Competencies for Privacy and Security Professionals: The Discrepancy in Perspective between Employers and Employees

REANATA MEKOVEC, DIJANA OREŠKI
Faculty of Organization and Informatics,
University of Zagreb,
Pavlinska 2, 42000 Varazin,
CROATIA

Abstract: - The demand for privacy and security professionals is expected to increase over the following years, but insufficient professionals will meet the market's requirements. Their professional skills are also inadequate due to a lack of a unique definition of appropriate competence. We present the occupational standard Information security and privacy architect, which includes a list of critical tasks. The latent class analysis (LCA) was used to identify groups of experts with similar perceptions of task necessities and expertise levels for privacy and security professionals and to account for heterogeneity among expert groups. Results indicated significant differences between employees and employers (top management) for all 19 tasks observed. A difference in the perception of responsibility and knowledge of privacy and security professionals results from a different perspective on security and privacy. Employers see the big picture and positions of the desired person, whereas employees only see their part in the task.

Key-Words: - competence, privacy professionals, security professionals, occupational standard, latent class analysis, information security and privacy.

Received: April 6, 2024. Revised: September 2, 2024. Accepted: October 2, 2024. Published: November 1, 2024.

1 Introduction

Although human societies have been linked to using ICTs for ages, what is novel about today's societies is their increasing reliance on ICTs and information and data as critical resources, [1]. The Internet and related technologies have fuelled innovation, economic value, and social welfare improvement for decades. Data on individuals circulating across a complicated ecosystem has many advantages. As a result, when people interact with systems, goods, and services, they might be unable to comprehend the possible effects on their privacy. Organizations may not truly understand the full depth of these effects on people, society, or their businesses, which can have an impact on their branding, financial results, and growth prospects in the future, [2]. We have a shortage of professionals identifying security and organizational measures to protect the collected data and a privacy competence gap. Most people in charge of the aforementioned issues lack the necessary competence; moreover, companies are unsure of what kind of employee profile they require or to whom they would entrust the task of managing the security and privacy system.

According to an ISACA report, the long-standing privacy skills gap is now posing a serious security risk, as a lack of training, poor app/service design, and failure to detect personal data are all contributing to an increase in data breaches, [3].

In 2021 and 2020, the number of privacy roles offered increased by 30% annually [4], in addition, Gartner is predicting that by 2026, 70% of boards will include one member with security experience [5] and 60% of organizations will shift from external hiring to “quiet hiring” from internal talent markets to address systemic security recruitment challenges. The security competence gap, on the other hand, is a challenge for both economic growth and national security since it endangers the networks, data, and IT systems that are the backbone of modern societies, [6]. Both quantitative and qualitative approaches can be used to analyze this deficiency. The quantitative problem is the lack of professionals to fill open positions, whereas the qualitative problem is the inadequacy of professional skills to fill market gaps. The number of students pursuing security or privacy as a qualification at the formal educational level has consistently climbed over the last year, but the number of graduates continues to fall far short of industry demand, [7].

Standardization is important for education because it serves as the foundation for developing educational standards and educational programs at all levels of professional education [8]. By establishing occupational and qualification standards, the Croatian classification framework encouraged standardizing the definition of requisite competence for a particular task. We provide the outcome of the development of the occupational standard called Information security and privacy architect, which includes a list of necessary tasks that a person with the defined profession should be able to perform.

Both employers (who employ the aforementioned professions) and employees (who hold occupations) were interviewed during the developing process. Our research aims to identify whether there are differences in the perception of key tasks of the occupational standard that describe the privacy/security specialist from the employer's and employee's perspectives. It is critical to determine whether the company owner or top management can identify the necessary knowledge and skills of privacy and security experts and those who are engaged in ensuring data protection daily (individuals). To achieve this aim, three guiding questions drive this study:

RQ1: Are there disparities in employers' and employees' opinions of the necessary competencies for the key tasks defined in the occupational standard to be performed?

RQ2 Are there disparities in perceptions of how frequently key tasks defined in occupational standards are performed?

RQ3: Do employers and employees have different perspectives on the level of expertise required to accomplish the key task defined in occupational standards?

2 Qualification Standard Development

With common interests and commitments, privacy and security are gradually merging. Organizations are training and making more personnel aware of privacy threats and needs, particularly those directly in charge of handling and safeguarding the firm's data, [9]. Suppose the ultimate responsibility for privacy-preserving design rests with software developers. In that case, there should be methods and solutions that serve as a mediator for translating end-user privacy rules into methodical and analytical lines of action to accomplish such privacy. Companies are required to use middleman technology to mitigate the chances of a violation in an age where privacy regulatory compliance is crucial, [10].

