Co-funded by the Erasmus+ Programme of the European Union

secureu
DIGITAL EDUCATION TOOLS FOR SECURITY RISK MANAGEMENT

ERASMUS+ cooperation partnership "Digital education tools for security risk management"

"ROUND TABLE DISCUSSIONS" IN 6 PARTNER COUNTRIES

REPORT

Project number: 2021-1-LV01-KA220-HED-000023056

The main aim of organising 6 round table discussions in Latvia, Lithuania, Finland, Spain, the Netherlands and Norway was to gather security and risk management specialists and to ask their opinion about questions like what we should teach to young security specialists, what skills are missing, what the future perspectives and perceived risks are for the security field and for the security specialist profession in general.

In the summer and autumn of 2022 7 events were organised:
8th June 2022, Riga, **Latvia**, Turiba University
17th June 2022, **Finland**, Laurea University
1st July and 29th August, 2022, Bodo, **Norway**, Nord University
13th September 2022, Barcelona, **Spain,** School of Prevention and Integral Safety and Security
22nd September 2022, Vilnius, **Lithuania**, Kazimieras Simonavičius University
23rd September 2022, Breda, **the Netherlands**, Avans University of applied science

Participants:
The participants were security specialists from various institutions and companies as well as academics and lecturers from partner Universities. Among the participants there were representatives from many Retail and Service industry enterprises, Police, a Joint Emergency Services Call Center, Social Insurance Institutions, Regional Health Authorities, Air Forces. In total 48 experts took part in those events and contributed to the content of this report.

SUMMARIZED OUTCOMES ARE AS FOLLOWS:

Skills of young security specialists – what skills are missing when they start their duties?

LATVIA

Latvian experts pointed out that in the security field work mostly specialists of the older generation, but the industry wants new specialists, motivated interested in the field.
Sector needs new professionals with a clear vision about the field of security.

Organisations need specialists with a good education, well trained managers. Those specialists should be able to think critically to assess risks, understand security systems, services.
Organisations need security professionals who are able to monitor and organize the preservation of material values and also environmental security - a safe environment in which there is no threat, neither internal nor external.

Main skills emphasized: ability to access risks, management skills, organisational skills, leadership, argumentation and critical thinking, knowledge and practical skills about the newest practice, solutions, and safety techniques.

LITHUANIA

In Lithuania, there is no basic (profile) education system for training of young security professionals, the country focuses only on the training of public security specialists (police, border security, prison security). It is very important to establish the fundamental basis to understand and describe who is *a security professional.*

The profile of security specialists/professionals should depend on the internal security goals set in the organization documents, and accordingly, on composition a group of security professionals; taking into account these factors, the skills, abilities and competences for the performance of functions and responsibilities are determined for each of the groups.

Security specialists can't be trained within the frame of universal profile, because the principle of universality is usually attributed to the head/lead of the organization's security group (usually with master's degree and professional experience); professionals – security specialists - should be profiled and based on this, training programs are prepared and implemented in basic and higher education institutions.

The prevailing opinion that *a security specialist performs only physical protection* should be changed fundamentally, because the market of security services requires a significantly wider profile of the security function, covering diverse scope of the knowledge and skills (e.g. financial, technical, security design, data analytics, digital literacy, etc.).

The current security services market is dominated by two functions: security risk officers (physical, cyber, etc.) and security compliance officers (fraud, information security).

The need for profile security education depends on the willingness of the organizations themselves to invest and have security specialists within the organization.

Main skills emphasized: wider profile of the security function - financial, technical, security design, data analytics, digital literacy skills. Skills should be defined based on needs of each organisations/company, also defined in internal security goals set in the organization documents.

NORWAY

Experts pointed out challenges that young specialists have limited experience since they are freshly graduated. More practical activities and exercise during their education will be fruitful and provide them hands-on experience to some degree.

Young specialists are missing information management skills and understanding of how to obtain a holistic view. The information management aspect of security is vital and sometimes students do not take it serious. Also there is a lack of analytical skills - being observant, learning how things work, asking questions and analysing decisions.

