Closing the gap

between the needs of the cybersecurity industry and the skills of tertiary education graduates

Study report

Authors

Janice Richardson
Veronica Samara
Olena Styslavska
Teuntje Manders

Published by ISC3C, October 2022

insight
Educating to Empower

NASK

SIDNfonds

50% of all employees will need reskilling by 2025,
as adoption of technology increases.

Source: Future of Jobs Report 2020, World Economic Forum.

Images by Clker-Free-Vector-Images and OpenClipart-Vectors from Pixabay

Table of contents

Executive Summary

In 2021, Working Group 2 of the IS3C (an IGF dynamic coalition focusing on Internet Standards, Security and Safety) launched a study on education and skills related to cybersecurity. The aim was to understand the importance accorded to transversal and professional competences by the cybersecurity sector and tertiary education establishments, and the estimated level of competence of young people entering the cybersecurity workplace from both perspectives. To define the scope of the study and develop a list of the required transversal and professional competences, 5 interviews were conducted with industry leaders from 5 different EU countries and the findings were then validated in interviews with tertiary sector representatives in two further countries. IGF Youth and AprIGF members were trained, and conducted another 21 interviews in 9 more countries worldwide in 2022, according to an established protocol.

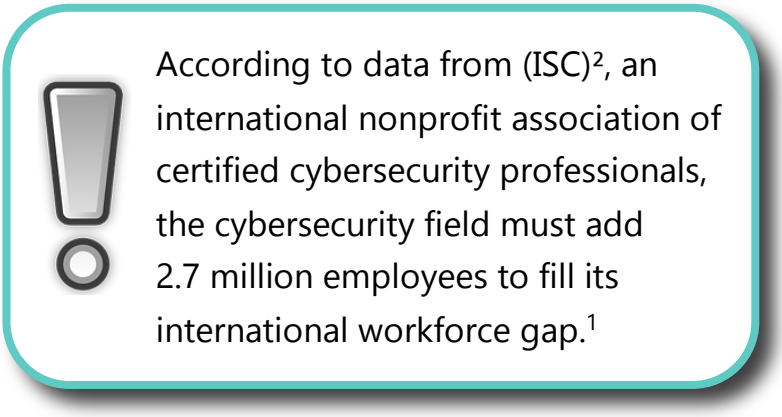
Of the total 235 respondents who completed the survey, 73% were male, 26% female, and 1% preferred not to indicate their gender. 19% were aged under 30 years. The under-representation of women and under 30-year-olds is indicative of the current lack of diversity in the cybersecurity sector. The survey questions were adapted according to whether respondents were from the business-industry or education sectors, though the same list of transversal and professional competences was retained for both. Respondents from business-industry (64% overall) placed approximately 10% more importance on both transversal and professional skills than the education sector, considering **critical thinking**, **problem-solving, teamwork** and **creativity** to be the top transversal skill requirements along with **risk prevention** and **security risk management** in professional skills. Respondents in the education group (36%) indicated **creativity** and **problem solving** as being the most important transversal competences, and rated **understanding of secure web communications and technologies** as the top professional requirement.

Only 67% of industry-business representatives – on average – rated the level of graduates on transversal competence as good or moderate, giving the highest rating to **oral** and **written communication skills,** and **teamwork** and the lowest on **holistic thinking**. Almost half of this group (44%) rated the average level of professional competences of graduates as low or very low, with the lowest rating given to **knowledge of cloud computing security**. The education group gave a similar assessment of their graduates' transversal competences, with **oral communication skills** and **problem solving** rated the highest, and **strategic thinking** and **holistic thinking** also rated low. On average, half of the respondents in the education group assessed graduates' competences positively (*very good* or *good*) with a top rating for **understanding of secure web communications and technologies** and a lowest for **knowledge of vulnerabilities and exploits of systems** and **knowledge of cloud computing security.**

Both industry-business and education groups place importance on similar transversal skills (**critical thinking**, **problem solving**, **teamwork**, **creativity** and **communication skills**), though the education group systematically places less importance on them. Their assessment of graduates' level of attainment is much closer, with higher ratings for **ethical thinking**, **problem solving**, **teamwork** and **communication skills** and the lowest for **holistic**, **strategic** and **interdisciplinary thinking**, and **business knowledge**. The gap between the two groups on the importance accorded to professional competences is much bigger. Education gives much less importance than industry-business on **understanding system logic** and **knowledge of mobile**

and IoT security, and more on **ability to write script or code**. The assessment of graduates' professional competences is much closer, with the highest rating given by both to **understanding of secure web communication and technologies**, and a low rating from both on **knowledge of cloud computing security**.

Findings from the overall study show that priorities of industry and education on transversal competences differ, though more in degree of importance accorded than in the area of focus. On the other hand, education seems to be lagging behind when it comes to developments in IoT, for example, where rapid evolutions are taking place. Suggestions put forward in the interviews and the survey underline a need for education to focus more on basics such as helping students better understand how systems and applications work, and how to overcome misleading search engine mechanisms. Seven recommendations have been drawn from the study. They range from improving collaboration between sectors, upgrading recruitment procedures to improve diversity, and raising awareness to encourage users to be more responsible about their own cybersecurity and to attract more young people to envisage employment careers in this rapidly growing economic sector.



[1] https://www.isc2.org/-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx

1. Introduction

What is the IS3C

The IS3C – a dynamic coalition to promote internet standards, security and safety – is a shared endeavour by stakeholders worldwide from the technical community, civil society, government policymakers, regulators, and corporate and individual adopters to improve safety and security online by achieving more widespread and rapid deployment of existing internet standards and ICT good practices. It was set up in 2020 within the Internet Governance Forum (IGF),[2] an international event organised by the United Nations and hosted in a different member country each year. Effective governance of the internet is necessarily underpinned by global awareness and respect of safety and security standards that aim to build trust within the online environment and contribute to the safety and security of its users.

The IS3C establishes an annual work plan implemented by 5 Working Groups, each with specific expertise in areas ranging from security by design and education and skills to supply chain management and data governance. The aim is to identify and bring together the critical security supply and demand factors, and propose the best options for the deployment of key standards and best practices on both sides, in the form of policy recommendations and practical guidance.

The expertise of Working Group 2 is in the area of education and the development of competences for citizens of all ages to maintain their own security, privacy and well-being online and actively contribute to advancing progress in digital products and services incorporating leading edge security standards and best practices. By scoping current levels of knowledge and skills of students and tertiary graduates, and expectations from industry and the business sector, the research described in this report is a fundamental step in defining next steps to achieve IS3C's goals.

Why cybersecurity is important

Digital technology has become an integral part of modern life, to such an extent that it is difficult to imagine life without it. More than 83% of the world's population, for example, are smartphone users (2022), a figure that is increasing at a rate of 4,9% per annum.[3] Anthropological research conducted across 4 continents in 2020-2021 describes online as *the place in which we now live*.[4] However, whilst constant connection to the internet has become commonplace, our online presence and digital traces represent a growing threat to personal safety, especially for younger or digitally illiterate individuals. Sadly, with a growing number of digital natives, the number of individuals with malicious intent, often seeking monetary gain, has increased as well. Cybersecurity, as a practice and societal standard, has therefore gained immense importance and is the only way to prevent privacy invasions and identity theft as well as other cybercrimes.

[2] https://www.intgovforum.org
[3] http://www.Statista.com
[4] https://www.weforum.org/agenda/2021/05/how-we-interact-with-smartphones-report/

Cybersecurity covers all of the means implemented by *a person, organization, or country and their computer information against crime or attacks carried out using the internet.*[5] The core function of cybersecurity is to protect the data individuals and organisations share or access via the internet, and therefore necessarily concerns both the security of the devices used to connect as well as the means used to store data. Most social, commercial, financial, entertainment, as well as political interactions and processes nowadays take place online.

It is estimated that, since 2007, more than 99.9% of all information is generated in digital format. The average person generates roughly 1.5 megabytes of data per day, and in 2021 we produced a global amount of 2.5 quintillion bytes of data daily.[6] The importance of cybersecurity will therefore continue to increase exponentially as we strive to protect the vast amounts of personal, business and government information kept online from unauthorized access, theft, misuse and damage.

Cybercrime increased dramatically worldwide with the Covid-19 pandemic in 2020-21[7] when schools, businesses and the workplace turned to the internet to continue their daily activity confronted with social distancing and public space shutdowns. Cybersecurity education is essential for every internet user from early childhood onwards, and involves a complex array of skills and knowledge that are constantly evolving as devices become more powerful and more firmly integrated into every facet of a person's life.

Although cybersecurity is the responsibility of every internet user, it has become a focal point of global business and largely depends on the vigilance, action and reactions speed, and innovativeness of software developers, dedicated cybersecurity companies and organisations. Yet the company SAP, a major world-wide player in the cybersecurity field, underlines that the industry is facing a systemic hiring and retention problem that must be addressed globally to ensure that the growing number of positions can be filled if we are to stay ahead of the ever-evolving threat landscape.[8]

The present study aims to investigate the essential transversal and professional skills required to address that challenge, within an ongoing approach to raise awareness of the importance of cybersecurity and build user-resilience through education.

[5] Cambridge Dictionary. (2022, September 28). cybersecurity definition. Retrieved 4 October 2022, from https://dictionary.cambridge.org/dictionary/english/cybersecurity?q=cybersecurity+

[6] Mapfre, F. (2021, December 27). *How much information is generated and stored in the world?* Fundación MAPFRE. Retrieved 5 October 2022, from https://www.fundacionmapfre.org/en/blog/how-much-information-is-generated-and-stored-in-the-world/

[7] Europol (2020). *Internet Organised Crime Threat Assessment (IOCTA)*, available at: https://bit.ly/348XZKi

[8] Elena Kvochko, chief trust officer at SAP. In https://www.scmagazine.com/news/careers/only-30-of-the-cyber-workforce-is-in-the-19-34-age-demographic%EF%BF%BC. Consulted on 7 October 2022.

2. Methodology

A two-phase approach

The present study has been built on a two-phase methodology aimed to document the specific competences expected of graduates when they begin their career in the cybersecurity industry and, from the perspective of both business and education sectors, take stock of the current average level of competences that graduates bring to the workplace. A secondary aim is to collect existing good practice in industry, that could help tertiary educational and vocational training fill the gap between supply and demand. In the following description of methodology and findings, the following key concepts are defined:

- **Competence** is understood according to the definition of the Council of Europe as the "ability to mobilise and deploy relevant values, attitudes, skills, knowledge and/ or understanding in order to respond appropriately and effectively to the demands, challenges and opportunities that are presented by a given type of context". In addition to this global and holistic use of the term "**competence**", the term "**competences**" (in the plural) refers to "the specific individual resources (namely, the specific values, attitudes, skills, knowledge and understanding) that are mobilised and deployed in the production of competent behaviour."[9]
- The **study** has focused on the interpretation of representatives from business, industry and education sectors on the knowledge and skill level required of a competent employee in today's cybersecurity sector, compared to the opinion of representatives from the field of education regarding the importance accorded to such skills and knowledge and the estimated level of competences achieved by their graduates. Attention was focused on two types of competences – transversal and professional.
- **Transversal competences** were understood as "competences that are typically considered as not specifically related to a particular job, task, academic discipline or area of knowledge, and that can be used in a wide variety of situations and work settings".[10]
- **Professional competences** were understood as "the combination of skills, knowledge attitudes and values that are specifically valued by professional associations, organizations and bodies within the cybersecurity sector".

The assessment of the current situation from the perspective of both the industry and education sectors was expected to contribute to the description of potential solutions to shorten the circuit between supply and demand and encourage broader take-up of good practice.

[9] RFCDC Glossary: at https://www.coe.int/en/web/reference-framework-of-competences-for-democratic-culture/glossary

[10] UNESCO (2019). *Assessment of transversal competencies: current tools in the Asian region*, Figure 1. At https://unesdoc.unesco.org/ark:/48223/pf0000368479

Study instruments

The first study phase comprised face-to-face and online interviews conducted with industry leaders in the cybersecurity sector between October 2021 and June 2022, to refine the research questions, scope cybersecurity in terms of needs and challenges, and gather examples of good practice. The 60-minute interviews were conducted by 10 interviewers from different linguistic and cultural background. The interviewers had a background in related domains and participated in two preliminary training sessions. They received a detailed guide for interviewers and recording templates to ensure comparability of the results. The interviews collated findings into 3 categories: competence requirements, challenges, and good practices. The interviews were conducted in close co-operation with IGF Youth [11]and Youth Summit participants, and representatives of the Asian-Pacific regional IGF (APrIGF). From the interviews, a model of the 14 transversal and 10 professional competences considered essential from the perspective of employers was developed. These made up **the list of competences** used in the second phase of the study.

The second phase was organized in the form of an online cross-sectional survey questionnaire to collect quantitative data to verify the model of competences, define the gaps and collect further examples of good practice. The survey was organized in two sections, see Figure 1.

In the first section participants responded to questions on demographics and were required to choose their employment sector: *industry-business* or *education (*including *school and tertiary)*. The questions in the second section were worded slightly differently for each of the two employment sectors, nevertheless maintaining the same two **lists of transversal and professional competences** for both sectors. Each question provided space for respondents to add their own suggestions. Two further open questions were added for the industry-business group.

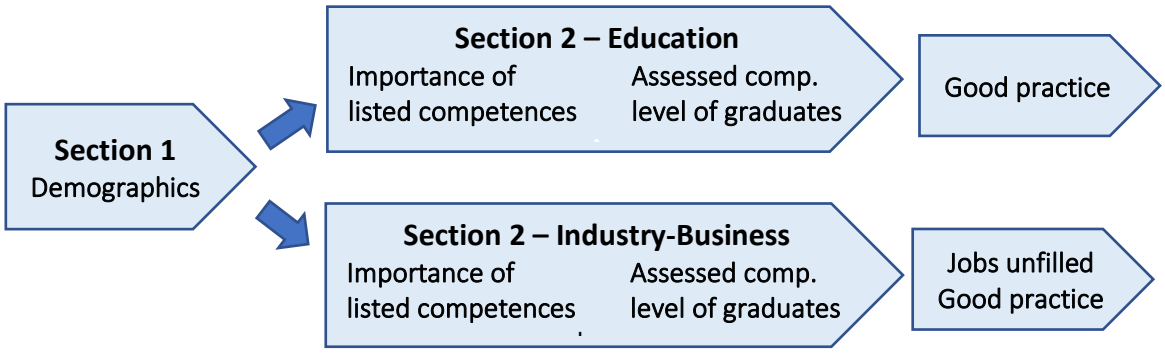


Figure 1. Structure of the survey questionnaire

The questionnaire for industry-business representatives asked respondents to:

- Rate the importance of **the list of competences** in the workplace;
- Rate the level of graduates working in their organisation according on the **listed competences**;
- Indicate which jobs they find the most difficult to fill, and the impact of this on their organization;

[11] IGF Youth and Youth Summit, at https://youthigf.com/

- Provide examples of good practice and suggest ways the situation could be improved.

Respondents from the education sector were asked to:

- Rate the importance accorded by their establishment to the **list of competences**;
- Rate the level of graduates on the **listed competences**;
- Provide examples of good practice in their establishment, and suggest solutions for improving the competences of graduates.

A 5-point Likert scale was used to measure both the importance accorded to the listed transversal and professional competences, and the assessed level of graduates in each of the listed competences.

The survey ran from 5 July to 20 September 2022, and was disseminated online via the personal networks of the IS3C, Youth IGF and APrIGF members.

"First, you need to attract diverse people. If we're all close-minded, one-minded, the sector won't be appealing for people with different backgrounds. The team then misses out on perspectives and aspects of security that are important. Diversity is helpful to see different things for different clients."

Female EU cybersecurity consultant

3. Findings

The interviews

Twenty-eight interviews were conducted in 16 different countries worldwide (see Figure 2); 5 key questions were used to guide the conversation. The lead researcher conducted the first seven interviews with industry and tertiary education leaders, with interviewees from government, industry and tertiary education sectors, the aim being to determine the scope and create a standard interview recording protocol. These interviews took place in seven countries: Belgium, Denmark, Italy, Luxembourg, Morocco, the Netherlands and Poland. Two online training sessions were then delivered to ten volunteer interviewers. The interviewers were, for the most part, university graduates especially interested in cybersecurity and internet governance; all were IGF Youth or APrIGF members. They conducted a further twenty interviews with high profile people involved in cybersecurity in their countries: Brazil, Ghana, Indonesia, Poland, Samoa, Sri Lanka, Sudan and Vietnam, plus one interview with a tech expert from Microsoft based in the USA. All data from the interviews was recorded in a shared online document using the above-mentioned interview recording protocol.

Figure 2: Interviews were conducted in 16 countries worldwide

The interview findings contributed to the development of the survey questionnaires, both in terms of structure and content. A number of interesting points arose from the interviews which will continue to serve as pointers towards areas worthy of further investigation. Several such points were also raised or validated by input in the open survey questions, including:

- **The big picture:** although all aspects of security require different sets of expertise, the existence of knowledge silos is slowing down the tracking and resolution of incidents. Cybersecurity evolves very rapidly, and people from different areas need to learn to share knowledge, skills, and expertise to bridge the silos and to cover the full picture. Organisations are increasingly looking for people with transversal competences because they are aware of this challenge.
- **Social diversity:** benefits organisations because it brings multiple perspectives on all areas of work and makes the job much more interesting. Narrow-mindedness doesn't leave room for different perspectives on aspects of security. It is important to get more young people involved, as they tend to use technology in different ways, and to encourage women to take up careers in cybersecurity, as they often take a more

granular approach. Knowledge-sharing, authenticity and openness are essential ingredients for successful team work.

- **Thinking skills**: critical- and abstract-thinking skills are essential. Being able to draw practical knowledge from work in labs, apply it in other situations, and check how the findings can be scaled up are all more important than the kind of learning obtained from a book. Designing cybersecure products and tackling cybersecurity incidents are complex processes that also require the ability to anticipate what the forthcoming threats may be and where they may come from.
- **Report-writing**: reports describing trouble-shooting strategies or indicating how issue have been handled need to be snappy, clear, and in layman's language. Cybersecurity teams have to be able to reach and convince all users to integrate preventive measures, and to see themselves as part of the solution. The challenge is to get strong messages across with cultural-political sensitivity, and without being technocratic.
- **Knowledge gaps**: a good understanding on how the internet backbone and administration systems work are central to knowing which environments are most fit for purpose. Students have trouble mastering the basic building blocks of how things, such as containers and kernels, work, because they lack knowledge on the history of digital developments. They are also often hampered by a poor understanding of algorithms and of blockchain, mobile and cloud security.
- **Education**: we have to make children enthusiastic about learning how their digital devices work, and help them see the possible downside and risks of using free technical tools. Teaching them how to search for information effectively is very challenging. Search engines usually rank things according to the number of times they've been referenced, which means that the oldest thing are listed first and it can be difficult to access the latest information. Things like knowledge-searching and -sharing, authenticity, cooperation, openness and self-management have to be developed in school from an early age.

The key concerns raised by most interviewees were validated in the findings from the survey questionnaire conducted in the second phase of this research. One issue repeatedly raised can be summed up in the words of Greg Bianchi from Microsoft USA: *The needs in the cybersecurity industry are huge. At the moment, the number of vacancies is enormous. This is due to the need for cybersecurity at many different levels. All types of experts are lacking*. *The problem of small numbers of women and other people historically excluded from communities makes it very difficult to get the right level of staff diversification*.[12]

[12] https://blogs.microsoft.com/blog/2021/10/28/america-faces-a-cybersecurity-skills-crisis-microsoft-launches-national-campaign-to-help-community-colleges-expand-the-cybersecurity-workforce/ and https://blogs.microsoft.com/blog/2022/03/23/closing-the-cybersecurity-skills-gap-microsoft-expands-efforts-to-23-countries/

The online survey questionnaire

The questionnaire was completed by 235 respondents, 64% from the business-industry sector, and 36% from the education sector. Responses came from 65 different countries[13] (see Figure 3).

Figure 3. Countries of residence of the questionnaire respondents

73% of respondents were male, 26% female, and 1% preferred not to indicate their gender. Male and female were fairly evenly distributed across both response groups. The under-representation of woman participating in the survey is indicative of the gender differences that exist across the cybersecurity sector. According to a 2022 study by (ISC)², [14] only 24% of all persons working in the cybersecurity sector are women. This is already significantly higher than a 2017 study by the same organisation that indicated that only 11% of women were employed in the sector. 44% of respondents

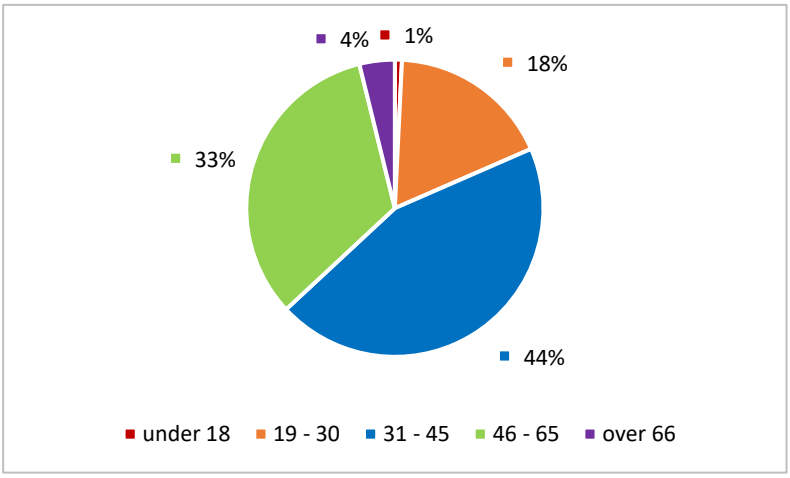


Figure 4. Age representation of survey respondents

[13] Afghanistan, Argentina, Australia, Austria, Aruba, Bangladesh, Belgium, Botswana, Brazil, Burkina Faso, Cameroon, Canada, Chad, Chile, Colombia, Congo, Cote d'Ivoire, Ethiopia, France, Fiji, Finland, Gambia, Germany, Ghana, Guinea, Haiti, Iceland, India, Indonesia, Kenya, Lebanon, Madagascar, Malawi, Malaysia, Mali, Mauritania, Morocco, Mozambique, Mexico, Nepal, the Netherlands, Nigeria, Norway, Panama, Philippines, Poland, Portugal, Russia, Rwanda, Serbia, South Africa, Senegal, Sudan, Sweden, Switzerland, Tanzania, Togo, Turkey, United Kingdom, Uganda, Ukraine, USA, Zimbabwe, Zaire, Zambia.

[14] https://www.isc2.org/research/women-in-cybersecurity. Consulted on 6 October 2022.

were aged between 31 and 45, 22% were in the 46 to 65 age bracket and just 18% were aged 19 to 30 (see Figure 4). 1% of the respondents was younger than 18, and 4% were aged 66 years or more. The age breakdown of respondents reflects an ongoing concern from business and industry: how to attract more young people to take an interest in careers in the cybersecurity sector. Recent research by CompTIA on the tech workforce, for example, found that 52% of those who work in cybersecurity are in the 35-54 age demographic, and only 30% of the cyber workforce is in the 19-34 age group.[15]

Industry-business rating of competence requirements in the workplace

On average, 86% of the business-industry group rated the listed transversal competences as *very important* or *moderately important* (see Figure 5). When *very important* and *moderately important* ratings are added together, **problem solving** and **teamwork** emerge as being rated the most important competences by the industry-business group, followed by **handling complexity**, **creativity**, and **critical thinking**.

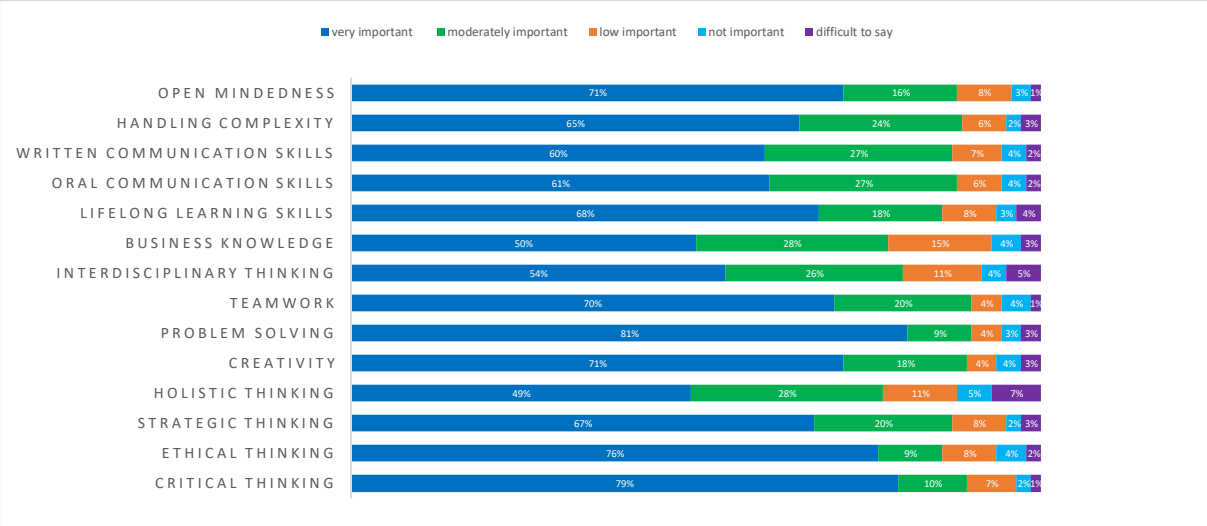


Figure 5. Industry-business: Importance of the transversal competences in the workplace

All 10 of the listed professional competences were rated as being *very important* or *moderately important* by at least 63%, and 82% on average, of the industry-business group (see Figure 6). **Risk prevention** and **security risk management** followed by **understanding of system logic** and of **secure web communications and technologies**. were rated as the top required competences, closely followed by **risk prevention management.**

[15] Research by CompTIA, quoted in https://www.scmagazine.com/news/careers/only-30-of-the-cyber-workforce-is-in-the-19-34-age-demographic%EF%BF%BC. Consulted on 6 October 2022.

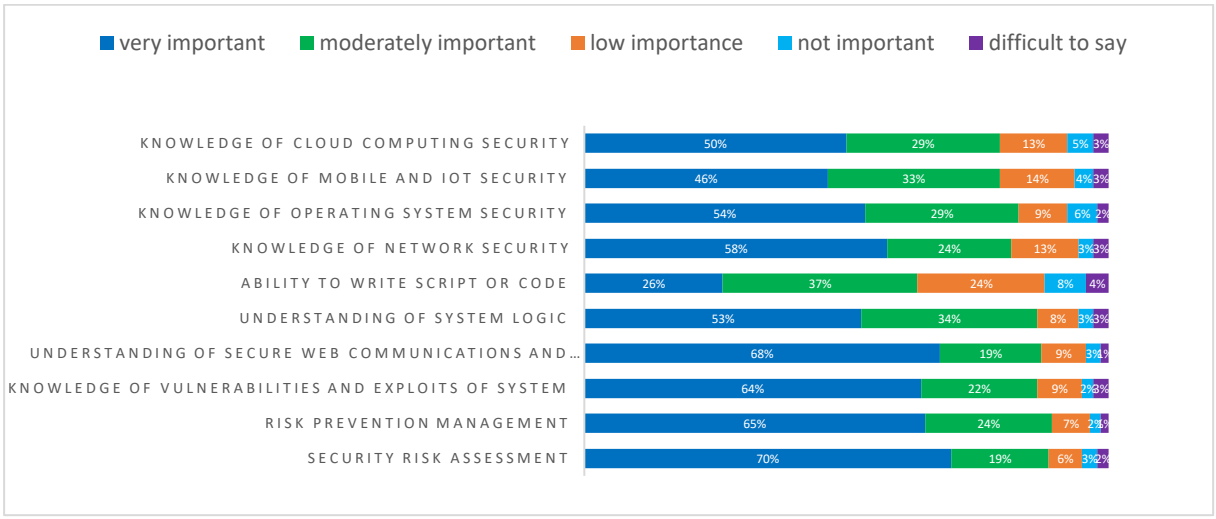


Figure 6. Industry-business group: Importance of the professional competences in the workplace

Eleven respondents added their own suggestions to the list of transversal competences the majority of which related to the ability to learn in a team, to learn independently, and to be open to knowledge-sharing. Responsibility, leadership, negotiation skills, multilingualism, respect of cultural diversity and psychological aspects of security (e.g. knowledge of social engineering) were also indicated - one or several times - under transversal competences.

For the majority of respondents in the industry-business group, the suggested **list of competences** appeared sufficiently comprehensive, although 21 respondents suggested additions to the list. However, most of the suggestions were very similar though more specific to the ones provided in the **list of competences**, and related mainly to data security, security awareness, network security and risk assessment.

Industry-business group evaluation of competences of graduates in the workplace

When asked to assess the level of transversal competences of the tertiary graduates employed by their organizations, on average 67% of industry-business respondents considered that graduates showed they had acquired acceptable levels on the overall list (see Figure 7). However, except for two competences, **open mindedness** and **lifelong learning skills,** the majority of respondents assessed the level as *moderate* rather than *good*.

The highest rated transversal competences were **oral communication skills** (82% rated them good or moderate), and **written communication skills** and **teamwork** (both at 78%). The lowest rated transversal competences were **holistic thinking** (only 48% considered graduates' level to be good or moderate), **business knowledge** (52%), and **strategic thinking** (55%).

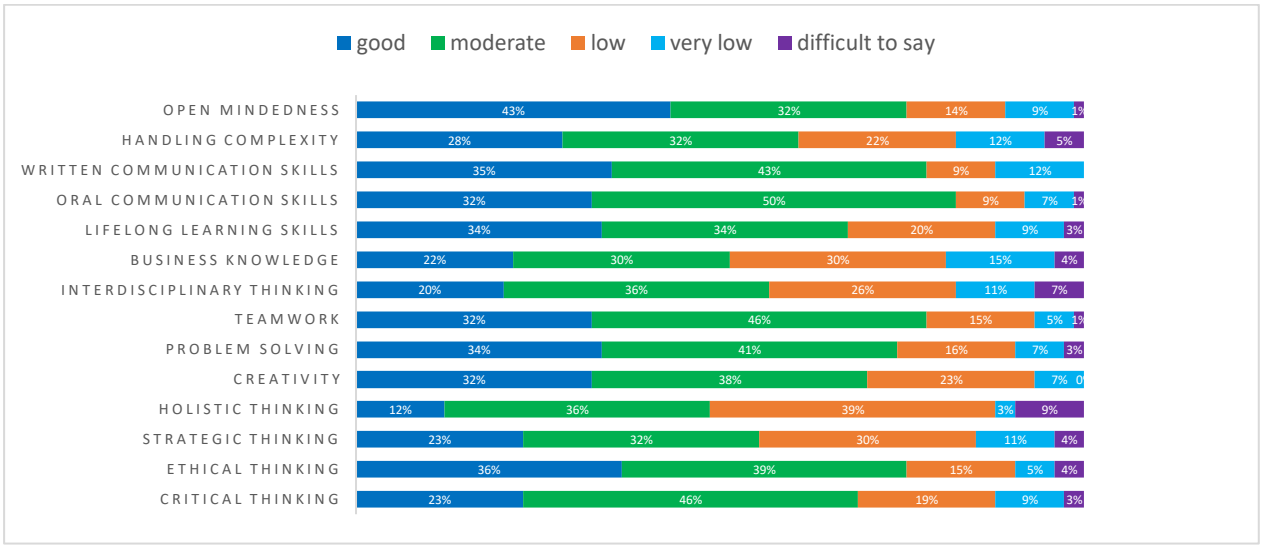


Figure 7. Business-industry assessment of graduates' transversal competences

Organisations showed less satisfaction with the professional competences of the graduates they hire; on average only 54% rated the items on the overall list of professional competences as good or moderate (see Figure 8), with more *moderate* rather than *good* ratings for all 10 competences. On average 44% of the respondents from the industry-business group assessed the professional competences of graduates as *low* or *very low*. The highest rated professional competences were **understanding of secure web communications and technologies** (65% selected good or moderate), **risk prevention management** (57%), **security risk management** and **knowledge of network security** (both at 56%).

The lowest rated professional competences were **knowledge of cloud computing security** (56% of industry-business respondents rated graduates' level on this competence *low* or *very low*), **knowledge of mobile and IoT security** (50%) and **knowledge of vulnerabilities and exploits of systems** (46% rated graduates' level in the competence *low* or *very low*).

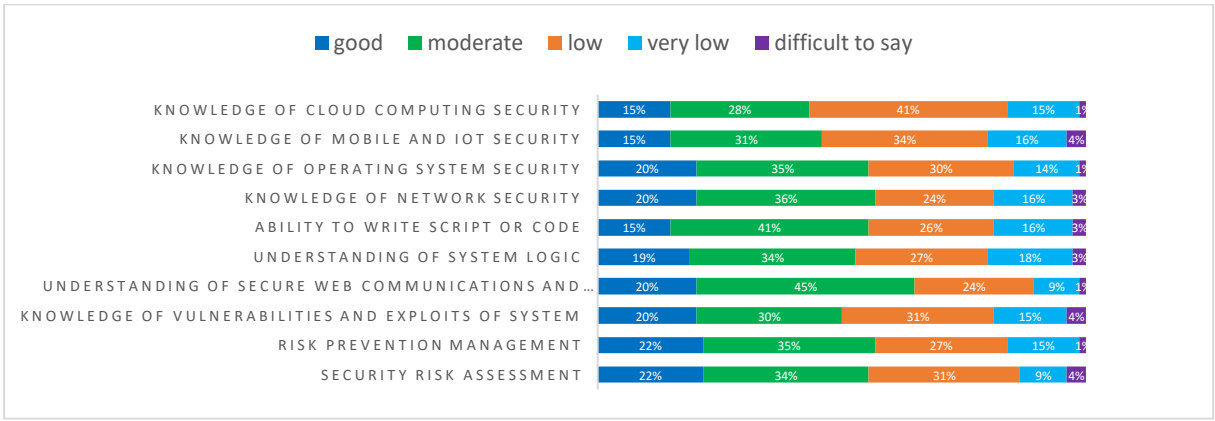


Figure 8. Business-industry assessment of graduates' professional competences

The educational sector perspective

Responses from the education sector on the importance of transversal competences were similar to those from the industry-business group, with 78% rating the competences on the overall list as *very important* or *moderately important* (Figure 9). The transversal competences considered to be most important were **creativity** (*very important* or *moderately important* for 87% of respondents), **problem solving** (for 86% of the group), **oral communication skills** and **teamwork** (for 82%). The transversal competences rated to be of *low importance* or *not important* were **business knowledge** (*low importance* or *not important* for 31%), **holistic thinking** (25%), and **strategic thinking** (21%). These low ratings appear to validate the viewpoint of the industry-business group that graduates are not sufficiently competent in these areas (comparison with Figure 7).

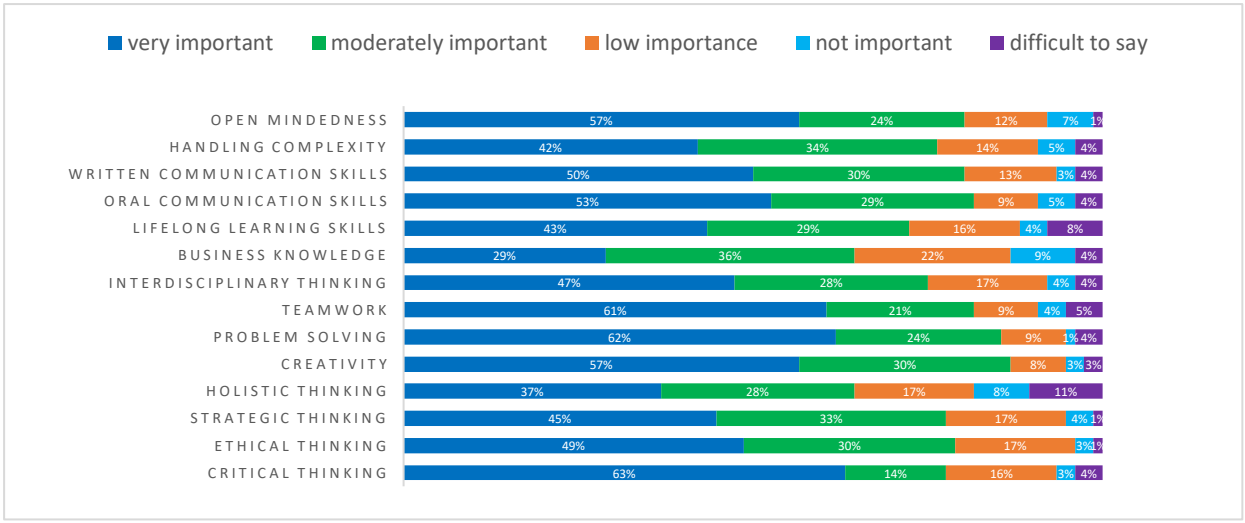


Figure 9: Education perspective on the importance of transversal competences

The majority of respondents in the education group were from the tertiary education sector. When asked about the importance of the 10 listed professional competences, 75% gave a *very important* or *moderately important* rating on **understanding of secure web communications and technologies** (see Figure 10). **Risk prevention management** and **knowledge of vulnerabilities and exploits of systems** were both considered *very important* or *moderately important* by 73% and 72% of education respondents respectively. Lowest ratings in level of importance were given to **ability to write script or code** (36% rated this of *low importance* or *not* important), **understanding of system logic** (32%), and **knowledge of mobile and IoT** (30%).

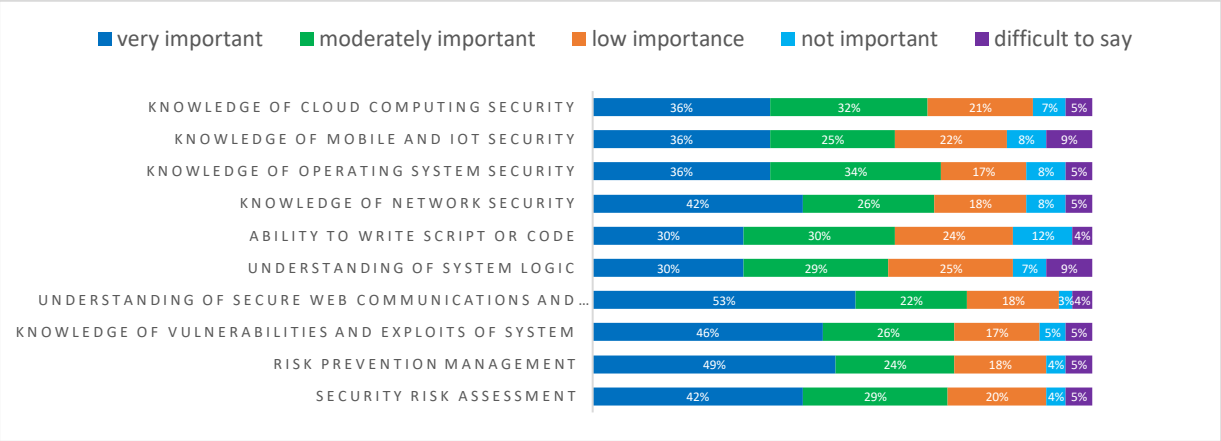


Figure 10: Education perspective on the importance given by the establishment to the professional competences

It is interest to observe that the opinion of the industry-business group on the importance of transversal and especially on professional competences of graduates, regardless of their geographic region, reflect to a certain extent the responses from the education sector on the importance of these competences.

Nineteen respondents from the education sector added other transversal competences to the list, including design thinking, ability to act safely in the digital environment, and the ability to protect one's own privacy in the digital environment. Other professional competences regarded to be important were:

- Understanding of digital environment and Internet;
- Policy compliance, knowledge of legal regulations and cyber law;
- Understanding of economic aspects of security;
- Ability to use IT support;
- Knowledge of emerging trends;
- Ability to use modern technology effectively.

Respondents from the education group also mentioned the importance of **digital inclusion** when technological transformation is taking place in the classroom.

The education group's assessment of the competence level of graduates

The education group gave a generally moderate assessment of the level of transversal competences of their graduates with an average 68% rating the listed competences *very good* or *good* (see Figure 11). **Oral communication skills** and **problem solving** were rated the highest with 78% of respondents assessing their graduates' level as *good* or *very good*, followed by **teamwork** at 76%. The lowest ratings were given to the following transversal competences: **business knowledge** (41% of education respondents ranked this *low* or *very low*), **strategic thinking** and **holistic thinking** (38% and 33% respectively).

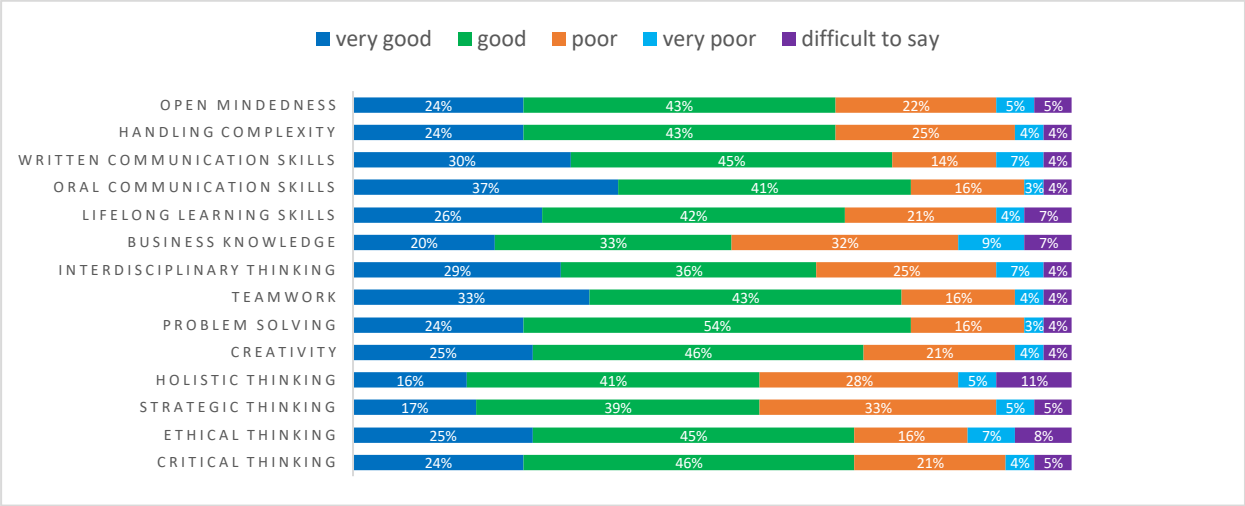


Figure 11: Education group's perspective on the transversal competences of their graduates

The general level of the professional competences of graduates, a crucial aspect from the perspective of the cybersecurity industry, was assessed even lower by representatives from the education sector than from the industry-business sector (see Figure 12). On average, only half of the respondents in the education group assessed graduates' competences positively (*very good* or *good*). **Understanding of secure web communications and technologies** was rated highest with 59% giving a *very good* or *good* rating, followed by **knowledge of network security** (56%) and **knowledge of operating system security** (51%). **Knowledge of vulnerabilities and exploits of systems** and **knowledge of cloud computing security** were both assessed to be poorly acquired competences with an overall *low* and *very low* rating of 47% and 45% respectively, followed by **understanding of system logic** (44%) and **knowledge of mobile and IoT security** (43%). This may highlight a gap between expectations of industry and objectives, or at least outcomes, of the education sector.

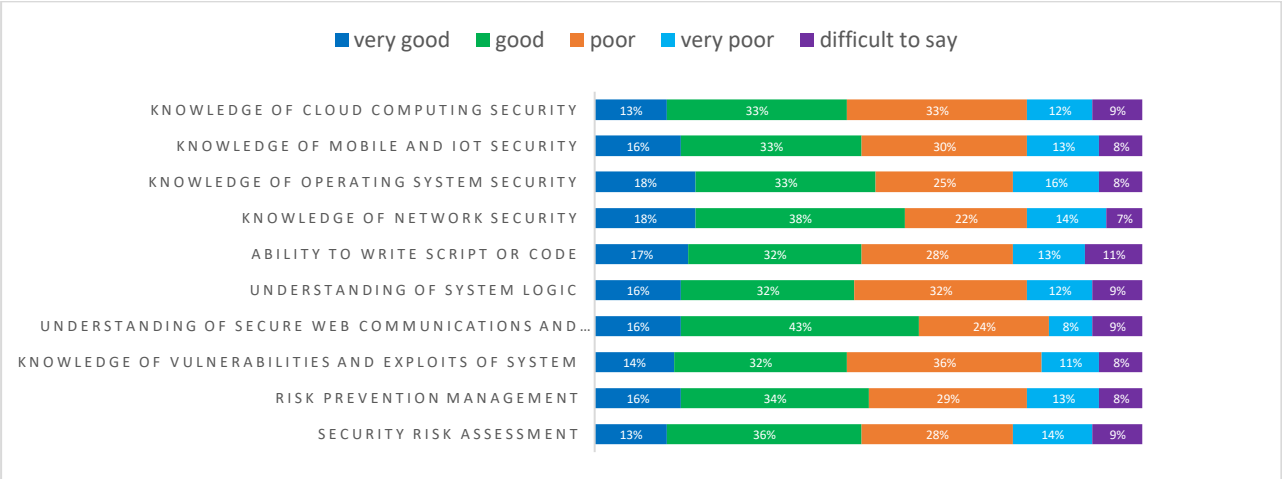


Figure 12: Education perspective on the professional competences of graduates

With small exceptions, the perspectives from both sectors are largely similar. Almost the same transversal and professional competences were pointed out as being the most and the least developed. Nevertheless, the representatives from the education sector seem a little more

optimistic about the competence level of their graduates than the industry-business sector about the competences of their graduate intake.

4. Defining the gaps, proposing solutions

A closer look at gaps related to transversal competences

The responses on the online survey questionnaire confirmed the assumptions drawn from the interviews. Stakeholders from both the education and the industry-business sectors appear to agree on the importance of the transversal and professional competences included in the model for the needs of cybersecurity in the contemporary world. However, respondents from the industry-business sector gave more importance to both lists of competences compared to the educational sector: 86% vs. 78% for the transversal competences and 82% vs. 68% for the professional competences (see Figures 13 and 15).

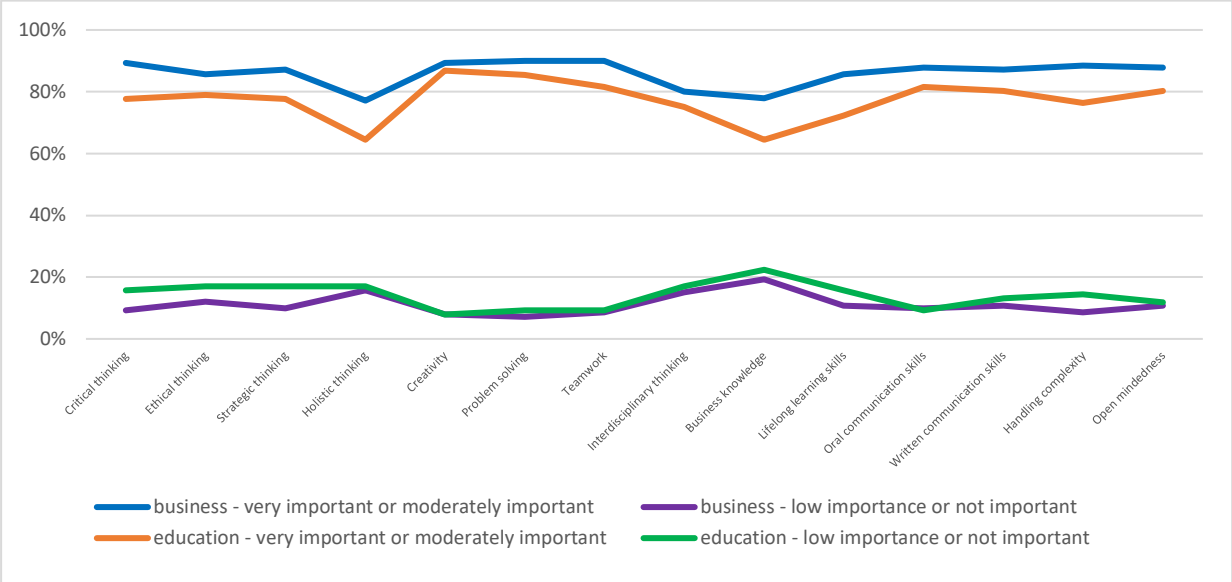


Figure 13: Comparison of responses between the industry-business and education groups on the importance of transversal competences

Both sectors rate **ethical thinking**, **problem solving**, **teamwork**, and **oral** and **written communication skills** to be reasonably good. **Critical thinking**, **creativity**, **lifelong learning skills**, **handling complexity**, and **open mindedness**, were rated as moderate. Lowest ratings were given to **strategic**, **holistic** and **interdisciplinary thinking**, and **business knowledge**.

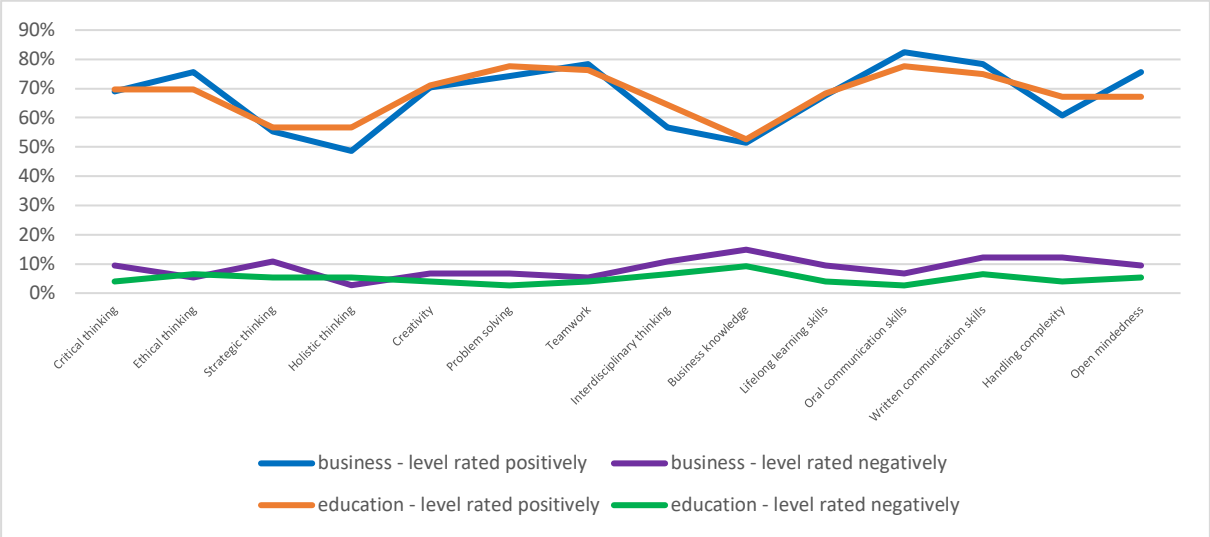


Figure 14: Comparison of responses between the industry-business and education groups on graduates' level of transversal competences

A closer look at the gaps related to professional competences

Although the education group respondents gave less importance to the development of professional competences (60% of respondents regarded the overall range of professional competences important, and 30% rated them not important), it seems to be, to a reasonable level, a common understanding in both sectors about the importance of professional competences (see Figure 15).

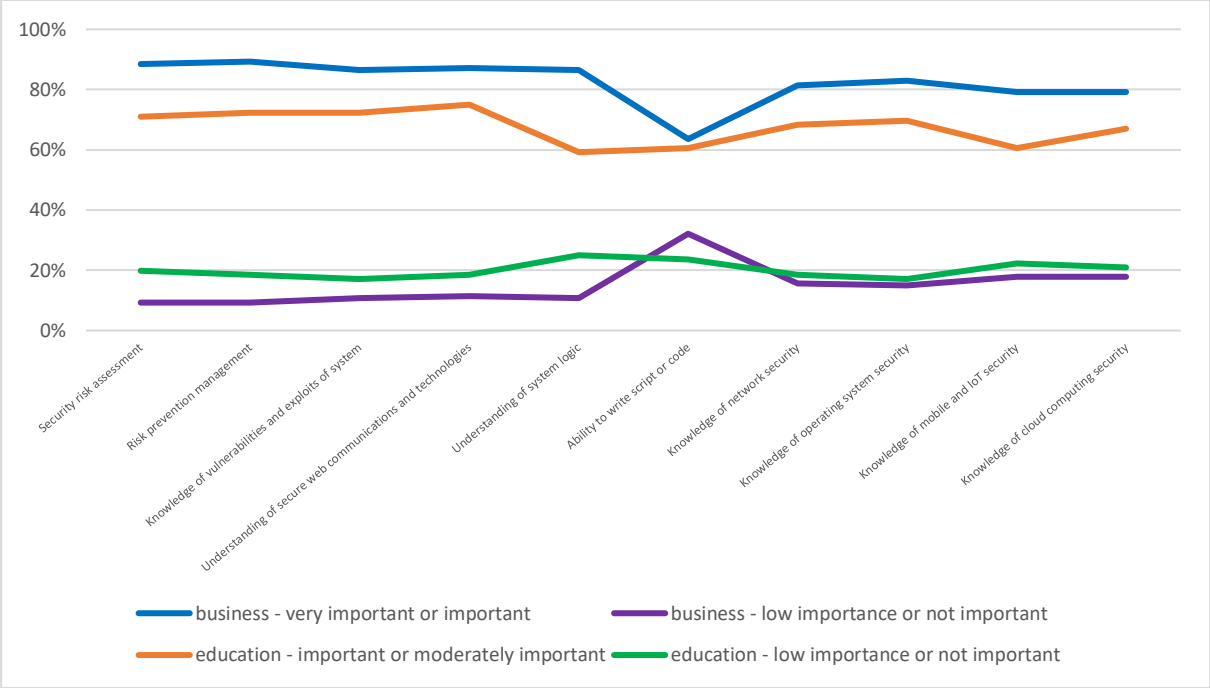


Figure 15: Comparison of responses between the industry-business and education groups on the importance of professional competences

Both groups of respondents presented similar opinions about graduates' level of professional competences. As shown on figure 16,[16] on average about half of the respondents from both groups assessed the level of development of professional competences positively, while on average 44% of respondents from business and 41% from education assessed the level as low or very low. None of the positive ratings (*very good* or *good*) for any competence reached 60% except for **understanding of secure web communications and technologies** (65% in the business sector and 59% in the education sector).

Another five professional competences assessed by both groups to be around 50%:

- Knowledge of operating system security;
- Knowledge of network security;
- Risk prevention management;
- Understanding of secure web communications…
- Security risk assessment;
- Understanding of system logic;
- Ability to write script or code.

Three professional competences were assessed by both groups to be poor:

- Knowledge of vulnerabilities and exploits of system;
- Knowledge of mobile and IoT security;
- Knowledge of cloud computing security.

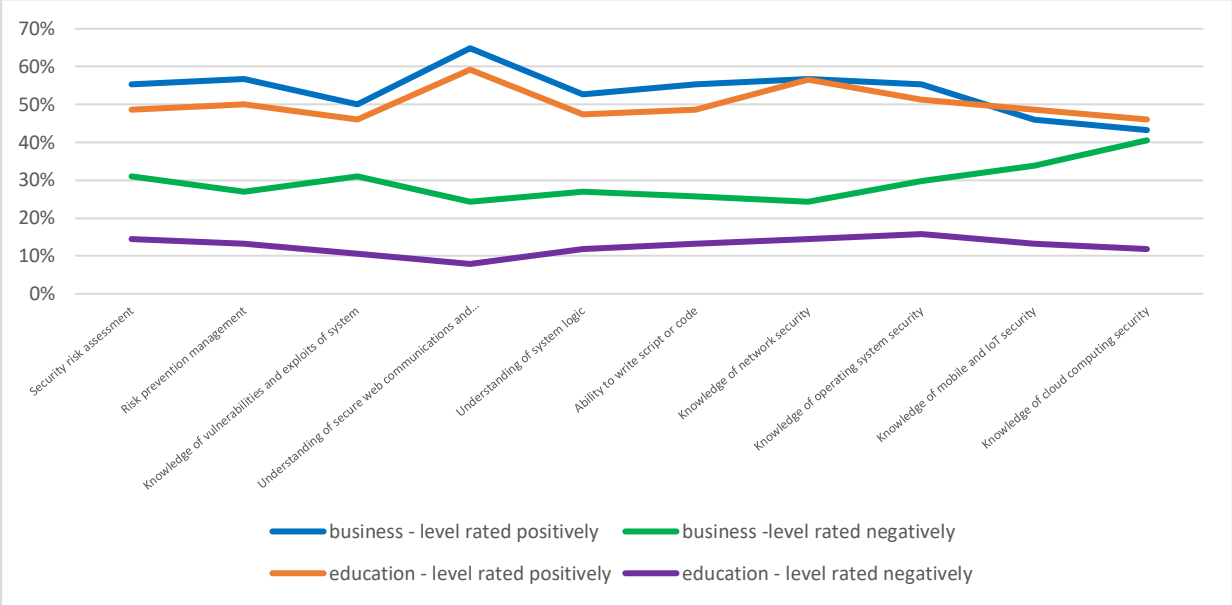


Figure 16: Comparison of responses between the industry-business and education groups on graduates' level of professional competences

Training to respond to current and emerging needs

The overwhelming majority of suggestions (52) and good practices (24) put forward by respondents described **Training** as the most effective solution. Different forms of training

[16] You can also consult figures 8 and 11

were mentioned ranging from online and hybrid to blended learning and offline sessions. Respondents cited courses, development programmes, workshops, meetings, seminars, projects, lectures, mentoring, news update, and experience exchange. Both offline and online modes were regarded as necessary. The most popular training methods appear to be problem-based, collaborative and peer-to-peer learning as opposed to fully instructor-led training. Both long-term customised development programmes and short-term events were regarded as necessary, as well as MOOCs, demos, lectures and presentations. Respondents frequently mentioned the need for in-house courses tailored to the needs of a particular organizations, though the role of external training was appreciated, especially when offered by renowned centres and organizations dealing with the issues of cybersecurity.

Some organisations offer training on a **regular** basis, while others propose it **ad-hoc**, and/or to newly recruited staff. Some prefer to implement **internal** training programmes, for example, conducted by an experienced employer to other staff members. Others prefer to respond to internal training needs by sending employees to the **external** events, or even encourage team leaders to select the courses which financed from the company's education budget. **Certification** and **Internships** were both mentioned, with examples given of internal certification based on the company's cybersecurity policy, and external certification offered by renowned organizations.

Successful training was described as being:

- Based on needs assessment;
- offering rapidly applicable and workable solutions;
- increasing motivation and awareness of employees;
- offering ready access to resources and tools that assist in developing necessary competences.

Other examples of good practice related to the personal development of staff included:

- Project work and learning by doing;
- In-company awareness raising;
- Mentoring;
- Peer reviewing and peer learning;
- Extensive documentation;
- Implementation of ISO 27001 and 22301;
- Recruitment processes including social engineering to hire highly motivated candidates;
- Security organization policy and Manual for personnel;
- Performance assessment discussions;
- Collaboration with universities;
- Exchanges between business units;
- Outsourcing.

There was also a common understanding expressed on the need for more budget to be allocated to the professional development of employees, though there was also a concern that well-trained professionals would leave their organizations to seek better opportunities.

Better coordination between education and industry

A second, very important success factor expressed by more than a half of respondents was **coordination and collaboration between education and industry**. Cybersecurity is considered to be an important topic at all levels of education, and requires updated information from industry to build the capacity of all citizens, not only those whose professional path would be closely connected with cybersecurity. A second clear expectation voiced was that the education cursus should be less theoretical and more connected with everyday challenges. Education should prepare learners to solve problems rather than memorise facts. "That would be a way to get graduates to do things better and be more ready for the industry", one respondent stated.

Comments from respondents related to education often touched on aspects such as:

- Establishing close cooperation and ongoing dialogue between training institutions and employers to provide trainers with updated information on the current needs of practice;
- Incorporating cybersecurity content in primary, secondary, tertiary and postgraduate education courses;
- Implementing updated course curricula that are in line with the current industry/ business needs;
- Earlier engagement of students with industry and business;
- Provision of opportunities for students to shadow professionals in the course of their studies.

The following suggestions were each expressed by at least 3 respondents:

- Closer cooperation between the industry-business sector and cybersecurity experts and organizations;
- Cybersecurity providers could offer free or affordable collaboration with CSOs;
- Increased attention of states to the issue of cybersecurity and relevant revision of legislation;
- Better promotion of cybersecurity careers among young people;
- Promotion of research and knowledge development in the sphere of cybersecurity;
- Knowledge-sharing facility set up between cybersecurity providers to avoid different companies focusing efforts where solutions already exist.

Further comments underlined the importance of encouraging more women to follow study paths in STEM (science, technology, engineering, mathematics), all rapidly growing economic sectors where diversity is necessary.

Closing the gap, from the perspective of the education sector

Thirty-four respondents from the education sector shared their suggestion on how the gap between the competence level of graduates and the expectations of industry can be bridged. Similar to suggestions made by respondents from the industry-business group, the most common proposal was to **establish close collaboration between education and the industry-business sector**, mainly in order to:

- Better understand the needs of employers;
- Adjust mutual expectations;
- Include cybersecurity issues into subject area curricula;
- Modernise methods of teaching and learning;
- Bring technology experts from the field to hold seminars on security;
- Organize internships, field visits, workshops, seminars, traineeships and student employment, mentoring programmes etc.

Respondents consider that pre-service training should include more:

- Specific cybersecurity modules (e.g. cloud security), on-demand;
- Cybersecurity case studies that can be integrated into broader courses;
- Practical skills development;
- Field work;
- More focus soft skills;
- Awareness raising about the importance of cybersecurity;
- Regular information updates;
- More possibilities to put theory into practice;
- Use of virtual multimedia opportunities.

Some respondents consider that all of the above-mentioned changes should be implemented at all levels of education, from primary and secondary through to tertiary. Several academics evoked the importance of factors such as:

- In-service teacher training at the primary and secondary levels;
- Relevant changes in educational legislation and standards;
- Broader support for information and communication changes in education systems;
- More attention paid to digital inclusion;
- Bridging gender equality and socio-economic equality gaps;
- Certification issues;
- Monitoring and evaluation of tasks in the education sector.

Difficult jobs to fill, and the impact on organizations

One of the supplementary questions to the industry-business group asked about the types of cybersecurity jobs proving the most difficult to fill. Based on findings from the interviews with leaders in the cybersecurity sector, four categories of jobs were proposed (see Figure 17). Seventy-five industry-business respondents pointed to cybersecurity managers being the most difficult role to fill, 74 respondents indicated information security architects, and 58 penetration testers. The role of network engineers appeared difficult to fill for 36 respondents.

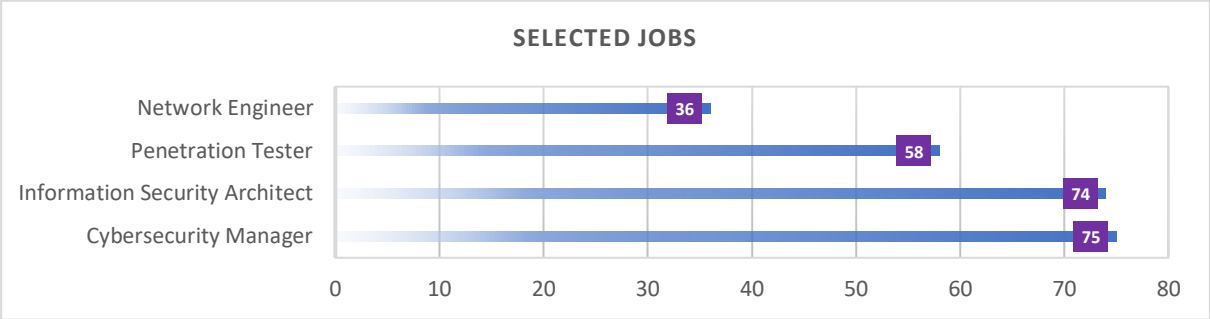


Figure 17: Industry-business perspective on jobs the most difficult to fill

This question allowed respondents to add to the list. Five job types were mentioned several times:

- Security cloud specialist
- Cloud backend engineer
- Machine-learning expert
- Digital forensics analyst
- Web3 engineer

According to the majority of respondents, this lack of specialists has a *strong* (45%) or *very strong* (24%) impact on their organization; 15% consider this has *no impact* or *low impact*, and another 16% find it difficult to estimate (see Figure 18).

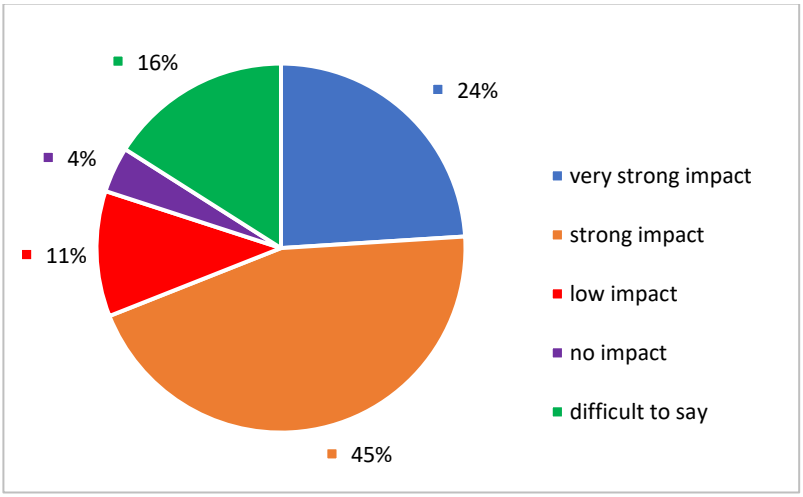


Figure 18: Impact of recruitment difficulties on the organisation

5. Conclusions and recommendations

Recommendations

Results from the study indicate that, at the global level, industry-business and education sectors broadly agree on the gap that exists between the needs and expectations of the cybersecurity industry and the level of transversal and professional competences that graduates bring to the workplace. The study also validates the proposed model of necessary transversal and professional competences to fill the gap, and this will now be slightly extended to include suggestions from the study.

Seven recommendations emerge from research, and these will be transposed into a plan of action for working group 2 of the IS3C in 2023:

1. **Improve education and training:** participants in the study almost unanimously agree that more, better competence development is the antidote to many of the challenges the cybersecurity sector is facing. They suggest moving away from the traditional face-to-face, online and hybrid training formats in favour of peer-learning and reviewing, mentoring, project work, design thinking, learning by doing, and formative assessment to meet society's rapidly evolving cybersecurity needs. Special focus should be given to developing more training and certification opportunities in countries such as Nepal, Vietnam, Samoa, and various regions in Africa where both interviewers and interviewees highlight the many career openings for certified cybersecurity experts going unfilled.
2. **Back to basics**: the creative capacity of young people entering the workforce in technology-related fields is, according to many research participants, being undermined by a lack of knowledge and interest on how things work. They imply that young people have become users and consumers rather than builders with only a superficial understanding of digital technology, a concern raised by several recent studies.[17] A deeper understanding of how things such as the internet backbone, cloud technology and blockchain work would trigger more innovation and encourage lateral thinking.

   Encouraging children to think about how the things they use in our everyday life function should be an integral part of primary and secondary school education, according to respondents. It helps develop critical thinking, and better understand issues commonly encountered online, such image and information manipulation and social-engineering strategies. A back-to-basics approach information search, too, would help people understand that search engines are counter-productive when looking for latest information or new ideas, since data is ranked by the number of times a document has been consulted meaning that usually older information comes out on top.
3. **Raise awareness of the importance of cybersecurity at all levels of education**: cybersecurity is a personal responsibility, just like health and well-being. IoT objects and wearable digital gadgets are an everyday aspect of most lives nowadays, and people should be made aware that protecting the security of their devices and being cognizant of their

[17] OECD (2019). *PISA 2021 creative thinking framework*. At https://www.oecd.org/pisa/publications/PISA-2021-creative-thinking-framework.pdf, and UNESCO (2022). *Re/shaping Policies for Creativity – Addressing culture as a global public good*. At https://www.unesco.org/reports/reshaping-creativity/2022/en

rights and responsibilities in the online environment is part and parcel of ensuring their cybersecurity. These concepts need to be embedded throughout education curricula if the internet is to become a place of trust. Making cybersecurity a fun part of school education could inspire more interest in it as a career, and would provide a solid grounding to overcome the superficiality of knowledge that has been critiqued in the point above. Society as a whole needs to understand the importance of security-related internet standards and ICT best practices for their own welfare and for the greater good. Safer and more secure online practices would lighten the demand on the cybersecurity sector by and perhaps also build more interest in cybersecurity careers.

4. **Improve collaboration between industry and education** to ensure that education keeps pace with emerging technological trends, has more access to up-to-date tools and resources, and a deeper understanding of the competence requirements for 21st-century citizens. Findings from the survey suggest that the education sector places less importance on transversal competences and, to a larger extent, on professional competences, than industry (see Fig. 13), though both gave similar opinions when asked about the level of graduates (see Fig. 12). Although the mission of education is far broader than catering to the needs of industry, closer collaboration could be to the advantage of both partners.

   To enable young people to develop their full learning potential and their future, they need to use and understand the digital technology they use on a daily basis, and educators need a solid understanding of today's information and communication tools and platforms. Respondents suggest that a closer collaboration with industry could also facilitate tool- and resource-sharing, and in the process open authentic opportunities for educational establishments to teach young people how to protect their privacy and data. The Danish CyberHub[18] was cited during one of the research interviews as being a durable model of collaboration between education and industry sectors.

5. **Boost diversity:** the under-representation of young people and women in the research reflects a general lack of diversity across the cybersecurity teams.[19] Yet diversity, according to recent business research, unlocks innovation by creating an environment where "outside the box" ideas are heard.[20] It helps teams make better decisions because it multiplies perspectives and ways of looking at issues and threats, and can avoid oversights when security measures are being put into place. Facial recognition ia a typical example.[21] Several years of judicial errors could have been avoided if early software versions had taken into account other skin and facial types than those of the mainly white male engineers. In a fast-evolving field such as cybersecurity, creativity, innovativeness, and a multi-facetted approach are essential to stay ahead of hackers and threats.

6. **Upgrade recruitment procedures**: careers in cybersecurity would be more appealing to young people and especially girls if they were able to discover during their early and teen years the exciting challenges, opportunities and flexibility the field offers. Online games, simulations and educational activities developed through industry-education partnerships could offer a solution. At the hiring stage, algorithmic biases discriminate against

[18] https://cyberhub.dk/danish-cyberstartups-overview/danish-cyberstartups/
[19] https://www.isc2.org/-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx
[20] Harvard Business Review at https://hbr.org/2013/12/how-diversity-can-drive-innovation
[21] https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html

populations not already interested or working in the sector, eliminating access of minority groups to certain employment opportunities. Poor knowledge sharing between education and cybersecurity sectors, tertiary and vocational education are also limiting a forward looking approach in adapting education and training towards the professional profiles in most demand. Finally, recruitment procedures are, according to several interviewees, time-consuming and often poorly adapted to hiring highly technical employees, though the use of social engineering strategies can overcome the latter issue.

7. **Scale up knowledge-sharing and good practice**: interesting good practices have been highlighted by both industry and education representatives in the study, and are rarely scaled up due to a lack of suitable mechanisms for this. An international good practice observatory has been suggested, built with the improved cross-sector collaboration that is proposed above. Effective knowledge management and sharing strategies, i.e. getting the right information to the right people in time, could provide a solution to many of the issues discussed throughout the study by upgrading recruitment, training and awareness raising processes.

The way forward

The fact that both the industry-business and education sectors worldwide recognize the existence of the competence gap and express similar opinions about the core competences is a positive step. Furthermore, both sectors appear to express the need for similar solutions to the problem, and tend to propose complementary ways to reach these solutions. Whereas respondents from industry-business showed more interest in training, respondents from the field of education favoured collaboration and experience exchange with industry, in order to be able to build realistic forward-looking learning programmes. Respondents from both groups were keen to describe the good practices they have implemented or encountered, which could facilitate the next steps towards achieving the goals.

The IS3C coalition could play an important role to play in bridging the competence gap by:

- Setting up a hub that could act as observatory of good practices and ensure ongoing dialogue;
- Raising awareness in industry and business sectors about the advantages of establishing closer cooperation with education sectors for the exchange of information, knowledge and solutions on cybersecurity, in order to support the development better adapted teaching programmes;
- Capacity building to promote knowledge-sharing across sectors, for example through train-the-trainer programmes;
- Encouraging and supporting the participation of the under-30 age group and women in capacity building programmes developed with representatives of industry and business;
- Supporting the revision and update of education curricula and the development of targeted teaching and learning resources (for example, education packs with theoretical and methodological content for training professionals).

Appendices

Appendix I - Interview questionnaire and table of interviews

Twenty-eight interviews were conducted in 16 countries worldwide. Five questions were developed, piloted and shaped in these initial interviews and discussions, to guide the conversation which lasted on average one hour:

1. What are the main cybersecurity competences your company looks for when hiring?
2. What are the main cybersecurity competence gaps you find between what your company looks for and what new graduates possess from university training?
3. How serious is this issue for your organisation?
4. Which cybersecurity professional profiles do you have most trouble filling?
5. Have you in some way been involved in addressing these gaps with either ministries of education or educational facilities and if so, what is your experience?

1	Brazil	Brazil	Sociedade Brasileira de Computação
2	Brazil	Brazil	Petrobas
3	Indonesia	Indonesia	Linknet
4	Indonesia	Indonesia	Xynesis International
5	Ghana	Ghana	Seltech Ghana
6	Ghana	Ghana	CyberGhana
7	Luxembourg	Netherlands	Ministry of Health, Wellbeing & Sport
8	Luxembourg	Denmark	KPMG
9	Luxembourg	Belgium	Cybersecurity consultant to EU
10	Luxembourg	Poland	University of Lodz, Poland
11	Luxembourg	Luxembourg	Ministry of Economy
12	Luxembourg	Morocco	National R&I Centre (CMRPI), Kenitra University
13	Luxembourg	Italy	Information Security consultant
14	Nepal	Nepal	InfoDevelopers Pvt. Ltd
15	Nepal	Nepal	Centre for Cyber Security Research and Innovation
16	Nepal	Nepal	Vairav Technology Security Pvt Ltd.
17	Poland	USA	Microsoft
18	Poland	Poland	NASK
19	Samoa	Samoa	Ministry of Communication, Info Tech (MCIT)
20	Samoa	Samoa	Office of the Regulator
21	Sri Lanka	Sri Lanka	Techone Global
22	Sri Lanka	Sri Lanka	DFCC Bank
23	Sudan	Sudan	SudanCERT
24	Sudan	Sudan	National Information Center - Sudan
25	Vietnam	Vietnam	TMG Solutions
26	Vietnam	Vietnam	Polaris Infosec
27	Vietnam	Vietnam	Bosch Global Software Technologies Co Ltd
28	Vietnam	Vietnam	RMIT University

Appendix II - Questionnaire for business representatives

SECTION 1

The purpose of this survey

The IS3C is an Internet Governance Forum Dynamic Coalition comprising stakeholders from business and education sectors as well as civil, government, regulatory and corporate communities with a specific interest in digital competences. It encourages the application of standards that will make internet services and networks safer, more secure and trustworthy.

The present survey will contribute to understanding and bridging gaps between the competences cybersecurity/ IT graduates have and the requirements of industry or business.

It will take you 15 to 20 minutes to complete the survey. In compliance with the GDPR, no personal information or IP address will be recorded or collected.

SECTION 2 [22]

About you

(optional - open text)

Age *

○ Under 18 ○ 18-30 ○ 31-45 ○ 46-65 ○ Over 65

Gender *

○ Male ○ Female ○ Prefer not to say

Country *

(drop-down menu "countries")

Professional sector *

○ Business/industry ○ Tertiary education ○ School education ○ Other (please indicate)

SECTION 3

Business / industry and other

(open text for description)

1(a) Please rate the importance you would accord in the workplace to the transversal competences below *

Scale: not important, low importance, moderately important, very important, difficult to say

- critical thinking
- ethical thinking
- strategic thinking
- holistic thinking
- creativity

[22] The questions marked with an asterisk * were mandatory, all others were optional

- problem solving
- teamwork
- interdisciplinary thinking
- business knowledge
- lifelong learning
- oral communication skills
- written communication skills
- handling complexity
- open mindedness

1(b) Please rate the importance you would accord in the workplace to the professional competences below *

Scale: not important, low importance, moderately important, very important, difficult to say

- security risk assessment
- risk prevention management
- knowledge of vulnerabilities and exploits of systems
- understanding of secure web communications and technologies
- understanding of system logic
- ability to write script or code
- knowledge of network security
- knowledge of operating systems security
- knowledge of mobile and IoT security
- knowledge of cloud computing security

1(c) Please indicate here any other transversal or professional competences that do not appear on the list, and that you consider very important

(optional – open text)

2(a) Please assess the average level of competence of graduates in your establishment in the transversal competences below *

Scale: very low, low, moderate, good, difficult to say

- critical thinking
- ethical thinking
- strategic thinking
- holistic thinking
- creativity
- problem solving
- teamwork
- interdisciplinary thinking
- business knowledge
- lifelong learning
- oral communication skills

- written communication skills
- handling complexity
- open mindedness

2(b) Please assess the average level of professional competence of graduates in your establishment in the areas below *

Scale: very low, low, moderate, good, difficult to say

- security risk assessment
- risk prevention management
- knowledge of vulnerabilities and exploits of systems
- understanding of secure web communications and technologies
- understanding of system logic
- ability to write script or code
- knowledge of network security
- knowledge of operating systems security
- knowledge of mobile and IoT security
- knowledge of cloud computing security

SECTION 4

Your ideas and suggestions

(open text)

3. **Please share any examples of good practice your organization implements to bridge the gap between your expectations and employees' competences (if you know of such examples). (Transversal and/or professional competences)**

   (open text)

4. **In your professional sector, which jobs do you consider the most difficult to fill (choose as many as you wish and add more as applicable)**

   - Penetration Tester
   - Cybersecurity Manager
   - Network Engineer
   - Information Security Architect
   - Other

5. **To what extent does the difficulty to fill these jobs impact your organisation or your sector?**

   ○ no impact ○ low impact ○ strong impact ○ very strong impact ○ difficult to say

6. **What solutions can you suggest to bridge the gap between your expectations and the competences of employees?**

   (open text)

Appendix III - Questionnaire for representatives of education

SECTION 1

The purpose of this survey

The IS3C is an Internet Governance Forum Dynamic Coalition comprising stakeholders from business and education sectors as well as civil, government, regulatory and corporate communities with a specific interest in digital competences. It encourages the application of standards that will make internet services and networks safer, more secure and trustworthy.

The present survey will contribute to understanding and bridging gaps between the competences cybersecurity/ IT graduates have and the requirements of industry or business.

It will take you 15 to 20 minutes to complete the survey. In compliance with the GDPR, no personal information or IP address will be recorded or collected.

SECTION 2

About you

(open text)

Age *

○ Under 18 ○ 18-30 ○ 31-45 ○ 46-65 ○ Over 65

Gender *

○ Male ○ Female ○ Prefer not to say

Country *

(drop-down menu "countries")

Professional sector *

○ Business/industry ○ Tertiary education ○ School education ○ Other (please indicate)

SECTION 3

Education sectors

(open text for description)

1(a) What is the level of importance given in your educational establishment to the transversal competences below? *

Scale: not important, low importance, moderately important, very important, difficult to say

- critical thinking
- ethical thinking
- strategic thinking
- holistic thinking
- creativity
- problem solving
- teamwork

- interdisciplinary thinking
- business knowledge
- lifelong learning
- oral communication skills
- written communication skills
- handling complexity
- open mindedness

1(b) If applicable, what is the level of importance given in your educational establishment to the professional competences below?

Scale: not important, low importance, moderately important, very important, difficult to say

- security risk assessment
- risk prevention management
- knowledge of vulnerabilities and exploits of systems
- understanding of secure web communications and technologies
- understanding of system logic
- ability to write script or code
- knowledge of network security
- knowledge of operating systems security
- knowledge of mobile and IoT security
- knowledge of cloud computing security

1(c) Please indicate here any other transversal or professional competences that do not appear on the list, and that you consider very important.

(optional – open text)

2(a) Please assess the average level of transversal competences of graduates from your establishment in the areas below *

Scale: very poor, poor, good, very good, difficult to say

- critical thinking
- ethical thinking
- strategic thinking
- holistic thinking
- creativity
- problem solving
- teamwork
- interdisciplinary thinking
- business knowledge
- lifelong learning
- oral communication skills
- written communication skills
- handling complexity

- open mindedness

2(b) If applicable, please assess the average level of professional competence of graduates from your establishment in the areas below

Scale: very poor, poor, good, very good, difficult to say

- security risk assessment
- risk prevention management
- knowledge of vulnerabilities and exploits of systems
- understanding of secure web communications and technologies
- understanding of system logic
- ability to write script or code
- knowledge of network security
- knowledge of operating systems security
- knowledge of mobile and IoT security
- knowledge of cloud computing security

SECTION 4

3. What solutions can you suggest to bridge the gap between the competences of graduates from your establishment and the expectations of industry?

(open text)

Appendix IV – Model of 14 transversal and 10 professional competences

Transversal competences

1. critical thinking
2. ethical thinking
3. strategic thinking
4. holistic thinking
5. creativity
6. problem solving
7. teamwork
8. interdisciplinary thinking
9. business knowledge
10. lifelong learning
11. oral communication skills
12. written communication skills
13. handling complexity
14. open mindedness

Professional competences

1. security risk assessment
2. risk prevention management
3. knowledge of vulnerabilities and exploits of systems
4. understanding of secure web communications and technologies
5. understanding of system logic
6. ability to write script or code
7. knowledge of network security
8. knowledge of operating systems security
9. knowledge of mobile and IoT security
10. knowledge of cloud computing security

In 2021, the IS3C (a dynamic coalition within the IGF focusing on Internet Standards, Security and Safety) launched a study to better understand the skill shortage in the cybersecurity sector. After a series of interviews conducted with industry, business and tertiary education leaders in 14 countries, a short list of transversal and professional skills was defined as the base-line in a survey set up to seek the viewpoint of a broader population. 235 respondents from 65 countries worldwide completed the survey.

Only one in four respondents were women and more than 80% were aged above 30 years. This reflects the lack of diversity across the cybersecurity sector which, according to many interviewees and survey respondents, largely contributes to the skill shortage the sector is facing.

Critical thinking, problem solving, teamwork and creativity emerged as the top transversal competence requirements for both educators and business representatives. Interestingly, respondents from the education sector placed on average 10% less importance on transversal skills than those from industry. Estimates from both sectors indicate that one in three young people entering the workforce have not mastered the list of transversal competences put forward.

Competences such as risk prevention and security management, respondents say, are not only professional competences but are essential for all digital technology users. Some respondents point out that outcomes would considerably improve if education could encourage young people to think more about the functioning of the tools and platforms they use in their daily lives.

One of the 17 United Nations' sustainable development goals for achievement by 2030 is to provide access to justice for all and build effective, accountable and inclusive institutions at all levels (SDG16). Reliable, secure digital infrastructures are pivotal to maintaining robust, dynamic institutions, and inclusion is undermined wherever diversity is lacking. To ensure a sustainable future, education (SDG4) must be fit for purpose, building on the needs of the individual and taking into account the future needs of society. In this publication, the IS3C outlines seven key recommendations built on the ideas, suggestions and good practices gathered from industry, business and education practitioners during this year-long study.

INTERNET STANDARDS, SECURITY AND SAFETY COALITION (IS3C)
MAKING THE INTERNET MORE SECURE AND SAFER

insight
Educating to Empower

NASK

SIDNfonds

Published by Insight S.A.