Given that organizations continue to rely on the Internet for conducting business and that humans continue to be the weakest link in security, it is imperative to understand an employee's level of security expertise to secure information and the systems that contain it.

Some frameworks address a common understanding of the roles, competencies, skills, and knowledge used by and for individuals, employers, and training providers across privacy and security domains, [2], [6], [11]. European Cybersecurity Skills Framework (ECSF), [6] defines 12 profiles: chief information security officer, cyber incident responder, cyber legal, policy & compliance officer, cyber threat intelligence specialist, cybersecurity architect, cybersecurity auditor, cybersecurity educator, cybersecurity implementer, cybersecurity researcher, cybersecurity risk manager, digital forensics investigator, and penetration tester. NIST Privacy Framework proposes privacy practices that support privacy by design concepts and assist organizations in protecting the privacy of individuals, [2]. E-Competence Framework [12] introduces transferable skills that can be applied to any ICT competency. In the IoT, AI, and Industry 4.0 age, transfer skills are required in all ICT-related operations. The fact that two of the seven stated transversal factors are security and privacy demonstrates the significance of this expertise. The global skills and competency framework for the digital world (SFIA) [11] provides a list of skills most relevant to various professional disciplines, industry topics, and complementary frameworks through several views, one of which is Information and cyber security.

Qualifications play an important role in improving employability, mobility, and access to higher education, [13]. The European Qualifications Framework (EQF) is a common European reference framework intended to make qualifications across countries and systems easier to read and comprehend. The core of the European Qualifications Framework is its eight reference levels, defined in terms of learning outcomes, particularly knowledge, skills, and autonomy-responsibility. The European Qualifications Framework has driven the creation of a comprehensive national qualification framework based on learning outcomes.

The Croatian Qualifications Framework (CROQF) is developing a mechanism for balancing supply and demand for work at the level of competencies, which is assisting in the modernization and reform of the Republic of Croatia's qualification system, [14]. CROQF introduces Occupational and Qualification standards. The Occupational Standard is a list of key tasks an individual performs in a certain occupation and competencies required for their successful performance. Qualification Standard is a set of learning outcomes for certain levels, volumes, profiles, types, and qualities. It is proven by a certificate, diploma, or other public document issued by an authorized legal entity.

In Croatia, no occupational standard currently addresses privacy and security competencies. The process of developing occupational standards was divided into four steps according to the defined methodology by Ministry of Labor and Pension System, Family and Social Policy [15]: (1) adjusting the questionnaire that will be used in research (defining key tasks and required knowledge and skills), (2) conducting the research, (3) systematizing the collected data, and (4) defining occupational standards with a list of key tasks and a list of competencies.

According to the Croatian Qualifications Framework methodology for developing occupational standards and sets of competencies [15] we conducted structured interviews with 24 leading IT companies in Croatia employees to define the occupational standards for information security and privacy architects. They were representatives of managers and lower-level workers (operatives). Interviews were performed with 12 representatives of employers (2 female and 10 male) and 12 representatives of employees (1 female and 11 male). Their task was to identify the duties of the person responsible for information security and data protection in the company. Then, they had to determine the required knowledge and skills to perform the task. Each knowledge and skill was assessed to determine whether they were required or optional and the level of expertise needed to perform the task.

Representatives of employers were chosen based on their representativeness like company size, business sector, kind of economic activity, and spatial distribution. The representative of each employer group is crucial, and this should be a leader who knows all positions in a profession (head of department/sector 75%, CTO 17%, and CEO 8%). When selecting employees, their competencies, domain of the privacy and security issues they deal with at their position were considered, as their understanding of the primary roles of the person who should be an Information security and privacy architect. Since we were defining a new occupational standard and job position that did not exist in Croatian occupation qualification, we tried to encompass all domains: telecommunication, radiocommunication, database management, customer support, IT infrastructure, payment infrastructure, and development of digital society. All of the employees had good (50%), very good (33%), and excellent (17%) insight into what the key task of officers dealing with privacy and security should be. During the performance of guided and structured interviews, all terminology (e.g., key task) must be explained and understood by employers and employees, and they must assess (a) the frequency of performance and (b) the level of competence required for each key task.