Main skills emphasized: More practical activities and exercises during studies – better practical skills for young specialists; skills to manage information, holistic view, analytical skills.

SPAIN

Experts emphasised the lack of communication skills of the young specialists. As we deal with so called "mute generation" we can observe communication and integration problems. There sometimes is a lack of empathy and assertiveness when interacting with middle-aged or elderly people. So it leads to communication problems in a traditional environment. Young specialists need training in active listening, cooperation and different ways of interacting. There should be change of profile of specialist: such qualities as intelligence, sense of belonging or ability to integrate, commitment. Also training in technology in a responsible manner should be focused.

Main skills emphasized: Communication skills, skills related to interaction with different generations, different communication techniques – active listening; technological skills.

FINLAND

Experts pointed out that there are cases when Higher education institutions are too careful in including the very basic things in security, such as in physical security or personnel security. Sometimes a student can “avoid” learning basics of information security and cybersecurity, which is not acceptable. It should be part of compulsory core studies.
New students have little knowledge of a business value chain: what can they do to provide added value and to protect the value chain?
Almost everyone knows about risk management, but more practice in different methods is recommended. Students need to try a lot of various methods and be able to find the suitable ones.
New professionals don’t always consider the strategy of the organization. They should be able to read and understand it and try to consider what they can do to support it. A university/UAS degree brings very good results in seeing the holistic view. Without one, a person might be good at a specific thing, but not see so well their role in the whole.
Also experts pointed out that HEIs should have opportunities for specialization.

Main skills emphasized: basics of security (including physical and personnel security), knowledge about business value chain, basics of information security and cybersecurity, practical skills in risk management, comprehension of organisations’ strategy, strategic management.

THE NETHERLANDS

Experts pointed out that the current curriculum has too much emphasis on the perfect company security strategy in business cases. Furthermore, there should be more private security management content in the curriculum (as opposed to private safety or public security) and more professional certificates offered.

There should be an enhanced focus on awareness that more legislation than merely the privacy laws is relevant.

It is important to create a common understanding of how to balance business risks and security risks, it is not right to focus on educating security managers to mitigate all security risks possible. Furthermore, it is important to foster a common understanding of the potential effects of security risks on primary business.

Theory should be put into practice - more problem based education is needed.

Motivation of the workers helps security. Creating platforms on which the workers can become involved is helpful. Security managers do not have to initiate efforts to create involvement, but they need to be prepared to assist the HR department by, e.g., becoming ambassadors.

Young specialists lack some communication skills, e.g. handling corrective talks with non-compliant staff members. Soft skills are the third factor in security management and must be learned. Skills which should be focused on are: stakeholder management skills, curiosity, tenacity, asking the right questions, coordinating skills, assertiveness, pro-activeness.

There should be more specialised content modules in the BA in years 3 and 4, like on IT security.

The increasingly international workforce requires increasing inclusivity and awareness of diversity.

Main skills emphasized: management skills, literacy in legal aspects, balancing business risks and security risks, soft skills, communication skills, IT/AI skills.

CONCLUSIONS

Experts from all countries highlighted several similarities and skills' groups which are important for young security specialists, no matter which country they come from:

Strategy	Strategic thinking, strategic management, understanding organisation's strategy, ability to balance business risks and security risks, holistic view.
Management	Better management skills, organisational skills, leadership skills.
Soft skills	Definitely – importance of soft skills – communication (including interaction and dealing with different generations, knowledge about generation studies, active listening, argumentation) critical thinking, media literacy.
IT, cyber-security	Ability to manage information security, cyber-security, technological and digital literacy.
Practice	More practice in study process. More problem based education.
Basics	At the same time it is vital not to avoid or exclude very basic information about security in the study process.

What qualities does one security professional have that make him/her a good member of a security team (any type)?

LATVIA

Ability to orientate in different situations, different security systems and issues in the broadest sense. Ability to communicate and collaborate; substantiate and argue their own point of view.

