

# Education Scan: Draft Deliverable

Claire Vishik, Intel; Maritta Heisel with Christina Menges, University Duisburg-Essen; Raul Riesco Granadino, INTECO, other group members

## Contents

|   |    |
|---|----|
| Executive Summary .....   | 2  |
| Introduction and status of the work.....  | 2  |
| Objectives .....  | 2  |
| Methodology & approach .....  | 2  |
| Preliminary Findings.....   | 3  |
| Recommendations.....  | 3  |
| 1. Introduction and background .....  | 5  |
| 1.1 Positioning of cyber-security .....   | 6  |
| 1.2 Early Awareness .....   | 6  |
| 2. Objectives .....   | 7  |
| 3. Methodology & approach .....   | 8  |
| 4. Analysis .....   | 9  |
| 4.1 Preliminary Findings.....   | 9  |
| 4.2 Collected Data.....   | 11 |
| 4.3 Conclusions from secondary sources.....   | 15 |
| 5. Achievements and Gaps.....   | 16 |
| 6. Recommendations.....   | 17 |
| 7. Future Work.....   | 17 |
| 8. Acknowledgements.....  | 17 |
| Appendix 1. Summary of Key Findings. ....   | 18 |
| Key aspect 1: Multi-disciplinary focus .....  | 18 |
| Recommendations.....  | 18 |
| Key aspect 2: Responsiveness to changes in technology and societal environment.....   | 19 |
| Recommendations.....  | 19 |
| Key aspect 3: End-to-end skill development .....  | 20 |
| Recommendations.....  | 20 |
| Key aspect 4: Alignment of curricula and training with demand for skills .....  | 22 |
| Recommendations.....  | 22 |
| Appendix 2. List of institutions with courses in various areas of cybersecurity, for which information was provided by individual contributors..... | 23 |

|  |    |
|--|----|
| Appendix 3. List of secondary sources evaluated..... | 45 |
| Bibliography .....                                   | 45 |

May 26, 2015

## Executive Summary

### Introduction and status of the work

NIS Platform working group on ICT research and innovation identified a snapshot of the education and training landscape for workforce development as one of the deliverables. The education scan working group initiated the collection of information on existing curricula and training programs. Information collection has started, but has not yet been completed. Consequently, we have also used secondary sources produced by similar projects to support the early conclusions and recommendations. For the purposes of this work, we have accepted a broad definition of cybersecurity that comprises a wide range of relevant topics, from cryptography, computer, information and network security to privacy, security economics, or legal, regulatory, and policy frameworks.

### Objectives

We have envisioned several objectives as part of this activity. The short term objectives include:

1. Collect sufficient information on cybersecurity higher education curriculum in member states of EU to form the first impression of trends and degrees of coverage in this area.
2. Collect sample information about training available in cybersecurity.
3. Start collecting secondary sources, i.e., work already performed by others to analyze some areas of cybersecurity education and skills development.
4. Form the first impression on gaps and formulate recommendations for development based on these findings.

The long term objectives are as follows:

1. Establish a data collection mechanism to continue to build our knowledge of the state of curriculum in cybersecurity available in the EU.
2. Define analysis methodology and formulate research questions to better understand the current state and future needs of education/training in cybersecurity. This work could include recommendations on benchmarking tools to enable education practitioners to analyze positioning with regard to other member states or peer institutions.
3. Formulate longer terms recommendations to address gaps as well as current and emerging needs in cybersecurity education and training.

### Methodology & approach

The effort asked the cybersecurity community to submit information about cybersecurity curricula and training in their countries. Since data collection has not been completed, we also relied on secondary sources to validate the views derived from early data, as data are still limited.

We have collected some information from a number of member states, including Germany, the UK, Greece, Cyprus, Italy, France, Portugal, Poland, Luxemburg, and other countries. This information was provided by individual volunteer contributors, and does not necessarily represent an official survey by EU institutions and organizations.

## Preliminary Findings

Analysis of secondary and primary data sources indicate that cybersecurity education is a fast growing field, and that training in this area has become available from various sources and awareness programs. Although coverage appears to be uneven for different European countries, the availability of coursework and training in cybersecurity and privacy is growing, especially in the area of core security curriculum.

Many gaps still remain. Soft definition of the “science of cybersecurity” has led to great diversity in training and curricula impeding the creation of common context in cybersecurity. Furthermore, there is a lack of differentiation between traditional programs offering fundamental security related curricula and more versatile cybersecurity programs with multi-disciplinary coverage and multi-faceted training materials.

The responsiveness of cybersecurity curricula and training to changes in technology remains low due to the lack of mechanisms to quickly develop and share materials on emerging threats or newly crucial skills. As a result, education and training provided under various cyber-security programs tend to coalesce around a useful common goal, but struggles to match the requirements of the dynamic workplace. Mechanisms are also missing for continuing education for those who already acquired undergraduate and graduate degrees or have focused on various aspects of cybersecurity in their work. Although some EU countries have made strides in bringing cybersecurity students in contact with industry and government for apprenticeship projects, these programs remain limited and don’t have solid sources of funding.

Cybersecurity is a very dynamic field. Like similarly fast paced environments, it suffers from the lack of reliable mechanisms to bring the results of research into the curriculum as quickly as possible and to engage students in academic research, and the lack of feedback mechanism between research and curricula reflects negatively on actionable nature of skills acquisition.

## Recommendations

Finally, we have put forward the following recommendations based on the work done so far:

1. Encourage activities with joint participation of people with different levels of proficiency, to make it easier to move from minimal awareness levels to greater understanding of cybersecurity and related issues.
2. Encourage earlier start for cybersecurity awareness and acquisition of basic skills, to coincide with independent use of connected devices. The earlier start will lead to greater proficiency in security and privacy skills by all consumers and will facilitate the introduction to more advanced and responsive curricula and greater understanding of cybersecurity requirement by computer scientists.
3. Establish a task force with an advisory focus to ensure quick and agile strategy development in cybersecurity and privacy education.
4. Support research to define curriculum & training requirements including coordination actions for these activities with end-to-end coverage (from minimal proficiency to dedicated curriculum).
5. Support multi-disciplinary curriculum and training, with clear goals for professional preparation, to ensure future workforce is capable to address complex cybersecurity problems.
6. Support community built sharable curriculum and training modules in order to make curricula and training more agile and responsive to real life security threats and changes in the technology environment.
7. Support for collaboration mechanisms with industry and government and internationally, in order to ensure consistent coverage of cybersecurity proficiency in all EU countries.

8. Support international collaboration and awareness campaigns, to ensure all EU countries are aligned on levels of proficiency and also aware of globally significant issues in cybersecurity.
9. Develop common terminology and a common body of knowledge for the cybersecurity area.

DRAFT

## 1. Introduction and background

The Cybersecurity strategy of the European Union was published in February 2013. As a part of the strategy, the European Commission invited the European Parliament and the Council to adopt a proposal for a Directive on a common high level of Network and Information Security (NIS) across the European Union. The purpose of the directive was to address national capabilities and preparedness, EU level cooperation, the take-up of risk management practices and information sharing. In the Cybersecurity strategy the European Commission also invites member states to step up national efforts on NIS education and training. The NIS Directive requires member states to adopt a national NIS strategy, which should address a number of issues. One of the issues that is to be addressed is an indication of the education, awareness raising and training programmes.

As a part of establishing the NIS Public-Private Platform, three working groups were established to investigate risk management, information exchange and incident coordination and ICT research and innovation. The working group on ICT research and innovation identified various deliverables, with one deliverable being a snapshot of the education and training landscape for workforce development. This snapshot can then be used to identify good practice within countries and identify barriers and possible incentives for countries to share good practice to further promote a single market for Cybersecurity products and enhance the reputation of the European Union as a world leader in this domain.

For the purposes of this work, we have accepted a broad definition of cybersecurity that comprises a wide range of relevant topics, from cryptography, computer, information and network security to privacy, security economics, or legal, regulatory, and policy frameworks. According to NICCS Portal Glossary<sup>1</sup>, cybersecurity in the narrow sense is

The activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation.

The source also offers an extended definition:

Strategy, policy, and standards regarding the security of and operations in cyberspace, and encompassing the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the global information and communications infrastructure.

It is obvious that the cybersecurity issues touch many aspects of everyday lives. Not surprisingly, the scope adopted for this project is very broad. Based on the definitions of the field, it is difficult to narrow down the scope of cybersecurity as a subject. And due to the multi-disciplinary nature of cybersecurity, it is impossible to avoid significant breadth in the subject matter.