Data analysis shows that some of the indicated key tasks are not performed at all in a certain occupation(s) - they can be deleted from the list. Tasks performed extremely infrequently or rarely can also be suggested for removal, while those performed frequently are unquestionably the main tasks. As a result, the proposition of occupational standard Information security and privacy architect is defined which encompasses the following key task:

1. Planning of information security and privacy systems, as well as organizational, technical, spatial, financial, and human resources for deployment and monitoring systems,
2. Planning and designing the organizational structure for the implementation of the information security and privacy system in the business system,
3. Conducting analysis and assessment of the current situation in terms of information security and privacy requirements,
4. Assessing potential risks based on the identification of information assets, the importance of data content, possible sources, and forms of threats using modern risk calculation methodologies,
5. Proposing ways to deal with identified threats and measures for risk reduction,
6. Developing a business system work plan in crisis conditions as well as proposing system recovery measures,
7. Conducting security and privacy vulnerability testing,
8. Managing the roles and responsibilities of tasks and assigning or withdrawing authorizations for information resources use,
9. Developing policies and procedures for the design, storage, use, and access of information system backups as well as password usage policies and procedures,
10. Implementing categorization of software and critical software, as well as developing a protocol for dealing with categorized software support in incident situations,

11. Periodic reporting to the Management Board on the overall security and privacy situation of the business system,
12. Managing software updates (on all user workstations) to reduce vulnerability,
13. Establishing procedures for exercising individual rights related to the protection of security and privacy,
14. Assisting in the description, presentation, and marketing of a product or service by security and privacy requirements,
15. Communicating with customers, suppliers, associates, and other stakeholders while developing information security and privacy systems as well as with the supervisory bodies within the business system and in the environment,
16. Exchanging experiences with similar business entities and professional associations in the country and abroad to harmonize and implement measures,
17. Collaborating on security and privacy improvement projects, as well as participation in the development, improvement, or innovation of products or services to meet security and privacy requirements while adhering to good practice, legislation, codes of conduct,
18. Defining indicators related to security and privacy based on which organization checks and monitors the progress of quality assurance, particularly in the development and/or upgrading of a product or service,
19. Raising moral and material responsibility for omissions or non-compliance with prescribed information security and privacy measures.

[16], introduce four perspectives on occupation: (1) focus on an occupation-specific set of skills, (2) focus on demand-side, (3) institution perspective, and (4) the relationship between culture and occupation. We argue that there are disparities in employers' and employees' opinions of the necessary competencies for the key tasks defined in the occupational standard to be performed. For every key task respondents should identify: (1) how frequently key tasks defined in occupational standards are performed and, (2) the level of expertise required to accomplish the key tasks defined in occupational standards.

3 Methodology

The latent class analysis (LCA) is employed to account for heterogeneity across different groups of experts. Latent class analysis (LCA) is a descriptive modeling technique that has gained popularity in social science disciplines and is considered methodologically superior to traditional cluster analysis. First, LCA is considered superior to cluster analysis because it provides a formal chi-square test of statistical significance. Second, unlike cluster analysis, LCA can be designed as an analytical tool for all data types, including categorical and/or numerical response variables. Third, covariates can be included in the LCA model to predict the latent class membership of respondents, [17]. LCA is used in a wide range of research fields to cluster respondents into small subgroups called latent classes. The goal of LCA is to define the smallest number of classes suitable for explaining the associations observed between manifest variables, [18].

The number of clusters in any clustering method is selected based on predetermined criteria. The Bayesian Information Criterion (BIC) in LCA is often the only criterion, with the lowest BIC value indicating the best-fitting model, [19]. BIC has numerous advantages compared to other information criteria. However, it has been shown that excessive reliance on BIC as the only criterion could be harmful to the analysis [20], and an integrative approach to choosing the number of clusters is needed, [21], [22]. Akaike information criterion (AIC) is another information-based criterion used to determine an optimal number of clusters. Akaike information criterion (AIC) is a measure of model fit. AIC and BIC are information-based criteria assessing model fit, based on -2LogLikelihood. In this study, 2 clusters were chosen as the optimal number of clusters, according to the BIC and AIC values, but also considering the separation of the clusters and interpretability.

LCA was used to identify mutually exclusive latent groups (clusters) of experts considered to be homogeneous based on their responses to indicator variables: (i) perceptions of the key tasks that a person with an occupation for which an occupational standard is developed is performed and (ii) necessary level of expertise for the task to be performed. This analysis aims to identify clusters of experts concerning their perceptions. Modeling details regarding parameter optimization and research results are presented in the next section.

