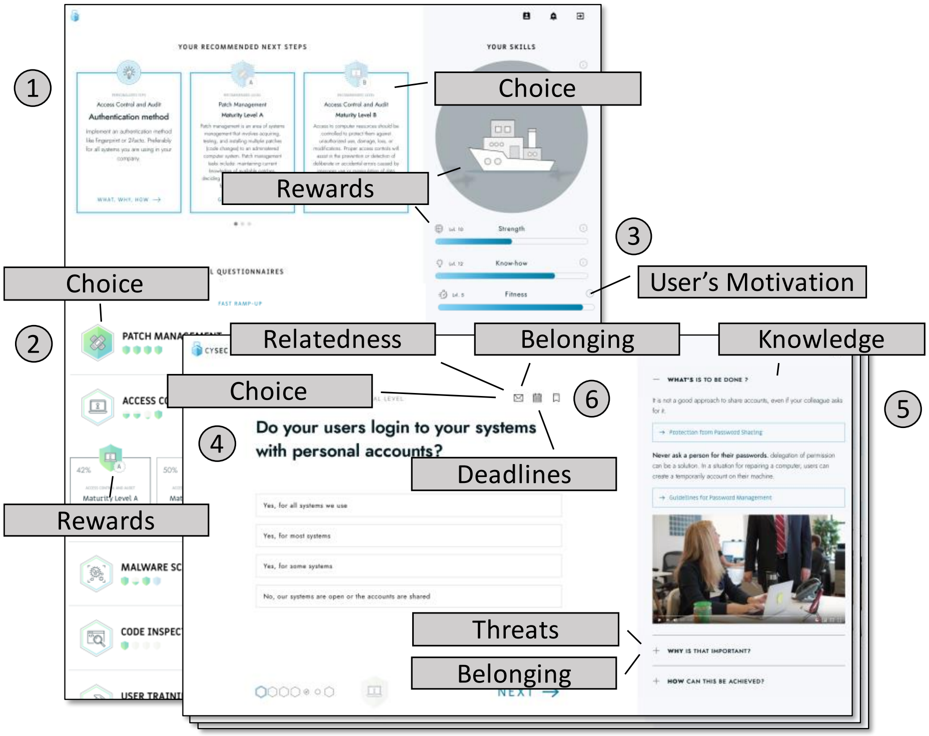
SMEs	Cybersecurity Experts
The SMEs are the entities deserving protection. An SME may be decomposed into the roles of management expected to define goals and policies, the employees whose behavior influences the SME's security, and the CISO [1] who coordinates incident response and security improvement. 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 organization's data, ICT infrastructure, and product and service offerings, and define policies giving rise to good security cultures, respectively train people in good security behavior. They appear in a number significantly smaller than the total number of SMEs.

Table 3. Roles in the cybersecurity ecosystem for SMEs

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 behavior and establish appropriate norms.

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

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 1951) cycles of selecting sensible security themes, implementing the recommended practice, checking progress, and adapting based on lessons learned. The tool offers memory allowing the


YOUR RECOMMENDED NEXT STEPS

Access Control and Audit
Authentication method
Implement an authentication method like Fingerprint or 2Facto. Preferably for all systems you are using in your company.
WHAT, WHY, HOW →

Patch Management
Maturity Level A
Patch management is an area of systems management that involves acquiring, testing, and installing multiple patches (code changes) to an administered computer system. Patch management tasks include: maintaining current knowledge of available patches, deciding

Access Control and Audit
Maturity Level B
Access to computer resources should be controlled to protect them against unauthorized use, damage, loss, or modifications. Proper access controls will assist in the prevention or detection of deliberate or accidental errors caused by

YOUR SKILLS
Lvl. 10 Strength
Lvl. 12 Know-how
Lvl. 5 Fitness

QUESTIONNAIRES
FAST RAMP-UP
PATCH MANAGEMENT
ACCESS CO
MALWARE SC
CODE INSPECT
USER TRAINI

Do your users login to your systems with personal accounts?

Yes, for all systems we use
Yes, for most systems
Yes, for some systems
No, our systems are open or the accounts are shared

WHAT'S IS TO BE DONE ?
It is not a good approach to share accounts, even if your colleague asks for it.
→ Protection from Password Sharing
Never ask a person for their passwords. delegation of permission can be a solution. In a situation for repairing a computer, users can create a temporarily account on their machine.
→ Guidelines for Password Management
WHY IS THAT IMPORTANT?
HOW CAN THIS BE ACHIEVED?
NEXT →

Figure 1. Main user interfaces of CYSEC and mapping of its features to SDT constructs

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

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).

Figure 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 4 describes how CYSEC operationalizes SDT.

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.

Table 4. Implementation of Nudges

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 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.