LITHUANIA

Constantly learning, improving qualifications and seeking new knowledge.

Be motivated and willing to work in the chosen security profession, be able to creatively apply acquired knowledge in daily activities.

Dutifulness and responsibility in carrying out assigned security tasks (security projects) and bringing them to final results.

Ability to communicate with the organization, i.e. a security professional cannot close himself in his assigned function field and think about security narrowly; the created security product should be used in the full scope of the organization’s activities and operations.

Understand the organization's business model and help achieve the organization's goals through the protection of the organization's resources (human, material, digital, etc.).

SPAIN

Soft skills related to proximity, to the extent that this is the model that requires most implementation.

Organizational intelligence in the field of proximity. Analysis of citizens' needs from the proximity model. Analysis of insecurity from proximity.

Work the predictive policing model. Interpreting citizens’ needs.

FINLAND

Enthusiasm about the mission of the organization; committed to the strategy and goals of the organization, understanding that they are supporting it; interested in development, to do better, courage to change things.

Wide experience, also outside of the required core; project working skills; a service attitude - understanding that security is a supporting function; social skills, cooperation skills, deep knowledge in own area – and recognise when you don’t know something.

THE NETHERLANDS

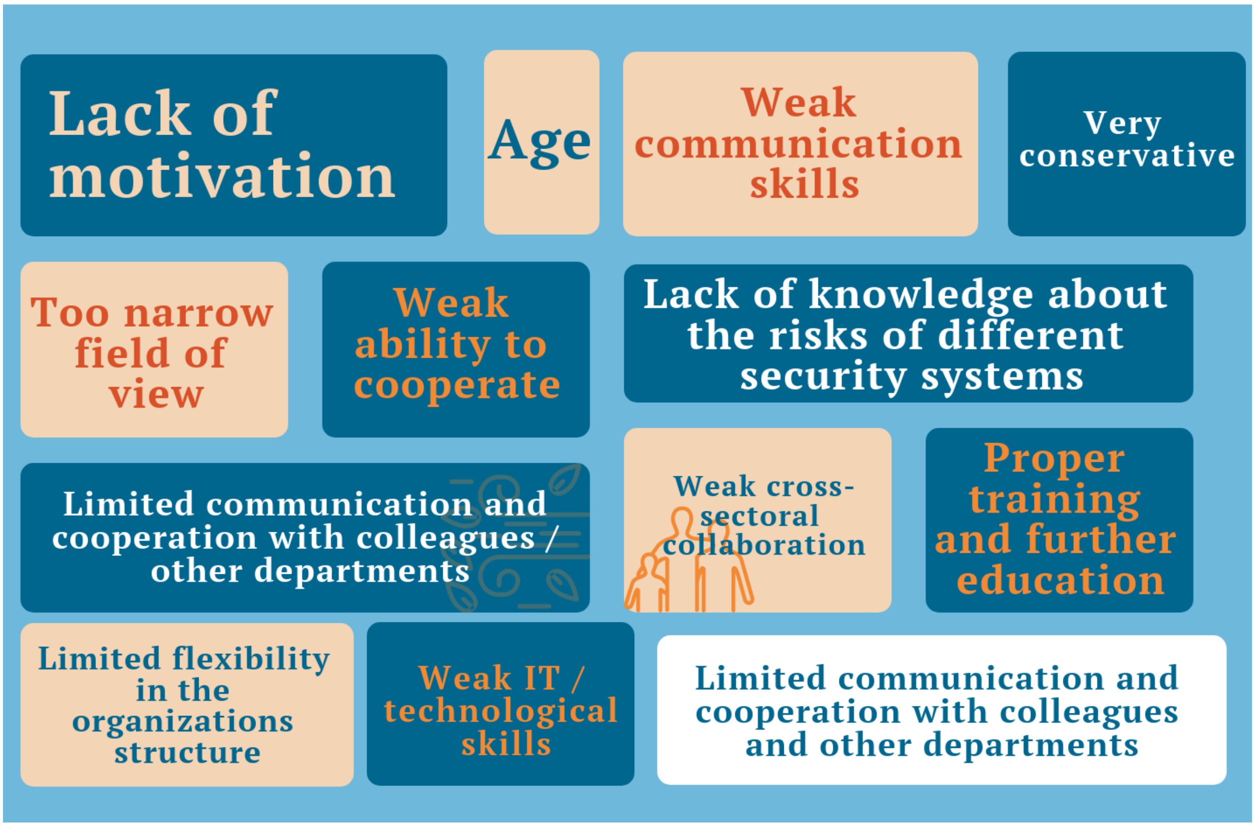
Ability to reinforce positive security behaviour. Investigative skills and asking thorough follow up questions. Awareness of threats related to using technical elements such as cameras, apps, software. Better than average understanding about primary processes, especially in IT and IT security.

Entrepreneurial spirit, analyzing & conceptual thinking capabilities, knowledge about applying LEAN.

NORWAY

Collaboration and team working, communication abilities and justifying their action with valid arguments; problem-solving, ability to approach a problem systematically, analytical capacities to look critical on things and to ask questions, team management and people management skills, to learn fast and be realistic, open to learning from failures, to connect educational content, general concepts to practical use.

What are the most significant weaknesses and «backfalls» in security professionals now?



Lack of motivation

Age

Weak communication skills

Very conservative

Too narrow field of view

Weak ability to cooperate

Lack of knowledge about the risks of different security systems

Limited communication and cooperation with colleagues / other departments

Weak cross-sectoral collaboration

Proper training and further education

Limited flexibility in the organizations structure

Weak IT / technological skills

Limited communication and cooperation with colleagues and other departments

Vision for the future

Future also for security field is information technologies, artificial intelligence and business analytics, cross-sectoral skills, building a link between business and security, cyber security, data security, technology literacy.

Specialists will have to be able to work with a wide variety of stakeholders. Security personnel will have to get out of the “bubble” and avoid doing security for security's sake. They will have to understand interdependencies of different functions within the organization and to outside of the organization.

Business continuity is more and more dependent on IT. More and more processes are automated, resumption time is slowly decreasing. However, everything is interdependent and therefore there is an increased vulnerability, particularly after Covid-19.

In the future, physical security will become less significant as a permanent function of the organization, the digitalization of the organization's business processes will cause a greater need for cyber security specialists and analytics of security information. Security professionals with data analytics and cross-sectoral knowledge and skills will be in demand on the security business market, who will be able to apply the processed data in the decision-making process using artificial intelligence tools. In the security business, the executors of security functions perform more of a "firewall" functions when security officers extinguish security incidents that have already occurred, however, in the future, area of integrated security risk and compliance management will become dominant in the security market, i.e. specialists with a broad spectrum of knowledge and skills on applying security requirements, able to identify, assess and manage security risk, to set and take actions addressing the identified risk, etc.

The labour market will demand specialists who have knowledge of risk and compliance management in order to ensure sustainable and high-quality provision of security services to the organization. The ability to understand the opportunities of integrating different security systems, their impact on the organization's activities and benefits, and the ability to work with various data that are relevant to the organization (analyse, compare, draw conclusions and provide solutions on how effectively manage risks with acceptable costs to the organization). In the future, various Security Competence Centres (HUBs) will be in high demand as security service providers, as it will become very expensive for organizations to have and retain security specialists with narrow professional expertise.

Within business continuity management there is a big move towards new platforms, networks and applications, for example, salary payments. Many different types of software or apps are involved, proxy systems, credentials checking, third parties, banks. These can be inside or outside the organisation. This ‘landscape of applications’ needs housekeeping in order to prevent large impact in case of, let’s say, a ransomware attack, to avoid a domino effect.

There is too much IT involved in the future and we already need to be so broadly developed in what we know: BCM, physical security, security culture etc. Sometimes even combined with safety management. Moreover, information security differs from IT security, and differs from Cyber security.