4 Research Results and Discussion

4.1 Results

LCA enables clustering by using categorical and continuous variables. Three cluster analyses were run separately specifying two-, three-, and four-cluster solutions. To determine the number of clusters the two-step cluster procedure was implemented. Bayesian Information Criterion (BIC) and Akaike's Information Criterion (AIC) were used to identify the optimal number of clusters. AIC and BIC are information-based criteria that assess model fit. Both are based on LogLikelihood - a technique which seeks to estimate the parameters of a model. When comparing the BIC and AIC values for the two models, the model with the smaller BIC and AIC is considered better. In general, BIC penalizes models with more parameters than AIC does.

Table 1. Clusters evaluation

No of clusters	LogLikelihood	BIC	AIC	Best
4	111.448	381.932	328.221	
3	113.273	376.332	326.546	
2	127.811	354.482	321.623	+

Results presented in Table 1 lead to choosing 2 (smallest BIC and smallest AIC) clusters. Taking also into consideration sample sizes in each cluster, and interpretability, the two-cluster solution was selected as the best one.

The results revealed the existence of two clusters for each group of tasks with different profiles. Experts of the same level of (i) organizational duties and (ii) insights into task requirements have similar perceptions.

Table 2 reports the two cluster profiles identified. Each cluster was named based on its key characteristics.

Table 2. Clusters` Distributions

Cluster code	Cluster 1	Cluster 2
Cluster name	Employees with complete insight into task requirements	Employers with average insight into task requirements
Size % (n)	60,67 %	39,33%

Cluster analysis was performed for all 19 tasks from the perspectives of two variables: The key task performed and the necessary level of expertise for the task to be performed. Results indicated significant differences between employees with complete insight into task requirements and employers with average insight into task requirements for all 19 tasks. In general, cluster 1 consists of experts considering the majority of the tasks are necessary to be performed, with a certain level of expertise ranging from fundamental to expert, depending on the specific task. On the other hand, cluster 2 consists of the experts who consider certain tasks unnecessary.

Cluster analysis used variable weighting to determine variables influencing the clustering process. Variables Insight into job requirements and Duties in an organization is shown to be the most important determinant of clustering affiliation.

These findings answer RQ1 indicating differences between employers' and employees' opinions of the necessary competencies for the key tasks defined in occupational standards to be performed.

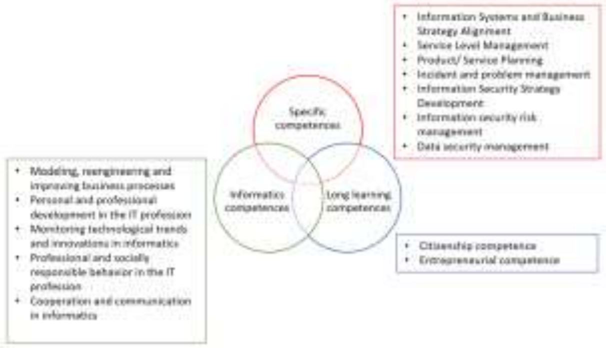
Information Systems and Business Strategy Alignment
Service Level Management
Product/ Service Planning
Incident and problem management
Information Security Strategy Development
Information security risk management
Data security management
Specific competences
Modeling, reengineering and improving business processes
Personal and professional development in the IT profession
Monitoring technological trends and innovations in informatics
Professional and socially responsible behavior in the IT profession
Cooperation and communication in informatics
Informatics competences
Long learning competences
Citizenship competence
Entrepreneurial competence

Fig. 1: Three competence categories

Each key task is associated with a set of competencies that privacy and security professionals must acquire to do their tasks. We divided these competencies into three categories (Figure 1): (1) specific competencies related to the domains of privacy and security, (2) informatics competencies related to the use of ICT in improving business processes, and (3) long learning competencies related to citizenship and entrepreneurial competence. Following that, we will highlight some tasks associated with each competency category. The process of defining competency categories is described in another paper published by the authors of this research, [23].

Figure 2 represents clusters for the task planning of information security and privacy systems, as well as organizational, technical, spatial, financial, and human resources for deployment and monitoring systems that can be connected with specific competencies (privacy and security domain).

Experts in cluster 1 consider Planning information security and privacy systems, as well as organizational, technical, spatial, financial, and human resources for deployment and monitoring systems, to be performed often or very often. In contrast, experts in cluster 2 think this task is not performed and is not necessary.