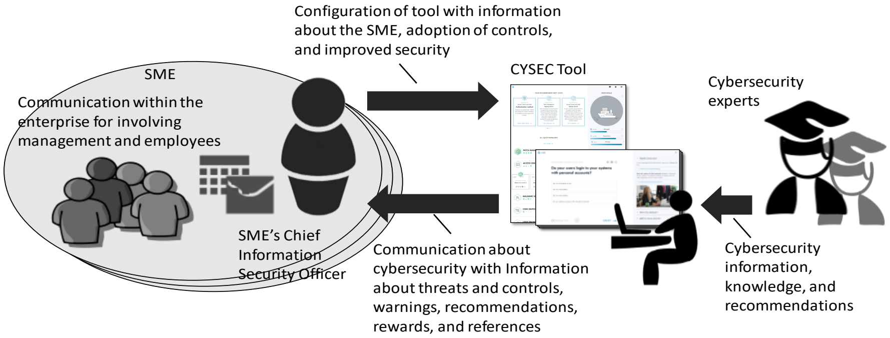

Configuration of tool with information about the SME, adoption of controls, and improved security
SME
Communication within the enterprise for involving management and employees
SME's Chief Information Security Officer
CYSEC Tool
Cybersecurity experts
Communication about cybersecurity with Information about threats and controls, warnings, recommendations, rewards, and references
Cybersecurity information, knowledge, and recommendations

Figure 2. Roles and flows of information and knowledge for improving cybersecurity

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 1951) improvement cycles. PDCA is established for decades already for structuring improvements in an organization.

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 organization 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 prioritized. 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 organization. The knowledge is communicated in the form of what should be done, why the action is important, and how the action can be realized 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 analyzing 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 analyzing the overall improvement progress, causes for inefficiencies, gaps, or other difficulties, and institutionalizing good practice. Inefficiencies could lead to abandoning one type of control and replacing it with a more user-friendly one. Gaps could lead to specialized improvements beyond what CYSEC was recommending. Institutionalizing could mean to define when to follow-up and revisit the security objective of the current PDCA cycle.

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 characterize 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 organizational aspects of cybersecurity and guide the users in establishing the appropriate cybersecurity organization. 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 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 this book, 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.

Lessons-Learned from SMEs' Do-It-Yourself Improvement

Twelve SMEs (project partners) utilized 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 utilized CYSEC during the piloting period. We conceptually organized 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 synthesized findings from the evaluation studies (by applying the qualitative method) at the end of the project.

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.

<u>Lesson 1</u>: 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 organized small meetings discussing the problems, and there is a person in charge of managing it and monitoring the plans."

<u>Lesson 2</u>: 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 behaviors 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."

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 realized 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 customized (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 customizable, 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 prioritization. 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' behaviors. We need access to patches, training courses, and personalizing security products."

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 personalized recommendations. We demonstrated how CYSEC implemented Self-Determination Theory to support effective security communication with SMEs for motivating sustainable self-endorsed forms of security behavior. 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.

Acknowledgements

This work was made possible with funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 740787 (SMESEC) and the Swiss State Secretariat for Education, Research and Innovation (SERI) under contract number 17.00067. The opinions expressed and arguments employed herein do not necessarily reflect the official views of these funding bodies.

REFERENCES

Alotaibi, M., Furnell, S., & Clarke, N. 2016. "Information security policies: A review of challenges and influencing factors," In *2016 11th International Conference for Internet Technology and Secured Transactions (ICITST)*, pp. 352-358. IEEE.

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

Cearley, D.W., Burke, B., Searle, S., Walker, M.J. 2017. "Top 10 strategic technology trends for 2018," Gartner.

Chipperfield, C., & Furnell, S. 2010. "From security policy to practice: Sending the right messages," *Computer Fraud & Security*, (2010:3), pp. 13-19.

Deci, E.L., Ryan, R.M. 1985. "The General Causality Orientations Scale: Self-determination in personality," *Journal of research in personality*, (19:2), pp. 109–134.

Deming, W.E. 1952. "Elementary principles of the statistical control of quality: a series of lectures," Nippon Kagaku Gigutsu Remmei: Japanese Union of Science and Engineering (JUSE).

Furnell, S. M., Gennatou, M., & Dowland, P. S. 2002. "A prototype tool for information security awareness and training, " *Logistics Information Management,* 15(5/6), pp. 352–357.

Gupta, A., & Hammond, R. 2005. "Information systems security issues and decisions for small businesses: An empirical examination," *Information management & computer security*, (13:4), pp. 297-310.

Hope, K. 2019. "Annual Report on European SMEs 2018/2019," European Commission. DOI:10.2826/500457.

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), pp. 139-154.

Knapp, K.J., Marshall, T.E., Rainer, R.K., Morrow, D.W. 2006. "The top information security issues facing organizations: What can government do to help," *Network security*, 1, 327.

Kraemer, S., Carayon, P., & Clem, J. 2009. "Human and organizational factors in computer and information security: Pathways to vulnerabilities," Computers & security, (28:7), pp. 509-520.

Moore, S., Keen, E. 2018. "Gartner Forecasts Worldwide Information Security Spending to Exceed $124 Billion in 2019," Gartner Press Release, Sydney, Australia.

Padayachee, K. 2012. "Taxonomy of compliant information security behavior," *Computers & Security*, (31:5), pp. 673-680.

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.

Siponen, M., Pahnila, S., & Mahmood, A. 2007. "Employees' adherence to information security policies: an empirical study," In *IFIP International Information Security Conference*, pp. 133-144, Springer, Boston, MA.

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), pp. 121-128.

Wood, P., Nahorney, B., Chandrasekar, K., Wallace, S., Haley, K., Davis, M., Rankin, S. 2016. "Internet Security Threat Report," Symantec Corporation, Volume 21.