Renata Mekovec and Dijana Oreški (2022): Competencies for professionals in the fields of privacy and security. In: Proceedings of the International Conference on Privacy-friendly and Trustworthy Technology for Society – COST Action CA19121 - Network on Privacy-Aware Audio- and Video-Based Applications for Active and Assisted Living

Competencies for professionals in the fields of privacy and security

Renata Mekovec, Dijana Oreški
University of Zagreb, Faculty of organization and informatics
renata.mekovec@foi.unizg.hr, *dijana.oreski@foi.unizg.hr*

Abstract

According to a new 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 (ISACA 2022). On the other hand, the cybersecurity skills shortage is a problem for both economic development and national security because it poses threats to the data, information technology systems, and networks that serve as the frontal bone of modern societies (De Zan and Di Franco 2019). This lack can be seen from two perspective: quantitative and qualitative. The quantitative issue is the insufficient supply of professionals to meet the job market's requirements, while the qualitative issue is the inadequacy of professional skills to meet the market's needs.

The demand for privacy professionals is expected to rise over the next year, with technical privacy roles growing faster than legal/compliance roles (ISACA 2022). There was a 30% year-over-year increase in available privacy roles in 2021 and 2020, with the trend expected to continue, if not accelerate, through 2022 and beyond (Haher et al. 2022). Furthermore, a gap between demand and trained talent is growing. The reasons for this shortfall are numerous and varied. At the formal educational level (university, college), the number of students pursuing privacy or/and cybersecurity as a qualification has steadily increased over the last decade

or so, but the number of graduates continues to fall far short of industry demand. It takes time to educate and train highly skilled professionals, as well as time to gain practical on-the-job experience. Meanwhile, investment in privacy and cybersecurity training has been severely hampered as budgets for non-profit and revenue-generating items have been cut or reduced (Naden 2021).

A single data protection officer or other function will be incapable of administering, supervising, and enforcing data protection requirements manually without the assistance of a team or at least one assistant. To address information system threats and vulnerabilities, these professionals must understand the entire business of the organization, have extensive knowledge of information technology, and specific expertise in information privacy and security. They are expected to recognize the importance of investing in security personnel in order to develop and protect their entire organization. Privacy and security are gradually merging, with mutual interests and responsibilities.

The benchmark survey (CISCO 2021) asked security professionals to identify their top three areas of responsibility. "Data privacy and governance" was chosen by these respondents the most frequently (32 percent), just ahead of "Assessing and managing risk" and "Analyzing and Responding to Threats." Data privacy has become a core competency for these teams, in addition to all of the usual security functions. Armstrong et al. (2018) propose that students (in the domain of security) should graduate with the following skills: 1) knowledge of and skills in identifying vulnerabilities and robustness of systems and applications; 2) conceptual familiarity with attack classes and attack stages; 3) knowledge of and skills in penetration testing principles and tools; and 4) knowledge of network traffic and network protocols. ACM provided guidelines for associate-degree cybersecurity programs that should encompass eight knowledge areas: data, software, component, connection, system, human, organizational and societal security (ACM and CCECC 2020). According to ENISA a certified higher education cybersecurity degree should include (De Zan and Di Franco 2019): (1) enough specific credits dedicated to cybersecurity courses and activities; (2) a structured curriculum, which may include a practical/training component or specific types of examinations and activities such as cybersecurity competitions; (3) a high-quality teaching faculty, which may include industry lecturers; (4) a broader multi-/interdisciplinary focus; and (5) outreach activities and programs. In order to address the cybersecurity skills shortage, the European Cybersecurity Skills Framework aims to create a common understanding of the roles, competencies, skills, and knowledge used by and for individuals, employers, and training providers across EU Member States (ENISA 2022). NIST Privacy Framework is proposing privacy practices that support privacy by design concepts and assist organizations in protecting the privacy of individuals (NIST 2020).

The e-Competence Framework (e-CF) - A Common European Framework for ICT Professionals in All Sectors is a standard for ICT professional competence that

defines the minimum requirements of competence in ICT workplace (16234-1 2016). e-CF introduces transferable skills that can be used across all ICT competences. Transfer skills are necessary in all ICT-related operations in the age of IoT, AI, and Industry 4.0. The fact that security and privacy are two of the seven stated transversal factors demonstrates the importance of these skills.

Qualifications play an important role in improving employability, mobility, and access to higher education (C 189/15 2017). The European Qualifications Framework (EQF) is a common European reference framework aimed at making qualifications easier to read and understand across countries and systems. The EQF's core are its eight reference levels, which are defined in terms of learning outcomes, namely knowledge, skills, and autonomy-responsibility. The EQF has been a driving force behind the creation of comprehensive national qualification frameworks based on learning outcomes. All countries that have accepted on to the EQF presume that such national frameworks are required to make their qualifications comparable across sectors and countries. 35 countries had formally linked ('referenced') their national qualification frameworks to the EQF by September 2021.