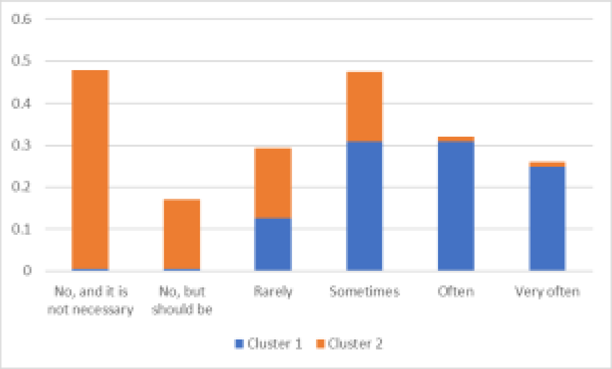

Fig. 2: Task Planning of information security and privacy systems, as well as organizational, technical, spatial, financial, and human resources for deployment and monitoring systems, is performed

There is a larger difference in perceptions between the two groups of experts for the task Proposing ways to deal with identified threats and measures for risk reduction (this task is connected with informatic competence) as shown in Figure 3. Most experts from cluster 2 believe this is not the necessary key task.

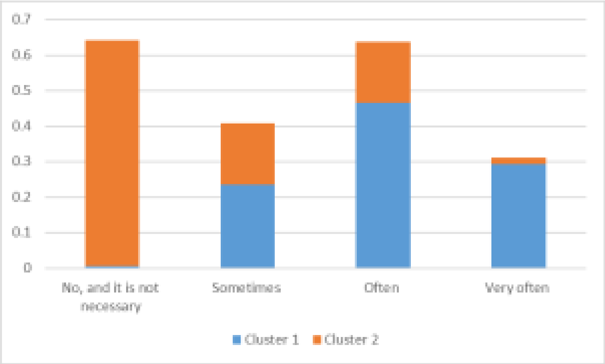

Fig. 3: Task Proposing ways to deal with identified threats and measures for risk reduction is performed

Figure 4 presents the difference in perceptions between the two groups of experts for the task of *Raising moral and material responsibility for omissions or non-compliance with prescribed measures in information security and privacy* (this task is connected with informatic competence). Most of the experts from cluster 2 believe that this is not the necessary key task. Most employers see this task performed sometimes or often, while most employers think this task is not necessary. It is interesting to note here that about 20% of employers perceive this task is performed very often.

Most of the experts in Cluster 2 consider task *Planning and designing the organizational structure for the implementation of the information security and privacy system in the business system* is not necessary. Experts in cluster 1 consider that the task is rarely performed. Similarly, experts in cluster 2 find the task of *Conducting analysis and assessment of the current situation in terms of information security and privacy requirements* unnecessary, and experts in cluster consider that task is sometimes performed. Similar patterns can be found for most of the tasks, such as *the Development of a business system work plan in crisis conditions as well as proposing system recovery measures* and *Conducting security and privacy vulnerability testing*. Presented information about cluster differences in perception of frequency of key task performance provides answers to research question RQ2.

When asked about the necessary level of expertise for the task to be performed, employers consider medium or advanced level while employees think it is not performed at this workplace (Figure 5, Figure 6 and Figure 7) therefore, the answer to RQ3 is: employers and employees have different perspectives of the level of expertise required to accomplish the key tasks defined in the occupational standard.

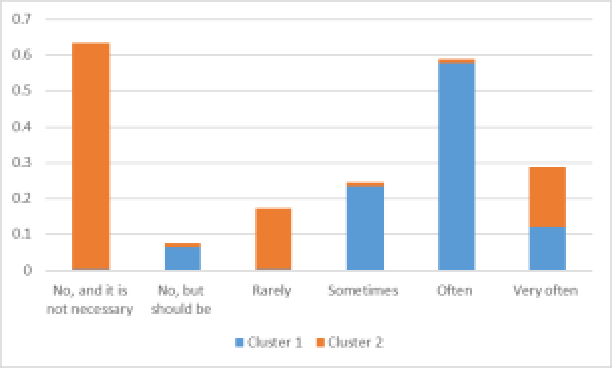

Fig. 4: Task Raising moral and material responsibility for omissions or non-compliance with prescribed measures in information security and privacy is performed

