Eastern Journal of European Studies
DOI: 10.47743/ejes-2026-0104 • JUNE 2026 • VOLUME 17, ISSUE 1

Exploring small business profiles in cybersecurity skills

Monica Mihaela Maer Matei [1;2], **Anamaria Năstasă**✉ [1;3], **Andreea-Monica Munteanu** [1;2], **Adriana AnaMaria Davidescu** [1;2], **Cristina Mocanu** [1], **Eliza Olivia Enno** [4]

[1] National Scientific Research Institute for Labour and Social Protection, Romania; [2] Bucharest University of Economic Studies, Romania; [3] Alexandru Ioan Cuza University of Iași, Romania; [4] Mitsui Bussan Secure Directions co. Ltd./ Cyber Resilience Division Analytics & Data Science, Japan

Abstract: Protecting sensitive data and ensuring secure operations in an interconnected world is crucial for companies, requiring new approaches and skills. This research paper aims to categorise small businesses based on their prioritisation of cybersecurity issues and their practices for handling cybersecurity tasks, with a focus on training and awareness. The Correspondence Analysis and Latent Class Model are used to identify associations between skills and firms' characteristics, respectively, to determine if there are hidden patterns among firms that might affect their responses. Using data collected from the Flash Eurobarometer 547 Cyberskills, we identified three distinct company profiles based on their attitudes towards cybersecurity (disengaged firms – 16%, partially engaged firms – 52% and proactive firms – 32%), influenced by turnover, industry and digital technology use. This research simplifies the data structure to understand small businesses' cybersecurity diversity. The results can inform research and practice by tailoring strategies and uncovering new insights.

Keywords: cybersecurity skills, latent class analysis, correspondence analysis, SMEs, European Union, Flash Eurobarometer 547

Introduction

As organisations become increasingly dependent on IoT and online operations, they become more exposed to cyberattacks, irrespective of their size, sector of activity, and private or public profile (Pruemmer et al., 2024), even if there are variations in cyberattack risks according to firms' size or economic activity. Finding adequate strategies and solutions to improve companies' security depends on technical solutions, specific processes to incorporate technical solutions, and human engagement, equipping employees, end-users, and citizens with adequate awareness and basic skills is becoming a must (Craigen et al., 2014; Zwilling et al., 2022; Bingöl et al., 2019).

✉ Centre for Research in International Economic Relations and European Studies, Alexandru Ioan Cuza University of Iași, Iasi, Romania; National Scientific Research Institute for Labour and Social Protection, Bucharest, Romania; e-mail: anamaria.nastasa@incsmps.ro.

HOW TO CITE: Maer Matei, M. M., Năstasă, A., Munteanu, A.-M., Davidescu, A. A., Mocanu, C., & Enno, E. O. (2026). Exploring small business profiles in cybersecurity skills. *Eastern Journal of European Studies*, *17*(01), 87-110. https://doi.org/10.47743/ejes-2026-0104

Cybersecurity has become an interdisciplinary field of study with multiple technical, psychological, and social solutions. It is necessary to understand and evaluate the type of information needed, then, if the information is adequately understood and applied, and, nonetheless, if individuals' intentions, attitudes, and motivations are adequately addressed and changed (Bada et al., 2019; Mersinas et al., 2025). In fact, psychological and nudge approaches to increasing cybersecurity have become more prevalent in the field, and the importance of human-related components in security breaches is more and more acknowledged (Mersinas et al., 2025)

Cyberthreats refer to network attacks, malware, phishing, and ransomware attacks, compromising mobile devices, as well as insider theft, sabotage, and accidental disclosure (Rawindaran et al., 2023), and they are becoming more and more complex and sophisticated (Saleem et al., 2017). As multiple aspects of life became more digitalised, citizens and firms alike became more prone to cybersecurity attacks (Lee & Wang, 2024; Zheleva et al., 2025; Armenia et al., 2021). The consequences of cybersecurity breaches are not always easily visible, and organisational plans to identify vulnerabilities and design interventions are often hampered and delayed. Cyberattacks have many negative consequences at the business level: productivity and financial gains are lost, and sensitive data, credibility, and reputation are damaged. Thus, training a cyber-resilient workforce is necessary for business sustainability (Pruemmer et al., 2024).

Thus, the countries' engagement in terms of cybersecurity has started to be tackled by the International Telecommunication Union, which developed a composite index (Global Cybersecurity Index) to measure 194 economies' cybersecurity commitments across five dimensions, including legal, technical, organisational, capacity building, and cooperation aspects. In recent years, countries have made significant progress in adopting measures that aim to diminish cybersecurity issues. In 2024, the Global Cybersecurity Index average score by country rose to 65.7 out of 100. Most countries still struggle with technical and capacity development activities, while they perform better in legal activities such as adopting laws and regulations related to cybercrime and cybersecurity activities. (ITU, 2024)

Lately, European firms have been more engaged in adopting AI technologies in their daily activities. The Nordic countries are more inclined to integrate AI capabilities within their operations than Eastern European countries (Eurostat, 2025a). Employing AI technologies in enterprises has both positive and negative impacts on cybersecurity. Firstly, AI adoption leads to rapid recognition of threats, making tasks easier by automating daily processes, easing the control of IT vulnerabilities, upgrading hardware, and, respectively, the software infrastructure. On the other hand, integrating AI into daily activities can intensify the already existing security issues among firms. The disadvantages of adopting AI include a growing need for skilled professionals, hardware and software infrastructure, along

with reskilling the workforce engaged in cybersecurity roles (Jada and Mayayise, 2024).

Our research aligns with the broader theme of examining the effects of digitalisation on the labour market and skills. In this study, we specifically focus on aspects related to cybersecurity, with an emphasis on small companies, given their limited resources for addressing these challenges. This research seeks to classify European small and medium enterprises by how they prioritise cybersecurity concerns and organise security-related activities within their enterprises. To this end, we apply Latent Class Analysis on microdata from the Flash Eurobarometer 547, to our knowledge, one of the first studies introducing this method on EU firm-level cybersecurity data. This approach allows us to identify hidden clusters of firms that share latent cybersecurity profiles, without imposing distributional assumptions. The resulting classification of SMEs by cybersecurity profiles provides a basis for policy recommendations at a more granular level compared to previous studies.

The research questions addressed in this paper are presented below:

RQ_1: Do European SMEs exhibit heterogeneous patterns regarding prioritising and addressing cybersecurity concerns?

RQ_2: Do enterprises' characteristics (company size, sector of activity, and the adoption and integration of digital technologies) influence how European SMEs prioritise cybersecurity activities?

The remainder of this paper is structured as follows: Section 1 reviews a series of the most recent works related to cybersecurity within small and medium-size enterprises; Section 2 presents the data used in this research, along with some correspondence analysis run to identify the associations existing between cybersecurity skills and recruiting methods, respectively, and the importance of cybersecurity. Section 3 highlights the methodology, and the main findings are depicted in Section 4, followed by the final section, where the main conclusions, along with discussion sections, can be found.

1. Literature review

As SMEs are essential for national and global economies, adequate governmental programmes and policies to support SMEs' behavioural change in investing in their security are necessary. Government policy, regulations, financial support, and cybersecurity training programmes must be part of an efficient approach to increasing SMEs' position in cyber defence (Mészáros & Țoca, 2025).

Due to their lack of knowledge and understanding, optimistic risk appraisals, and financial and human resource barriers, as well as the high costs of technical solutions, SMEs are more exposed to cyberattacks (Saleem et al., 2017; Wilson et al., 2023). Moreover, SME executive managers are continuously underestimating the risks and effects of cyberattacks based on a false belief that cyberattacks are more targeted at large firms and corporations compared to small and medium-size

enterprises (Kurpjuhn, 2015; Chaudhary et al., 2023). Ncubukezi (2023) found that small businesses face significant risk from both targeted and opportunistic threats and yet remain largely unprepared for either.

Previous literature identified some major impediments to SMEs' cybersecurity resilience. One barrier for SMEs, for both employees and employers, is a lack of awareness of specific cybersecurity risks (Rombaldo Junior et al., 2023; Erdogan et al., 2023). The lack of cybersecurity awareness is viewed as a consequence of resource constraints due to a lack of support for management and an overreliance on technical aspects (Chaudhary et al., 2023). Another reason for the lack of awareness is the usability of materials and delivery methods (Chaudhary et al., 2023; Abawajy & Kim, 2010). Another barrier is related to the lack of cybersecurity literacy among personnel and management. The literature emphasises the need for higher education programmes and other continuing training education opportunities (Ulrich et al., 2020; Rombaldo Junior et al., 2023). Moreover, financial resources are the root cause of limited literacy and awareness regarding cybersecurity. Studies indicate that smaller firms (especially in developing countries) are facing more difficulties in allocating financial and human resources for cybersecurity, compared to larger firms (Rombaldo Junior et al., 2023; Chaudhary et al., 2023). In this vein, Standaert, Evens, and Andries (2026) showed that firms with higher financial resources and management prioritisation of cybersecurity measures have higher levels of cybersecurity maturity. And consequently, on average, firms with higher levels of cybersecurity maturity are more likely to report fewer cybersecurity incidents (Dinkova et al., 2024).

Implementing solutions to increase cybersecurity is costly and requires skilled personnel, but SMEs intend to orient their strategies in these strategic directions (Rawindaran et al., 2023). Studies addressing the evidence on the benefits of education and training for cybersecurity are beginning to reach consensus on their positive importance for improving organisational behaviours at all levels (Pruemmer et al., 2024).

However, studies also evidenced that awareness campaigns have a limited impact, with low or even no significant changes at the behaviour level (Bada et al., 2019). Providing training and designing awareness campaigns using methods based mostly on written information will have limited to no impact on behaviour change. Also, even when they have adequate cyberattack awareness, individuals apply only common and minimal protective measures (Zwilling et al., 2022). Using innovative and serious games and new technological applications proved to be more effective (Bada et al., 2019).

Cybersecurity is a crucial and highly specialised activity that requires a highly specialised workforce; the efforts of SMEs to keep pace with trending developments in the cyber defence field are more challenging than those of larger companies (Rawindaran et al., 2023).

Several qualifications and certifications, as well as education and training programmes, exist in the field of cybersecurity. However, it is difficult for companies, especially SMEs, to determine which skills are relevant to their cyber defence needs (Furnell, 2021). Cybersecurity skills cover a wide range, from non-technical skills, rather specific to what we may call an organisational culture, to more technical ones supporting the security of networks and devices. So, companies usually face skills shortages and gaps in the field; the smaller the firm, the higher the difficulties (Berry and Berry, 2018). Some sets of skills may require a dedicated educational programme or route to be developed, while others may only need a couple of modules integrated into broader qualifications, thus making it difficult for companies to identify adequate employees (Furnell, 2021) and for educational institutions to design programs to meet the businesses' needs. Studies focused on cybersecurity professionals have shown that both soft skills and hard skills are relevant (Ullah et al., 2026; Furnell, 2021). Ullah et al. (2026) showed that the most needed soft skills are related to communication, project management, access management, vulnerability management, and problem-solving. Among technical skills, information security, information technology, and security clearance ranked highest, followed by network security, incident response, security operations, and security controls. Information security is a skill that appears in almost all roles.

The same researchers found out that the most sought-after certifications in cybersecurity roles are Certified Information Systems Security Professional (CISSP), Certified Information Systems Auditor (CISA), and Certified Information Security Manager (CISM). Regarding programming languages, their research revealed that Java and JavaScript are among the most used by cybersecurity professionals.

Cybersecurity challenges, technical solutions, and skills are constantly evolving, so SMEs need guidance and expertise to keep up with rapid developments in the field. Therefore, informed and rapid managerial decisions are a must (Rawindaran et al., 2023). On the other hand, it has been proven that cybersecurity improvements are associated with positive organisational outcomes. For example, cybersecurity readiness is positively related to financial and non-financial performance (Hasan et al., 2021).

Previous findings emphasised the barriers to SMEs' cybersecurity, including lack of awareness, limited literacy, and resource constraints (Rombaldo Junior et al., 2023) and classified the skills needed of cybersecurity professionals (Ullah et al., 2026), the literature on how small companies prioritise and operationalise cybersecurity skills, and how recruitment practices shape the types of tasks assigned to employees, is still very limited. This study addresses this gap by uncovering distinct profiles of firms based on their cybersecurity practices and by revealing the association between how companies fill cybersecurity roles and the complexity of skills they prioritise.

2. Data and descriptives

This study's findings are based on data gathered using the Flash Eurobarometer 547 Cyberskills. Between April and May 2024, 12916 EU27 companies were surveyed. The respondents are IT managers or individuals responsible for decision-making within the company (such as managing directors, general managers, CEOs, financial directors, and HR managers). The FE 547 includes firms operating in five major sectors by NACE 2 Rev. classification, as Manufacturing (C), Industry (B, D, E, F), Retail (G), Transport, accommodation and entertainment (H, I, R), Service activities (J, K, L, M, N, S), Education, health and social work (P, Q).

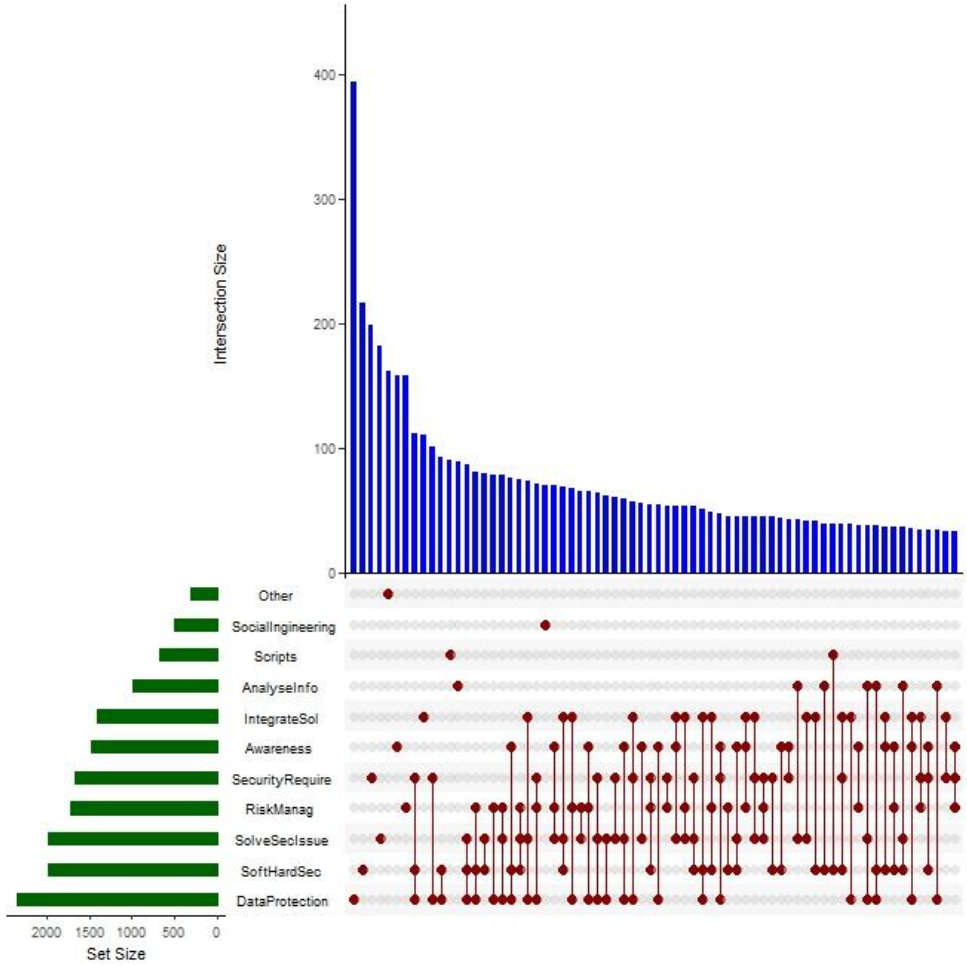
We are analysing 9136 small companies with less than 50 employees using or having at least one of the following tools: An online bank account, Online ordering or payment systems, Reservations software with client database, A website for your business, Web-based applications for payroll processing, e-signature etc., Cloud computing or storage, Internet-connected 'smart' devices, a company intranet, an internet-based video or voice calling service.

The primary objective of the study is to understand the cybersecurity skills companies prioritise and their strategies for addressing this issue within the small business landscape. Hence, we initially utilised a tool for visualising information based on questions with multiple answers. This visualisation emphasises the size of each category and the intersections between them. We are analysing the answers to the question "Which of the following cybersecurity skills are most important in your company?".

Each company can select up to 3 of the following alternatives:

- Perform social engineering (SocialEngineering),
- Develop codes, scripts and programmes (Scripts),
- Carry out working-life practices of the data protection and privacy issues (Data protection),
- Collect, analyse and correlate cyber threat information (AnalyseInfo),
- Develop security and privacy requirements (SecurityRequire),
- Analyse, assess and review software or hardware security (SoftHardSec),
- Identify needs in cyber security awareness, training and education (Awareness),
- Integrate cybersecurity solutions to the organisation (IntegrateSol),
- Identify and solve cybersecurity-related issues (SolveSecIssue),
- Implement cybersecurity risk management and ensure compliance with regulations and standards (RiskManag).

Figure 2. The most important cybersecurity skills



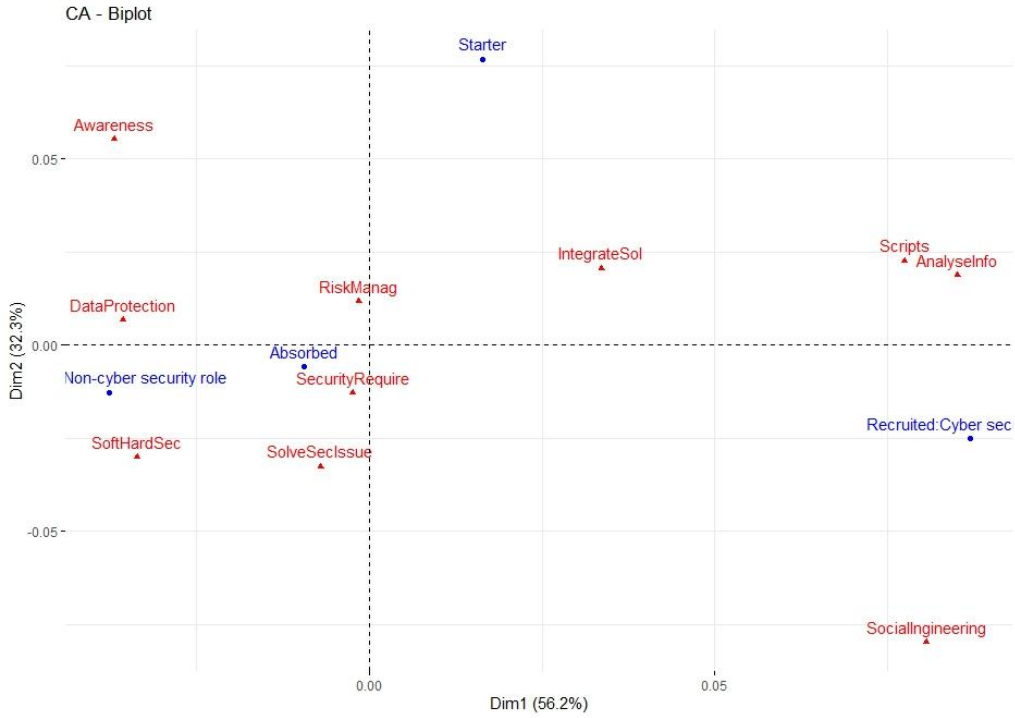
Source: authors' computation in RStudio 4.1. using Flash Eurobarometer 547

The skills mentioned as very important by a large number of companies are those related to data protection. In general, these competencies are selected together with others, but a large number of companies choose this type of competence as the only important one. Most European firms (93%) use various measures to address issues with data and IT systems, such as a lack of integrity or even confidentiality (Eurostat, 2024). The commonly adopted measures by EU firms are utilising strong password authentication (83%), backing up data in other locations (80%), followed by network access control processes (50%). The prominence of data protection skills reflects the regulatory pressure exerted by the General Data Protection Regulation

(GDPR), which came into force in 2018, requiring all organisations handling EU citizens' data to implement data governance practices (Narla, 2024).

The next step was about uncovering any associations between these categories of skills and other practices/characteristics of the companies. To achieve this goal, we used a multivariate analysis technique, namely correspondence analysis. This tool is based on the contingency table computed for the categorical variables. By transforming this matrix using singular value decomposition, we reduce the dimensionality and synthesise the information within a two-dimensional plot. This representation allows us to understand which are the main associations. Moreover, the Chi-square test is used to establish the significance of the relationship.

Figure 3. Correspondence map between cybersecurity skills and recruiting practices



