Research Report

Information Security Education for SMEs – Unlocking potential, increasing awareness

Funded by the Erasmus+ Programme of the European Union

TeBelSi

Funded by the
Erasmus+ Programme
of the European Union

This document was produced within the scope of the ERASMUS+ Project “Teilzertifizierung im Berufsfeld Informationssicherheit – TeBeiSi”, Project ID: 2018-1-EN02-KA202-005218

Funded by the
Erasmus+ Programme
of the European Union

TeBelSi

Content

List of Figures

List of Tables

1 Introduction: Partial Certification in Information Security

Information Security has increased sharply in importance across recent years. With a surge of data breaches, firms held hostage to malware attacks internationally, and the strategic use of cyber warfare as a means to extend political power in foreign spheres, digitalization is no longer perceived only as a redeeming solution for struggling businesses, but also as a vital source of risk that merits vast measures of protection. Risks arise in manyfold contexts, but can be rooted in two spaces: on-premise and cyber.

Holistic approaches to tackle the existing and increasing threat situation are needed. In the face of diffuse and intangible risk scenarios, individuals, both in the private and corporate domain, tend to depreciate the importance of information security risk detention as a means of sustainable governance and management. In order to come by this broad lack of awareness, which translates from the public sphere into the corporate world, awareness rising, sensitization and education measures need to be taken. In the meanwhile, firms need to understand how they can approach the topic of information security with an individual strategy, which fits the own need, and, the own budget. To support firms in this challenge the study “Information Security Education for SMEs” was conducted. The study set out the objective to shed light into the training and personnel needs of SMEs to find solutions for the persistent lack of skilled workers.

The subtitle “Unlocking potential, increasing awareness” thereby provides a hint regarding the most important resource: existing personnel in SMEs. Many employees possess skills and knowledge which they acquired throughout their career, which they are more often than not not even aware off. The acquisition of non-formal and informal learning, especially in technology and innovation driven sectors like information security provide rich resources which can be harvested by means of competence validation and recognition. To facilitate the recognition process, the TeBeISi project team developed learning units and with the support of the present survey, provides tools and ressources for SMEs to identify suitable employees for the uptake of new responsibilities in the domain of information security.

The TeBeISi project strives to contribute to business practice and meeting the daily reality of SMEs from across the EU. This study deepens the understanding of decision makers, recruiters and interested individuals in the field of information security and the development of assets and requirements of information security and information security personnel in SMEs. To achieve this objective, the study is structured as follows: chapter two provides an overview about existing research of information security in SME and personnel requirements, chapter three provides background to the TeBeISi research methodology and the context in which this study was designed, chapter 4 presents the findings of the quantitative questionnaire, chapter five derives briefly the most important guidelines for SMEs and, finally, chapter six concludes with an outlook onto future developments.

2 Literature Review

The deployment of information systems and information technology has become a prerequisite for the success of businesses in all economic sectors. Without information technology, working with information is not only ineffective but also impossible (Hallová et al. 2019). Moreover, our dependence on these systems is increasing every day. However, with the rapid development of modern technologies and information systems, the potential for misuse is also increasing (Smith, 2003; Leede et al., 2005; Kumar et al., 2011).

In today's world, in which all individuals and companies depend on information technology, information security and data protection are important elements that require particular attention. In this respect, the European Union (EU) Directive concerning measures for a high common level of security of network and information systems across the Union[1] and the General Data Protection Regulation[2] (Kogenhop, 2020) are important factors. The regulatory initiative of the European Commission reflects the increased need for legislative guidance, as rapid technological developments and globalisation have created new challenges for the protection of personal data and information (Wilkinson, 2018).

In recent years, new forms of information technology (e.g. sensors and mobile devices) have dramatically expanded what can be measured and analysed, posing entirely new challenges for security and privacy (Weber, 2010; Newell & Marabelli, 2015; Sicari, Rizzardi, Grieco, & Coen-Porisini, 2015; Lee, Cho & Lim, 2018). The potential for customers to be affected by security and privacy issues related to information systems makes these challenges central to business practitioners (Sicari et al., 2015; Sicari et al., 2016). On the other hand, managers of organisations need to use new information technology tools to store not only personal data but also confidential data to remain competitive in the 21st century. Meanwhile paper-based data storage is obsolete due to the potential of electronic data storage, organisations are rapidly adopting new technologies and electronic storage has become commonplace in many countries (McAfee, 2010).

The growing trend towards storing data in electronic format, as well as the increasing connectivity of the internet and the resulting exposure to cyber criminals, has led to the development of specific data protection requirements (McAfee, 2010). Data storage technologies must have data protection measures in place and users working with the data must be trained to understand the risks of leaking company data to unauthorised persons. Organisational leaders need to be aware of the serious consequences of electronic data leaks. In the same instance as employees who do not comply with information security (Siponen, Mahmood & Pahnila, 2009), Managers of organisations who are careless in the acquisition and management of electronic data expose their firms to risks and threats (Northhouse, 2010). Managers need to exercise caution and self-control in order to benefit the company, especially in terms of data security (Guinote & Vescio, 2010). One of the key challenges in information security management is to understand how organisational, individual and technical factors combine to influence information security outcomes in an organisation (Wilkinson, 2018).

[1] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union 2016.

[2] European Union 2016.

Recent research shows that in many cases, electronic data leakage in small companies is the result of poor leadership and management practices. Managers in organisations make the most important decisions and if managers do not deal with information technology issues properly, they threaten the survival of the business (Davies & Hertig, 2008). A possible mitigating factor was proposed by Noguerol und Branch (2018), arguing that corporate managers can positively influence employee behaviour in the area of data security by fostering a healthy work environment and fostering interpersonal relationships.

Companies of all sizes around the world are suffering from a lack of cyber security, and many of them are exposed to cybercrime. However, electronic data leakage is a concern especially for smaller firms. Among others, SMEs face financial constraints, sometimes ineffective managers, and a lack of attention to small problems that are not directly related to business (O'Rourke, 2003; Adamkiewicz, 2005; Goodwin, 2005; Baker & Wallace, 2007).

Despite the increasing threat of cyber incidents from outside, employees remain the main source of security incidents (Richardson, 2008; PwC, 2017). Human resources inside the organisation can be more dangerous than those outside the organisation because they are familiar with the organisation's information systems and access data through their normal work activities (Herath & Rao, 2009a, 2009b; Bulgurcu, Cavusoglu, & Benbasat, 2010; Johnston & Warkentin, 2010; Siponen & Vance, 2010). Information security policies are supposed to ensure the security of information (Bulgurcu, Cavusoglu, & Benbasat, 2010), but research shows that many security incidents are caused by employees ignoring or being unaware of security policies (Willison & Warkentin 2013, Path to Cyber Resilience, 2016).

Researchers and practitioners increasingly consider organisational information security to be a socio-technical issue, requiring not only technical but also managerial approaches (Burns, Roberts, Posey, Bennett, & Courtney, 2018). Due to the widespread use of information technology in companies, employees are often entrusted with continuous access to company information and information systems to carry out their job-related duties. Despite this increased operational flexibility, organisations are less able to monitor the behaviour of employees with access to confidential data (Herath & Rao, 2009). Therefore, in order to improve the protection of organisations' valuable information assets in the context of the proliferation of technology, proactive information security training for employees is central to the information security of organisations (von Solms & von Solms, 2009; D'Arcy, Hovav & Galletta, 2009; Albrechtsen & Hovden, 2010; Puhakainen & Siponen, 2010; Karjalainen & Sipo-nen, 2011; Posey, Roberts, Lowry, Bennett & Courtney, 2013). Research shows that organisations identify employee awareness programmes as a top priority in their information security budgets (PWC, 2015), and information security executives state that employee training is one of the most important activities needed to implement a successful information and data security strategy (van Zadelhoff, Lovejoy & Jarvis, 2014).

Employee training is the most effective non-technical means of ensuring information security in organisations and preventing employees from disclosing sensitive information to unauthorised parties (Colwill, 2009; Peikari, Shah, & Lo, 2018). Training can increase employees' knowledge and awareness of the threats and consequences of a security breach and help prevent such incidents (Kluge, 2007; D'Arcy Hovav & Galletta, 2009).

Employee education and training is a means for organisations to reduce the risk of internal security failures (Burns, Roberts, Posey, Bennett & Courtney, 2015; Barlow, Warkentin, Ormond, & Dennis, 2018). It is an important prerequisite and has a positive impact on information security behaviour. Well-designed employee training programmes can help to reduce information security risks to an organisation (Anderson & Agarwal, 2010; Liang & Xue,

2010; Bulgurcu, Cavusoglu, & Benbasat, 2010; Johnston & Warkentin, 2010; Whitman & Mattord, 2012; Jenkins & Durcikova, 2013; Johnston, Warkentin & Siponen, 2015). According to researchers (Gardner & Thomas, 2014; Posey, Roberts & Lowry, 2015), continuous education and training of employees in data and information security is an effective way to shape their information security behaviour and compliance with an organisation's information security policy. Employees with adequate information security knowledge are able to prevent threats and attacks, resulting in increased confidentiality, integrity and availability of information within the organisation (Sabeeh & Lashkari, 2011). It is noted that due to the dynamic nature of information security threats and vulnerabilities, employee training and education should be a regular and ongoing practice in an organisation (Yoo et al., 2018; McConnell, 2020).

While processing personal data is unavoidable for many SMEs, it is often not their core business and they lack sufficient human or financial resources to ensure proper compliance. In particular, SMEs are not prepared to adopt information security measures simply because they are not required to have documented information security due to their small size (Kuusisto, & Ilvonen, 2003; Doherty, & Fulford, 2005). SMEs are mostly aware of the GDPR, but lack the resources to comply with the requirements; they lack the organisational capacity to implement the requirements of the GDPR and information security within their organisation. The most common data protection and information security challenges faced by SMEs include: understanding what changes need to be made to comply; designing and developing new processes and procedures related to the processing of personal data; and staff awareness of the importance of data protection. Despite numerous opinions and guidelines on GDPR issued by regulators and data protection experts, there is a lack of practical, easy-to-understand and targeted guidance for SMEs on how to implement data protection legislation in practice (Jasmontaitė-Zaniewicz, Calvi, Nagy & Barnard-Wills, 2021). It highlights that in particular SMEs actualize the need for targeted, sector-specific training and advice based on examples, and case studies that reflect the specificities of these organizations (Barnard-Wills, Cochrane, Matturi, & Marchetti, 2019).

3 TeBeISi – Method and Approach

Information Security in SMEs, as of now, is a understudied topic and not much is known concerning the needs and requirements of SMEs across the EU. Meanwhile in Data Protection legislative obligation (GDPR) have lead to a rapid increase in measures taken and awareness among SMEs, information security has been treated by many entities much more as a “nice to have” – and wasn’t pursued with much effort or dedication. The introduction of Information Security Management System, or the certification of firms and individuals, is only slowly creeping into the conscion of employees and firm owner. Nonetheless, it has been established that among the many factors comprising the security of the firm, the human factor, i.e. the employee, the management and, ultimately, the information security officer, can make the biggest difference.

The TeBeISi-project set out the objective to provide insights into the state of play of information security in SME and to gain deeper insights into training and education possibilities for SMEs in order to overcome the skilled labour shortage.

3.1 Research Subject

The research agenda on which the TeBeISi project was based mainly rooting in three iterative steps: first, benchmarking of common practices (IO1 and IO2), second, needs analysis (IO3) and the development of proper tools and recommendations for firms, individuals and educational institutions (IO4 and IO5). By analysing the market situation, especially the role of existing certifications and tools in the context of competence recognition and transparency. From the requirement analysis, a process has been developed which is represented in **Figure 1**.

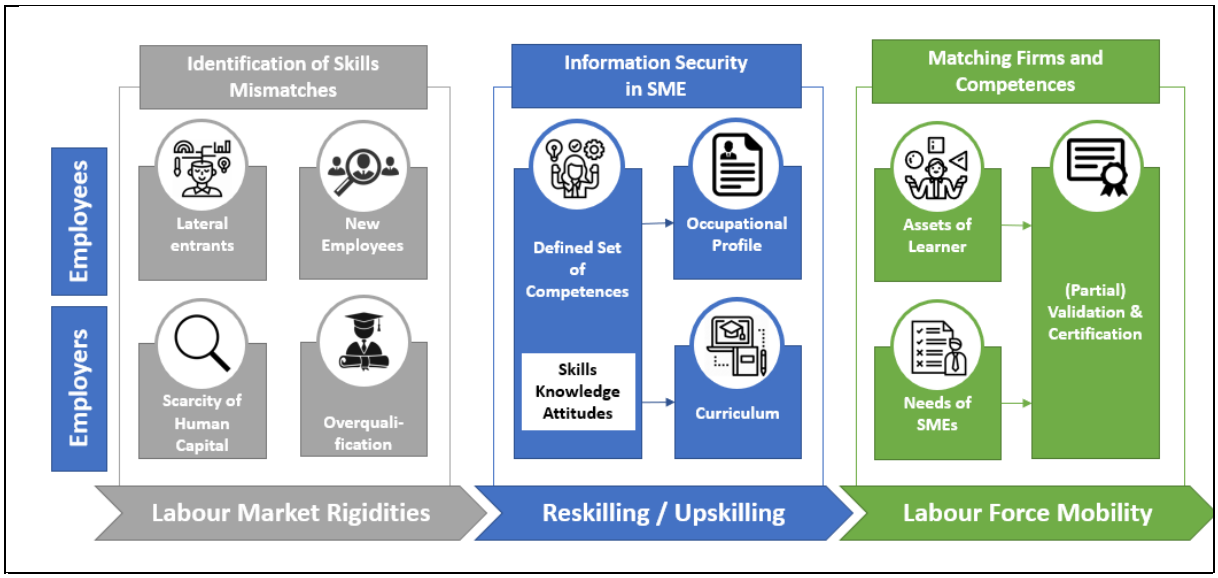


Figure 1: A way out - The TeBeISi solution to overcome the skills gap in the information security labour market.