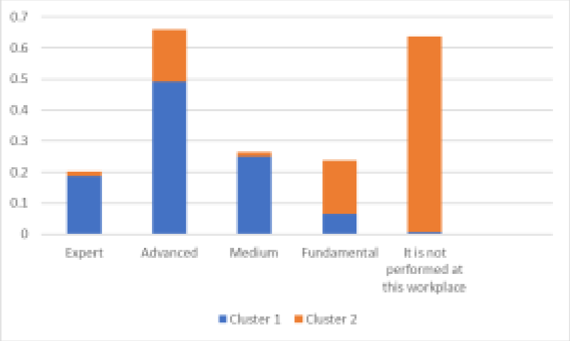

Fig. 5: Necessary level for the task of Planning information security and privacy systems, as well as organizational, technical, spatial, financial, and human resources for deployment and monitoring system to be performed

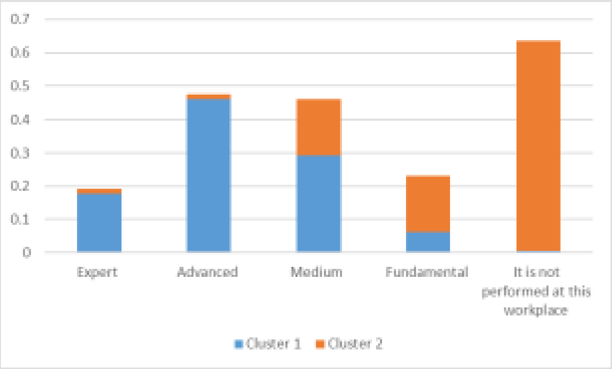

Fig. 6: Necessary level for the task of Proposing ways to deal with identified threats and measures for risk reduction to be performed

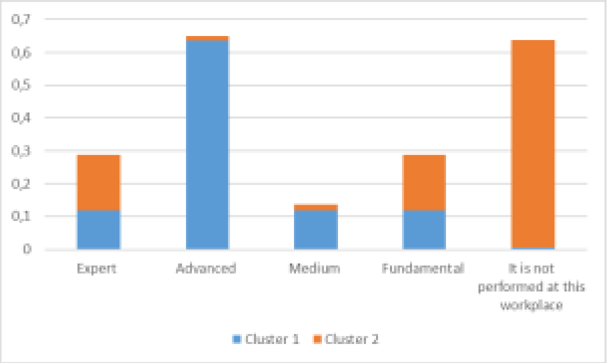

Fig. 7: Necessary level for the task of Raising moral and material responsibility for omissions or non-compliance with prescribed measures in the information security and privacy to be performed

4.2 Discussion

In this paper, we provide the results of developing the occupational standard called Information security and privacy architect, which contains a list of key tasks that a person in the specified profession should be able to accomplish. Occupational standards enable companies to arrange work activities around specified tasks while also informing (possible) employers and workers about required skills and the workplace environment. The purpose of our study was to determine whether there are discrepancies in the perceptions of key tasks of the occupational standard from the viewpoints of employers and employees.

Key findings from the presented study are:

- there are differences between employers' and employees' opinions of the necessary competencies for the key tasks defined in occupational standards to be performed (answer to RQ1),
- there are disparities in employers' and employees' perceptions of how frequently key tasks defined in occupational standards are performed (answer to RQ2),
- employers and employees have different perspectives on the level of expertise required to accomplish the key tasks defined in occupational standards (answer to RQ3).

Several conclusions emerge from our analysis. Firstly, there is an enormous demand for security and privacy professionals. Unfortunately, organizations that employ the aforementioned specialists cannot adequately define their responsibilities and skills. They are lost in the sea of professional certificates given by private institutions and the rising number of hacker attacks that they were unaware of and do not know how to respond to. On the other hand, potential employees are uninformed of the competencies that need to be acquired through formal and informal education.

Therefore, it is necessary to involve all stakeholders when developing occupational and qualification standards and connecting them to the curriculum (educational program). Our results show that employer and employee perspectives of occupation may differ. For the employer, the job candidate must have the necessary knowledge to do specific tasks well. Privacy and security professionals are professionals who design, develop, implement, manage, and protect the data and technology that power the digital world and must have certain ICT skills and competencies. To address information system threats and vulnerabilities, these professionals must understand the organization's entire business, have extensive knowledge of information technology, and have specific experience in information privacy and security. They must recognize the value of investing in security personnel to develop and protect their organization. But without the assistance of a team or at least one assistant, a single data protection/security officer will be incapable of manually administering, supervising, and enforcing data protection requirements.