While we focus on Masters' curriculum, we recognize that coursework in undergraduate and graduate curricula in specialized areas like cybersecurity cannot be easily separated from graduate programmes.

Similarly, training in cybersecurity topics are used in a variety of ways, depending on the organizations that employ them. We therefore don't make a distinction in this report between a beginner or advanced training, although these distinctions are pertinent for future work.

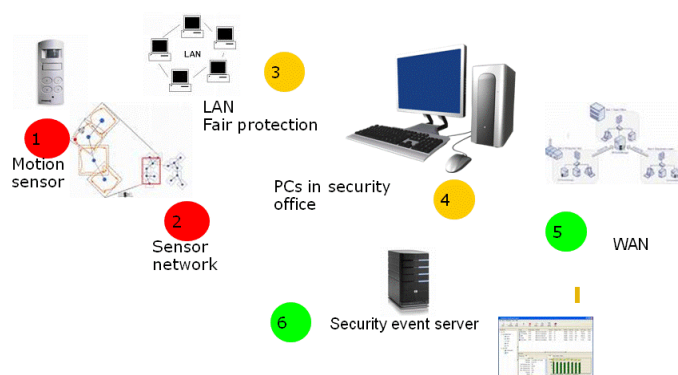
---

<sup>1</sup>[http://niccs.us-cert.gov/glossary#letter\\_c](http://niccs.us-cert.gov/glossary#letter_c) NICCS is National Initiative for Cybersecurity Careers & Studies

## 1.1 Positioning of cyber-security

With increasing diversity and mobility of the computing environment, a general approach to cybersecurity is no longer possible. Generalization is at variance with the fact that most processes are cross-domain (see Figure 1 below) and collectively participate in defining risk levels that are attributable to transactions and activities, both in security and privacy. Most environments are dynamic, with entities (e.g., devices and users) joining and leaving domains during a process. However, our approaches at defining levels of risk (and levels of trust) do not include a good assessment of the diversity and dynamism of the environment. Instead, they are directed only to one part of the ecosystem or one participant in a process.

Figure 1. Cross-domain processes



Attempts to present cybersecurity or privacy as monolithic affect our views on cybersecurity and privacy, including our views in education and skill development in these subjects.

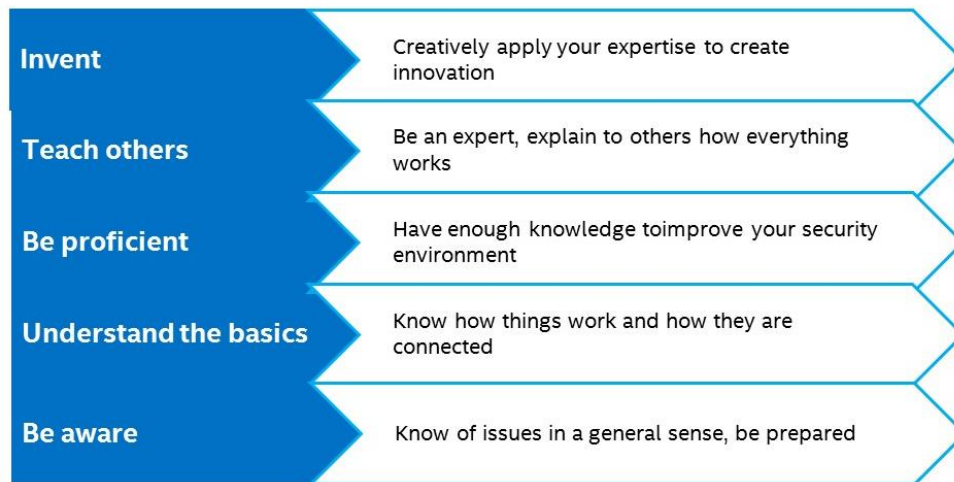
## 1.2 Early Awareness

Although the subject of this report is higher education and professional level training, we recognize that, with the digital world becoming part of everyday life from an early age, awareness of cybersecurity and privacy issues and elementary skill development should become organic. When the students reach higher education levels with basic skills in cybersecurity, most students and consumers will have the ability to assess cybersecurity risks in everyday lives, and it will be easier to develop more diverse and multidisciplinary curricula and training.

We can illustrate the levels of proficiency as a stack, starting with passive awareness and moving toward innovation at the highest level (see

Figure 2 below)

**Figure 2. Levels of Proficiency**



Although, as we observe, significant progress was made in teaching cybersecurity, we need to assume also that the degree of innovation in this area would increase significantly if a greater number of individuals progressed to the basic skills level and were able to move on to achieve proficiency. These insights are out of scope for this study, but we believe that, when we assess the state of cybersecurity curricula and skills developments, we also need to understand the negative impact the loss of opportunity early in the skill development cycle is likely to have on innovation.

## 2. Objectives

As we discussed in the introduction, cybersecurity is a multi-disciplinary area of knowledge. Knowledge of the principles and foundations of cybersecurity draws from many disciplines and behaviors. Non-specialist practical knowledge of best practices in cybersecurity is necessary for all users of technology, including consumers, and accepted best practices determine, in part, how technology is used and how it is taught.

We have envisioned several objectives as part of this project, short term as well as longer term. The short term objectives include.

1. Collect sufficient information on cybersecurity higher education curriculum in member states of EU to form the first impression of trends and degrees of coverage in this area.
2. Collect sample information about training available in cybersecurity.
3. Start collecting secondary sources, i.e., work already performed by others to analyze some areas of cybersecurity education and skills development.
4. Form the first impression on gaps and formulate recommendations for development based on these findings.

We understand that informal collection of information as undertaken for this project may offer an incomplete and sometimes biased picture. So far, we have not found inconsistencies of views among those who participated in data collection and shared their insights.

However, in order to avoid bias, we also seek to establish a mechanism, by which data collection from primary sources could be continued leading to a more in depth analysis of the education environment and education needs in cybersecurity.

In order to provide visibility into the development of the education landscape in cybersecurity, we think it is important to continue data collection beyond these initiatives. ENISA will house the resulting database at: <http://cybersecuritymonth.eu/references/universities>

A longer term development mechanism makes it easier to formulate long term objectives. Some of these objectives are dependent on the insights gleaned from primary and secondary data, and they remain work in progress. The long term objectives are as follows:

1. Establish a data collection mechanism to continue to build our knowledge of the state of curriculum in cybersecurity available in the EU.
2. Define analysis methodology and formulate research questions to better understand the current state and future needs of education/training in cybersecurity. This work could include recommendations on benchmarking tools to enable education practitioners to analyze positioning with regard to other member states or peer institutions.
3. Formulate longer terms recommendations to address gaps as well as current and emerging needs in cybersecurity education and training.

The work conducted for the NIS Platform initiative is so far exploratory, as the due date of the report allows. When this effort is concluded, in addition to the report, we hope to initiate a data collection mechanism as well as improve communication among cybersecurity education practitioners. We aim at providing awareness of available courses and training, as well as some understanding of gaps. We hope to define the initial set of recommendations in this report, and use it as an input in other programs currently focusing on similar issues.

In short, this work is intended to set the general direction based on data samples and insights in secondary sources, but assumes that comprehensive analysis and broader recommendations will emerge as the findings of this and other projects in this area are aggregated.

We also hope that a community of practice will emerge as a result of this work.

### 3. Methodology & approach

In 2003, a report was published on the state of cybersecurity training by academic institutions in Europe<sup>i</sup>. The study came in response of the Communication on Network Security: Information Policy Approach issued by the European Commission in 2001. The study, Fondazione Rosselli, was entitled:

“Cybersecurity Curricula in European Universities.” It included six countries: Greece, Belgium, France, Germany, Italy, UK. The study used a methodology similar to this study: acquire insights based on survey containing minimal information on content and level of university courses. But because of the views on cybersecurity more than ten years ago, the report focused on the narrow view on cybersecurity, putting emphasis on information security courses, with the focus on cryptography. Other areas were considered, but to a lesser degree.

With regard to general methodology, we used an approach compatible with the 2003 report, but adopted a broad multi-disciplinary view of cybersecurity and relied on secondary sources to check views derived from data, as data are still limited.

The NIS effort was successful in mobilizing many of those who teach cybersecurity curriculum and some of those who build cybersecurity training to respond by providing information on various programs and training elements, the last data set being still very limited.