The Croatian Qualifications Framework - CROQF is building a harmonization mechanism supply and demand for work at the level of competencies, which is helping to modernize and reform the qualification system in the Republic of Croatia (NN 22/2013). There is currently no occupational standard in Croatia that addresses privacy and security competencies. According to CROQF methodology for developing occupational standards and sets of competencies (Ministarstvo rada i mirovinskog sustava obitelji i socijalne politike) we conducted structured interviews with 24 employees of leading IT companies in Croatia to define the occupational standards for information security and privacy architects. They were managers' and lower-level employees' representatives (operatives). Their task was to express which jobs are performed by the company's person in charge of information security and privacy. Then they had to figure out what knowledge and skills are needed to do the job. Each knowledge and skill were evaluated to determine whether it was required or optional, as well as the level of expertise required to complete the task.

As result proposition of occupational standard Information security and privacy architect is defined which encompass following key jobs (and competences):

- Planning of information security and privacy systems, as well as organizational, technical, spatial, financial and human resources for deployment and monitoring system,
- Planning and designing the organizational structure for the implementation of the information security and privacy system in the business system,
- Conducting analysis and assessment of the current situation in terms of information security and privacy requirements,

- 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,
- Proposing ways to deal with identified threats and measures for risk reduction,
- Development of a business system work plan in crisis conditions as well as proposing system recovery measures,
- Conducting security and privacy vulnerability testing,
- Managing the roles and responsibilities of jobs and assigning or withdrawing authorizations for information resources use,
- Developing policies and procedures for the design, storage, use and access of information system backups as well as passwords usage policies and procedures,
- Implementing categorization of software and critical software, as well developing a protocol for dealing with categorized software support in incident situations,
- Periodic reporting to the Management Board on the overall security and privacy situation of business system,
- Management of software updates (on all user workstations) in order reduce vulnerability,
- Establishing procedures for exercising individual rights related to protection security and privacy,
- Assist in the description, presentation, and marketing of a product or service in accordance with security and privacy requirements,
- 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,
- Exchanging experiences with similar business entities and professional associations in the country and abroad in order to harmonize and implement measures,
- Collaboration 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,
- Defining indicators related to security and privacy on the basis of which organization checks and monitors the progress of quality assurance, particularly in the development and/or upgrading a product or service,
- Raising moral and material responsibility for omissions or non-compliance with prescribed measures in the information security and privacy.

In addition to defining the structure of an occupational standard for Information security and privacy architects, we highlight variables important for identifying key jobs in the study. The latent class clustering analysis (LCA) is employed to account for heterogeneity across different groups of experts. LCA is data mining method

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 jobs that a worker with an occupation for which an occupational standard is developed are performed and (ii) necessary level of expertise for the job to be performed. An aim of this analysis was to identify clusters of experts with regard to their perceptions. We have developed numerous cluster models to identify optimal number of groups. The results revealed the existence of two latent clusters for each group of the jobs (e.g. workplace preparation, occupational jobs related to the workplace...), with different profiles. Experts of the same level of: (i) duties in organization and (ii) insights into jobs requirements, have similar perceptions.

References

Armstrong, Miriam E., Keith S. Jones, Akbar Siami Namin, and David C. Newton. 2018. "What Vulnerability Assessment and Management Cybersecurity Professionals Think Their Future Colleagues Need to Know." 1082–1082. doi: 10.1145/3159450.3162250.

ISACA. 2022. "Privacy in Practice 2022."

Naden, Clare. 2021. "ISO - The Cybersecurity Skills Gap." Retrieved April 12, 2022 (https://www.iso.org/news/ref2655.html).

16234-1, EN. 2016. E-Competence Framework (e-CF) - A Common European Framework for ICT Professionals in All Sectors - Part 1: Framework.

ACM, and CCECC. 2020. Cybersecurity Curricular Guidance for Associate-Degree Programs.

C 189/15. 2017. 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 the Establishment of the European Qualifications Framework for Lifelong Learning.

CISCO. 2021. Cisco 2021 Data Privacy Benchmark Study - Forget by the Pandemic: The Age of Privacy.

ENISA. 2022. European Cybersecurity Skills Framework Draft v0.5 Work In Progress APRIL 2022.

Haher, Rachael, Jared Coseglia, Lauren Strait, Michelle Shanik, Marketing Manager, Jess Barre, Sarah Roberts, Sarah Brown, Amelia Channell, and Brittany Hall. 2022. Data Privacy Jobs Report 2022.

ISACA. 2022. Privacy in Practice 2022.

Ministarstvo rada i mirovinskog sustava obitelji i socijalne politike. 2021. Metodologija Za Izradu Standarda Zanimanja i Skupova Kompetencija.

NIST. 2020. NIST PRIVACY FRAMEWORK: A TOOL FOR IMPROVING PRIVACY THROUGH ENTERPRISE RISK MANAGEMENT, VERSION 1.0.

NN 22/2013. 2013. The Croatian Qualifi Cations Framework Act.

De Zan, Tommaso, and Fabio Di Franco. 2019. ENISA: Cybersecurity Skills Development in the EU - The Certification of Cybersecurity Degrees and ENISa's Higher Education Database.