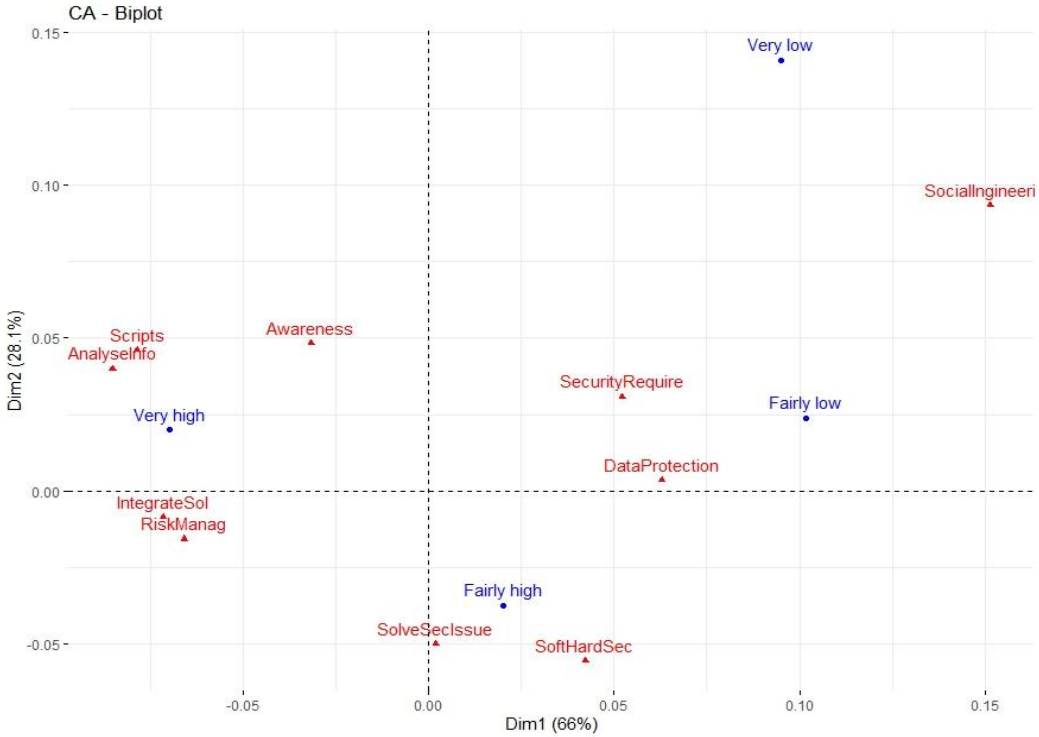
Source: authors' computation in RStudio 4.1. using Flash Eurobarometer 547

We conducted tests to determine if there is a connection between the skills considered important and cybersecurity awareness, as indicated by the percentage of employees who have received training in the last 12 months. However, our analysis did not confirm this hypothesis. We also used correspondence analysis to investigate whether the difficulty in recruiting staff for cybersecurity tasks is associated with the type of skills valued by companies. Once again, we found no significant relationship.

The relationship between the types of skills considered important for ensuring cybersecurity and the way firms fill positions dedicated to these tasks was explored (X-squared = 34.498, df = 27, p = 0.15). However, this result does not reject the null hypothesis of independence and should therefore be interpreted with caution. The observed patterns are reported descriptively, without inferring a systematic association between skill priorities and recruitment practices.

The roles focused on cyber skills are filled by firms using the "How did the employees directly involved in cybersecurity within your company enter this role?" question from FE 547. Enterprises can choose multiple answers, having four possibilities: (1) recruited from a non-cyber security related previous role (Non-cyber security role); (2) recruited from a previous role in cyber security (Recruited Cyber security role); (3) absorbed this role into an existing non-cyber security related role (Absorbed) and (4) as a career starter, for example, a graduate (Starter).

Figure 3. Correspondence map between cybersecurity skills and priority



Source: authors' computation in RStudio 4.1. using Flash Eurobarometer 547

Thus, the correspondence analysis map suggests that the companies that hire employees with no previous experience in cybersecurity and place them directly in cybersecurity roles tend to focus on implementing data protection and privacy

practices in the workplace or analysing, assessing, and reviewing software or hardware security. On the other hand, companies that integrate cyber security responsibilities into existing non-cyber security roles are generally seeking individuals with skills in developing security and privacy requirements, as well as identifying and resolving cyber security issues. Recruiting individuals with previous cybersecurity experience is more common among companies interested in tasks such as collecting, analysing, and correlating cyber threat information, or developing code, scripts, and programmes.

Therefore, companies hiring employees with no prior cybersecurity experience tend to consider only less complex tasks like implementing data protection and privacy practices or assessing and reviewing the security of software and hardware. This suggests that these companies prioritise roles that require procedural or compliance-based tasks, which are not demanding specialised cybersecurity expertise. This aligns with Furnell (2021) and Ullah et al. (2026), who noted that cybersecurity positions cover diverse types of skills, both technical and non-technical. Moreover, Furnell (2021) emphasizes that firms may have difficulties in finding a suitable workforce to match the diversity of skills and qualifications. This may indicate that firms may resort to a non-experienced workforce in handling procedural tasks.

Integrating cybersecurity responsibilities into non-cybersecurity roles is a common strategy adopted by companies to develop security and privacy requirements, as well as to identify and resolve cybersecurity issues (Rombaldo Junior et al., 2023; Erdogan et al., 2023). These companies leverage the technical expertise and problem-solving skills of their existing employees to meet cybersecurity needs. By distributing responsibilities across current roles, they aim to address resource constraints effectively. This finding is in line with previous findings from the literature (Rombaldo Junior et al., 2023).

There is a significant link between the skills that are considered important and the priority given to cybersecurity (X-squared = 84.21, df = 27, p-value = 8.558e-08). Companies that prioritise cybersecurity value skills such as collecting, analysing, and correlating cyber threat information and developing codes, scripts, and programmes. On the other hand, companies that do not prioritise cybersecurity value skills related to carrying out working-life practices of data protection and privacy issues and developing security and privacy requirements.

As a result, companies that prioritise cybersecurity are characterised by proactive strategies focused on acquiring technical skills such as threat analysis and tool development to counteract those threats. They recognise that cyber threats are complex and can have catastrophic consequences.

Companies that do not prioritise cybersecurity tend to adopt a reactive strategy, emphasising foundational skills such as implementing privacy practices and defining security requirements. Consequently, their perceived exposure to cyber-attacks appears lower. This reactive strategy indicates a low-risk perception widely

documented in the SME literature. SMEs underestimate their probability of having cyberattacks based on a false belief that they are too small to be targeted (Kurpjuhn, 2015; Chaudhary et al., 2023; Wilson et al., 2023). As a consequence, these firms are applying only common and minimal protective measures (Zwilling et al., 2022).

In conclusion, the initial analysis of the data showed variations in cybersecurity practices among small companies. We plan to further investigate this by developing a statistical model based on key variables capturing aspects related to recruitment, training, and priority. This distinction can help shape workforce development and training programmes. It ensures that skill-building matches the organisation's capabilities or constraints.

3. Method

Latent class analysis (Lazarsfeld, 1950; Goodman, 2002; Lee & Wang, 2024) is a statistical model that aims to classify the analysed entities into latent classes based on a pattern of their characteristics measured as categorical variables.

This approach has elements in common with both factor analysis and cluster analysis. Factor analysis estimates latent factors that explain the covariances of the observed variables. These latent factors were continuous numerical variables. Similarly, LCA identifies latent groups that explain the observed variation in manifest variables. If, in cluster analysis, the calculated distances between two entities were used and the final result was the membership of each item to a class, in LCA, the result is the probability of belonging to one of the classes and is based on modelling the joint distribution of some observed items in terms of a number of latent classes.

The advantages of Latent Class Analysis (LCA) can be summarised in two key aspects: (i) it enables the extraction of information from categorical variables, and (ii) it does not impose strict limitations on the distribution of the analysed variables. The model is based on two main assumptions: multinomial distribution and local independence. The concept of local independence means that the indicator variables are independent within each class. The parameters estimated by the LCA model are divided into two categories: the proportion of observations in each class (class probabilities) and the probability of observing a specific response to a given variable within each class (conditional probabilities). The probability that an entity i, which belongs to class c, records a specific vector of J categories for the indicator variables (under conditions of independence) is represented as follows:

$$f(Y_i;\pi_c) = \prod_{j=1}^{J}\prod_{l=1}^{k_j} {\pi_{jcl}}^{Y_{ijl}} \quad (1)$$

where:

- There are J categorical variables, each with k_j categories, j=1,J
- N is the number of observations, i=1, N

- $Y_{ilj} = 1$ if for entity i, variable j takes l category, $l = 1, k_j$.
- We are considering C classes.
- Conditional probability π_{jcl}= the probability that the observations in class c to record l level for variable j.
- For each class: $\sum_{l=1}^{k_j} \pi_{jcl} = 1$
- The model is based on a weighted sum of C contingency tables.
- The weights are denoted by p_c. These are known as aprioric probabilities, unconditional probabilities showing the probability that an entity belongs to a class before considering its responses for the manifest variables.
- Maximum likelihood estimation maximises the log-likelihood function:

$$\sum_{i=1}^{N} ln\left(\sum_{c=1}^{C} p_c \prod_{j=1}^{J} \prod_{l=1}^{k_j} \boldsymbol{\pi_{jcl}}^{Y_{ijl}}\right) \quad (2)$$

Model estimation in Latent Class Analysis (LCA) is conducted using Maximum Likelihood and the Expectation-Maximisation (EM) algorithm. The process begins with randomly selected initial values for two parameters. These initial values are then used to calculate the probabilities of individuals belonging to specific classes. This cycle continues until the likelihood function reaches its maximum value. To determine the final model selection, information criteria such as AIC (Akaike Information Criterion) and BIC (Bayesian Information Criterion) are employed.

4. Findings

We are conducting an investigation to determine if there are hidden groupings of firms that may be influencing the observed responses. The hidden category we are trying to identify will show the different groups that the analysed firms belong to. We used latent class analysis to see if the firms that responded could be sorted into similar groups based on their answers to questions about recruitment, awareness, and training in the cybersecurity field. This analysis is focused on small firms with fewer than 50 employees.

We have selected items comprising the same number of categories. We are investigating four manifest variables described in Table 1. The manifest variables were chosen because they capture an important dimension of cybersecurity in small firms. Priority captures the strategic importance of cybersecurity within the organisation. Outsourcing captures the use of external expertise. The presence of employees with cybersecurity roles shows the organisational human resource allocation, and training or awareness indicates investment in workforce development.

The manifest indicators were selected from the Flash Eurobarometer 547 item set on the basis of their relevance to cybersecurity skills and practices in small

businesses. Additional selection criteria included the complementarity of the dimensions captured across indicators, sufficient response availability, and meaningful variation across firms.

Table 1. Manifest variables

Variable	Meaning	Levels
Priority	Priority given to cybersecurity issues	(High, Low)
Outsourcing	Outsourcing certain cybersecurity activities	(Yes, No)
EmployeesCyber	Having at least one employee with a cybersecurity role	(No, Yes)
TrainingAwareness	If the company provided training or awareness raising about cybersecurity to its employees	(Yes, No)

Source: authors' representation

We followed the general procedure specific to LCA, meaning that we ran models with different numbers of classes and then compared the models' fit to select the final one. Table 2 presents the goodness-of-fit statistics used to select the number of latent classes. Latent class analysis was conducted in R using the poLCA package (Linzer & Lewis, 2011), which estimates LCA models with the expectation-maximisation algorithm.

Akaike Information Criterion (AIC) and Bayesian Information Criterion (BIC) are measures of the relative quality of the model, with lower values indicating better fit. The likelihood ratio/deviance statistic (G^2) measures the goodness-of-fit using the difference between the observed and expected frequencies. Obviously, smaller values indicate a better fit. Another goodness-of-fit statistic is based on the chi-square distribution (X^2), with smaller values indicating a better fit.

The minimum AIC and BIC criteria indicate the 3-class model. Moreover, the Likelihood ratio/deviance statistic and Chi-square goodness-of-fit indicate the adequacy of this model to the observed data. The maximum log-likelihood is higher for the 3-class model, indicating its superiority compared to the one with 2 classes. The 3-class model adds complexity, as suggested by the number of estimated parameters, but the improvements across all the criteria mentioned above demonstrate that this is justified.

Therefore, the results show that the companies can be divided into three groups comprising companies with similar responses. The numerical outputs extracted from the LCA model show the proportion of businesses exhibiting a specific behaviour within each class and the conditional probabilities by outcome variable for each group. This information is shown in Table 3 and is depicted in Figure 4.

Table 2. Assessing model fit

	2 classes	3 classes
AIC	40895.41	40793.19
BIC	40958.91	40891.97
G^2 (Likelihood ratio/deviance statistic)	119.87	7.65
X^2(Chi-square goodness of fit)	119.75	7.84
Maximum log-likelihood	-20438.7	-20382.6
Number of estimated parameters	9	14
Residual degrees of freedom	6	1

Source: authors' computation in RStudio 4.1. using Flash Eurobarometer 547

The probabilities in Table 3 indicate the likelihood of businesses in each class choosing each response option for the respective question.

Businesses in class 1 are characterised by low importance given to cybersecurity, a lack of outsourcing of cybersecurity activities, a lack of employees with cybersecurity-related roles, and a lack of cybersecurity training. According to the estimated class population shares, approximately 16% of companies belong to this class.

Companies in the second category prioritise cybersecurity. They either outsource cybersecurity to external individuals or other companies while also having their own employees handle these issues. However, they have not provided cybersecurity training to their employees. This category encompasses approximately 52% of the companies analysed. The occurrence of this class may be partly explained by the difficulty small firms face in evaluating the return on cybersecurity investments (Armenia et al., 2021). Moreover, the concentration of firms in Class 2 reinforces Rombaldo Junior et al.'s (2023) idea that awareness without adequate resources and literacy is insufficient for effective cyber defence.

Table 3. Conditional item response probabilities, by outcome variable, for each class

	Class 1	Class 2	Class 3
Priority (low)	**0.78**	0.21	0.05
Outsourcing (no)	**0.92**	0.39	0.34
Employee with cybersecurity roles (at least 1)	0.12	**0.65**	**0.87**
Training/Awareness (no)	**0.97**	**0.87**	0.32
Class shares	0.16	0.52	0.32

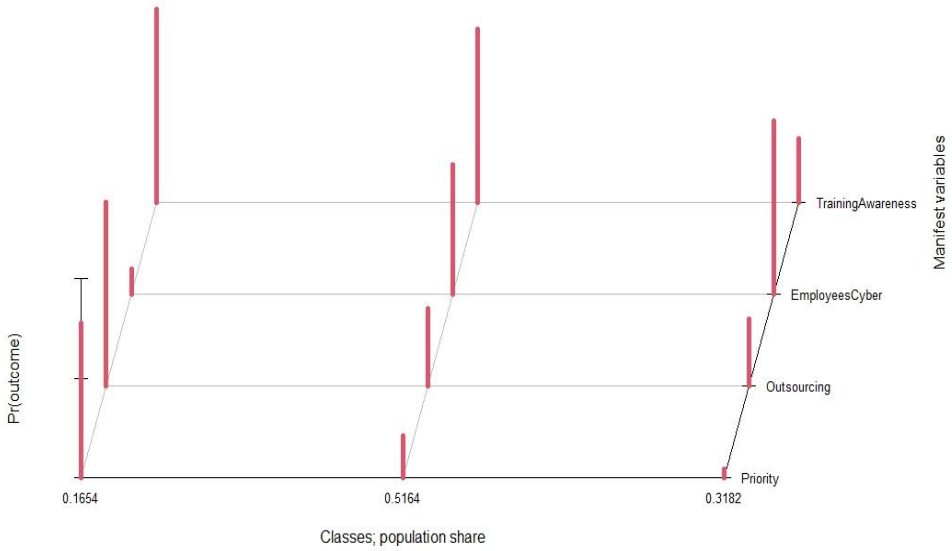
Source: Authors' computation in RStudio 4.1. using Flash Eurobarometer 547

The third category comprises approximately 32% of the companies included in the analysis. Cybersecurity is a top priority for them, and they have their own resources dedicated to cybersecurity while also outsourcing certain aspects.

Companies in this category have provided cybersecurity training or awareness programmes to their employees within the past 12 months.

Figure 4 illustrates these findings, supporting the first research question as European SMEs exhibit heterogeneous cybersecurity profiles. The red bars show the conditional probabilities of belonging to the second category for each manifest variable by latent class. Priority, employee involvement in cybersecurity roles and company initiatives to raise awareness or provide training, influences class segmentation. Lee and Wang (2024) identified two classes of individuals, "at-risk" and "cautious" of cybercrimes across 28 European countries. Our study extends this type of heterogeneity at the SME level by showing similar clusters based on their cybersecurity engagement.

Figure 4. Latent class representation



Source: authors' computation in RStudio 4.1. using Flash Eurobarometer 547

These results emphasise the need for customised strategies for different types of companies. Companies with lower cybersecurity priority (Class 1) could benefit from targeted interventions to raise awareness about the risks of neglecting cybersecurity. Meanwhile, firms with higher cybersecurity priorities (Class 2) might focus on refining their existing strategies or expanding employee training.

5. Characteristics of the companies within each class

Next, we utilised the vector of predicted class membership from the LCA model, and we investigated the factors influencing class membership. The posterior

probability of cases belonging to each latent class is used to ascertain the predicted class. We examined five variables: annual increase in turnover, total turnover exceeding 500,000 EUR in 2023, membership in the NACE J (Information and Communication) sector, use of cloud computing or storage, and use of Internet-connected 'smart' devices, none of which served as manifest indicators in the LCA model. Weighted chi-squared tests (accounting for probabilistic class membership) revealed significant differences across all five variables (all p-values < 0.001), confirming that the three latent classes are differentiated along dimensions of firm size, sector, and digital infrastructure adoption, highlighting the hypothesis that firms' characteristics influence the modality of handling cybersecurity issues within enterprises.

In conclusion, companies in the third category that prioritise cybersecurity, invest in resources to address cybersecurity issues, and outsource certain tasks have experienced growth in turnover. They have achieved an above-average turnover and have a higher market share in the Information and Communication sector. Additionally, these companies are implementing modern digital technology solutions to a greater extent. Prioritising cybersecurity is associated with business growth and the adoption of digital technologies.

Table 4. Latent class membership probabilities

	Class 1 (n=1019)	**Class 2** (n=5314)	**Class 3** (n=2233)	χ^2	***p-value***
Share of companies showing an annual increase in turnover	40%	47%	52%	28.14	<.001
Share of companies with a total turnover in 2023 higher than 500.000 Euro	23%	45%	54%	194.13	<.001
The share of companies in the economic activity NACE J - Information and Communication	1.90%	4.70%	12%	86.17	<.001
Share of companies using Cloud computing or storage	32%	56%	67%	260.36	<.001
Share of companies using Internet-connected 'smart' devices	59%	67%	73%	49.2	<.001

Source: authors' computation in RStudio 4.1. using Flash Eurobarometer 547

This investigation's contribution is simplifying the data structure to understand small businesses' heterogeneity in cybersecurity. Our findings could

contribute to better decisions in research and practice, such as customising strategies or gaining new insights about different groups of companies.

Conclusions and discussions

This current study analysed the SMEs' cybersecurity practices across Europe using correspondence analysis and latent class analysis on data from 9,136 small companies surveyed in Flash Eurobarometer 547. Our analysis identified three different classes of companies based on their cybersecurity practices. The SMEs are divided into disengaged firms (16%) that largely neglect cybersecurity, partially engaged firms (52%) that recognise cybersecurity as a priority but do not invest in employee training, and proactive firms (32%) that combine internal resources, outsourcing, and training programmes for cybersecurity.

Our correspondence analysis revealed that recruitment practices are connected with the types of cybersecurity skills firms prioritise. Companies hiring workers without prior cybersecurity experience are more likely to use those employees for procedural, compliance-based tasks such as data protection and privacy practices. On the other hand, SMEs that recruit more experienced professionals use those workers for threat analysis and programme development. These results are in line with Furnell (2021) and Ullah et al. (2026), who showed that cybersecurity skills cover a broad spectrum of competencies from highly technical niche skills to non-technical organisational and communication competencies. Moreover, data protection, as the most valued skill across firms, reveals the regulatory pressure of the GDPR (Narla, 2024).

The results also showed that companies not prioritising cybersecurity adopt reactive strategies, such as foundational skills, such as privacy practices and security requirements. These results emphasise what the literature widely documents as low-risk perception (Kurpjuhn, 2015; Chaudhary et al., 2023; Wilson et al., 2023). By comparison, firms prioritising cybersecurity emphasise technical skills such as threat intelligence and code development. Moreover, the analysis on firm characteristics showed that proactive firms (Class 3) exhibit higher turnover growth, above-average revenues, and greater adoption of digital technologies such as cloud computing and smart devices. These findings may reflect that cybersecurity is also associated with business resilience and competitiveness. On the other side, the characteristics of disengaged firms, such as lower turnover, low digital technology adoption, and low cybersecurity investment, emphasise the causes and consequences of not implementing cybersecurity measures.

From a theoretical point of view, the variation among the three classes can be primarily interpreted through the Resource-Based View. According to the Resource-Based View, firm heterogeneity in specific outcomes is shaped by differences in organisational resources and capabilities, such as human capital, knowledge, technology, managerial capacity, and other assets (Barney, 1991; Wernerfelt, 1984;

Mladenova et al., 2025). This framework is especially relevant when explaining how classes differentiate in their access to, and mobilisation of, organisational resources. For example, class 1 firms seem resource-constrained and disengaged as they do not outsource cybersecurity services, rarely do they have employees in cybersecurity roles, and provide no training. Class 2 firms display partial resource mobilisation, because they combine cybersecurity priority with some internal arrangements, but without investment in employee training. Class 3 firms display the most grown resource configuration, integrating internal roles, outsourcing, and training. Moreover, in line with resource view, class 3 is also more likely to have higher resources coming from higher turnover levels, and by operating in domains that offer advantages for digital assets, such as in information and communication activities, and by using digital technologies such as cloud computing and smart devices. Institutional Theory can also offer insights into our results, by explaining why less mature firms may still prioritise data protection and privacy-related skills. For example, regulatory pressures to comply with the GDPR and AI Act create coercive isomorphism among SMEs, pushing firms toward similar baseline practices, such as hiring cybersecurity personnel, especially in the case of firms in Class 2 and Class 3 (DiMaggio & Powell, 1983).

Understanding these groups enables more targeted interventions instead of a one-size-fits-all policy approach. These findings can guide both policymakers and company leaders in making informed decisions to enhance cybersecurity readiness and improve practices in various organisations. For partially engaged firms, targeted interventions beyond awareness-raising should be used, such as practical methods, serious games, and accessible frameworks tailored to SME constraints (Bada et al., 2019; Chaudhary et al., 2023). On the other hand, universities should design modular training pathways because some cybersecurity competencies require dedicated programmes while others can be integrated into broader qualifications (managerial and communication skills) (Furnell, 2021; Ullah et al., 2026). The integration of cybersecurity responsibilities into non-cybersecurity roles helps where there are resource constraints (Rombaldo Junior et al., 2023), but these measures must be followed by training and support to avoid the de-prioritisation of security activities documented in the literature (Ulrich et al., 2020).

Class-specific policy recommendations rooted in EU-level cybersecurity instruments can also be drawn from our results. For Class 1 of disengaged firms, specific national policies should focus on supporting small firms to reach a minimum cybersecurity baseline, rather than sophisticated professionalisation instruments. For instance, stakeholders such as national cybersecurity authorities, SME agencies, NGOs, chambers of commerce, or sectoral organisations should develop a basic cyber hygiene support scheme for the SMEs covered in this class. The measures of the scheme should target the NIS2 Directive's cybersecurity risk-management measures, covering risk assessment, incident response, business continuity, cyber

hygiene training, access control, asset management, and multi-factor authentication, where appropriate (European Parliament and Council of the European Union, 2022).

For Class 2 of partially engaged firms, policy measures should be based on turning cybersecurity priority into employee training. A specific recommendation is an ECSF-based training support scheme for employees who have absorbed cybersecurity responsibilities into non-cybersecurity roles. ECSF can be used to map the skills and competencies required for role profiles, thereby further developing or designing cybersecurity-related training programmes to address skills and knowledge gaps within these organizations (European Union Agency for Cybersecurity, 2022a, 2022b).

Concerning Class 3 of proactive firms regarding cybersecurity, policy should support progression from basic cybersecurity readiness to specialized measures. As already mentioned, these firms already combine internal roles, outsourcing, and training. As a result, the most relevant recommendation is to develop modular ECSF-aligned qualification pathways linked to specific role profiles and deliverables. More specifically, these firms should focus on developing roles related to cybersecurity risk management, through the Cybersecurity Risk Manager profile; incident response, through the Cyber Incident Responder profile; threat intelligence, through the Cyber Threat Intelligence Specialist profile; and security-by-design for digital infrastructures, systems, and services, through the Cybersecurity Architect profile (European Union Agency for Cybersecurity, 2022c).

Data on digital intensity in Europe show that very low or low digital intensity firms are unevenly distributed across Europe. Somewhat high shares in these lower-intensity categories are found in a number of Central and Eastern European (CEE) countries, such as Bulgaria, Hungary, Latvia, Slovakia, Croatia, Lithuania, Slovenia, Poland, and Romania (Eurostat, 2025b). The CEE countries are not a homogeneous group, but this pattern indicates that many firms in this region may face more challenges in moving from basic digitalisation to more sophisticated cybersecurity capacities. This means the first and second classes identified in our research are meaningful for CEE economies, as they describe firms that could use digital tools but do not have cybersecurity practices, internal skills, and employee training. These findings may be relevant for the wider European integration challenges. Closing the digital divide means not only access to technologies but also support for cybersecurity skills and for building organisational capabilities.

This study presents some limitations. Our analysis is cross-sectional, capturing firms' cybersecurity profiles at a single point in time, preventing us from seeing if firms are transitioning from one class to another in time. To account for this limitation, future research must use longitudinal studies to track the same firms over time and assess the changing firms' cybersecurity profiles. Moreover, the quantitative approach cannot capture possible factors related to decision-making processes, motivations, and barriers that may influence the cybersecurity profiles of SMEs. To account for this, future studies must use qualitative approaches, such as

interviews or case studies with firms, which can provide a deeper insight into possible mechanisms that may influence firms' cybersecurity profiles. Several limitations specific to the latent class analysis approach should be acknowledged. First, it assumes local independence, meaning that the latent class variable fully explains the associations among manifest indicators, which may not hold perfectly in practice. Therefore, future research should consider more flexible extensions of standard LCA. Second, the latent class solution is sensitive to the selection of the manifest indicators. The class structure identified here reflects the particular set of cybersecurity-related variables available in the dataset.

A further limitation is that the analysis does not estimate separate latent class models for CEE and non-CEE Member States. This was avoided because regional disaggregation of the already restricted sample of small digitally active firms could reduce the stability of the latent class solution. Future research should address this limitation through a larger sample comparing CEE and Western European SMEs. Such an approach would show whether the same three cybersecurity profiles are present across Europe or whether CEE firms are more concentrated in the disengaged and partially engaged classes.

Acknowledgement: This research has been conducted with the support received through the project "City-Focus - City: Future Organisation of Changes in Urbanisation and Sustainability", project code CF 23/27.07.2023, financed through National Recovery and Resilience Plan for Romania within project call – PNRR-III-C9-2023-I8 PNRR/2023/Component 9/Investment 8. [Financed by the European Union – NextGenerationEU].

References

Abawajy, J., & Kim, T. H. (2010, December). Performance analysis of cyber security awareness delivery methods. In *Security Technology, Disaster Recovery and Business Continuity: International Conferences, SecTech and DRBC 2010, Held as Part of the Future Generation Information Technology Conference, FGIT 2010, Jeju Island, Korea, December 13-15, 2010. Proceedings* (pp. 142-148). Berlin, Heidelberg: Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-17610-4_16

Armenia, S., Angelini, M., Nonino, F., Palombi, G., & Schlitzer, M. F. (2021). A dynamic simulation approach to support the evaluation of cyber risks and security investments in SMEs. *Decision Support Systems*, *147*, 113580. https://doi.org/10.1016/j.dss.2021.113580

Bada, M., Sasse, A. M., & Nurse, J. R. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? *arXiv preprint arXiv:1901.02672*. https://doi.org/10.48550/arXiv.1901.02672

Barney, J. B. (1991). Firm resources and sustained competitive advantage. *Journal of Management, 17*(1), 99–120. https://doi.org/10.1177/014920639101700108

Berry, C. T., & Berry, R. L. (2018). An initial assessment of small business risk management approaches for cyber security threats. *International Journal of Business Continuity and Risk Management*, *8*(1), 1-10. https://doi.org/10.1504/IJBCRM.2018.090580

Bingöl, U., Mete, H., & Özkan, Y. (2019). Comparative qualitative analysis of Turkey and Estonia in the IT sector vacancies. *Eastern Journal of European Studies*, *10*(2), 197-220. https://ejes.uaic.ro/articles/EJES2019_1002_BIN.pdf

Chaudhary, S., Gkioulos, V., & Katsikas, S. (2023). A quest for research and knowledge gaps in cybersecurity awareness for small and medium-sized enterprises. *Computer Science Review*, *50*, 100592. https://doi.org/10.1016/j.cosrev.2023.100592

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. *Technology Innovation Management Review*, *4*(10), 13-21. https://doi.org/10.22215/timreview/835

DiMaggio, P. J., & Powell, W. W. (1983). The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. *American Sociological Review, 48*(2), 147–160. https://doi.org/10.2307/2095101

Dinkova, M., El-Dardiry, R., & Overvest, B. (2024). Should firms invest more in cybersecurity? *Small Business Economics*, *63*(1), 21-50. https://doi.org/10.1007/s11187-023-00803-0

Erdogan, G., Halvorsrud, R., Boletsis, C., Tverdal, S., & Pickering, J. B. (2023, February). Cybersecurity awareness and capacities of SMEs. In *Proceedings of the 9th International Conference on Information Systems Security and Privacy—ICISSP* (pp. 296–304). https://doi.org/10.5220/0011609600003405

European Parliament and Council of the European Union. (2022, December 27). *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). Official Journal of the European Union, L 333*, 80–152. https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng

European Union Agency for Cybersecurity. (2022a). *European Cybersecurity Skills Framework (ECSF).* https://www.enisa.europa.eu/topics/skills-and-competences/skills-development/european-cybersecurity-skills-framework-ecsf

European Union Agency for Cybersecurity. (2022b). *European Cybersecurity Skills Framework (ECSF) user manual.* https://www.enisa.europa.eu/sites/default/files/publications/European%20Cybersecurity%20Skills%20Framework%20User%20Manual.pdf

European Union Agency for Cybersecurity. (2022c). *European Cybersecurity Skills Framework (ECSF): Role profiles.* https://www.enisa.europa.eu/sites/default/files/publications/European%20Cybersecurity%20Skills%20Framework%20Role%20Profiles.pdf

Eurostat. (2024). ICT security in enterprises. https://ec.europa.eu/eurostat/statistics-explained/index.php?title=ICT_security_in_enterprises

Eurostat. (2025a). 20% of EU enterprises use AI technologies. https://ec.europa.eu/eurostat/web/products-eurostat-news/w/ddn-20251211-2

Eurostat. (2025b). *Digitalisation in Europe – 2025 edition.* https://ec.europa.eu/eurostat/web/interactive-publications/digitalisation-2025

Furnell, S. (2021). The cybersecurity workforce and skills. *Computers & Security*, *100*, 102080. https://doi.org/10.1016/j.cose.2020.102080

Goodman, L. A. (2002). Latent class analysis: The empirical study of latent types, latent variables, and latent structures. In J. A. Hagenaars & A. L. McCutcheon (Eds.), *Applied latent class analysis* (pp. 3–55). Cambridge University Press. https://doi.org/10.1017/CBO9780511499531.002

Hasan, S., Ali, M., Kurnia, S., & Thurasamy, R. (2021). Evaluating the cyber security readiness of organizations and its influence on performance. *Journal of Information Security and Applications*, *58*, 102726. https://doi.org/10.1016/j.jisa.2020.102726

International Telecommunication Union. (2024). *Global Cybersecurity Index 2024* (5th ed.). International Telecommunication Union. https://www.itu.int/dms_pub/itu-d/opb/hdb/d-hdb-gci.01-2024-pdf-e.pdf

Jada, I., & Mayayise, T. O. (2024). The impact of artificial intelligence on organisational cyber security: An outcome of a systematic literature review. *Data and Information Management*, *8*(2), 100063. https://doi.org/10.1016/j.dim.2023.100063

Kurpjuhn, T. (2015). The SME security challenge. *Computer Fraud & Security*, *2015*(3), 5-7. https://doi.org/10.1016/S1361-3723(15)30017-8

Lazarsfeld, P. F. (1950). The logical and mathematical foundation of latent structure analysis. In S. A. Stouffer, L. Guttman, E. A. Suchman, P. F. Lazarsfeld, S. A. Star, & J. A. Clausen (Eds.), *Studies in social psychology in World War II: Vol. 4. Measurement and prediction* (pp. 362–412). Princeton University Press. https://gwern.net/doc/psychology/1950-stouffer-theamericansoldier-v4-measurementandprediction.pdf

Lee, C. S., & Wang, Y. (2024). Typology of cybercrime victimization in Europe: A multilevel latent class analysis. *Crime & Delinquency*, *70*(4), 1196-1223. https://doi.org/10.1177/00111287221118880

Linzer, D. A., & Lewis, J. B. (2011). poLCA: An R package for polytomous variable latent class analysis. *Journal of Statistical Software*, *42*, 1–29. https://doi.org/10.18637/jss.v042.i10

Mersinas, K., Bada, M., & Furnell, S. (2025). Cybersecurity behavior change: A conceptualization of ethical principles for behavioral interventions. *Computers & Security*, *148*, 104025. https://doi.org/10.1016/j.cose.2024.104025

Mészáros, E. L., & Țoca, C. V. (2025). Toward a systemic framework for evaluating the European Union's resilience to hybrid threats. *Eastern Journal of European Studies*, *16*(2). https://doi.org/10.47743/ejes-2025-0203

Mladenova, I., Vladimirov, Z., & Harizanova, O. (2025). Digital transformation, organisational capabilities, and SME performance-size matters. *Eastern Journal of European Studies*, *16*(1), 216-238. https://doi.org/10.47743/ejes-2025-0110

Narla, N. R. (2024). Help wanted: Evolving privacy roles and the widening privacy skills gap. *ISACA Journal*, (1). https://www.isaca.org/resources/isaca-journal/issues/2024/volume-1/help-wanted-evolving-privacy-roles-and-the-widening-privacy-skills-gap

Ncubukezi, T. (2023). Risk likelihood of planned and unplanned cyber-attacks in small business sectors: A cybersecurity concern. *In R. L. Wilson & B. Curran (Eds.), Proceedings of the 18th International Conference on Cyber Warfare and Security (ICCWS 2023) (pp. 279–290). Academic Conferences International Limited.* https://doi.org/10.34190/iccws.18.1.1084

Pruemmer, J., van Steen, T., & van den Berg, B. (2024). A systematic review of current cybersecurity training methods. *Computers & Security, 136, 103585.* https://doi.org/10.1016/j.cose.2023.103585

Rawindaran, N., Jayal, A., Prakash, E., & Hewage, C. (2023). Perspective of small and medium enterprise (SME's) and their relationship with government in overcoming cybersecurity challenges and barriers in Wales. *International Journal of Information Management Data Insights*, *3*(2), 100191. https://doi.org/10.1016/j.jjimei.2023.100191

Rombaldo Junior, C., Becker, I., & Johnson, S. D. (2023). Unaware, unfunded and uneducated: A systematic review of SME cybersecurity. *arXiv preprint arXiv:2309.17186*. https://doi.org/10.48550/arXiv.2309.17186

Saleem, J., Adebisi, B., Ande, R., & Hammoudeh, M. (2017, July). A state of the art survey-Impact of cyber attacks on SME's. In *Proceedings of the international conference on future networks and distributed systems*. https://doi.org/10.1145/3102304.3109812

Standaert, T., Evens, T., & Andries, P. (2026). Cybersecurity maturity of Flemish firms: Drivers and consequences. *Computers & Security*, *165* 104868. https://doi.org/10.1016/j.cose.2026.104868

Ullah, F., Ye, X., Fatima, U., Wu, Y., Akhtar, Z., & Ahmad, H. (2026). What skills do cybersecurity professionals need?. *Information & Computer Security*, 1-19. https://doi.org/10.1108/ICS-01-2025-0027

Ulrich, P., Frank, V., & Timmermann, A. (2020). The dark side of data science-an empirical study of cyber risks in German SMEs. *Procedia Computer Science*, *176*, 2615-2624. https://doi.org/10.1016/j.procs.2020.09.307

Wernerfelt, B. (1984). A resource-based view of the firm. *Strategic Management Journal*, *5*(2), 171–180. https://doi.org/10.1002/smj.4250050207

Wilson, M., McDonald, S., Button, D., & McGarry, K. (2023). It won't happen to me: surveying SME attitudes to cyber-security. *Journal of Computer Information Systems*, *63*(2), 397-409. https://doi.org/10.1080/08874417.2022.2067791

Zheleva, R., Petkova, K., & Zdravkov, S. (2025). Divergent paths of SME digitalization: a latent class approach to regional modernization in the European Union. *World*, *6*(4), 144. https://doi.org/10.3390/world6040144

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber security awareness, knowledge and behavior: A comparative study. *Journal of Computer Information Systems*, *62*(1), 82-97. https://doi.org/10.1080/08874417.2020.1712269