In brief, the existing labour market rigidities can be describing as two-fold: on the one hand, there is simply a low number of specialists available on the market. This scarcity even worsens due to the fact that most available specialists are highly qualified – often too highly, as they become too expensive for SMEs to afford. Current practices in firms are similar to those in the

entire IT sector: many lateral entrants are becoming active in the sector, and completely new workers start to set up their career in this promising domain. The solution developed by the TeBeISi project consequently starts with the analysis of Skills Knowledge and Competences required in SMEs, to construct a specific curriculum designed around the needs of SMEs. It has become evident that, not only from the perspective of qualification, requirements in SMEs differ vastly from the requirements in larger corporations, which is why the project suggests a different occupational profile to account for these differences. The occupational profile and the curriculum are based on the determined competences among SMEs. Finally, a check-up of firms needs and employees' competences supports firms in identifying suitable candidates, which predispose of valuable treats for the work in the field of information security and which are eager to re-educate themselves and advance their career in a new field, The investment into existing personnel and the upskilling of the own labour force is thereby considered to be the most economic possibilities for firms and workers to overcome the skills need.

The present study supports this agenda in several ways: First, it aims to identify requirements from a managerial perspective, considering hiring strategies, open positions, information security awareness and company culture. Second, technical requirements re being evaluated, considering specifically social, but also technical skills. In both domains, items have been developed throughout a series of expert interviews and focus groups. Therefore, thirdly, the present questionnaire provides a confirmation and peer validation of the findings established via a mixed method research design.

3.2 Method

The mixed method research design leading to the development of competence profiles and the TeBeISi curriculum consists of four central elements, the results of which have been stirred and used iteratively throughout the project implementation First, in a desk research, certifications and occupational profiles have been analysed, yielding insights into taught competences and competences inherent to and expected from practitioners operating on the market. Nonetheless, this research was constrained by the finding that only barely the specific case of SMEs is being considered, and that it remains unclear what sets apart the basic needs of an SMEs and the more advanced requirements of larger operations. Therefore, emphasise was put on the detailed observation for the SME context, including the involvement of different SME stakeholders (entrepreneurs, chambers of commerce, specific researchers etc), the consideration of SME specific literature and the analysis of SME specific certification processes and available courses in the partner countries.

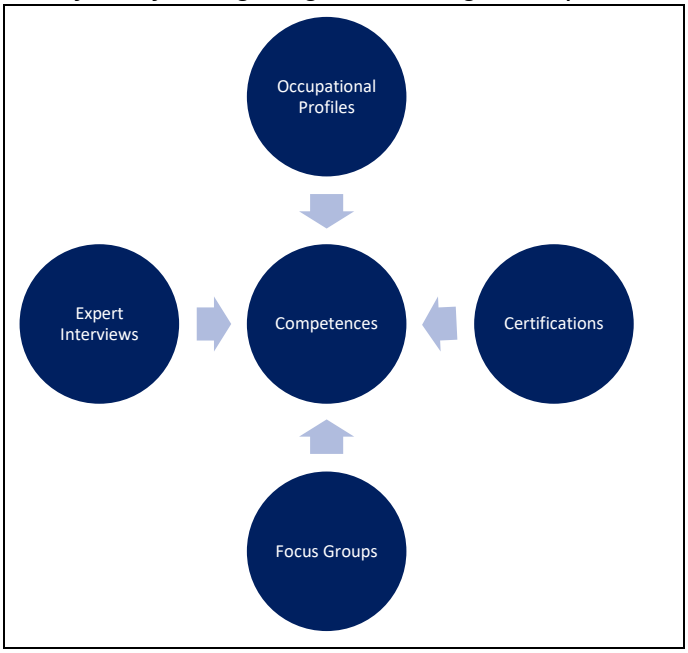


Figure 2: The TeBeISi research agenda

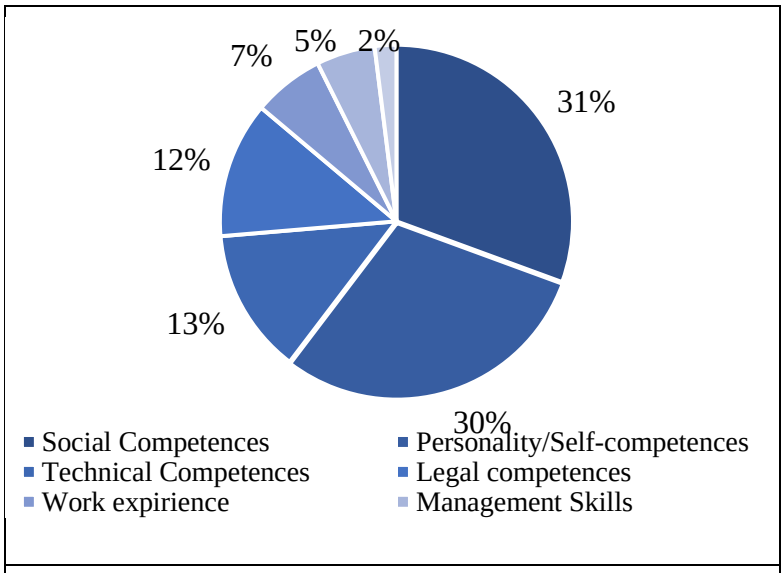


Figure 3. Competences critical for success

Throughout a series of expert interviews and focus groups, conducted in Lithuania, Italy, Germany, and Poland with employers, employees and educational providers, competences of information security practitioners have been analysed. From the qualitative analysis, in depth information concerning the importance of technical, methodological, social and personal skills have been extracted, and specific items in each category identified. The entire analysis is available in the "Information Security Competences – a qualitative analysis of Expert Interviews on Knowledge and Skills of Professionals in Information Security" document.

The particular items identified have been reformulated and bundled into learning units according to the ECVET standard of learning outcomes (c.f. IO4). In the present survey, these units have been put up for evaluation in terms of frequency and importance in the firms, so that the final results will yield insights into the priority if firms and the most urgent tasks that need to be carried out.

4 Study: Information Security Education and Training for SMEs

Within the scope of the project, the TeBeISi-project group conducted the survey “Information Security Education for SMEs” with the aim to gain insights into current practices on information security in small and medium sized enterprises, the demand for knowledge, skills and competences and the prospects of SMEs to deal with the existing challenges of scarce resource availability. The survey on information security education for SMEs aims at identifying learnings and expertise in specific sub-fields in the vocational domain of information security in the realm of small and medium sized enterprises. The survey was conducted via Limesurvey. In a period of around 6 weeks 160 participants, information security specialists, owners and CEOs of SMEs as well as recruiting and IT experts responded to the online survey disseminated in the project partner countries, mainly Poland, Germany, Lithuania, Italy, and Austria.

The study is composed of two major aspects on the one hand, requirements from the perspective of recruiters, i.e., HR departments and business owners was sought, focusing on major aspects they take into account throughout the recruiting process. On the other hand, IT departments and information security specialists were asked to provide their view on technical requirements and competence benchmarking for new employees in the sector. Further, both addresses were asked to provide information about firm culture and personality traits of successful employees. To this end, validated items from Ingela et al. (2005) for company culture and Ramos-Villagrasa et al. (2019) for job performance were used. For the questionnaire, the scales were retransformed into 5-point Likert scales. Participants were presented questions according to their position. The questionnaire was developed under IO3 of the TeBeISi project and is available alongside the remaining project output documents.

4.1 Description of Data

The majority of companies that participated in the survey belongs to the field of micro-, small and medium sized enterprises (more than three-quarters). The remaining quarter consists of, among others, large enterprises (5 %), governmental (6 %) and non-governmental organizations (8 %). Whenever necessary, only the values for SMEs were considered. **Figure *4*** shows the distribution of total participants according to the firm size. For the definition of firm-size, the common European definition has been used respecting number of employees and turnover. (European Commission 2021).

The companies operate in different industries, like human health and social work, education or in the field of professional, scientific and technical activities, according to the NACE Rev. 2 classification (Eurostat 2008). 10% of the companies are operating in the information and communication sector (Figure 5).

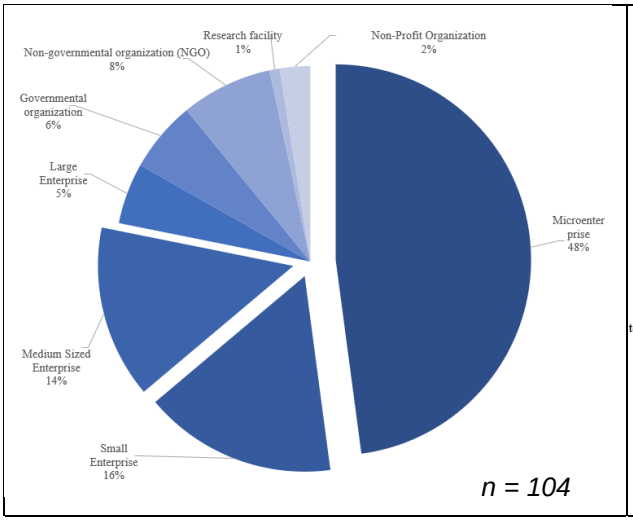


Figure 4: "Which firms participate in the survey?"

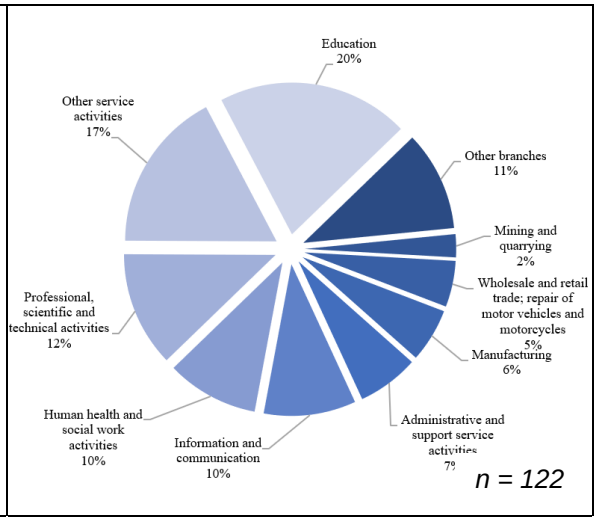


Figure 5: "In which branch of industry does your company operate?"

For the survey, it was important to know the type of activity of the participants in the firm, i.e. either IT and Information Security experts or CEO / recruiter in an SME, as functional work responsibilities involving information security change. According to their answers, participants were shown different questions in the Survey. As can be seen in Figure 4 and Figure 5, two-thirds of the participants are working as managing director or in the human resources department. This group answered questions related to company culture, competences in the company, education in the company or technologies used in the company.

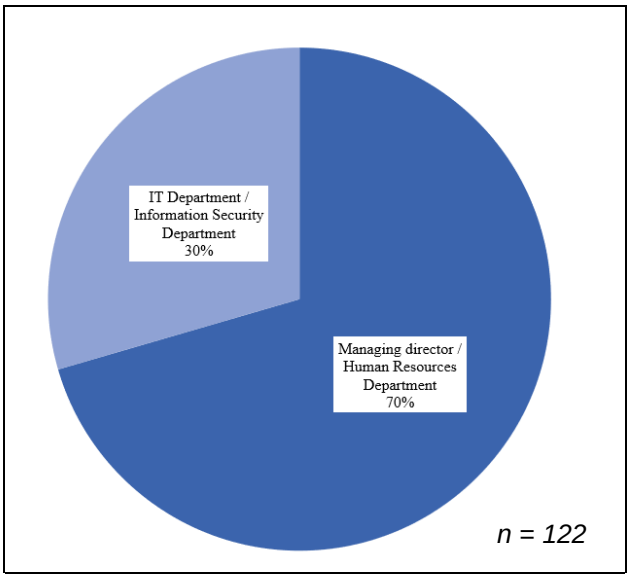


Figure 6: "What is your role in the company?"

Meanwhile, respondents from the IT or information security department were shown questions focussing onto their own work performance, personality traits and questions related to IT management in the company. This distinction was made to account for the different perspectives into information security, with a managerial focus on the side of firm owners and a technical focus on the side of the information security experts.

Considering the origin of the respondents, almost half of the participants indicated the operation of their firm to be mainly based in Italy.[3] Besides, the firms are also active in Lithuania, Germany, Poland, Austria and Czech Republic (Figure 7). Finally, a brief outlook on the gender distribution: There is a slight majority of male participants with 38 out of 102 participants being female (Figure 8). Unfortunately, the size and distribution of participants did not allow for country or gender comparisons, which needs to be taken into account when interpreting the results. All graphics in the following will illustrate either a comparison of SMEs or non-SMEs. If not being stated otherwise, only the answers of SMEs were accepted in the analysis.

[3] It was controlled whether the unbalanced participation quota impacted the objectivity of the results. Testing of data with and without Italian participants did not yield any significant differences in the results of the different question groups, which is why this risk can be neglected.

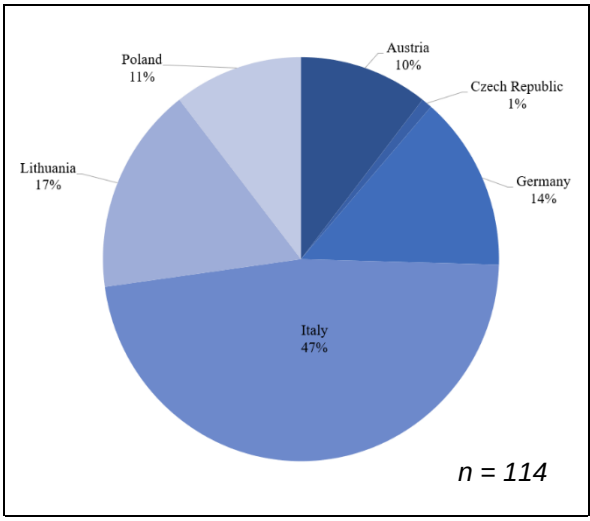


Figure 7: "In which country does your company mainly operate?"

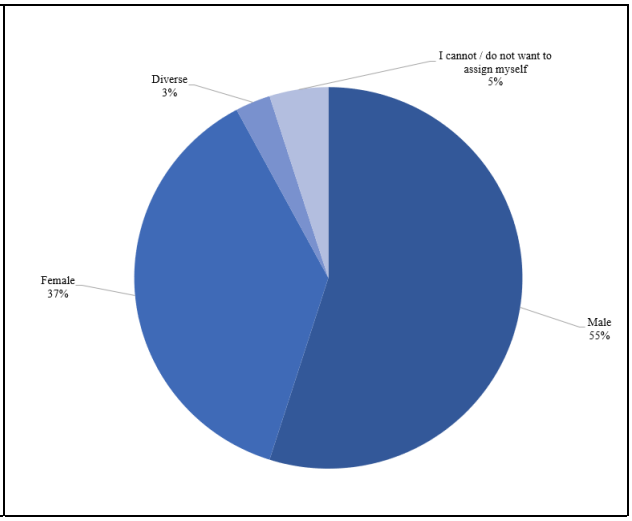


Figure 8: "How does the gender distribution look like?"

4.2 Analysis

The main part of the survey can be differentiated in to two groups: managerial and technical aspects of information security in SMEs. Meanwhile the first aspect entails chapter 4.2.1 Company Culture, 0

Competences in the company, 4.2.3 Information security in SMEs and 4.2.4 Information security in the company: personnel requirements, the latter entails competence specific questions in chapter 4.2.4 Information security in the company: personnel requirements, 4.2.5 Self-assessment of competencies, 4.2.6 Personality (Big Five) and 4.2.7 Work Performance

4.2.1 Company Culture

With the end to reveal differences about the firms which have implemented information security measures in comparison to those who have not company culture was identified as a crucial aspect separating firms from one another. Consequently, the first step for the participants was to characterize the company culture itself. To analyse company culture the brief scales suggested by Jöns et al. (2005) were used, using a 5-Point Likert scale with 1 and 5 as extremes.

In this context, respondents were asked to describe their companies along the characteristics “Strategy”, “Structure”, “Leadership” and “Cooperation”. For these characteristics, the authors developed 18 questions, illustrated in

Table ***1***. As can be seen below, a significant difference in agreements exists among the 18 items. It needs therefore to be mentioned that some of the items are positively formulated, and some negatively. Consequently, a direct comparison does not yield immediate and telling results. More importantly, the aggregation of categories to the four domains mentioned above need to be considered in this context.

Question	N	Mean	Std. Dev.	Var.	Kurtosis	Std. Err.
The company is highly customer-oriented.	83	4.37	0.79	0.63	3.34	0.52
The company is open towards innovations.	83	4.19	0.82	0.67	1.73	0.52
The company is highly quality-oriented.	84	4.13	0.97	0.93	0.47	0.52
The company is characterised by team orientation.	84	3.96	0.94	0.88	0.98	0.52
The company is highly performance-oriented.	83	3.96	0.94	0.89	1.30	0.52
Managers place great trust in the employees.	82	3.91	0.77	0.60	-0.19	0.53
Employees place great trust in the managers.	84	3.87	0.89	0.79	1.32	0.52
Employee information has a high priority.	82	3.76	0.90	0.80	-0.57	0.53
Employees are involved in decision-making.	82	3.67	0.99	0.99	0.29	0.53
Conflicts are addressed openly in the company.	83	3.55	0.93	0.86	0.12	0.52
The company is strongly hierarchically organised.	84	2.94	1.25	1.57	-0.98	0.52
The company has a bureaucratic management style.	84	2.64	1.09	1.20	-0.82	0.52
The relationship between employees is characterised by competition.	84	2.52	1.11	1.24	-0.56	0.52
When mistakes and problems occur in the company, first of all culprits are sought.	84	2.26	1.03	1.06	-0.27	0.52
The leadership style in the firm is authoritarian.	83	2.24	1.11	1.23	-0.52	0.52

Table 1: "Please indicate to what extent the following characteristics describe the company you work for or the organization you work for".

The abovementioned characteristics can be distinguished by strategy, structure, leadership and cooperation. The authors define these categories as follows: Customer-orientation, openness towards innovations, a high quality- and performance orientation are part of the strategy field. Regarding the company structure it is important to know if the firm has a bureaucratic management style and if the company is strongly hierarchically organized. Last point leads to the next category leadership. Within this area, leadership style, priority of employee information and involvement of employees in decision-making play a significant role. Besides, participants are questioned about the situation if mistakes and problems occur in the company. Finally, subjects like team-orientation, trust of employees towards managers, dealing with conflicts in the company and the relationship between employees are part of the category cooperation.

As Figure 9 shows, the companies in the survey have a relatively high strategic orientation, low degree of hierarchical structure and a low degree of directive leadership. It is conspicuous that companies which are not be part of the SME sector have a slightly higher value in the structure field. It can be assumed that especially big companies are more hierarchically organized than small and medium enterprises. With regard to strategy, leadership and cooperation only marginal differences between SME and non-SME can be observed.

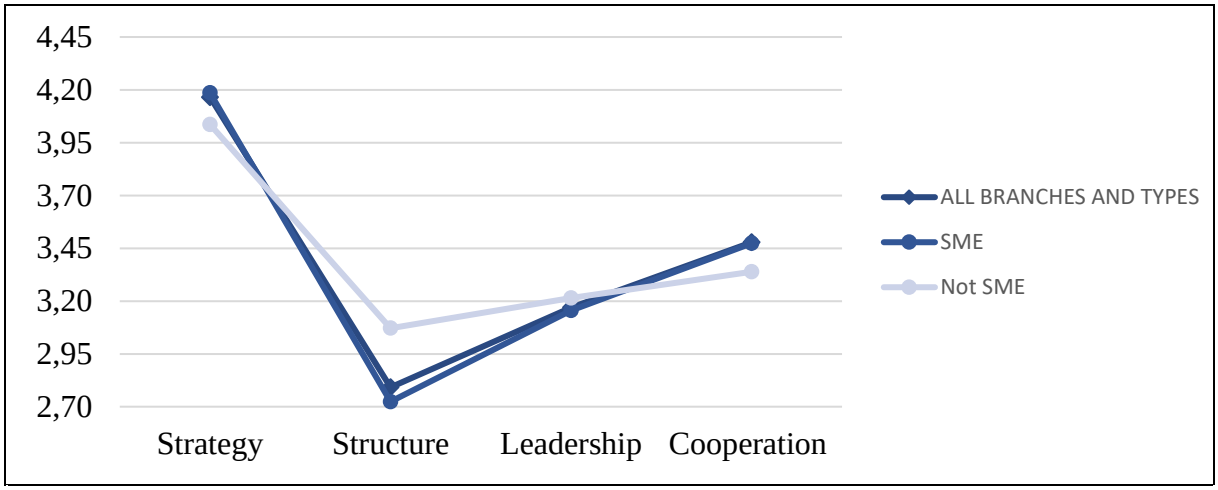


Figure 9: Characteristics grouped into the following categories "Strategy, Structure, Leadership, Cooperation" – all firms

Concerning the initial question of this part of the survey, it can be noted that a slight difference exists in the degree of cooperation, strategy and leadership, which is higher in firms that have taken information security measures in comparison to firms that did not.

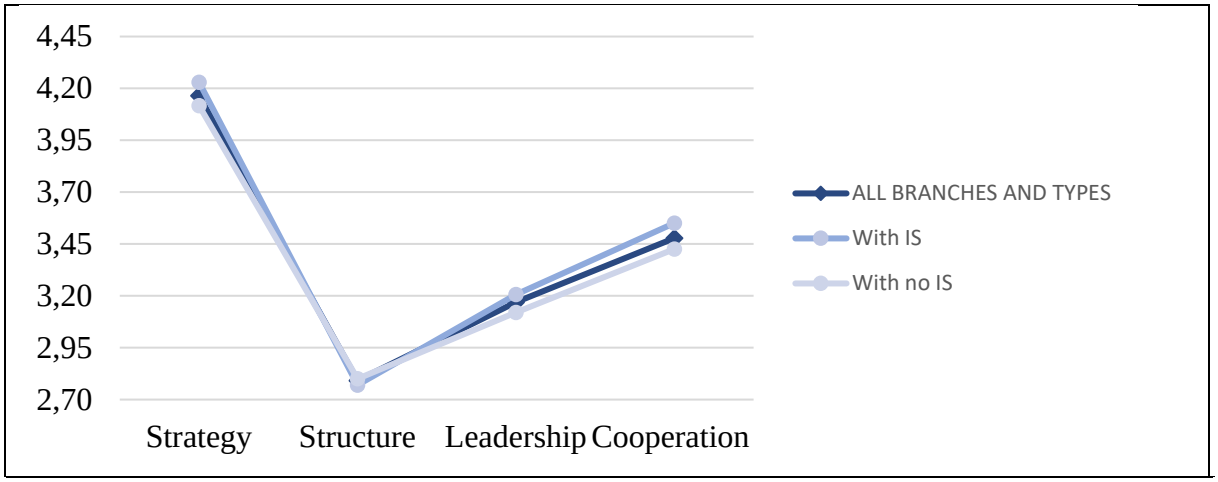


Figure 10: Characteristics *grouped into the following categories "Strategy, Structure, Leadership, Cooperation" – firms having an Information Security strategy and firms that don't*

4.2.2 Competences in the company

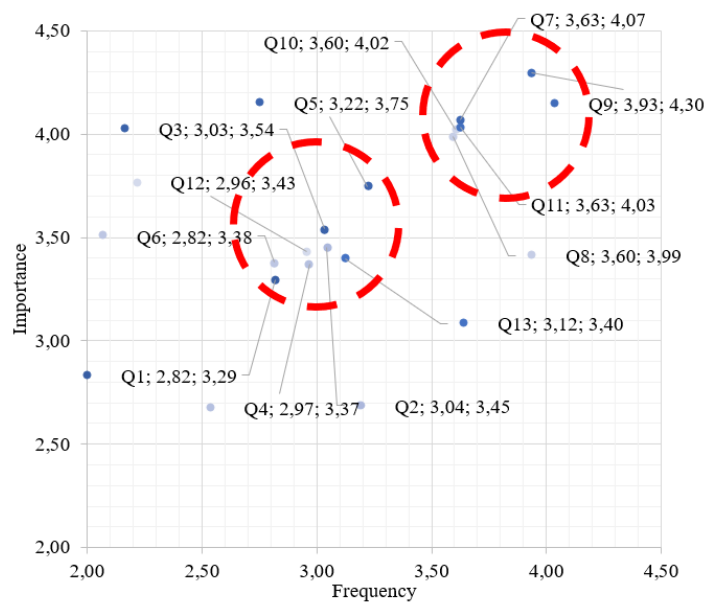
Within the scope of the survey, it was a focal point to gain deeper insights into the most important competences in the field of information security employees should provide when working in an SME. The respondents were asked to take a closer look at the information security strategy in their company and the tasks that are especially relevant. Table 2 shows an overview of different tasks and activities. The importance of the particular activity is measured between "5 – very important" and "1 – not at all", and the frequency between "5 – very often" and "1 – never".

Question	Code
Analysis of business processes and preparation of strategic reports on data protection and information security	Q1
Track and report on changes inside and outside the organisation that affect the organisation's security strategy	Q2
Write company policies on the systematic handling of certain information and data	Q3
Develop recommendations for equipment to be procured, taking into account the company's information security and data protection requirements	Q4
Carry out (information) activities to raise employees' awareness of safety risks in their daily work and to spread safety awareness among the workforce	Q5
Create training plans for the company to regularly train employees on information security and data protection	Q6
Install firewall and anti-virus software Carrying out updates and applying elementary methods to check the security of the software used in the company and preparing appropriate documentation	Q7
Securing mobile devices, communication channels and data storage through passwords or other means of authentication	Q8
Carrying out routine data backups and applying proper conduct methods in accordance with the GDPR to data processing in the company	Q9
Set up administrator accounts and restrict access rights among staff according to the security levels set	Q10
Establish passwords for individual staff access and a secure storage and recovery process	Q11
Create policies and processes for the occurrence of any claims	Q12
Coordinating the needs of managers and employees of the company and providing both parties with information and insights from the company	Q13

Table 2: "Tasks and activities in the field of information security"

Figure 11 shows the results in a cross-tabulation (the frequency is displayed on the x-axis; the importance is displayed on the y-axis). In general, none of the mentioned activities show a low degree of importance or frequency. However, two groups of activities can clearly be distinguished, one with both a disposition to high frequency and importance, the other to medium frequency and importance. The groups have been circled in red in the figure below.

The first group of competences indicate high values in both frequency and importance. To this group belong competences regarding “security testing”, “encoding”, “password management” and “role-based access control”. Within this group, “data management”, i.e. carrying out routine data backups and applying proper conduct methods in accordance with the GDPR to data processing, is characterized by the highest overall value concerning importance and frequency (Q9: 3.93; 4.30). On the other hand, activities in the field of “process/ stakeholder/ compliance management”, “ICT procurement”, “sensitization & influencing”, and “education & training” can be grouped together. All competences are considered to be rather important, the frequency, however, cannot be said to be specifically often. The respondents characterize the field “process management” as least important and least frequent. This area is about the analysis of business processes and preparation of strategic reports on data protection and information security. Nevertheless, the value of 2.82 shows that the topic definitely receives attention in companies.



Learning Units	Code
Process Management	Q1
ICT Risk Management	Q2
Compliance Management	Q3
ICT Procurement	Q4
Sensitization and influencing	Q5
Education and Training	Q6
Security Testing	Q7
Encoding	Q8
Data Management	Q9
Role based access control	Q10
Password Management	Q11
Business Continuity Management	Q12
Mediation and Stakeholder management	Q13

Figure 11: Competences in the company – Results

The figure below focuses on the analysis of competences in SME (Figure 12). The data describe the difference of importance between SME and non-SME: the closer a value lies to zero, the lesser the difference. Therefore, larger values entail larger differences. Positive values stance that competences are more important and frequently used in SMEs, meanwhile negative values represent the opposite. All competences already mentioned can be found in the cross-tabulation. Regarding the description of the axes, it has to be paid attention: In this case, the x-axis shows the importance; the y-axis shows the frequency. It can be mentioned that the domain data management is considered more important and more frequently used in SMEs, too. Figure 11 already showed the high importance of data management (see Q9). The following aspect is especially interesting in the context of partial certification in information security: Code Q6 describes competences and activities in education and training. As Figure 12 shows code Q6 can be found in the field, which is characterized by competences which are

less important and less frequently used in SMEs. Creating training plans to regularly train employees on information security and data protection are obviously less important for SMEs. It is shown that all competences are quite important (mean > 3.3) and frequently used (mean > 2.8). The most important and frequently used competences are the usual tasks of the average system administrator, e.g. creation of backups, installation of anti-virus software and firewalls or establishing of the individual passwords.

4.2.3 Information security in SMEs

In this section the respondents answer more detailed questions related to the information security in their companies. The issue to be examined concerns the reasons which have prevented the company from investing in improving information security (Figure 13). The participants here are only those who chose SME as company type.

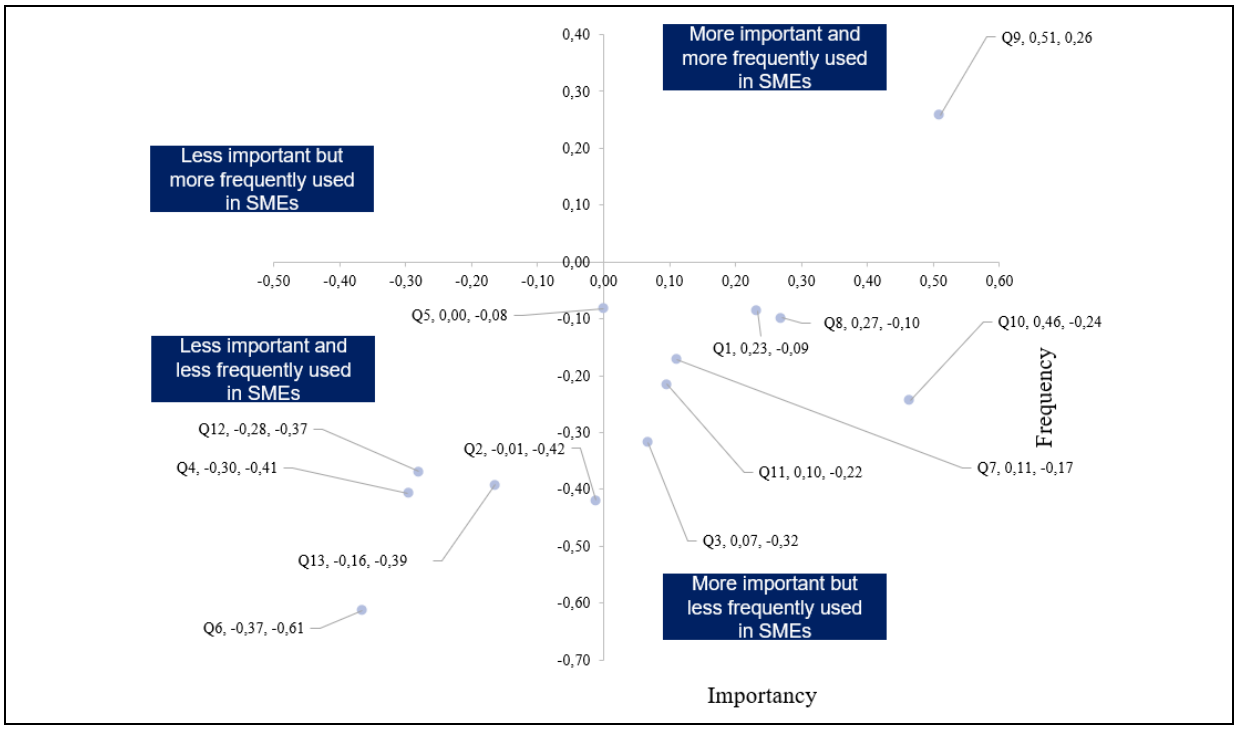


Figure 12: Analysis of competences in SME

As shown in the figure below the major reason is that there are not enough financial resources in the companies (more than 30 % of the respondents gave this reason). Besides, the lack of offers from service providers is also an important aspect regarding the investment problem in the field of information security. On the one hand, about 15 % stated that this problem does not apply in their company, or the firms managed to cover its needs: an aspect which can be considered quite positive. On the other hand, almost one-third of the participants don't perceive any need or rather no priority and stated that other topics have been more important so far. A quite serious point which shows that the topic about information security is not yet central in all companies. Finally, the aspect regarding available personnel seems to play a rather less important role. Only about 4 participants indicated a relation between the lack of personnel and the investment problem in information security.

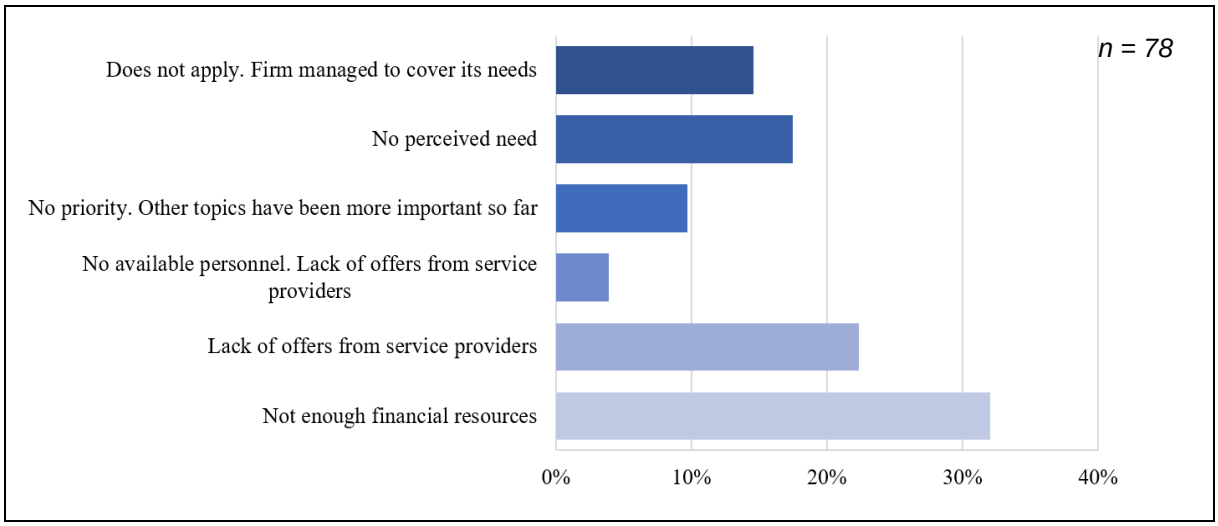


Figure 13: "What reasons have prevented your company from investing in improving information security to date?"

The respondents stress the importance of particular types of education necessary for information security in the company. In this context it was asked what type of education or training is necessary/ helpful/ etc. for an employee tasked with ensuring information security in a firm. It has to be mentioned that there is a difference between necessary skills or trainings ("must-haves") and helpful skills or trainings ("nice-to-have"). Figure 14 shows a great importance with regard to on-the-job experience. Almost half of the participants see this point as "must-have". Moreover, in-house training or continuing education is also relevant and helpful. In general, it can be seen that respondents prefer to have an employee with experience rather than with education. All formats of non-classical studying are just a bit less crucial and more important than all kind of university education.

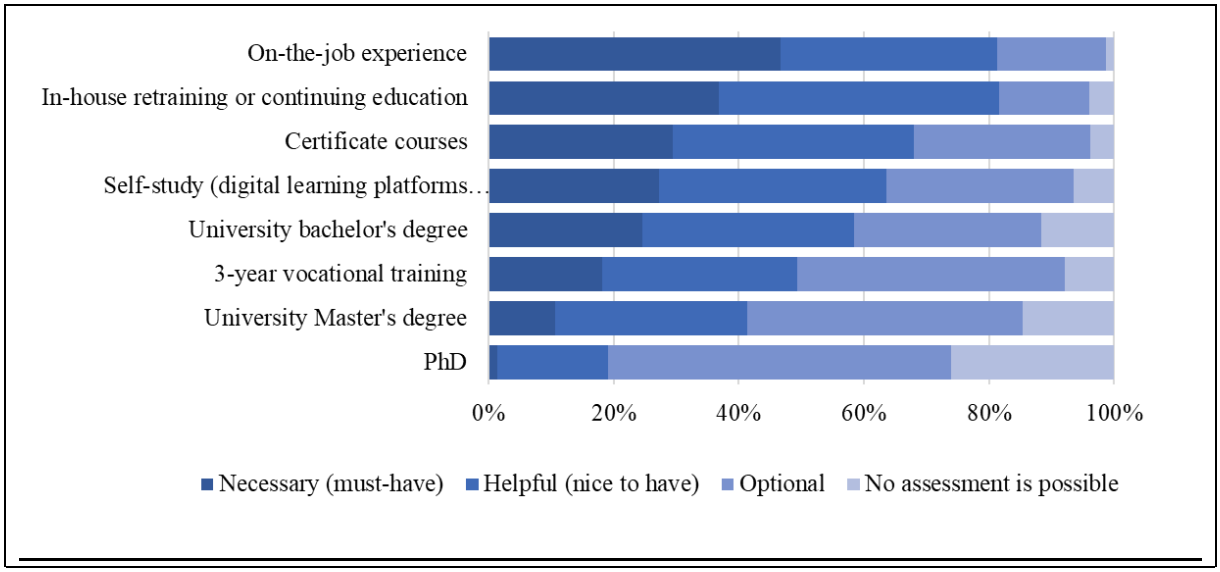


Figure 14: "Building on your experience, what type of education or training is necessary/helpful/optional for an employee tasked with ensuring information security in your organization?"

Within the scope of the survey respondents have been asked about possible options for increasing information security, too (Figure 15). The opportunity to increase qualification of employees is most popular and has been chosen for almost 50% of the time. The other option is to purchase a third-party service, which has been selected 30% of the time. However, creation and filling of a new position or covering the risks through insurance is not as popular.

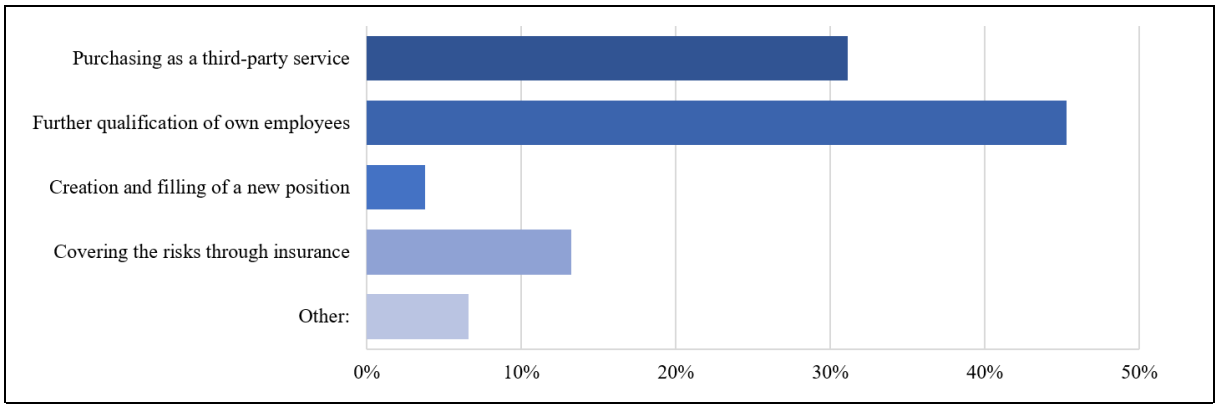


Figure 15: Possible options for increasing information security

The study with regard to information security in SMEs shows that there is a lack of finance and third-party services in the field of information security – major reasons concerning the investment problem in abovementioned area. This is especially important because respondents want to use a third-party service to improve information security in their company. Due to the lack of finance and supply on the market of security services, it seems that our respondents prefer to improve qualifications of their employees to maintain the entertainable level of information security. This is in line with educational requirements: respondents prefer to hire someone with experience rather than with education.

4.2.4 Information security in the company: personnel requirements

A further point which was analysed within the scope of the survey was the personnel requirement regarding information security in the company. To this end, differentiation not only between SMEs and non-SMEs were analysed, but also the different situations of firms considering the existence of information security incidents. Especially the latter provides a clear picture of changing attitudes of firms towards information security and information security spending. The existence of information security incidents is shown in Figure 16.

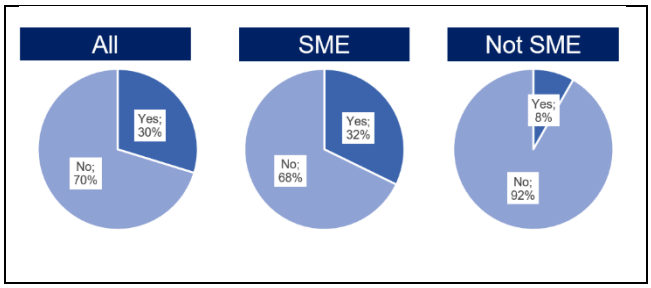


Figure 16: "Are you aware of any information security incidents within the last 2 years or is there a suspicion of a security incident?"

With the end to understand more about the personnel reality in firms, respondents were asked how many employees they currently deploy with main focus of work concerning information security, and how many employees they plan to employ among the coming years. It becomes apparent that there is normally one employee who is formally responsible for information security in most of the companies. Even in non-SMEs are usually not more workers responsible for this field of activity (Figure 17). Above is shown whether there is personnel employed, below can be seen the equivalent numbers of the firms that affirmed the first question.

Further it was asked how many open information security positions are in the company. As Figure 18 shows, about 50 % of the respondents answered that there are currently no open positions in information security in their firm. When considering the appearance of an information security incident (IS) a sharp increase in positions created can be noted. Among the firms who did not have an information security incident (NO IS), around 90 % don't have a specific position for information security. This number decreases to only 20 % in comparison to firms who experienced an incident. Comparable numbers have been reported for the existence then more than one position, illustrating the initiative that firms take after an attack.

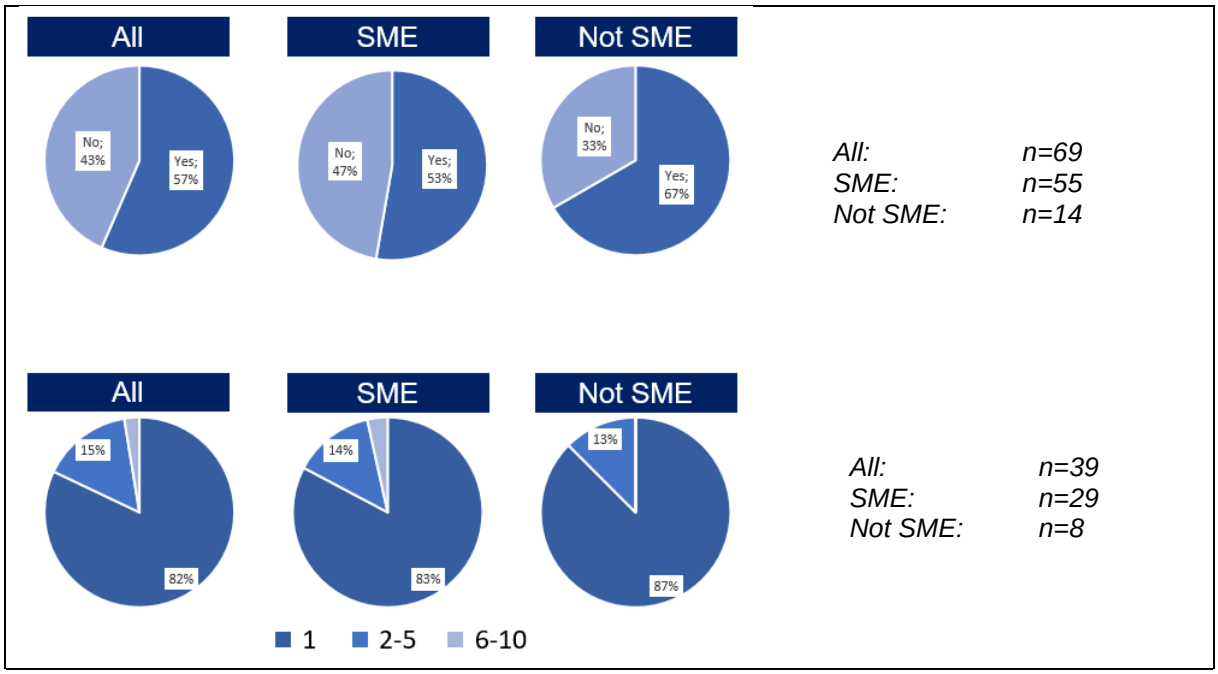


Figure 17: "Are there employees in your company who are formally responsible for information security? (above) – If so, how many?" (below)

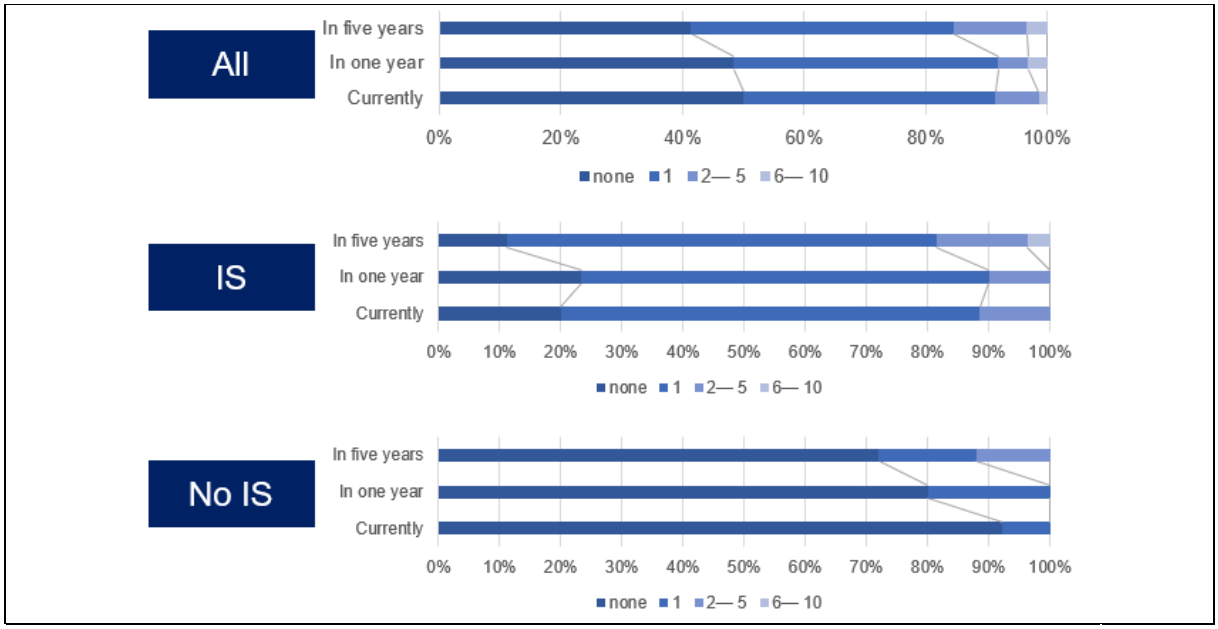


Figure 18: "How many open information security positions are there in your company?"

In this context, respondents were further asked how they tackle the human resource needs in information security so far. Figure 20 shows that especially non-SMEs attach great importance to further training of employees. Looking at SMEs, it can be seen that the purchase of “information security” service from third-party providers is approximately equivalent to further training of employees. Hiring new employees, in contrast, is less significant for the companies. It can be concluded that across the board, the development of internal capacities and further training of own employees is considered to be the most suitable solution for most firms. Nonetheless, there is a caveat to validity of the data reported, which becomes evident when considering firms which experienced an information security incident, and firms which did not. As can be seen in Figure 21 the item “no measures” decreases from 31 % (most frequently named) among firms without an information security incident to only 10% (least named) among firms with an information security incident.

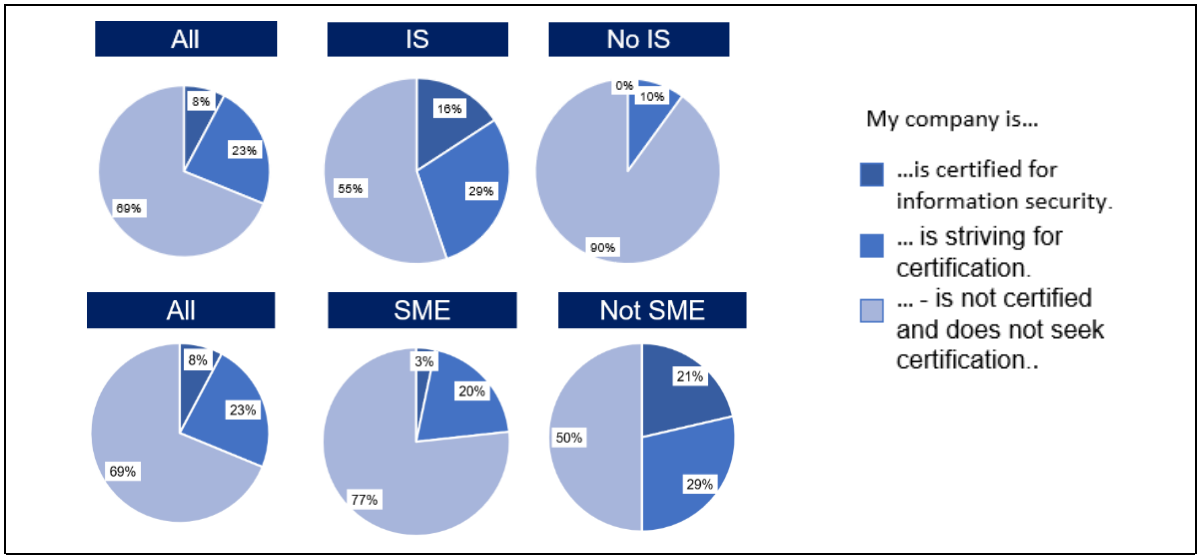


Figure 19: Business certification for information security

Analogue numbers can be observed by the existence of certifications among SMEs and non-SMEs, as well as among firms with an information security incident. Meanwhile certification are barely prominent among SMEs (3 %), they are completely absent among SMEs without an information security incident. For firms which had an incident, numbers both for existing certifications and planned certifications significantly increase.

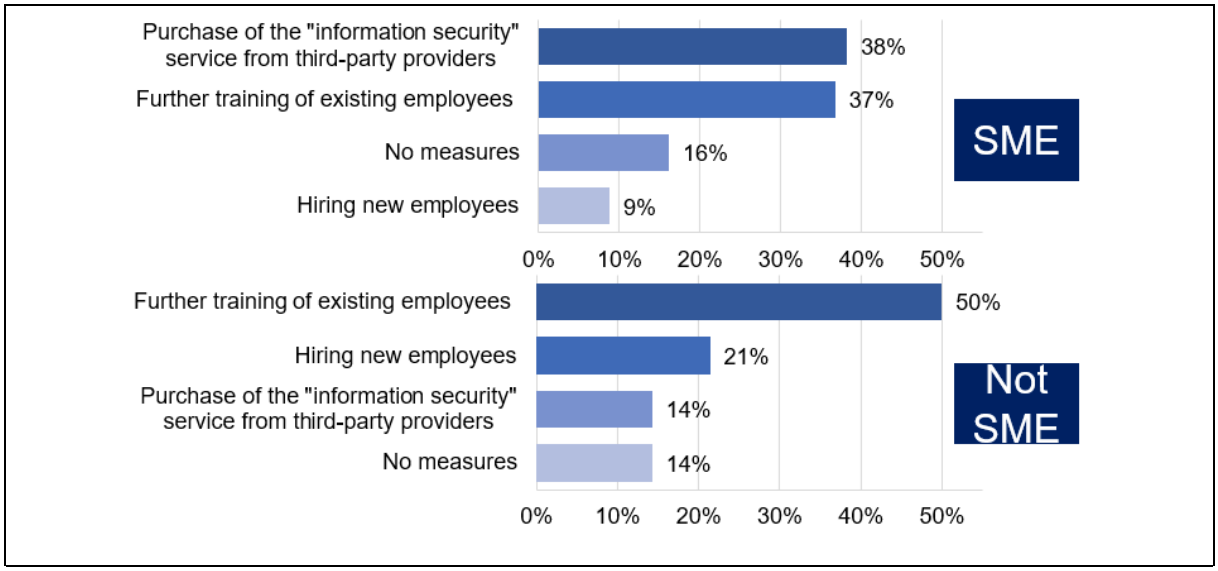


Figure 20: “How are you tackling the human resource needs in the area of information security so far?”

Considering the scope of this survey, it is not only important to understand the situation of certification and investment, but also the measures already undertaken to deal with information security challenges. As seen in the figure below two-third of the respondents answered this question in the negative. However, this also means that about 30 % answered in the affirmative.

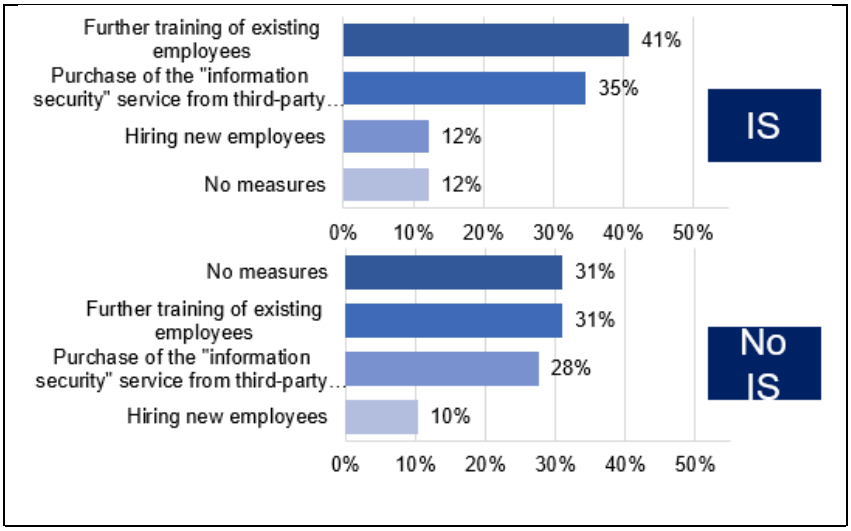


Figure 21: "How are you tackling the human resource needs in the area of information security so far?" – IS and No IS

Considering the findings from Figure 18 and Figure 21 the sentiment that firms only get active after an attack becomes apparent. Not only do firms see the need for the creation of a full-time equivalent position, but they also look deeper into possibilities of improving their information security by any means. It can be concluded that the existing sentiment among information security practitioners and the information security community, "learning by pain" is an accurate description of the reality in most firms. The understanding to take acute measures and to invest resources into employees grows most often than not after an attack – when the damage is already done.

4.2.5 Self-assessment of competencies

Within the scope of the survey respondents were asked to evaluate themselves with regard to relevant education and training activities in the field of information security. They had available a scale from "0 – No Experience", "1 - General knowledge", "2 - General knowledge plus practical experience", "3 - Advanced theoretical knowledge" to "4 – Advanced theoretical knowledge plus practical experience". The figure below shows that password and data management were often mentioned. This includes for example establishing passwords or carrying out routine data backups. From the values obtained the averages were taken and enlisted in the figure below. Meanwhile respondents on average felt most experienced with password management, data management and education and training, less confidence was expressed concerning the compliance ensurance, encoding and employee sensitization.

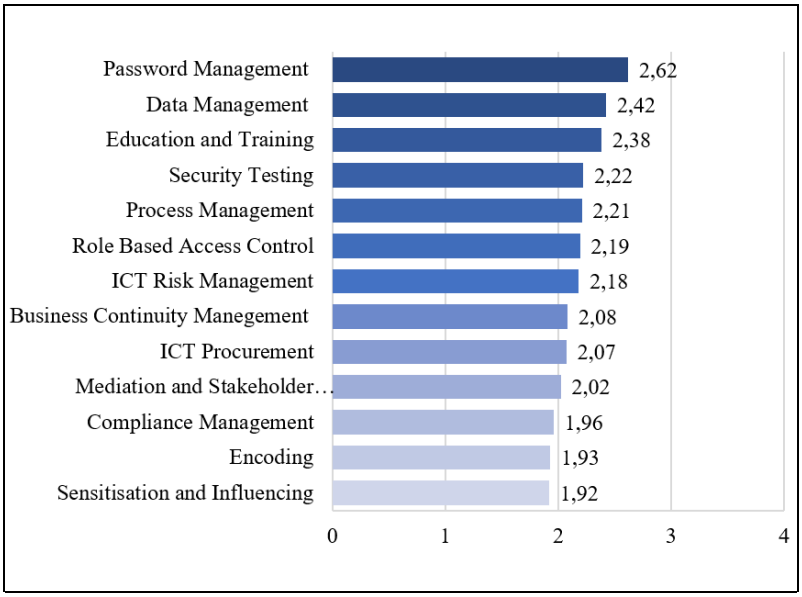


Figure 22: "Please evaluate yourself: Which of the following education and training activities can you perform?"

4.2.6 **Personality (Big Five)**

Throughout many discussions with experts, it became clear that the job of information security poses special requirements onto practitioners considering their social skills. However, it became evident that in the majority of cases, it was implicitly also referred to personal characteristics. In this regard, the "correct attitude" does not limit itself to the conduct with employees and within the realm of the workplace, but the conduct in general considering the disposition of character treats. It is therefore an intention to with this survey to shed some light into the disposition of character traits and job performance among information security experts. The results can be seen as an indication of favourable preconditions for new employees in the work place.[4] To this end, the Big five personality traits (Rammstedt et al. 2013) were deployed, providing a five-factor model of grouping of personality traits. According to this model, the following five basic factors describe most personality traits in dichotomous, where each trait entails two extremes:

Dimension	High Scores	Low Scores
Openness	inventive/curious	consistent/cautious
Conscientiousness	efficient/organized	extravagant/careless
Extraversion	affectionate, joiner, talkative, fun loving, active, passionate	reserved, loner, quiet, sober, passive, unfeeling
Agreeableness	friendly/compassionate	critical/rational
Neuroticism	sensitive/nervous	resilient/confident

Table 3: Dimensions of Big-5.

The BFI-10 is a 10-item scale measuring the abovementioned traits. This scale was specifically developed to be short and designed for situations in which respondents are limited in time. Each BFI-10 scale consists of one true-scored and one false-scored item, e.g., to obtain the measurement of openness, the value from question six is extracted from question ten's value. The higher the result, the more inventive/curious a person is.

Nr.	Items	Polar-ity	Subscale
1	I am rather reserved reserved.	-	Extraversion
2	I trust others easily and believe in the good in people.	+	Agreeableness
3	I am rather comfortable and tend to laziness.	-	Conscientiousness
4	I am rather relaxed and handle stress well.	-	Neuroticism
5	I have few artistic interests.	-	Openness
6	I am outgoing and sociable.	+	Extraversion
7	I tend to criticize others.	-	Agreeableness
8	I complete tasks thoroughly.	+	Conscientiousness
9	I get nervous easily.	+	Neuroticism
10	I have an active imagination.	+	Openness

Table 4: Structure of BFI-10

[4] The reference to the following personality profiles for future use needs to be taken with thoughtful consideration of several limitations such measurement methods entail. First, personality is not a stable construct and changes over time. The result received from the questionnaire is likely to vary across several repetitions over time. Secondly, social desirability can not be excluded, as participants tend to answer what they would like to be, instead of providing a truthful picture.

From the histograms below it can be inferred that among all respondents, people tend to be efficient/organized rather than extravagant/careless (see conscientiousness). Answers are also positively distributed in openness; we can see that more respondents identify themselves as inventive/curious rather than consistent/cautious (see openness). Respondents are almost equally distributed among definitions of extraversion, with a marginal positive leniency, i.e. respondents are considered to be more outgoing/energetic than solitary/reserved (to a very limited extent). The opposite situation can be observed for neuroticism and agreeableness. In this case respondents are more resilient/confident and critical/rational rather than sensitive/nervous and friendly/compassionate respectively. The overall leniency can be seen in Figure 24.

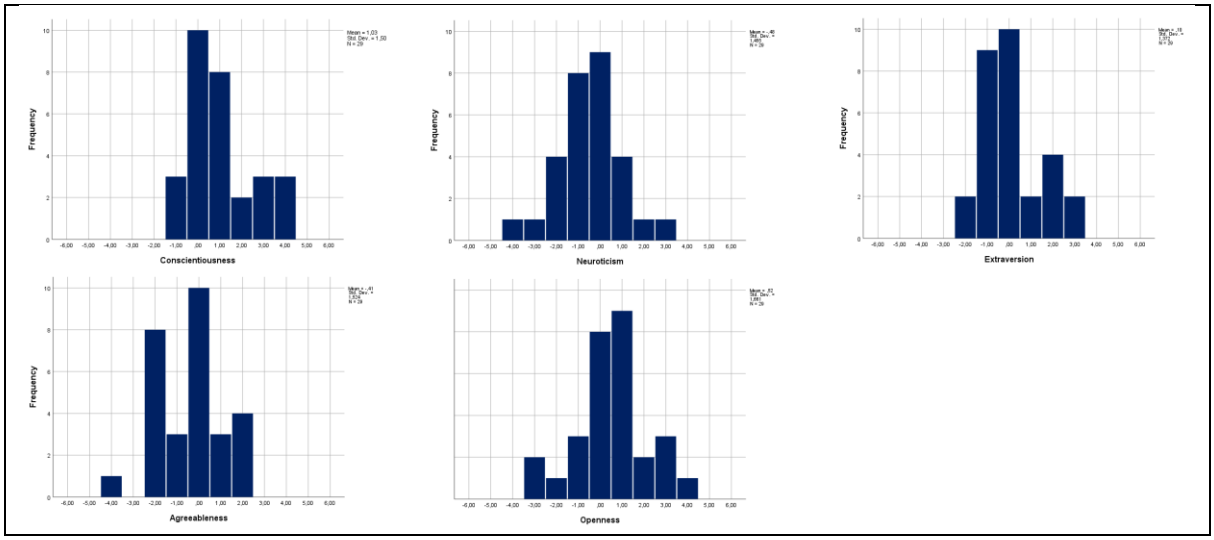


Figure 23: Big-Five histograms observed for information security practitioners.

From the leniency several crucial assumptions about the character traits of information security experts can be inferred. Most dominant factor is the positive value for conscientiousness, entailing strong dispositions towards efficient and organized conduct. The negative values for neuroticism supports the sentiment from experts, that resilience and confidence in the own work play important roles on the job. Further, experts can be characterized to be consistent and cautious (openness), critical and rational (agreeableness) and to a limited extent reserved (extraversion).

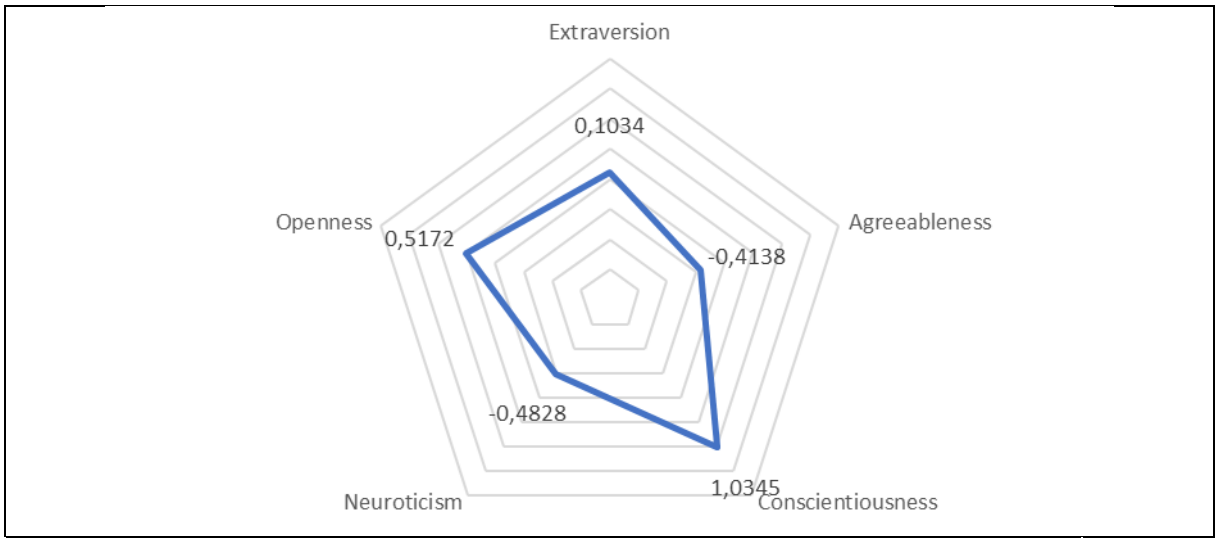


Figure 24: Big-Five, mean value comparison

As we can see from the charge matrix shown in Table 5, generally, all items show their highest charge on the corresponding factor, in line with the hypotheses. That speaks in favour of the validity of the approach in our case.

Item	E	A	C	N	O
I see myself as someone who is reserved.	**,411***	0.067	0.212	-0.264	-0.169
I see myself as someone who is generally trusting.	**-,422***	**-,572****	-0.054	-0.081	0.210
I see myself as someone who tends to be lazy.	-0.163	0.138	**-,597****	0.097	0.294
I see myself as someone who is relaxed, handles stress well.	0.193	0.039	0.113	**-,379***	-0.233
I see myself as someone who has few artistic interests.	-0.101	-0.006	**-,375***	0.089	**,670****
I see myself as someone who is outgoing, sociable.	**-,635****	**-,401***	-0.194	0.067	0.095
I see myself as someone who tends to find fault with others.	0.091	**,538****	-0.154	0.283	-0.026
I see myself as someone who does a thorough job.	0.281	0.039	**,566****	-0.335	-0.264
I see myself as someone who gets nervous easily.	-0.137	0.350	-0.271	**,678****	0.000
I see myself as someone who has an active imagination.	0.191	0.267	0.175	-0.137	**-,493****

Table 5: "Validity test: Correlation between Items and groups"

The reserved respondents are thinking of themselves as relaxed ones. They also believe they do a thorough job and have an active imagination. Respondents that marked themselves as generally trusting, also more outgoing and sociable. Lazy respondents have few artistic interests, are outgoing and sociable, but also find fault with others. Relaxed ones think they do a thorough job and have an active imagination. Those who tend to find fault with others get nervous easily and see themselves as someone who has an active imagination. Finally, “thorough” respondents have an active imagination.

4.2.7 **Work Performance**

This part is based on the Individual Work Performance Questionnaire (IWPQ). IWPQ is an 18-item scale developed by Ramos-Villagrasa et al. (2019) to measure the three main dimensions of job performance:

- task performance (5 items)
- contextual performance (8 Items)
- counterproductive work behaviour (5).

All items have a recall period of three months and a 5-point rating scale (0 = seldom to 4 = always for task and contextual performance; and 0 = never to 4 = often for counterproductive work behaviour). For counterproductive behaviours, the scale entails a negative polarity, so that lower values are more desirable, as this translates into lower counterproductive behaviours generally. The respective values are illustrated in Figure 25 to Figure 27, the final profile combined in Figure 28.

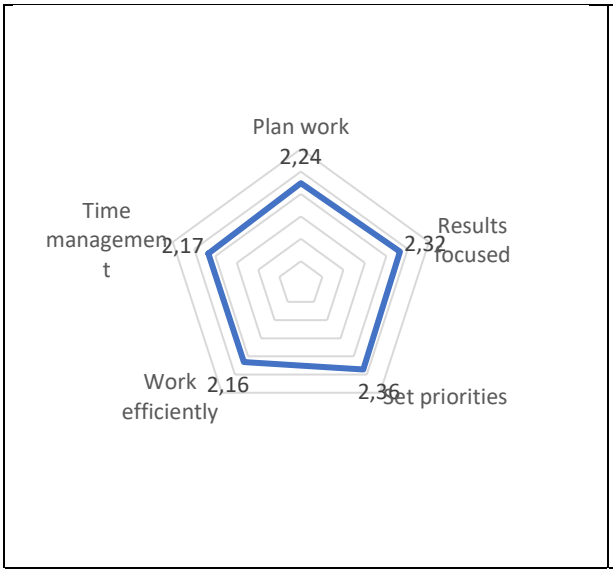


Figure 25: Task Performance

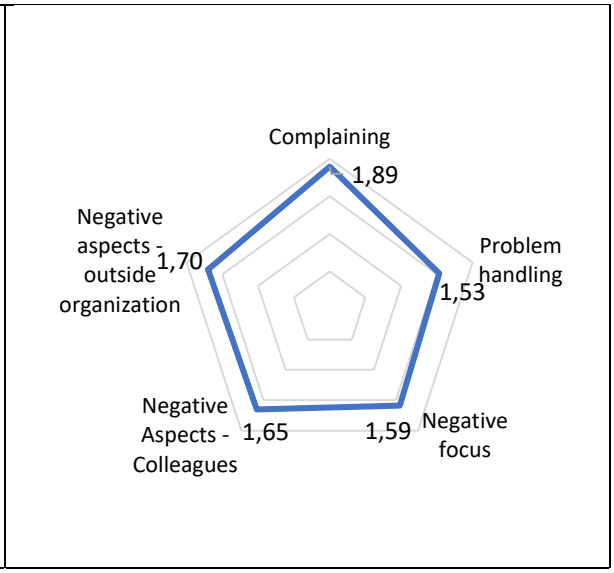


Figure 26: Counterproductive Behavior

It sticks out that participants dispose of a low score for counterproductive behaviours, underpinning the result from the BIG.5 test that resilience and high-tolerance rate are important aspects for the work of an information security practitioner. Looking into the individual categories, most prominent factors are “updating job related knowledge” (2,32) and “active participation” among contextual performance, a weak “focus on the negative aspects of the work” (1,59) and strong “problem handling” orientation (1,53) among counterproductive behaviours and high focus on “setting priorities” (2,36) and “results focused” (2,32 in task performance.

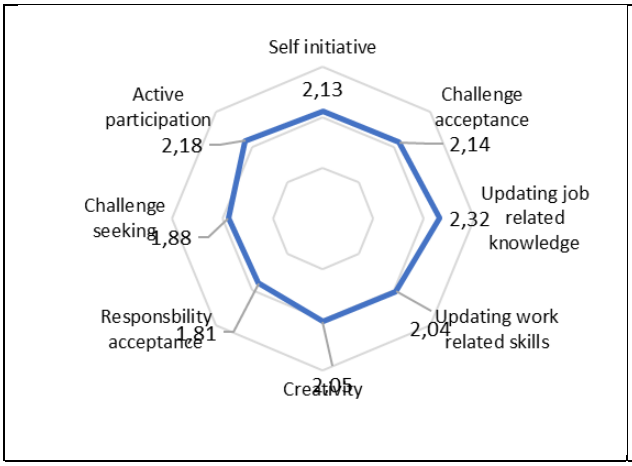


Figure 27: Contextual Performance

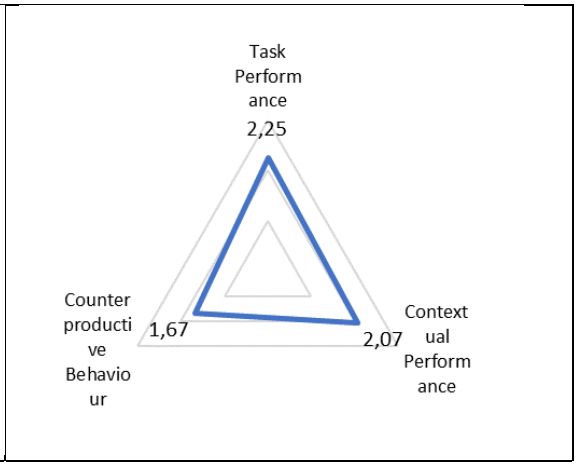


Figure 28: IWPQ results for Information security experts

As shown in Figure 28, the measure for task performance is higher than other measurements, and the measurement for contextual performance is higher than one for counterproductive behaviour. These findings are in line with previous studies. Still, the task performance is significantly lower than baseline findings of other articles, indicating problems in this field - higher measures for counterproductive behaviour support this finding. Measurement for contextual performance is also lower than one from other studies, but not significantly.

In conclusion, we can say that the participants from the IT and information security field are less productive than those usually observed in the relevant studies.

4.3 Summary

All in all, the study provides important insights regarding information security in SMEs. Concerning the situation on the labour market and the capacity in the companies, it has to be mentioned that there is no employee who is formally responsible for information security to date in more than 50 % of the firms. If participants answered in the affirmative, only one employee is responsible for this field of activity in most cases. Looking at the development of job offers little changes can be observed. A fraction of companies will create about six to ten jobs in the area of information security in the next five years.

The findings substantiate the existing sentiment of “learning by pain”, i.e. that first an incident has to occur before firms engage in security activities. This statement is underpinned by the consistent findings concerning certifications, creation of specific positions and generally measures taken concerning information security.

Concerning the required type of education and training the great importance of job-experience can be pointed out. Almost half of the participants stated that this is especially relevant. In general, respondents prefer to have an employee with experience rather than with education. In lights of the existing scarcity of hiring possibilities on the labour market, firms consider the further qualification of existing employees to be the most feasible options to cover the human resource need.

Finally, an assessment of characteristic traits via the Big 5 personality test and the IWPQ, important traits of employees have been identified which can be determined among new employees in the field. Among a strong disposition of resilience in both tests, especially an organized working routine and a critical and analytical approach have been determined as characteristic traits among information security specialists.

5 Guide for SMEs

Data protection and information security gained significant relevance as ICT application became more intense in organizational and management processes within SME's. The pressure of SME's to better manage information security and data protection arise from several directions. First, the process and data management in SME's became highly dependent on ICT infrastructure. Second, the legislation surrounding privacy and data protection was strengthened and codified in higher detail. Third, the public awareness about the right to privacy and responsibility for personal data usage is heightened. Several data leakage incidents worldwide also played a part in realizing that information security is a priority issue when using digital services. SME's were affected by digitalization in lower rates compared with big enterprises. However, significant part of them work with personal digital records. Some of the SME's manage sensitive data. All of those factors lay a foundation for better regulating and assurance of information security and data protection in SME's. Updated regulation from European Union left some SME's struggling with finding or preparing suitable staff that could fulfill stricter requirements for information security and data protection.

Based on the literature review and information gathered during project results dissemination events, it can be concluded that there are multiple areas for SME's where information security and data protection issues require additional attention. The following guidelines stress the main considerations and possible solutions for the issues related to information security and data protection that SME's face.

1. Implementation of GDPR resulted in significant changes in digital and physical records management practices for SME's. Some organizations did not have proper physical and digital infrastructure to fulfill the new requirements. In majority of the cases the transitional period before GDPR implementation was used to compensate infrastructural shortcomings. One of the most tangible actions for SME's is to audit physical infrastructure condition and fix the shortcomings that defy requirements for proper information security and data protection assurance in organization. Firstly, there needs to be an inner document that would define the procedures and regulations related to information security and data protection (including binding corporate rules if organization transfers data to non-EU counties). Secondly, there needs to be physical access limitations to physical records (lockers, safes, limited access areas). Personnel needs to be informed about procedures related to data management (information disclosure restrictions, keeping the records closed from public access, data usage consent policies, password and workplace security policies, user rights management).

2. Data subjects (clients) need to be informed about the data management practices in the areas where their data are being used. Clients need to give a grant the access personal data, and to be informed about the right to ask for correction of related data, object to processing, withdraw consent on accessing the data, file a complaint, ask for deletion of the records, object transactions of data with other data management subjects.

3. Another area where SME's face inconsistencies with information security and data protection regulations is collection of data that should not be collected or stored. The data is usually being collected because of outdated processes of workflows. In some instances, data are being tied to information systems or other digital identification measures. To avoid such cases SMEs should focus on keeping the minimal amount of data necessary and deleting the data if their purpose of usage is irrelevant. Existing records should be stored and managed based on transparent algorithms and procedures. Such security policies as "clean desk", or "locked screen" should be considered as default in SME's.

4. Fourth guideline is related with the quality of education and certification. Literature analysis and direct stories from the SME's employees reveal that for small and medium organizations certification is not the most optimal way in choosing the candidates who could work with private information. The main criterion is knowledge and competencies that would cover ICT and legal domain, as well as other more interdisciplinary social skills. SMEs usually don't have proper resources to hire well-trained specialist to upkeep the informational infrastructure. Also, the fields of operations for various SME's also vary greatly. This creates a problem where universal training courses or certificates do not equip the employees with specific knowledge, applicable in narrow domains. SMEs require practically applicable and scenario-based training courses with the real-life examples. One of the ways how to ensure this information to be available is to document the processes within organization and later share the experiences through professional networks or community events. Alternatively, SMEs could initiate cooperation with higher education institutions that could scientifically analyze the cases enriching existing body of knowledge in specific domains.

5. The final guideline is related with the inconsistencies or imperfections in legal regulations. For some institution's information and personal data exchange limitations may be a serious burden in order to secure the interests of their clients. For instance, a retirement home has a constant resident who has no family members left. In case of emergency the resident is being taken to the hospital, the current institution does not give private information to the third parties (including retirement home). If the client is being transferred to another hospital, the retirement home needs to do their own investigation in order to find their resident. In this case both institutions obey the law but the situation creates legal gaps that require fixing. SMEs should initiate correction or initiation of legal norms (through political representatives) that would cover such issues.

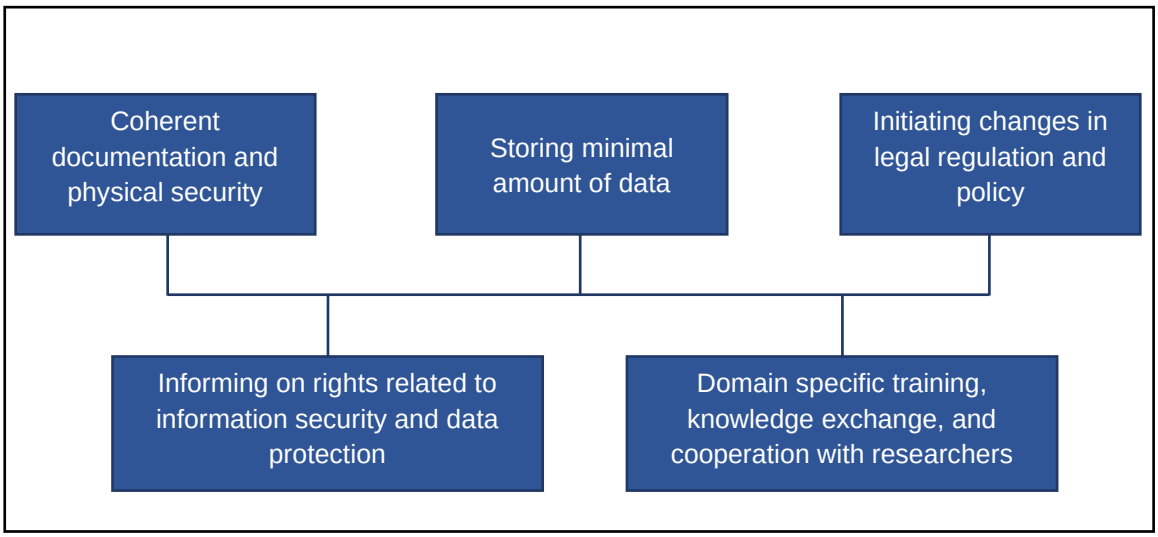


Figure 29: Guidelines based on common problems that SME's face in information security and data protection

6 Outlook & Recommendations

During the implementation of the TeBeISi project, the activities revealed that the need for information security and personal data protection training for small and medium enterprises and social institutions is high. These organizations often face financial disadvantages in hiring a professional data protection officer, so often these functions are assigned to another employee. The aim is to comply with GDPR requirements and ensure the protection of personal data of both customers and company employees. The project also showed that training on information security and personal data protection is relatively expensive and that SMEs are very happy to receive quality training on the use of GDPR free of charge (Erasmus plus project-supported training) and to improve staff competencies in information security and personal data protection areas.

The questionnaire developed during the project allowed employees of small and medium enterprises to assess their existing competencies in the field of information security and personal data protection. The curriculum created during the project gives stakeholders the opportunity to choose the appropriate training. Associated partners, SMEs, educational institutions and public authorities expressed interest in continuing the path of the TeBeiSi project and to built upon the results of the project in future initiatives. Therefore, the project partners plan to continue joint activities and to develop and test a training package in all project partner countries during the next project.

The implemented project activities allow to recommend companies to pay more attention to internal communication and training (both by organizing trainings in companies and by sending employees to trainings). All employees, especially those who come into direct contact with personal data in the work environment, should be aware of data protection requirements, be constantly trained on what personal data is, how to recognize it, what can and cannot be done with personal data. It is also necessary to make a realistic assessment of the requirements for the collection of personal data, i.e. to maintain a surplus fund, only necessary for the collected personal data. Small and medium sized enterprises as well as social service institutions should assess the impact of GDPR and identify problem areas, which would allow time for employee training and awareness-raising.

It is also suggested that companies first carry out an audit of the personal data they collect and hold, in order to identify which data processing operations to focus on. This would help reveal which processes related to personal data management and information security require additional attention and staff competencies to be improved. From the questionnaire conducted it can be inferred that SMEs are most comfortable with investments into existing employees, yielding the most cost-effective trade-off regarding resources needed and security.

7 Literature

Adamkiewicz, S. L. (2005). *The correlation between productivity and the use of information security controls in small businesses.* Dissertation Abstracts International, 66(03), 1541B. (UMI No. 3167184).

Albrechtsen, E., & Hovden, J. (2010). Improving information security awareness and behaviour through dialogue, participation and collective reflection. Anintervention study. *Computers & Security, 29*(4), 432–445. doi: 10.1016/j.cose.2009.12.005

Anderson, C. L. & Agarwal, R. (2010). Practicing safe computing: A multimethod empirical examination of home computer user security behavioral intentions. *MIS Quarterly*, *34*(3), 613-643.

Baker, W. H., & Wallace, L. (2007). Is information security under control? *IEEE Security & Privacy,* 5, 36-44. doi:10.1109/MSP.2007.11.

Barlow, J. B., Warkentin, M., Ormond, D., & Dennis, A. R. (2018). Don't Even Think About It! The Effects of Antineutralization, Informational, and Normative Communication on Information Security Compliance. *Journal of the Association for Information Systems*, *19*(8), 689–715. doi: 10.17705/1jais.00506

Barnard-Wills, D., Cochrane, L., Matturi, K. & Marchetti, F. (2019). *Report on the SME experience of the GDPR*. https://www.trilateralresearch.com/wp-content/uploads/2020/01/STAR-II-D2.2-SMEs-experience-with-the-GDPR-v1.0-.pdf

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. doi: 10.2307/25750690

Burns, A. J., Roberts, T. L., Posey, C., Bennett, R. J., & Courtney, J. F. (2018). Intentions to Comply Versus Intentions to Protect: A VIE Theory Approach to Understanding the Influence of Insiders' Awareness of Organizational SETA Efforts. *Decision Sciences*, *49*(6), 1187–1228. doi:10.1111/deci.12304

Burns, A.J., Roberts, T.L., Posey, C., Bennett, R.J., & Courtney, J.F. (2015). Assessing the role of security education, training, and awareness on insiders' security related behavior: An expectancy theory approach. *Proceedings of the IEEE 48th Hawaii International Conference on Systems Sciences, HI.* doi:10.1109/HICSS.2015.471

Colwill C. (2009). Human factors in information security: the insider threat–who can you trust these days? Information Security Technical Report, *14*(4),186–96. doi:10.1016/j.istr.2010.04.004

D'Arcy, J., & Hovav, A. (2009). Does one size fit all? Examining the differential effects of IS security counter measures. *Journal of Business Ethics*, *89*(1),59–71. doi:10.1007/s10551-008-9909-7

D'Arcy, J., Hovav, A, Galletta, D. (2009). User awareness of security counter measures and its impact on information systems misuse: a deterrence approach. *Information Systems Research*, *20*(1), 79-98. doi: 10.1287/isre.1070.0160

Davies, J. S., & Hertig, A. C. (2008). *Theory and practice of asset protection. Security, supervision and management*. Burlington, MA: Elsevier.

Doherty, N. F., & Fulford, H. (2005). Do Information Security Policies Reduce the Incidence of Security Breaches: An Exploratory Analysis. *Information Resources Management Journal, 18*, 20-38.

Easttom, C. (2006). *Computer security fundamentals*. Upper Saddle River, NJ: Prentice Hall.

Path to Cyber Resilience: Sense, Resist, React. EY's 19th Global Information Security Survey 2016-17. https://www.ey.com/Publication/vwLUAssets/EY-giss-india/$FILE/EY-giss-india.pdf

Eurostat (2008): NACE Rev. 2. Online verfügbar unter https://ec.europa.eu/eurostat/de/web/nace-rev2, zuletzt geprüft am 08.07.2021.

European Comission (2021): SME definition - Internal Market, Industry, Entrepreneurship and SMEs. Online verfügbar unter https://ec.europa.eu/growth/smes/sme-definition_en, zuletzt aktualisiert am 30.08.2017, zuletzt geprüft am 08.07.2021.

Gardner, B., & Thomas, V. (2014). *Building an information security awareness program: Defending against social engineering and technical threats*. New York, NY: Elsevier.

Goodwin, B. (2005, February 14). *Big guns target supply chain threat. Computer Weekly*. http://www.computerweekly.com/.

Guinote, A., & Vescio, K. T. (2010). *The social psychology of power*. New York, NY. The Gilford Press.

Hallová, M., Polakovič, P., Šilerová, E., & Slováková, I. (2019). Data Protection and Security in SMEs under Enterprise Infrastructure. *Agris On-Line Papers in Economics & Informatics*, *11*(1), 27–33. doi:10.7160/aol.2019.110103

Herath, T., & Rao, H. R. (2009a). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, *47*(2), 154–165. doi: 10.1016/j.dss.2009.02.005

Herath, T., & Rao, H. R. (2009b). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems*, *18*(2), 106–125. doi: 10.1057/ejis.2009.6

Yoo, C.W., Sanders, G.L., & Cerveny, R.P. (2018). Exploringthe influence of flow and psychological ownership on security education, training, and awareness effectiveness and security compliance. *Decision Support Systems*, *108*, 107-118. doi: https://doi.org/10.1016/j.dss.2018.02.009

Jasmontaitė-Zaniewicz, L., Calvi, A., Nagy, R. & Barnard-Wills, D. (2021). *The GDPR Made Simple(r) for SME's*. doi: 10.46944/9789461171092

Jenkins, J. L. & Durcikova, A. (2013). What, I shouldn't have done that?: The influence of training and just-in-time reminders on secure behavior. *Proceedings of the International Conference on Information Systems*. AIS. https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.661.9290&rep=rep1&type=pdf

Johnston, A. C. & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *MIS Quarterly*, *34(*3), 549-566. doi: 10.2307/25750691

Johnston, A. C., Warkentin, M., & Siponen, M. (2015). An enhanced fear appeal framework: Leveraging threats to the human asset through sanctioning rhetoric. *MIS Quarterly, 39*(1), 113-134. doi: 10.25300/MISQ/2015/39.1.06

Jöns, Ingela; Hodapp, Markus; Weiss, Katharina (2005): Kurzskala zur Erfassung der Unternehmenskultur. Online verfügbar unter http://psydok.psycharchives.de/jspui/handle/20.500.11780/349.

Karjalainen, M., & Siponen, M. (2011). Toward a new meta-theory for designing information systems (IS) security training approaches. *Journal of the Association for Information Systems*, *12*(8), 518–555.

Kluge, EH. (2007). Secure e-health: managing risks to patient health data. International Journal of Medical Informatics**,** *76* **(**5–6**)**, 402-406**.** doi: 10.1016/j.ijmedinf.2006.09.003

Kogenhop, G. (2020). Tooling for optimal resilience. *Journal of Business Continuity & Emergency Planning*, *13*(4), 352–361.

Kumar, V., Batista, L. & Maull, R. (2011). The Impact of Operations Performance on Customer Loyalty. *Service Science*, *3*(2), 158-171. doi:10.1287/serv.3.2.158

Kuusisto, T., & Ilvonen, I. (2003). Information Security Culture in Small and medium size enterprises. *Frontiers of e-business research*, 431-439.

Lee, J. K., Cho, D., & Lim, G. G. (2018). Design and validation of the Bright Internet. *Journal of the Association for Information Systems*, 19(2), 63-85.

Leede, J. & Looise, J. K. (2005). Innovation and HRM: Towards an integrated framework. *Creativity and Innovation Management, 14* (2), 108-117. doi: 10.1111/j.1467-8691.2005.00331.x.

Leilanie Del Prado-Lu, J. (2005). *Gender, information technology, and health*. Quezon City, Philippines: The University of the Philippines Press.

Liang, H. & Xue, Y. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the Association for Information Systems*, *11*(7), 394-413.

McAfee, I. (2010). *A good decade for cyber crime*. http://www.mcafee.com/ca/resources/reports/rp-good-decade-for-cyber crime.pdf.

McConnell, J. P. (2020). *UNIX Administrator Information Security Policy Compliance: The Influence of a Focused SETA Workshop and Interactive Security Influence of a Focused SETA Workshop and Interactive Security Challenges on Heuristics and Biases Challenges on Heuristics and Biases*. https://nsuworks.nova.edu/cgi/viewcontent.cgi?article=2127&context=gscis_etd.

Mohjel Eghdam, A., Khameneh, S., Hasankhni, H, Moghadam, S., Zamanzadeh V. (2013). Nurses' performance on Iranian nursing code of ethics from Patients' perspective. *26*(84),1–11. doi: 10.5681/jcs.2013.027

Newell, S., & Marabelli, M. (2015). Strategic opportunities (and challenges) of algorithmic decision-making: A call for action on the long-term societal effects of datification. *The Journal of Strategic Information Systems, 24*(1), 3-14. doi: 10.2139/ssrn.2644093

Noguerol, L. O., & Branch, R. (2018). Leadership and Electronic Data Security within Small Businesses: An Exploratory Case Study. *Journal of Economic Development, Management, IT, Finance & Marketing*, *10*(2), 7–35.

Northouse, P. G. (2010). *Leadership: Theory and practice* (5th ed.). Thousand Oaks, CA: Sage.

O'Rourke, M. (2003). Cyber attacks prompt response to security threat. *Risk Management, 50*(1), 8.

Peikari, H. R., T., R., Shah, M. H., & Lo, M. C. (2018). Patients' perception of the information security management in health centers: the role of organizational and human factors. *BMC Medical Informatics & Decision Making*, *18*(1), 1–13. doi:10.1186/s12911-018-0681-z

Posey, C., Roberts, T. L., Lowry, P. B., Bennett, R. J., & Courtney, J. F. (2013). Insiders' protection of organizational information assets: Development of asystematics-based taxonomy and theory of diversity for protection-motivated behaviors. *MIS Quarterly, 37*(4), 1189–1210. doi: 10.25300/MISQ/2013/37.4.09

Posey, C., Roberts, T., & Lowry, P.B. (2015). The impact of organizational commitment on insiders' motivation to protect organizational information assets. *Journal of Management Information Systems, 32*(4), 179–214. Doi: 10.1080/07421222.2015.1138374

Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: An action research study. *MIS Quar-terly*, *34*(4), 757–778. doi: 10.2307/25750704

Rammstedt, Beatrice; Kemper, Christoph J.; Klein, Mira Céline; Beierlein, Constanze; Kovaleva, Anastassiya (2013): A Short Scale for Assessing the Big Five Dimensions of Personality. 10 Item Big Five Inventory (BFI-10). In: GESIS - methoden, daten, analyse 7 (2), S. 233–249.

Ramos-Villagrasa, Pedro J.; Barrada, Juan R.; Fernández-del-Río, Elena; Koopmans, Linda (2019): Assessing Job Performance Using Brief Self-report Scales: The Case of the Individual Work Performance Questionnaire. In: Revista de Psicología del Trabajo y de las Organizaciones 35 (3), S. 195–205. DOI: 10.5093/jwop2019a21.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (2016). In: Official Journal of the European Union L 119, S. 1–88.

Richardson, R. (2008). *CSI computer crime and security survey*. http://www.cse.msstate.edu/~cse6243/ readings/CSIsurvey2008.pdf.

Sabeeh, A., and Lashkari, A. H. (2011). *Users' Perceptions on Mobile Devices Security Awareness in Malaysia.* International Conference for Internet Technology and Secured Transactions, Abu Dhabi: IEEE, 428-435.

Sicari, S., Cappiello, C., De Pellegrini, F., Miorandi, D., & Coen-Porisini, A. (2016). A security-and quality-aware system architecture for Internet of Things. *Information Systems Frontiers*, *18*(4), 665-677.

Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks*, *76*, 146-164. doi: doi.org/10.1016/j.comnet.2014.11.008

Siponen, M., & Vance, A.O. (2010). Neutralization: New insights into the problem of employee systems security policy violations. *MIS Quarterly*, *34*(3), 87–502.

Siponen, M., Mahmood, M., & Pahnila, S. (2009). Are employees putting your company at risk by not following information security policies? *Communications of the ACM*, *52*(12), 145-147. doi: 10.1145/1610252.1610289

Smith, M. (2003). Business process design: correlates of success and failure. *The Quality Management Journal, 10* (2) 38-49. doi: 10.1080/10686967.2003.11919062.

The European Parliament and the Council of the European Union (2016). *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union*. https://eur-lex.europa.eu/eli/dir/2016/1148/oj (accessed 31st January, 2020).

The European Parliament and the Council of the European Union (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.* https://eur-lex.europa.eu/eli/reg/2016/679/oj (accessed 31st January, 2020).

van Zadelhoff, M., Lovejoy, K., & Jarvis, D. (2014). *Fortifying for the future: Insights from the 2014 IBM Chief Information Security Officer Assessment*. https://www.ibm.com/smarterplanet/us/en/centerforappliedinsights/article/ciso_insights.html.

von Solms, S. H., & von Solms, R. (2009*). Information security governance*. NewYork, NY: Springer.

Weber, R. H. (2010). Internet of Things: New security and privacy challenges. *Computer Law & Security Review, 26*(1), 23-30. doi: 10.1016/j.clsr.2009.11.008

Whitman, M.E., & Mattord, H.J. (2012). *Principles of Information Security* (4thed.). Boston, MA: Course Technology.

Wilkinson, G. (2018). General Data Protection Regulation: No silver bullet for small and medium-sized enterprises. *Journal of Payments Strategy & Systems*, *12*(2), 139–149.

Willison, R., & Warkentin, M. (2013). Beyond deterrence: An expanded view of employee computer abuse. *Management Information Systems Quarterly*, *37* (1): 1–20. doi:10.25300/MISQ/2013/37.1.01

Research Report

We thank the co-authors and editors:

Simon Rath

Prof. Irena Žemaitaitytė

Mgr. Agata Katkonienė

Assoc. Prof. Marius Kalinauskas

Prof. Odeta Merfeldaitė

Assoc. Prof. Asta Railienė

Ivan Kharitonov

Teresa Rauenbusch

Teilzertifizierung im Berufsfeld Informationssicherheit - TeBeISi

Funded by the Erasmus+ Programme of the European Union

https://information-security-in-sme.eu/.