We have collected information from a number of member states, including Germany, the UK, Greece, Cyprus, Italy, France, Portugal, Poland, Luxemburg, and other countries. And we are encouraged, by continued inquiries, that additional information is forthcoming. We include the list of institutions that submitted information in Appendix 1. We would like to stress that this information was provided by individual volunteer contributors, and does not necessarily represent an official survey by EU institutions and organizations.

We have formulated, for the first stage, the following research questions:

1. Are the cybersecurity courses predominantly offered as part of dedicated cybersecurity programs or as individual courses within more general curriculum?
2. Are cybersecurity courses predominantly provided as complete courses or modules within more general security courses?
3. Is cybersecurity curriculum represented predominantly through general purpose security courses or dedicated cybersecurity courses?
4. Does the recognized multidisciplinary nature of cybersecurity come through in the curriculum, or are courses dedicated primarily to one topic (e.g., policy, user psychology, economics, computer & device security)?
5. Is the curriculum taught predominantly in academic departments (e.g., computer science or economics) or in professional schools (law, international relations, and business) or both? Are multi-disciplinary degrees in cybersecurity available?
6. Is there a strong relationship between cybersecurity awareness programs and training& curriculum in cybersecurity?
7. Are cybersecurity training materials predominantly built for specific organizations and departments, or general purpose training is commonly used, at least for beginners?

While data collected is incomplete, and it would be premature to perform statistical analysis, we were able to form some initial views on the state of the curriculum with regard to the initial research questions. These views are presented below.

## 4. Analysis

### 4.1 Preliminary Findings

The data we collected as well as information gleaned from secondary sources permit us to form some impressions about the state of security curriculum. We present some of the preliminary findings under the research questions that we have attempted to answer. We have been aided in these answers by more specific questions we posed to analyze the data collated so far (see below).

**1. Are the cybersecurity courses predominantly offered as part of dedicated cybersecurity programs or as individual courses within more general curriculum?**

The first impression is that there is a lot of fragmentation in the field. Curriculum on core elements in security has been available for a while, either as complete courses or elements of coursework. In addition to technical courses, social science curriculum in psychology, economics, law, and policy, especially with the focus on privacy, has been developed.

While the availability of curricula on some elements of cybersecurity is a positive development, multi-disciplinary synthesis of such coursework has remained rare.

**2. Are cybersecurity courses predominantly provided as complete courses or modules within more general security courses?**

Different education systems in different member states make it difficult to answer this question in a general way. However, it appears that the inventory of curriculum components includes both complete courses and course modules, with complete courses readily available.

**3. Is cybersecurity curriculum represented predominantly through general purposes security courses or dedicated cybersecurity courses?**

We have found a dearth of courses that focus on cybersecurity specifically, if cybersecurity is defined as **the body of technologies, processes and practices designed to protect networks, computing devices, programs and data from attack, damage or unauthorized access**. Instead, the predominant type of courses continues to focus on general technical and societal aspects of security and privacy.

**4. Does the recognized multidisciplinary nature of cybersecurity come through in the curriculum, or are courses dedicated primarily to one topic (e.g., policy, user psychology, economics, computer & device security)?**

We have found a lack of coursework that seriously integrates societal and technical aspects of cybersecurity. Without individual review of all courses or descriptions of the programs provided online and in secondary sources, it is impossible to confirm that at least some multidisciplinary elements are introduced in a lasting way during teaching. Even if such integration is pervasive, it is clear that it is insufficient. The lack of multidisciplinarity is the most serious concern we have with regard to available curriculum.

Multiple programs exist, in Europe and beyond, that count multi-disciplinary curriculum in cybersecurity among their most important characteristics. We can name Oxford, Royal Holloway, Vrije University, and several other schools as homes to multidisciplinary programs. However, education systems developed no lasting mechanisms to introduce multidisciplinary components in core curriculum, beyond offering social sciences and technology courses alongside each other rather than provide integration of several bodies of knowledge.

**5. Is the curriculum taught predominantly in academic departments (e.g., computer science or economics) or in professional schools (law, international relations, and business) or both? Are multi-disciplinary degrees in cybersecurity available?**

Both environments have become sources of training for cybersecurity professionals, although academic preparation remains predominant. Evidence was provided that introduction of cybersecurity curricula is beneficial for academic institutions, especially small colleges and universities. Institutions of this type in the US, for example, reported significant increase in enrollment after being designated a Center of Excellence<sup>2</sup>. The number and maturity of multidisciplinary initiatives remain insufficient.

**6. Is there a strong relationship between cybersecurity curriculum, awareness programs and training in cybersecurity?**

We have insufficient data to make conclusions on the existing relationship between cybersecurity curriculum and available information or certification-connected training. The dynamic nature of cybersecurity makes it imperative to forge such a relationship, in order to provide a light-weight mechanism to bring skills up-to-date.

**7. Are cybersecurity training materials predominantly built for specific organizations and departments, or general purpose training is commonly used, at least for beginners?**

Studies we have reviewed, including one commissioned by Australian government that compares initiatives in different countries seems to indicate that for awareness training as well as beginners' cybersecurity education general purpose approaches are used, regardless of the specific nature of the audience. As expected, in-depth training and specialized curricula are more focused on specific objectives.

## 4.2 Collected Data

We have started collecting information at the beginning of 2014, and since then, we have acquired some data about a number of programs in a dozen European countries. We are grateful to the volunteers for these contributions (see Table 1).

Although the data are not comprehensive, they give us a preliminary view of the curriculum available and general characteristics of such curriculum. The information collected is too sketchy to permit us to compare approaches in different member states at this time, but, with the online database operational, we hope it will be possible in the future.

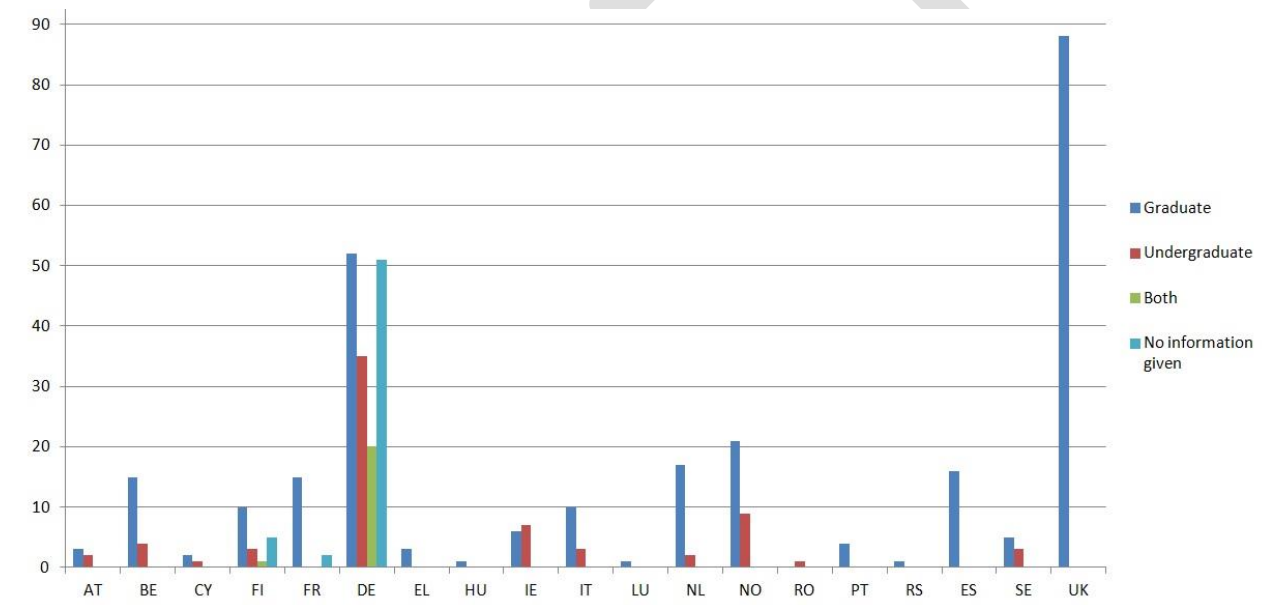
**Table 1. Data collected so far:**

| Country     | Undergraduate | Graduate | Training |
|-------------|---------------|----------|----------|
| Austria     | +             | +        |          |
| Belgium     | +             | +        | +        |
| Cyprus      | +             | +        |          |
| Finland     | +             | +        |          |
| France      |               | +        |          |
| Germany     | +             | +        | +        |
| Greece      |               | +        |          |
| Hungary     |               | +        | +        |
| Ireland     | +             | +        |          |
| Italy       | +             | +        | +        |
| Luxemburg   |               | +        |          |
| Netherlands | +             | +        |          |
| Norway      | +             | +        |          |
| Romania     | +             |          |          |
| Spain       | +             | +        |          |

<sup>2</sup><http://csrc.nist.gov/nice/index.htm>

|        |   |   |   |
|--------|---|---|---|
| Sweden | + | + |   |
| UK     | + | + |   |
| Turkey |   |   | + |

**Figure 3. Numbers of graduate and undergraduate courses per country.**



Most of the curriculum elements submitted so far come from Computer Science, Computer Engineering, Information Systems, or Information Management departments. We have scant information on multidisciplinary programs focusing on cybersecurity, although information about these programs is a key part of this project.

Information on training programs and seminars come from Germany, Italy, Turkey, Hungary and Belgium. Therefore, the dataset is still incomplete and only gives a first impression.

Based on the data collected so far, we developed more specific research questions to better understand the data:

For university curricula:

- A. In which disciplines are most courses offered? (e.g., Computer Science, Information Security, etc.)?

- B. Are there courses offered in disciplines which are not directly related to IT (e.g., Business Administration, Law, etc.)?
- C. Can the topics be clustered into overall topics or research fields (e.g., Hacking, Cryptography, IT Security, etc.)? Which fields are covered most/least?
- D. Comparing the countries: Are there any similarities in the courses offered, or any distinctive differences?

For training:

- E. Can the courses be clustered into overall topics? (e.g., Hacking, Data Protection, Secure Software, etc.)
- F. Are relevant topics missing in the training which is offered? (Maybe this is covered in an organization which is not part of the dataset yet)
- G. Who is the main audience? (e.g., Project Managers, Data Protection Managers, System Administrators, etc.)
- H. Is there some audience which is excluded from the training yet, but should be included? (Maybe this is covered in an organization which is not part of the dataset yet)
- I. Which are the types of organizations that offer the training courses? (e.g., Universities, research organizations, consultancies, etc.)
- J. Comparing the countries: Are there any similarities in the training courses offered, or any distinctive differences?

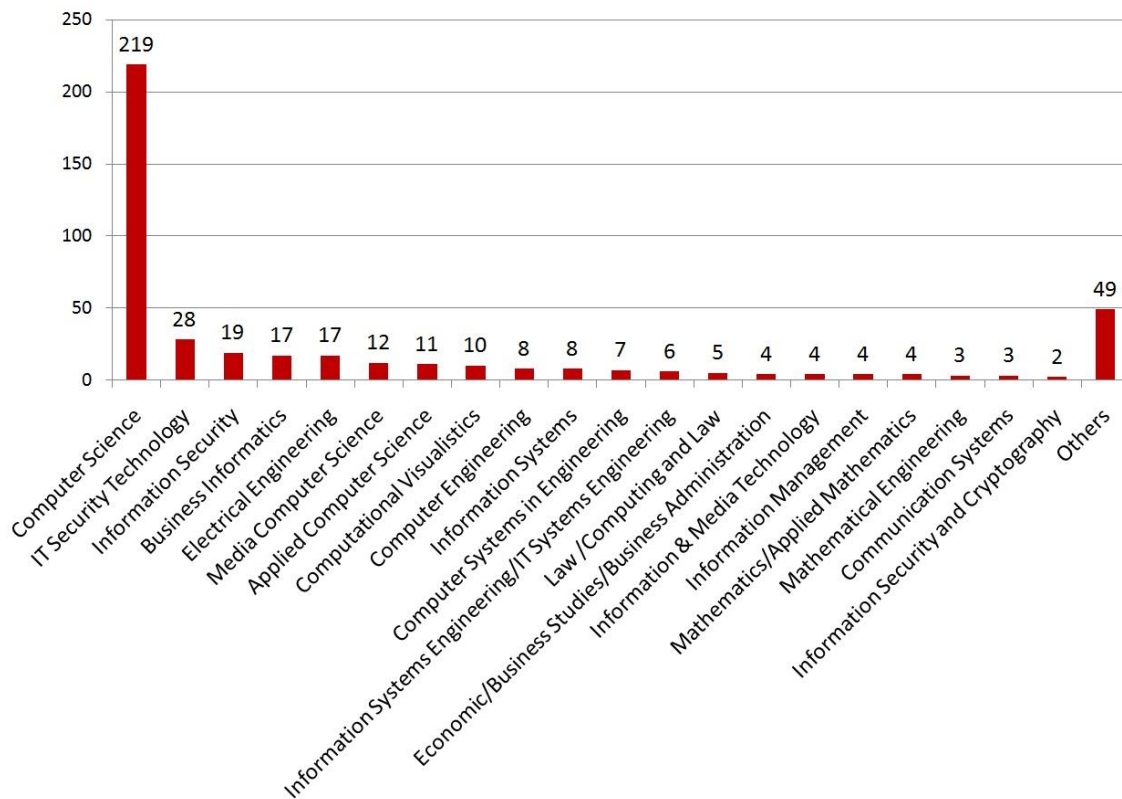
We are now able to provide answers to some of these questions, to illustrate the progress:

**A. In which disciplines are most courses offered? (e.g., Computer Science, Information Security, etc.)?**

As shown in

Figure 4, most courses are offered in the discipline of Computer Science with a large distance to the subsequent disciplines, IT Security Technology, Information Security, Business Informatics and Electrical Engineering. Note: The column “Others” covers all disciplines in which only one course per country is offered.

**Figure 4. Number of Disciplines in which most courses are offered.**



**B. Are there courses offered in disciplines which are not directly related to IT (e.g., Business Administration, Law, etc.)?**

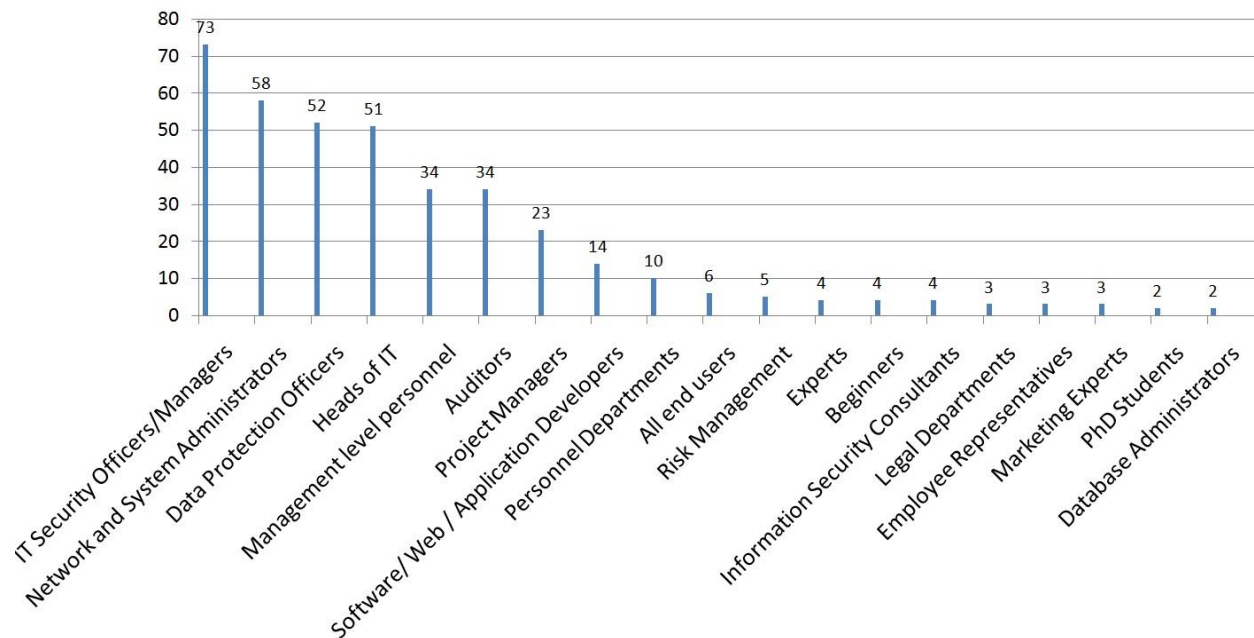
Figure 4 shows that there are some courses which are not directly related to IT disciplines, in which a few courses are offered. The subjects range from Business Studies and Business Administration, to Law, Media related disciplines or Mathematics. Even though these disciplines do not represent the overall majority, they demonstrate that the field of cybersecurity has acquired breadths in the last 10 years, and now spans into some fields which are only distantly related to IT and IT Security.

Even though the material on training is still limited, we were able to provide answers to two of the questions. Please note that the database for this evaluation is still incomplete and is only based on the five countries which have provided their data yet.

**G. Who is the main audience? (e.g., Project Managers, Data Protection Managers, System Administrators, etc.)**

As displayed in Figure 5, the main audience of the training courses dedicated to cybersecurity are IT Security Officers/Managers, Network and System Administrators, Data Protection Officers, Heads of IT Departments, the Management level and Auditors.

**Figure 5. Main Audience.**



#### H. Which types of organizations offer the training courses? (e.g., Universities, research organizations, consultancies, etc.)

The training courses are offered by private, academic or public research organizations, as well as by some non-profit organizations. Besides universities, the organizations can overall be divided into training centers, consultancies (e.g., Business Consulting or IT Security Consulting), IT Security Service Providers or IT Security Specialists.

### 4.3 Conclusions from secondary sources

Because of the early stage of data collection, some of the conclusions we reached draw from several secondary sources used during the first stage of this work. Government reports and other organizations have published reports associated with cybersecurity skills. These reports were reviewed by the group members. The list of secondary sources used is provided in Appendix II.

The reports and other secondary sources offer the following insights into the state of cybersecurity skills and education:

1. They acknowledge the skills shortage for cybersecurity professionals (e.g., UK Government report on cybersecurity skills or RAND report for the US as well as numerous other sources), with jobs going unfilled because of the lack of qualified professionals. At the same time, they acknowledge significant growth in the education of cybersecurity professionals over the last ten years.
  - a. RAND report concludes that the shortage is predominantly at the high end of the profession and concerns predominantly the federal government, while industry and academia developed avenues to deal with shortage of skills at the high end of the profession through additional education and, in industry, internal promotion. RAND report concludes that the shortage will self-correct through a combination of activities.

- b. The UK Government report indicates that the skills shortage is connected to the fact that cybersecurity profession is not yet well defined, the view that this group also shares. The activities directed to alleviate the skills shortage include a new GCHQ Certification scheme or accreditation of 11 additional certification programs. Differently from RAND report, this report states that it will take many years and focused programs to alleviate the skills shortage.
  - c. The IBM report on “Cybersecurity Education for the Next Generation” states that, while the number of cybersecurity programs (under various names) increased significantly over the past ten years, with 160 programs certified as Centers of Excellence in the US alone, the perceptions of a strong skills shortage remain strong, with the growing demand created by government and industry.
  - d. The comparative report on cybersecurity education commissioned by the Australian government attempts to highlight gaps in content in relations to the diversity of the audiences.
2. They pinpoint the need for greater collaboration of government and industry, the sources of employment, and academia, predominant source of training.
  - a. While government and academia recognize that jobs go unfilled because of dearth of skilled professionals, survey of academia (quoted in the IBM report) showed that 60% of academics believe training is adequate for the requirements of the workplace.
  - b. While many industry members, including SAP, Microsoft, Intel, ARM, and many other have established programs to support the design of adequate curriculum in security, these efforts remain fragmented and received minimal support from funding agencies in Europe and elsewhere.
3. The sources highlight the importance of certification and awareness campaigns in shaping the skills, both by professionals and users of information.
4. They acknowledge that the field is so large and so dynamic, with so many interdependencies, that building a more complete picture and shared context remains a top priority.

## 5. Achievements and Gaps

Analysis of literature and primary data sources indicate that cybersecurity education is a fast growing field, and that training in this area has become available from various sources and awareness programs. Among the main achievements, we would like to mention the following:

1. Increase in number of university programs focusing on various aspects of cybersecurity.
2. Emergence of a number of government initiatives supporting the development of cybersecurity skills and related professions.
3. Emergence of awareness programs in EU member states and ENISA-driven coordinated European awareness program.
4. Emergence of several efforts working on assessing the needs of cybersecurity education and training.
5. Growing number of organizations and enterprises providing cybersecurity training to all members/employees.

Among the gaps, the following stand out:

1. Lack of general agreement on the “science of cybersecurity,” leading to great diversity in training and curricula offered under the name of cybersecurity. Creation of common context in cybersecurity needs to be encouraged.

2. Lack of differentiation between traditional programs offering fundamental security related curricula and cybersecurity programs. While fundamental preparation is always key to good education, multidisciplinary skills necessary to a cybersecurity professional need to be included in many more programs.
3. Dearth of multidisciplinary programs and related degrees, as well as multi-faceted training materials. At a minimum, technologists focusing on cybersecurity need to have good understanding of privacy, legal and regulatory frameworks, economics or usability issues. Likewise, those focusing on legal and societal issues need to acquire a solid understanding of technology.
4. Lack of mechanisms to quickly create and share materials on emerging threats or newly crucial skills, to ensure that education provided under various cyber-security programs is up to date and matches the requirements of the dynamic workplace.
5. Lack of mechanisms for continuing education for those who already acquired undergraduate and graduate degrees.
6. Although some EU countries have made strides in bringing cybersecurity students in contact with industry and government for apprenticeship projects, to help forge a practical foundation for the application of skills, these programs are usually limited and don't have solid sources of funding.
7. Cybersecurity is a very dynamic field. Like similarly fast paced environments, it suffers from the lack of reliable mechanisms to bring the results of research into the curriculum as quickly as possible and to engage students more in academic research.

## 6. Recommendations

Finally, we have put forward the following recommendations based on the work done so far:

1. Encourage activities with joint participation of people with different levels of proficiency, to make it easier to move from minimal awareness levels to greater understanding of cybersecurity and related issues.
2. Encourage earlier start for cybersecurity awareness and acquisition of basic skills, to coincide with independent use of connected devices. The earlier start will lead to greater proficiency in security and privacy by all consumers and will facilitate the introduction to more advanced curricula and greater understanding of cybersecurity by computer scientists.
3. Establish a task force with an advisory focus to ensure quick strategy development in cybersecurity and privacy education.
4. Support research to define curriculum & training requirements including coordination actions for these activities with end-to-end coverage (from minimal proficiency to dedicated curriculum).
5. Support for multi-disciplinary curriculum and training, with clear goals for professional preparation, to ensure future workforce is capable to address complex cybersecurity problems.
6. Support for community built sharable curriculum and training modules in order to make curricula and training more agile and responsive to real life threats and changes in the environment.
7. Support for collaboration mechanisms with industry and government and internationally, in order to ensure consistent coverage of cybersecurity proficiency in all EU countries.
8. Support international collaboration and awareness campaigns, to ensure all EU countries are aligned on levels of proficiency and also aware of globally significant issues in cybersecurity.
9. Develop a common terminology and a common body of knowledge for the cybersecurity area.

## 7. Future Work

We expect online data collection tool will permit us to collect more information from member states, and we hope that data collection will continue beyond this project to provide materials for future analyses. We also are looking for a home to house a collection of relevant links and reports from past efforts on cybersecurity education.

We also expect to collect more information about available training, an area where data available from secondary courses is also limited.

With regard to the report itself, the next version will include a more extended narrative on analysis of the primary and secondary information collected as well as more information on existing cybersecurity curricula.

We will release the report to WG3 for comment and input, especially with regard to analysis and recommendations. If WG3 community recommends it, we will engage communities beyond WG3 in further review and refinement of the current early draft.

## 8. Acknowledgements

We would like to thank ENISA and specifically Daria Catalui for the support of this initiative.

This is a placeholder to acknowledge numerous participants in this project – pending their agreement to be included.

## Appendix 1. Summary of Key Findings.

---

### Key aspect 1: Multi-disciplinary focus

For the purposes of this work, we have accepted a broad definition of cybersecurity that comprises a wide range of relevant topics, from cryptography, computer, information and network security to privacy, security economics, or legal, regulatory, and policy frameworks. According to NICCS Portal Glossary<sup>3</sup>, the extended definition is as follows:

Strategy, policy, and standards regarding the security of and operations in cyberspace, and encompassing the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the global information and communications infrastructure.

Although there is general agreement about multi-disciplinary nature of cybersecurity, it remains difficult to reflect the need for multi-disciplinarity in teaching and training environments, because of the diverse skill sets required for truly integrated programs. While a number of multi-disciplinary programs and centers are in place, acquiring in-depth skills in multiple subjects rather than lighter supplemental skills around the area of specialization remains rare. As a result, professionals with understanding of technology as well as law, policy, psychology, or economics are uncommon. Yet, professionals with multi-disciplinary skills continue to be at the top of the lists of skills gaps, according to reports and surveys.

Multi-disciplinary research that is necessary to feed multi-disciplinary programs also continues to be fragmented. Although efforts had been made to support multi-disciplinary approaches to cybersecurity, funding mechanisms, availability of publications and conferences that support multi-disciplinary work are insufficient.

Ultimately, fragmentation of knowledge in cybersecurity impacts all aspects of society, from the technology environment to legal and policy frameworks.

---

### Recommendations

2. Support multi-disciplinary curricula and training, with clear goals for professional preparation, to ensure future workforce is capable to address complex cybersecurity problems.
3. Continue to build infrastructure to encourage multi-disciplinary skill development in cybersecurity including curricula and programs in higher education, funding for multi-disciplinary research, and establishment of multi-disciplinary work.
4. Establish prizes for successful multi-disciplinary work in cyber-security.

---

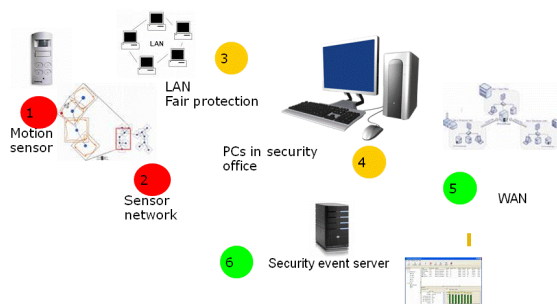
<sup>3</sup>[http://niccs.us-cert.gov/glossary#letter\\_c](http://niccs.us-cert.gov/glossary#letter_c) NICCS is National Initiative for Cybersecurity Careers & Studies

---

## Key aspect 2: Responsiveness to changes in technology and societal environment

With increasing diversity and dynamic nature of the computing environment, a static approach to teaching cybersecurity skills is no longer effective. Today, most environments are dynamic, with entities (e.g., devices and users) joining and leaving domains. Most processes are cross-domain operating in ecosystems with multiple security models and different vulnerabilities.

**Figure 1. Cross-domain processes**



The issues of security composition in complex environments or security and privacy challenges arising at the intersection of several domains remains unresolved, and effects of this complexity on security remain unknown. Preparation and training of cybersecurity professionals continues to focus on one domain, further impacting technologists' understanding of inter-dependencies that need to be considered.

Approaches used for teaching technical and societal aspects of cybersecurity continue to focus on the development of fundamental skills and knowledge in key areas, similarly to teaching fundamental sciences or law. It remains crucial to acquire fundamental skills, and the importance of this aspect of education and training will never decrease. No continued education is possible before solid fundamental skills are acquired. However, the dynamic nature of the technology environment, as well as reactive components and positioning of cybersecurity make it imperative to create additional mechanisms to acquire and continue to develop new skills and knowledge as the environment evolves.

The emergence of the new mechanisms to address the quick evolution of technology and usage models will permit us to prepare professionals with deep fundamental knowledge and the ability to solve the new problems as they emerge. Better knowledge of the connections and dependencies in the ecosystem will make it easier to select more effective solutions.

A more responsive approach to evolving technology environment in cybersecurity curricula and training is needed to help ensure quicker alignment of approaches to teaching cybersecurity across the EU, rapid awareness of emerging global issues or new solutions, and greater competitiveness of the EU members.

---

### Recommendations

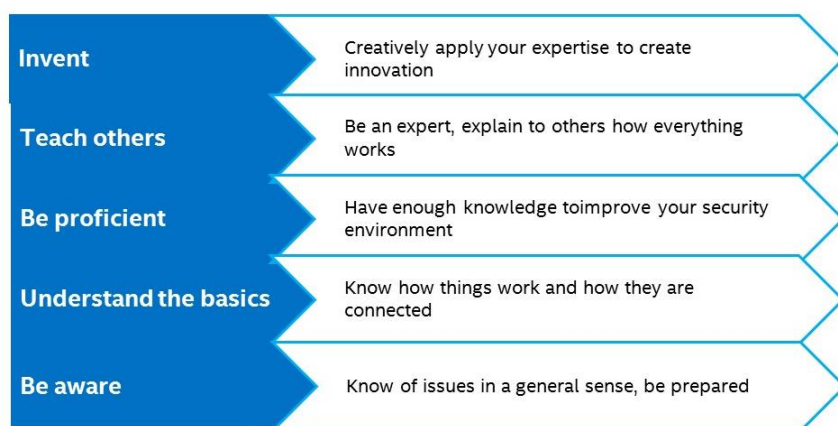
5. Establish a task force with an advisory focus to provide recommendations to increase agility, responsiveness, and multi-disciplinarity in cybersecurity and privacy education.
6. Devise mechanisms to develop and deploy community built sharable curriculum and training modules in cybersecurity in order to make curricula and training more agile and responsive to real life security threats and changes in the technology environment
7. Support international collaboration and awareness campaigns, to ensure all EU countries are aligned on levels of proficiency and aware of globally significant issues in cybersecurity

---

### Key aspect 3: End-to-end skill development

With the digital world becoming integral part of everyday life from an early age, awareness of cybersecurity and privacy issues and elementary skill development should become more organic. Acquiring fundamental skills earlier and organically, as part of regular education, will not only help develop the competence of consumers to take important decisions, but also the preparation of experts and innovators in cybersecurity and privacy. We can illustrate the levels of proficiency as a stack, starting with passive awareness and moving toward innovation at the highest level (see Figure 2 below). Ensuring that more people move from the lowest to the higher levels of proficiency will positively affect the technology environment; development of secure devices, networks, and applications; effective remediation following cybersecurity attacks, and, ultimately, innovation. Focusing on higher education and expert training only is likely to have reduced impact through the loss of opportunity for talent development early in the skill development cycle.

**Figure 6. Levels of Proficiency**



---

### Recommendations

1. Support research to define curriculum & training requirements including coordination actions for these activities with end-to-end coverage (from minimal proficiency to dedicated curriculum).
2. Establish a task force with an advisory focus to address strategic requirements of end-to-end cybersecurity and privacy education in order to develop consistent analysis of the dependences among different levels of education and establish concrete measures to encourage continued acquisition of skills in cybersecurity.
3. Support research to develop new mechanisms to provide greater visibility of cybersecurity and privacy vulnerabilities when using common devices, systems, applications, and processes.
4. Support programs focusing on interaction of people with different levels of proficiency.
5. Encourage earlier start for cybersecurity awareness and acquisition of basic skills, to coincide with independent use of connected devices. The earlier start will lead to greater proficiency in security and privacy skills by all consumers and will facilitate the introduction to more

advanced and responsive curricula and greater understanding of cybersecurity requirement by computer scientists

6. Encourage entrepreneurship in cybersecurity defining a path from skills acquisition to innovation.

DRAFT

---

#### Key aspect 4: Alignment of curricula and training with demand for skills

Most reports on cybersecurity skills agree that the shortage of cybersecurity professionals is becoming more acute and highlight the sharpest shortages occurring either with regard to the latest skills or at the top of the profession where experience or multi-disciplinary knowledge are essential. The shortage continues to be felt in government, while industry and academia developed some avenues to deal with shortage of skills at the high end of the profession through additional education and, in industry, internal promotion. The skills shortage is connected to the fact that cybersecurity profession is not yet well defined, negatively affecting the effectiveness of cybersecurity education and training.

The complexity of the technology environment and regulatory frameworks as well as quick evolution of technology and cybersecurity threats creates a great diversity of needs among potential employers that remains hard to address.

Greater collaboration of stakeholders in cybersecurity – governments, academia, and industry—is necessary to align perceptions of the needs for skills and vehicles to combine theoretical and practical training. While many industry members and other communities have established programs to support and encourage the design of adequate curricula in cybersecurity, these efforts remain fragmented and receive minimal support from funding agencies in Europe and elsewhere.

Similarly, apprenticeship and internship programs continue to develop as needs for employees with cybersecurity skills is growing, but very few innovative mechanisms to support short term skill development programs have been established.

Finally, awareness of skills in high demand remains delayed and imperfect, putting additional pressures on students, educators, job seekers, and employers and negatively affecting competitiveness of the EU countries.

---

#### Recommendations

1. Support development and enhancement of collaboration mechanisms with industry and government and internationally, in order to ensure consistent coverage of cybersecurity proficiency in all EU countries
2. Encourage new flexible models for short terms internships and training in operational environments to develop purpose-based acquisition of top-priority skills.
3. Establish mechanisms to increase awareness of skills in high demand to increase competitiveness of job seekers.
4. Establish high quality mechanisms for on demand acquisition of high priority skills, open across the EU, including the countries where such mechanisms may not be readily available.

Appendix 2. List of institutions with courses in various areas of cybersecurity, for which information was provided by individual contributors.

| Country | University                                | Course title (local, English)  | Course level (Undergrad, grad) | Discipline (e.g., computer science)   |
|---------|---|--|--------------------------------|---|
| Austria | University of Innsbruck                   | Information Security   | Graduate                       | Computer Science  |
| Austria | University of Innsbruck                   | IT-Security Architectures  | Graduate                       | Computer Science  |
| Austria | Vienna University of Technology           | Internet Security  | Undergrad Course               | Computer Science  |
| Austria | Vienna University of Technology           | Advanced Internet Security   | Graduate Course                | Computer Science  |
| Austria | Vienna University of Technology           | Introduction to Security   | Undergrad Course               | Computer Science  |
| Cyprus  | Ledra College                             | BSc Cyber Security   | Undergraduate BSc              | Computer Science  |
| Cyprus  | University of Cyprus, Nicosia             | MSc/BSc Internet Computing/Computer Science  | Graduate/UG MSc/BSc            | Computer Science  |
| Cyprus  | Open University of Cyprus                 | Information & Communications Systems   | MSc/PhD pathways Graduate      | Computer Science/Computer Engineering/Information Systems/Communication Systems |
| Finland | University of Turku                       | Cryptography and Data Security   | Graduate                       | Information Security and Cryptography   |
| Finland | University of Turku                       | Network Systems Security   | Graduate                       | Information Security and Cryptography   |
| Finland | University of Helsinki                    | Tietoturvan perusteet (Introduction to Computer Security)  | Undergraduate                  |   |
| Finland | University of Helsinki                    | Cryptography and Network Security  |                                |   |
| Finland | University of Helsinki / Aalto University | Mobile Platform Security   |                                |   |
| Finland | University of Helsinki / Aalto University | Software Security  |                                |   |
| Finland | Aalto University                          | Noin fifty-sixty? Kurssi epävarmuuden käsitteistä, käsittelystä ja käsittämättömyydestä (About fifty-sixty? Exchange rate uncertainty, concepts, processing and incomprehensibility) |                                |   |

|         |                          |   |                        |   |
|---------|--------------------------|---|------------------------|---|
| Finland | Aalto University         | Information Security  | Undergraduate/Graduate |   |
| Finland | Aalto University         | Science and Technology and Design of Security and Terrorism: Contemporary and Historical Perspectives | Graduate               |   |
| Finland | Aalto University         | Security of Communication Protocols   |                        |   |
| Finland | Aalto University         | Information Security Technology   | Undergraduate          |   |
| Finland | Aalto University         | Laboratory Works in Networking and Security   | Graduate               |   |
| Finland | Aalto University         | Information Security and Usability  | Graduate               |   |
| Finland | Aalto University         | Network Security  | Graduate               |   |
| Finland | Aalto University         | Seminar on Network Security   | Graduate               |   |
| Finland | Aalto University         | Special Assignment in Networking and Security   | Graduate               |   |
| Finland | Aalto University         | Special Course in Information Security  | Graduate               |   |
| Finland | Aalto University         | Cryptography and Data Security  | Undergraduate          |   |
| France  | Eurecom                  | Cyber-Crime and Computer Forensics  | Grad                   | Computer Science  |
| France  | Eurecom                  | System and Network Security   | Grad                   | Computer Science  |
| France  | Eurecom                  | Secure Communications   | Grad                   | Computer Science  |
| France  | Eurecom                  | Security applications in networking and distributed systems   | Grad                   | Computer Science  |
| France  | Eurecom                  | Imaging for Security Applications, Watermarking & Biometrics  | Grad                   | Computer Science  |
| Germany | RWTH Aachen              | IT-Security 1   | Graduate               | Business Administration, Computer Science, Mathematics, Media Informatics, Software Systems Engineering |
| Germany | Universität Augsburg     | Software- und Systemsicherheit / Software and System Security   | Graduate               | Computer Science  |
| Germany | Freie Universität Berlin | Rechnersicherheit / Computer Security   | Graduate               | Computer Science  |

|         |   |  |          |  |
|---------|---|--|----------|--|
| Germany | Freie Universität Berlin                        | IT-Sicherheit / IT-Security  | Graduate | Computer Science   |
| Germany | Freie Universität Berlin                        | Kryptographie und Sicherheit in Verteilten Systemen / Cryptography and Security in Distributed Systems                     | Graduate | Computer Science   |
| Germany | TU Berlin                                       | Sicherheitsaspekte in der Softwaretechnik / Security aspects in Software Engineering                                       | Graduate | Computer Science, Computer Engineering   |
| Germany | Ruhr-Universität Bochum                         | Projekt Eingebettete Sicherheit / Project Embedded Security  | Graduate | IT Security/Information Technology   |
| Germany | Ruhr-Universität Bochum                         | Security and Privacy in Wireless Networks  | Graduate | IT Security/Information Technology   |
| Germany | Ruhr-Universität Bochum                         | Netz- und Datensicherheit / Network and Data Security  | Graduate | Applied Computer Science, IT Security/Information Technology   |
| Germany | Ruhr-Universität Bochum                         | Praktikum Security Appliances / Practical Course Security Appliances   | Graduate | IT Security/Information Technology   |
| Germany | Brandenburgische Technische Universität Cottbus | IT-Sicherheit / IT-Security  | Graduate | Computer Science, Engineering Economics, Technology and Innovation Management, Information and Media Technology, eBusiness |
| Germany | Universität Dortmund                            | Sicherheit und Softwareengineering / Security and Softwareengineering  | Graduate | Computer Science, Applied Computer Science   |
| Germany | TU Dresden                                      | Trustworthy and Energy-Efficient Smart Grids   | Graduate | Computer Science, Media Computer Science, Information Systems Engineering  |
| Germany | TU Dresden                                      | Komplexpraktikum Datenschutz in der Anwendungsentwicklung / Practical course on Data protection in Application Development | Graduate | Computer Science, Media Computer Science   |

|         |   |   |                        |   |
|---------|---|---|------------------------|---|
| Germany | TU Dresden                                  | Komplexpraktikum<br>Datenschutzfreundliche<br>Technologien im Internet /<br>Practical Course on Friendly<br>Data Protection Technologies<br>on the Internet   | Graduate               | Computer Science, Media<br>Computer Science   |
| Germany | TU Dresden                                  | Anwendungsforschung<br>Datenschutz und<br>Datensicherheit / Applied<br>Research on Data Protection<br>and Data Security   | Graduate               | Computer Science  |
| Germany | Universität<br>Duisburg-Essen               | Entwicklung sicherer<br>Software / Development of<br>save and secure Software   | Undergraduate/Graduate | Applied Computer Science,<br>International Studies in<br>Engineering, Electrical<br>Engineering and Information<br>Technology |
| Germany | Heinrich Heine<br>Universität<br>Düsseldorf | Sicherheitskritische Systeme /<br>Safety Critical Systems   | Graduate               | Computer Science  |
| Germany | Uni Erlangen-<br>Nürnberg                   | Datenschutz und Compliance<br>/ Data protection and<br>Compliance   | Graduate               | Computer Science  |
| Germany | Uni Erlangen-<br>Nürnberg                   | IT-Security Projekt / IT-<br>Security Project   | Graduate               | Computer Science  |
| Germany | Uni Erlangen-<br>Nürnberg                   | IT-Sicherheits-<br>Konferenzseminar / IT-<br>Security Conference Seminar  | Graduate               | Computer Science  |
| Germany | Goethe Universität<br>Frankfurt a. M.       | Informations- und<br>Kommunikationssicherheit:<br>Infrastrukturen, Technologien<br>und Geschäftsmodelle /<br>Information and<br>Communication Security -<br>Infrastructures, technologies,<br>and business models | Graduate               | Computer Science, Business<br>Informatics   |
| Germany | Goethe Universität<br>Frankfurt a. M.       | Privacy vs. Data: Business<br>Models in the digital, mobile<br>Economy  | Graduate               | Computer Science  |
| Germany | Goethe Universität<br>Frankfurt a. M.       | Identity management in the<br>crossroad: business interests<br>and users' privacy   | Graduate               | Computer Science, Business<br>Informatics   |

|         |                                       |   |          |  |
|---------|---------------------------------------|---|----------|--|
| Germany | Goethe Universität Frankfurt a. M.    | Mobile Business II - Application Design, Applications, Infrastructures and Security           | Graduate | Computer Science   |
| Germany | Goethe Universität Frankfurt a. M.    | Privacy in Online and Enterprise Social Networks  | Graduate | Computer Science   |
| Germany | Westfälische Hochschule Gelsenkirchen | Datenschutz und Ethik / Data Protection and Ethics  | Graduate | Internet Security  |
| Germany | Westfälische Hochschule Gelsenkirchen | Internet-Sicherheit A + B / Internet Security A + B   | Graduate | Internet Security  |
| Germany | Westfälische Hochschule Gelsenkirchen | Programmiermethodik und Sicherheit / Programming methodology and Security                     | Graduate | Internet Security  |
| Germany | Westfälische Hochschule Gelsenkirchen | Grundlagen der IT-Sicherheit / Fundamentals of IT Security                                    | Graduate | Internet Security  |
| Germany | TU Hamburg-Harburg                    | Application Security  | Graduate | Computer Science/Engineering, Information and Media Technologies,    |
| Germany | TU Ilmenau                            | Network Security  | Graduate |  |
| Germany | TU Ilmenau                            | Schutz von Kommunikationsinfrastrukturen / Protection of Communications Infrastructure        | Graduate |  |
| Germany | Universität Karlsruhe                 | Fortgeschrittene Verschlüsselungstechniken / Advanced Ciphering Techniques                    | Graduate |  |
| Germany | Universität Karlsruhe                 | Praktikum Kryptographie und Datensicherheit / Practical Course Cryptography and Data Security | Graduate | Computer Science and Similar Disciplines                             |
| Germany | Universität Koblenz-Landau            | IT-Risk-Management  | Graduate | Information Management, Computer Science, Computational Visualistics |

|         |                            |  |          |   |
|---------|----------------------------|--|----------|---|
| Germany | Universität Koblenz-Landau | Sicherheit und Zuverlässigkeit für mobile Anwendungen / Security and reliability for mobile applications | Graduate | Information Management, Computer Science, Computational Visualistics  |
| Germany | Universität Lübeck         | SOA, Sicherheit und Runtime-Verifikation / SOA, Security and Runtime Verification                        | Graduate | Computer Science  |
| Germany | Universität Lübeck         | Sicherheit in Netzen und Verteilten Systemen / Security in Networks and Distributed Systems              | Graduate | Computer Science  |
| Germany | Universität Magdeburg      | Multimedia and Security  | Graduate | Computer Visualistics, Business Informatics, Computer Systems in Engineering, Computer Science, Data & Knowledge Engineering                              |
| Germany | Universität Magdeburg      | Selected Chapters of IT Security   | Graduate | Computer Visualistics, Computer Systems in Engineering, Computer Science, Business Informatics, Computational Mathematics, Data and Knowledge Engineering |
| Germany | Universität Magdeburg      | Advanced Security Issues in Medical Systems  | Graduate | Medical Systems Engineering   |
| Germany | Universität Magdeburg      | Praktikum IT Sicherheit / Practical Course IT Security   | Graduate | Computer Science, Computer Visualistics, Business Informatics, Computer Systems in Engineering, Data & Knowledge Engineering                              |
| Germany | LMU München                | IT-Sicherheit - Sicherheit vernetzter Systeme  | Graduate | Computer Science, Media Computer Science  |
| Germany | Universität Potsdam        | Network Security in Practice   | Graduate | IT Systems Engineering  |
| Germany | Universität Potsdam        | Privacy and Security in IPv6   | Graduate | IT Systems Engineering  |
| Germany | Universität Potsdam        | Sicherheit in komplexen IT-Landschaften / Security in complex IT environment                             | Graduate | IT Systems Engineering  |
| Germany | Universität Regensburg     | Sicherheit datenintensiver Anwendungen / Security of data-intensive applications                         | Graduate | Business Informatics  |

|         |                         |   |               |   |
|---------|-------------------------|---|---------------|---|
| Germany | Universität Siegen      | Kryptographische Verfahren und Anwendungen I / Cryptographic processes and applications I   | Graduate      |   |
| Germany | Universität Siegen      | Kryptographische Verfahren und Anwendungen II / Cryptographic processes and applications II   | Graduate      |   |
| Germany | Universität Trier       | Moderne Kryptographie (IT-Sicherheit III) / Modern Cryptography (IT-Security III)   | Graduate      | Computer Science, Business Informatics, Applied Mathematics |
| Germany | Universität Trier       | Ausgewählte Kapitel der Informationssicherheit und Kryptographie (IT-Sicherheit IV) / Selected Topics on Information Security and Cryptography (IT-Security IV) | Graduate      | Computer Science, Business Informatics                      |
| Germany | Universität Augsburg    | Safety and Security   | Undergraduate | Computer Science  |
| Germany | Universität Augsburg    | Internetsicherheit / Internet security  | Undergraduate | Computer Science  |
| Germany | Ruhr-Universität Bochum | Vertiefungspraktikum Security Appliances / Immersion Practical Course Security Appliances   | Undergraduate | IT Security/Information Technology                          |
| Germany | FH Bonn-Rhein Sieg      | Sicherheit in Netzen / Network Security   | Undergraduate | Computer Science  |
| Germany | TU Braunschweig         | Grundlagen der Sicherheit in Netzen und verteilten Systemen / Foundations of Network Security and Distributed Systems   | Undergraduate | Computer Science  |
| Germany | Universität Dortmund    | Werkzeugunterstützung für sichere Software / Tool support for secure Software   | Undergraduate | Computer Science, Applied Computer Science                  |
| Germany | Universität Dortmund    | Fachprojekt Softwaretechniken für sichere Cloud-Computing Systeme / Project Software techniques for secure Cloud-Computing Systems                              | Undergraduate | Computer Science, Applied Computer Science                  |

|         |                            |   |               |  |
|---------|----------------------------|---|---------------|--|
| Germany | TU Dresden                 | Sicherheit in Computersystemen / Security in Computer Systems                         | Undergraduate | Computer Science, Media Computer Science   |
| Germany | TU Dresden                 | Datenschutz in der Anwendungsentwicklung / Data protection in Application Development | Undergraduate | Computer Science, Media Computer Science   |
| Germany | Uni Erlangen-Nürnberg      | IT-Sicherheits-Konferenzseminar / IT-Security Conference Seminar                      | Undergraduate | Computer Science, Medical Engineering  |
| Germany | TU Hamburg-Harburg         | Computersicherheit / Computer Security  | Undergraduate | Information Technology   |
| Germany | Universität Koblenz-Landau | Datenschutz / Data Protection   | Undergraduate | Information Management, Business Informatics   |
| Germany | Universität Koblenz-Landau | Grundlagen der IT-Sicherheit / Fundamentals of IT Security                            | Undergraduate | Information Management, Computer Science, Computational Visualistics                           |
| Germany | Universität Magdeburg      | Sichere Systeme / Secure Systems  | Undergraduate |  |
| Germany | Universität Magdeburg      | Secure Infrastructures Project  | Undergraduate | Computer Science, Business Informatics, Computer Visualistics, Computer Systems in Engineering |
| Germany | Universität Magdeburg      | Ausgewählte Kapitel der IT-Sicherheit / Selected Chapters of IT-Security              | Undergraduate | Computer Science, Business Informatics, Computer Visualistics, Computer Systems in Engineering |
| Germany | Universität Magdeburg      | Sicherheitsfragen eingebetteter Systeme / Safety Issues of Embedded Systems           | Undergraduate | Computer Science, Business Informatics, Computer Systems in Engineering, Computer Visualistics |
| Germany | Universität Magdeburg      | Grundlagen IT-Sicherheit / Fundamentals of IT Security                                | Undergraduate | Computer Science, Business Informatics, Computer Systems in Engineering, Computer Visualistics |
| Germany | Universität Potsdam        | Internet Security: Weaknesses and Targets   | