Management Summary Research and advisory report Education and the Cybersecurity Labour Market

Platform Talent voor Technologie

dialogic
innovatie • interactie

In opdracht van Ministerie van Economische Zaken en Klimaat

Management Summary

> *'Our society is deeply dependent on the internet and other digital networks, services, and products. Developments in digitalization are progressing rapidly, offering many opportunities but also create challenges on various issues in the field of cyber resilience. Adequate cybersecurity is essential for organizations as part of sound business operations, just like maintaining control over their financial management; it is a fundamental factor that is omnipresent and necessary, otherwise, our safety and continuity are at risk, and our economy could stall.'*[1]

To ensure adequate cybersecurity in the Netherlands, the presence of sufficiently trained cybersecurity professionals is an essential requirement. The Ministry of Economic Affairs and Climate aims to gain a clear quantitative and qualitative understanding of the current shortages in the Dutch cybersecurity labour market, the expected growth, and the possibilities to better align education and the labour market (also described as an action in the Dutch Cybersecurity Strategy Action Plan 2022-2028).

Platform Talent voor Technologie (PTvT) and Dialogic have addressed nine research questions from September 2023 to February 2024, focusing on mapping demand and supply (labour market and educational opportunities). This has provided input for 12 recommendations, including implementation proposals, on which (policy) instruments can be deployed in the short and long term to strengthen the cybersecurity labour market. The results of this research are presented in two reports:

1. The research report on Education and the Cybersecurity Labour Market.
2. The accompanying advisory report.

This management summary contains the results of both reports: the current state of education and the labour market for cybersecurity professionals and twelve recommendations to better align the demand for cybersecurity professionals with the cybersecurity education supply (public as well as private).

Research report on education and the cybersecurity labour market

Various data collection methods were employed in this study to map out the labour market and educational opportunities. Through data analysis of various national sources, demand and supply were quantitatively depicted. This data was verified and qualitatively supplemented through questionnaires, interviews, and workshops conducted with members from the education sector and the labour market. Various parties involved in current cybersecurity human capital activities contributed to the qualitative data collection and interpretation of the results.

Education

Within the secondary vocational education (in dutch: mbo), the requirements for a student to obtain a mbo diploma are nationally defined in the relevant qualification files. The Minister of Education, Culture, and Science (in dutch: Ministerie van OCW) determines these qualification files. In the educational offerings, we see that in the mbo domain, there has been attention to cybersecurity in three current qualification files for the ICT domain in recent years (table 1). In the renewal of these qualification files (effective August 1, 2024), it is explicitly outlined what students should know and be able to do in the field of cybersecurity. Additionally, three mbo initiatives have been identified that are currently developing programs.

[1] https://www.cybersecurityraad.nl/documenten/brieven/2024/02/05/brief-aan-de-informateur

[2] Onderzoeksrapportage Onderwijs en Arbeidsmarkt cybersecurity, PTvT en Dialogic, 2024

Combination of ICT Programs	Number of mbo’s
ICT employee level 2 Software developer level 4 Allround employee ICT systems & devices (All-round IT Systems & Devices Employee) level 3 Expert IT systems & devices level 4	32
Software developer level 4 Employee IT systems & devices level 3 Expert IT systems & devices level 4	5
Software developer level 4 Allround employee IT systems & devices level 3	1
Software developer level 4	2

Table 1: Offer of mbo ICT programs

The substantive focus of the mbo (secondary vocational education) programs mainly lie on technical factors and, to some extent, on management and organizational approaches. Due to the variation in how the ICT programs shape their education, it has not been possible to precisely determine the extent of cybersecurity within the curriculum. Enquiries with program managers reveal that at some mbo institutions, cybersecurity is a standard component of the ICT program, while others rely more on the options provided by elective modules. The total number of students in these programs remains approximately the same, around 23,000 students per year respectively. Over the past few years, an average of 6,000 certified ICT students have graduated annually.

The program directors identify the following four challenges: [1] the need to update teachers, [2] limited student intake, [3] inadequate facilities, and [4] the rapid emergence of new developments, such as AI. Apart from ICT programs, there is hardly any, and often no, attention to cybersecurity in the rest of the mbo programs. Initial steps, such as pilots, are being taken, for example, within security guard training curricula.

At the higher education level (hbo and wo - universities), within the NVAO-accredited programs, the following number of programs exist (see Table 2). The upcoming cybersecurity programs are still in the development phase, accreditation phase, or initiation phase.

Full Cybersecurity Studies	Number
Hbo	5
Wo	5
Total	**10**
Specialization/Elective Track in Cybersecurity within Programs	**Number**
Hbo	18
Wo	11
Total	**29**
Compulsory Component in Cybersecurity > 6 ECTS in Programs	**Number**
Hbo	6
Wo	7
Total	**13**
Upcoming Cybersecurity Programs	**Number**
Hbo	8
Wo	1
Total	**9**

Table 2: Overview of the numbers of relevant programs in the field of cybersecurity at hbo and wo levels

Over the past three years, the influx of students with a relevant cybersecurity component to their education has remained fairly stable, being around 3,000 students annually. The number of graduating students has been increasing annually, especially in programs fully dedicated to cybersecurity, or among students who have chosen a specialization/elective track in cybersecurity within their studies.

Across the spectrum of programs, both at hbo and wo levels, there seems to be more commonly a multidisciplinary approach. However, there is little to no emphasis on competence development in education across all studies (mbo and higher education), which would enable students to develop didactic knowledge and skills.

Interviews and questionnaires with teachers, professors, and management highlight various challenges, including: [1] Shortage of teachers with sufficient knowledge. [2] The content of the curriculum, which needs to offer both a broad profile and specialized profiling within the cyber domain. [3] The rapid pace of development in the cybersecurity world combined with the lack of flexibility to respond. [4] The perception of cybersecurity education as a technical field, affecting student recruitment and expectation management. [5] Lack of resources for education materials, hybrid learning spaces, etc.

Within the Lifelong Learning (LLL) options, there appears to be an extensive non-funded educational offering[3], with approximately 20% focused on the most 'in-demand' cybersecurity certificates in the job market. While there are many providers, one provider stands out with a notedly extensive portfolio of offerings. Education is available in various formats, with hybrid forms becoming more common. There are also numerous regional activities and offerings for SMEs and citizens, although the reach and impact are challenging to assess.

Private educators indicate that individuals in cybersecurity upskilling, reskilling, and lifelong learning face various obstacles, such as insufficient time allocated by employers and lack of access to funding for education and training purposes.

Labour Market

The demand of the labour market has been assessed by analysing current job vacancies. It's acknowledged that not all demand will be captured through this method, as some positions may be filled without being advertised.
The vacancy analysis reveals a growing demand for cybersecurity expertise in the job market, from approximately 8,000 in 2018 to around 19,000 in 2022, both for specialized cybersecurity profiles (Cybersecurity (CS) High) and broader job profiles where cybersecurity is a component (CS Low).

[3] Non-funded education is not subsidized by the Ministries of Education, Culture, and Science (OCW) and Economic Affairs (EZK).

Number of vacancies requesting cybersecurity expertise

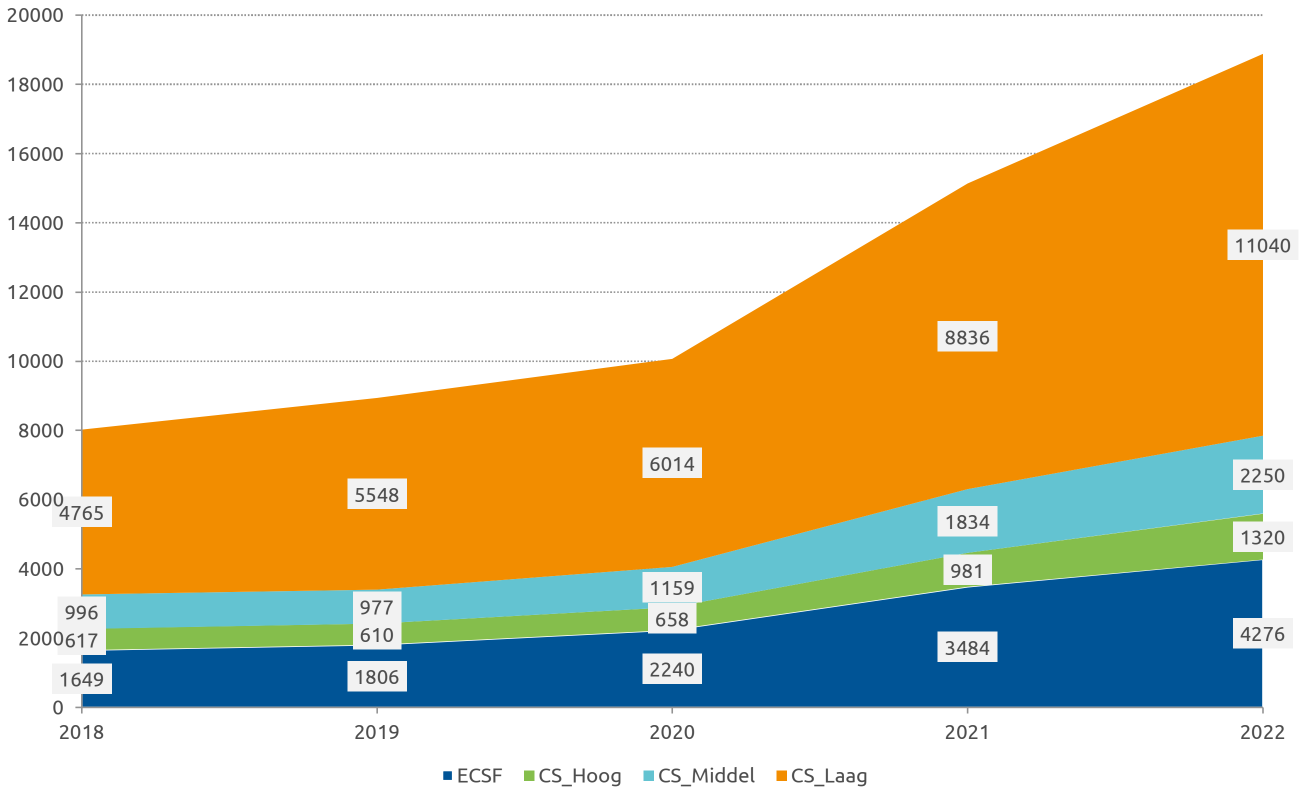

Figure 1: Number of Vacancies Requesting Cybersecurity Expertise. Source: Jobdigger, modified by Dialogic

This demand varies by province and has a focus on mid-level and senior positions requiring hbo or wo-level education. The majority of demand for cybersecurity expertise comes from the government and the IT sector, with most cyber vacancies being at organizations such as the Police, PWC, CGI, EY, Tax Authorities, ING, ABN AMRO, Capgemini, KPMG, and the Ministry of Defense. Organizations that deal more extensively with cybersecurity also have a higher demand for specialized profiles.

The population of cybersecurity professionals is relatively young, with two-thirds being male and one-third female. Employees with immigration or labour migration backgrounds appear to be significant in the sector: approximately 5-10% of new entrants are attributed to foreign workers coming to work in the Netherlands. In 2021, there was an outflow of almost 25% of the population, with ~2% of the outflow retiring and another ~2% emigrating.

Across the board, considerable technical knowledge is required to operate within cybersecurity, but the required skills and tasks are largely non-technical. Vacancies referring to the European Cybersecurity Skills Framework (ECSF) profiles emphasize the technical component more than other types of cybersecurity profiles. While the demand for cybersecurity expertise and underlying skills is growing significantly in absolute terms, the relative ratio between different types of knowledge and skills remains stable.

Explicit requests for a cybersecurity certificate are found in 15% of vacancies. The most requested certificates are CISSP, CISM, and CISA[4]. Specialist cybersecurity profiles often require a certificate; for example, 77% of Chief Information Security Officer (CISO) vacancies request a certificate. For Penetration Testers, who test computer systems and apps for security vulnerabilities, this is the case in 58% of vacancies.

Future Developments

The introduction of the Network and Information Security Directive (NIS2), the Cyber Resilience Act (CRA), and further developments in AI will significantly impact the cybersecurity job market. NIS2 is expected to increase demand for cybersecurity professionals across various ECSF profiles, from Chief Information Security Officers (CISO) to Implementers, Analysts, Auditors, and Pentesters. The CRA is expected to broaden the demand for cybersecurity professionals, likely with the most significant impact on cyber integrators. The continued development and use of AI will reduce the demand

[4] Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), Certified Information Systems Auditor (CISA)

for certain tasks performed by humans, but will also create new tasks requiring new competencies. ECSF profiles such as Penetration Tester, Cyber Threat Intelligence Specialist, and Digital Forensics Investigator are most likely to see significant AI involvement. Organizations where cybersecurity plays a relatively minor role and which are not subject to NIS2 and/or CRA are likely to continue opting for 'hybrid' roles combined with external hiring/purchasing/organization of cybersecurity expertise.

Alignment between Education and the Labour Market

The notion that education and all concrete job vacancies in the labour market could perfectly match is a misconception. This is because learning must take place over several years and in different contexts (work environment, training, etc.). Therefore, this research looked at the demand in the labour market for junior positions and the alignment of those positions with educational programs. In higher education, we see a relatively insufficient number of hbo and wo graduates with a specialized cybersecurity profile compared to the demand in the labour market. However, the number of hbo/wo graduates who have had a 'substantial' component of cybersecurity in their education is in line with the demand. Similarly, the quantitative demand for mbo cybersecurity junior personnel matches the outflow from the two relevant mbo-4 programs. Thus, there is a sufficiently large pool of new employees, but it cannot be definitively stated whether this pool is adequate. It is highly likely that there is more competition for these positions, leading to a shortage in the cybersecurity job market.

In terms of content, the labour market demands competencies of the 'Technical' and 'Management & Organization' types. These components are also evident in programs with a specialization in cybersecurity. The focus on 'Legal' competencies is particularly noticeable in programs where cybersecurity is not a specialization. However, competencies in 'Education' (e.g., teaching) are nowhere to be found, neither in the programs nor in junior-level job vacancies.

A significant challenge for the cybersecurity job market seems to lie in Lifelong Learning, both in terms of attracting and retaining (current) cybersecurity professionals. This requires consideration of the difference between the role someone is coming from and the role they need to enter. These differences can not be too great; there must be a 'bridgeable step.' It is crucial to carefully assess which set of acquired skills and knowledge forms a sufficient basis to bridge the gap. Certifications play a significant role in the cybersecurity job market, especially for more specialized cybersecurity profiles. These certifications and associated training programs serve as a means to bridge the gap between the aforementioned differences.

Additionally, addressing the challenges mentioned above in regular education is essential; doing so will improve the quantitative and qualitative intake of regular programs and will better align them with the demands of the labour market.

Advisory report

The cybersecurity job market is characterized by a multitude of profiles requiring various cybersecurity expertise. It is a multidisciplinary field where technical knowledge and skills, as well as legal, management, and organizational competencies, are needed. Future developments such as the Network and Information Security Directive (NIS2), Cyber Resilience Act (CRA), and the development and deployment of AI will lead to greater and more varied demands for expertise in the cybersecurity job market in the coming years.

At the same time, within cybersecurity education, there is a large number of programs with their own specific focus. Given the broad diversity of cybersecurity expertise, the variety of target audiences, and rapid changes, coordinated efforts from multiple parties are required to comprehensively meet the demands of the cybersecurity job market.

From Research to Recommendations

The entire system of education and employment is vast and diverse. As described in the research report, the job market involves various types of expertise, a large number of different types of organizations, and numerous job profiles where cybersecurity expertise is relevant. In education, there are different types of institutions (primary, secondary, vocational, higher, university, lifelong learning) and a wide variety of programs focusing either entirely or partially on cybersecurity. Individuals navigating through the education and employment system notedly possess their own motivations, contexts, and dynamics. All involved parties and their interactions form the entire system of education and employment. Each experiences their own challenges and bottlenecks.

While this advisory report presents the need for an adequate number of cybersecurity professionals as ‘one challenge’, we want to emphasize that in reality, it comprises a collection of numerous smaller sub-problems spread across the entire education and employment chain. Therefore, there will be no one-size-fits-all solution to address all the sub-problems in the entire chain. The notion that one or a few efforts or initiatives can solve the entire issue is, in our view, unrealistic.

In this advisory report, a deliberate choice has been made to formulate twelve recommendations regarding what should be done, supplemented with concrete examples of how these recommendations could be implemented. We consciously chose not to specify in detail who should do what for two important reasons:

1. **Practical feasibility:**
   Numerous efforts are required at various points in the education-employment chain, and detailing all these efforts at a micro level is practically unfeasible. Conversely, it is pointless to mention only one or a few recommendations as it oversimplifies the issue. Therefore, the recommendations are formulated at an aggregate level that is concrete enough but not overly detailed. The recommendations are further elaborated in this advisory report (Chapters 3 to 5) and supplemented with concrete example initiatives from practice (Appendices 5 to 8).

2. **Consensus:**
   The recommendations need to be operationalized by the involved parties. Depending on certain values, beliefs, and starting points, different stakeholders will want to approach the recommendations differently. Throughout this process, substantive and procedural choices need to be made, which, in our opinion, should be made by the involved parties themselves. This will enhance ownership and consensus among the relevant parties.

Recommendations

Seven key points in the entire education-employment chain were identified in the research report, on which the recommendations should focus. During a meeting on January 17 with over 40 stakeholders (from education, business, relevant ministries, and the Human Capital ecosystem), these seven points were discussed to gather advice, actions, and tools. Supplemented with activities from international Human Capital cybersecurity policies, the input was then tested, refined, and categorized. This has led to the following twelve recommendations, divided into recommendations for the **entire ecosystem (1-4)**, **the job market (5-8)**, and **education (9-12)**.

#	Recommendations	Explanation
1	Develop a shared language and common understanding of 'Cybersecurity Expertise'	It is essential to have a clear, shared understanding of what 'demand' and 'supply' actually mean. Without a common language, there is a high risk of discussing different facets of cybersecurity expertise, making coordinated action difficult. A shared language can strengthen the collective understanding of the state of 'demand' and 'supply'. This includes working on a shared information position regarding data collection (e.g., CBS surveys), data processing (e.g., shared and supported job classifications), and data accessibility (e.g., through a joint dashboard).
2	Implement targeted coordination on education- employment alignment	Cybersecurity professionals and expertise encompass a wide variety of job types, expertise, and educational backgrounds. The scope is so broad that no single party can meet the required expertise alone. Coordinated action is needed to align the market demand and educational supply across the entire spectrum of cybersecurity, covering the full demand without unnecessary duplication of efforts.
3	Address the full potential talent pool	Given the increasing demand for talent, it is important to utilize as much potential talent as possible. This means focusing more on diversity and inclusion in general. Specifically, efforts can be made to attract underrepresented gender groups and explore how to better utilize existing cybersecurity talent with a vocational education background for the sector.
4	Seek collabouration between and within regions, sectors, and chains	Regions differ in terms of demand and supply of cybersecurity professionals. Within regions, it is important to consider the regional context and connect demand and supply effectively. Within sectors and value chains, collaboration is also beneficial, as sectors often have a sector-specific knowledge base for cybersecurity professionals. Additionally, cross-sector and value chain collaboration can be pursued, for instance, to enhance the cybersecurity of SMEs in complex value chains.
5	Increase the visibility and appeal of the profession	Employers in cybersecurity can adjust the perception of the profession and its professionals. The attractiveness can be enhanced by highlighting the wide variety of roles and expertise (not just technical), the broad scope of the field, and the importance of working in this sector.
6	Promote reskilling, upskilling, and lifelong learning for horizontal and vertical development	To encourage cybersecurity professionals to further professionally develop themselves, employer demand needs to be stimulated. Development pathways offer career prospects, helping professionals understand the possibilities and relevant offerings. Collaboration between education providers (both public and private) and employers should ensure a current and varied offering that encourages all employees to continue developing. These pathways can also facilitate horizontal development, making a career transition to cybersecurity more appealing.
7	Enhance professional retention through sectoral mobility	Regional and local collaboration between employers can create attractive conditions to retain cybersecurity professionals within the sector. For example, by jointly creating one job that offers opportunities to explore various employers within the network and collectively seeking the right match.
8	Improve the starting position of recent graduates	By facilitating the transition from education to the business world and intentionally focusing on the training and development of new employees, employers can bring junior professionals to the desired level more quickly. This increases the likelihood of retaining junior professionals in the cybersecurity sector, allowing them to undertake intermediate level tasks sooner.

9	Increase interest in studying and working in cybersecurity	Developing interest in a specific field begins at a young age. In primary and secondary education, more attention can be given to digital technology and skills in general, and cybersecurity specifically. The perception of these subjects and the study and work in the field is a crucial factor in the choice of study and career. Educational institutions can present cybersecurity more clearly and attractively within various follow-up programs in vocational and higher education, not only in specialized cybersecurity programs but also in legally or economically oriented programs relevant to cybersecurity.
10	Strengthen the frameworks and materials for cybersecurity education	To better integrate cybersecurity into the entire education chain, good frameworks and materials are necessary. There is a need for more detailed core objectives and continuous learning paths/curricula and educational materials starting from foundational education. In vocational education, ICT programs' qualification dossiers specify what students should know and be able to do at the end of their training, with increasing attention to cybersecurity. For higher education, joint content and curricula can be developed for both cybersecurity-specialized and related programs. In higher vocational education, cybersecurity could be made mandatory within ICT programs. For university education, a pool of professors could be established to ensure comprehensive educational offerings.
11	Involve the job market more closely in education	The cybersecurity job market changes rapidly. For education, it is important to stay well-connected with the job market to understand current demands. The job market can also play a significant role in providing the expertise needed to adequately train students. Together with the job market, work can be done on current skills for students, addressing teacher shortages, creating context-rich learning environments, flexible education, and joint promotion of the field.
12	Enhance and increase the attractiveness of teaching in cybersecurity	Teaching in cybersecurity must be made attractive for both current and prospective teachers. Existing cybersecurity teachers should be retained and optimally utilized. Hybrid roles, combining teaching with employment in businesses, can help. Additionally, investments in professional development for teachers to keep their cybersecurity knowledge up to date should be encouraged. Making this more accessible through financial support for ICT teachers, internships at companies, and national masterclasses is beneficial. Given the shortage of teachers, reskilling to become a cybersecurity teacher should be made more accessible, with programs like Make IT Work offering attractive reskilling opportunities to IT and cybersecurity with job guarantees and minimal costs for participants.

Follow-up on recommendations

In the realm of Human Capital in cybersecurity, there are numerous diverse initiatives. However, based on the observation of many discussions, it appears that these initiatives lack inter connection and coordination, resulting in insufficient impact. To prevent policy coordination failures, it is crucial to designate a clear entity (e.g., one of the involved Ministries) with sufficient mandate, position, and resources to be responsible for coordinating and following up on these recommendations. A coordination group, comprising representatives from the national government, education sector, and business community, can oversee all recommendations and ensure coherence.

Each involved Ministry can then determine which recommendations are suitable for incorporation into the current infrastructure, programs, and regulations. The recommendations within the areas of education, labour market, and ecosystem can then be best discussed in heterogeneous working groups that include representatives from the national government (including the coordinating Ministry), education, business community, and other relevant parties. Within these working groups, the recommendations will be discussed, and further approaches will be determined. A good connection between national, regional, and local approaches is essential.

The above recommendations specifically apply to the cybersecurity job market. When following up on the recommendations and further implementation, it is important to consider the efforts being undertaken by various sectors, the overall shortages on the labour market tightness, and the specific ICT-broad area. The risk of policy competition is high in these times of scarce human capital: various sectors are competing targeting.

When multiple domains make uncoordinated efforts to attract the same individuals, it results in significant costs and little to no net gain for the Netherlands. Aligning with existing policies and measures, with a specific focus on cybersecurity, can mitigate these risks and lead to more efficient policies.

Colophon

Sonja Kleter, Dialogic
Manon Schrijnemaekers, PTvT
Marion Sieh, PTvT
Arthur Vankan, Dialogic
Loes Willems, PTvT

Contacts:
Contact person Platform Talent voor Technologie:
Marion Sieh
m.sieh@ptvt.nl

Contact person Dialogic:
Arthur Vankan
vankan@dialogic.nl

Mailing Address:
Platform Talent voor Technologie
Postbus 76
2501 CB Den Haag

Visiting Address:
Oranjebuitensingel 6 (4e etage)
2511 VE Den Haag