Our research focused on the perceptions of employers and employees on important tasks that one privacy and security expert should do. Our findings reveal differences in employers' and employees' perceptions of the competencies required to perform the essential tasks described in occupational standards. Our findings fit with the perspectives on occupation suggested in [16]. First, an individual viewpoint emphasizes particular skill sets in a given occupation. Another option is to look at the tasks and occupations from the perspective of the demand side, [24]. An institutional viewpoint on occupation is the third. Individuals supply (employees) and employers demand common skill sets. As a result, both parties are interested in forming and expressing skill-set expectations to improve the efficiency of matching between supplied and demanded skills.

Secondly, organizations are attempting to teach and educate more employees about privacy risks and requirements, particularly those directly accountable for an organization's data and its security. The benchmark survey respondent [9] were asked to identify their top three areas of responsibility. Surprisingly, "Data privacy and governance" was chosen by these respondents the most frequently (32 percent), barely ahead of "Assessing and managing risk" and "Analysing and Responding to Threats." Data privacy has become a core capability for these teams, in addition to all of the traditional security functions. Security teams are responsible not only for keeping unauthorized persons out but also for increasingly collaborating with privacy teams to guarantee that those authorized to access data do so correctly. Data privacy has become a core competency for these teams, in addition to all of the usual security functions upon using technical privacy solutions like encryption, user transparency, user control, user access, automatic data expiration, data anonymization, user deletion, and temporal data.

The digital space has to be safe and secure. All users should feel powerful and protected, from youth to old age. The educational system should be actively involved in achieving this goal. Occupational standards are developed using a tool known as the qualification framework, which includes not just market demand but also employer requirements for/from employees. The occupational standard encompasses lifelong competencies, digital competencies, social and communication abilities, and skills relevant to a particular employment sector. Considering that the occupational standard authorized by the competent authority (minister) in the particular country specifies the competencies that must be met in the educational program that provides the appropriate qualification is crucial. This defines what the individual performing the particular position must learn in his formal education. By including companies and staff in developing such a standard, the quality of education programs and those who will be educated according to it will be improved. Even if they disagree on (1) the necessary competencies for the key tasks defined in occupational standards to be performed, (2) how frequently key tasks defined in occupational standards are performed, and (3) the level of expertise required to accomplish the key tasks defined in occupational standards.

5 Conclusion

Developing an occupational standard and identification of key tasks is not easy. One of the first necessary steps is to assess different stakeholders and capture their views. In this paper, we have analyzed the perspectives of employers and employees. Cluster analysis grouped respondents' perspectives perfectly into two groups: employers and employees thus revealing large differences in their answers. By comparing the clusters, differences appear for all tasks included.

A rarely presented perspective of both management and employers seeks challenges and opportunities in defining standards.

The findings presented in this paper demonstrate the disparity between the employee's and the employee's vision. The employer seeks a candidate with the necessary knowledge and skills to do the task. Employee results, on the other hand, can be said to be more realistic because they know what kind of work they are dealing with and what they can do independently.

There are several limitations of the research, First, the small sample should be considered when generalizing results. Second, there are alternative methods which could be employed in data analysis.
In future work, we plan to apply supervised machine learning algorithms to the collected data to develop predictive models. We plan to enhance the presented results from two points: (i) by providing more detailed insights into differences because sensitivity analysis of predictive models will detect variables contributing to those differences, and (ii) by enabling prediction of the perspective and validation of the presented approach.

Declaration of Generative AI and AI-assisted Technologies in the Writing Process

During the preparation of this work the authors used Grammarly for language editing. After using this service, the authors reviewed and edited the content as needed and take full responsibility for the content of the publication.

References:

[1] Pagallo, U. (2022). The Politics of Data in EU Law: Will It Succeed? *Digital Society*, *1*(20). https://doi.org/10.1007/s44206-022-00021-3.

[2] NIST. (2020). NIST Privacy Framework. In *January 16, 2020* (p. 43), [Online]. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01162020.pdf (Accessed Date: October 1, 2024).

[3] ISACA. (2022). *Privacy in Practice 2022*.

[4] Haher, R., Coseglia, J., Strait, L., Shanik, M., Manager, M., Barre, J., Roberts, S., Brown, S., Channell, A., & Hall, B. (2022). *Data Privacy Jobs Report 2022*.

[5] Addiscott, R., & Michaels, A. (2023). *Top Trends in Cybersecurity 2023*. Gartner.

[6] ENISA. (2022). *European Cybersecurity Skills Framework Draft v0.5 Work In Progress APRIL 2022* (Issue April)

[7] Naden, C. (2021). *ISO - The cybersecurity skills gap*, [Online]. https://www.iso.org/news/ref2655.html (Accessed Date: October 1, 2024).

[8] Frolova, O. Y., Fomina, L. V, & Shmeleva, Z. N. (2021). The personnel competence qualification formation in the agro-industrial complex production systems: managerial aspect. *IOP Conference Series: Earth and Environmental Science*.

[9] CISCO. (2021). *Data Privacy Benchmark Study, Forged by the Pandemic: The Age of Privacy Contents* (pp. 1–21), [Online]. https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-privacy-benchmark-study-2021.pdf (Accessed Date: October 1, 2024).

[10] Olukoya, O. (2022). Assessing frameworks for eliciting privacy & security requirements from laws and regulations. *Computers & Security Journal*, *117*.

[11] The SFIA Foundation. (2021). *SFIA view: information and cyber security*. SFIA 8, [Online]. https://sfia-online.org/en/sfia-8/sfia-views/information-and-cyber-security?path=/glance (Accessed Date: October 1, 2024).

[12] e-Competence Framework (e-CF) - A common European Framework for ICT Professionals in all sectors - Part 1: Framework, (2019).

[13] Council recommendation of 22 May 2017 on the European Qualifications Framework for lifelong learning and repealing the recommendation of the European Parliament and of the Council of 23 April 2008 on establishing the European Qualifications Framework for lifelong learning, Official Jurnal of the European Union (2017). [Online]. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017H0615(01) (Accessed Date: October 1, 2024).

[14] The Croatian Qualifications Framework Act, Pub. L. No. NN 22/2013 (2013).

[15] Ministry of Labor and Pension System, Family and Social Policy. (2021). *Metodologija za izradu standarda zanimanja i skupova kompetencija*.

[16] Haupt, A., & Ebner, C. (2020). Occupations and Inequality: Theoretical Perspectives and Mechanisms. *KZfSS Kölner Zeitschrift Für Soziologie Und Sozialpsychologie Volume*, *72*, 19–40.

[17] Li, J. (Justin), Bonn, M., & Kim, J. H. (2020). A latent class segmentation analysis of gamblers in a gambling destination. *Journal of Destination Marketing & Management*, *16*, 100433. https://doi.org/10.1016/J.JDMM.2020.100433

[18] Pavlić, I., Vojvodić, K., & Puh, B. (2020). Consumer Segmentation in Food Retailing in Croatia: A Latent Class Analysis. *Market-Tržište*, *32*(Special Issue), 9–29. https://doi.org/10.22598/MT/2020.32.SPEC-ISSUE.9.

[19] Lezhnina, O., & Kismihók, G. (2022). Latent Class Cluster Analysis: Selecting the number of clusters. *MethodsX*, *9*, 101747. https://doi.org/10.1016/J.MEX.2022.101747

[20] Dziak, J. J., Lanza, S. T., & Tan, X. (2014). Effect Size, Statistical Power, and Sample Size Requirements for the Bootstrap Likelihood Ratio Test in Latent Class Analysis. *21*(4), 534–552. https://doi.org/10.1080/10705511.2014.919819.

[21] Hennig, C., & Liao, T. F. (2013). How to find an appropriate clustering for mixed-type variables with application to socio-economic stratification. *Journal of the Royal Statistical Society: Series C (Applied Statistics)*, *62*(3), 309–369. https://doi.org/10.1111/J.1467-9876.2012.01066.X.

[22] Nylund-Gibson, K., & Choi, A. Y. (2018). Ten frequently asked questions about latent class analysis. *Ranslational Issues in Psychological Science*, *4*(4), 440–461. https://doi.org/https://doi.org/10.1037/tps0000176.

[23] Mekovec, R., Ruben Picek, Sandra Lovrenčić, & Čalopa, M. K. (2022). Creating

jobs for future computer professionals. *Proceedings of the Central European Conference on Information and Intelligent Systems*, 391–397.

[24] Carlton, M., Levy, Y., & Ramim, M. (2019). Mitigating cyber attacks through the measurement of non-IT professionals' cybersecurity skills. *Information & Computer Security*, 2056–4961.

Contribution of Individual Authors to the Creation of a Scientific Article (Ghostwriting Policy)

The authors equally contributed to the present research, at all stages from the formulation of the problem to the final findings and solution.

Sources of Funding for Research Presented in a Scientific Article or Scientific Article Itself

No funding was received for conducting this study.

Conflict of Interest

The authors have no conflicts of interest to declare.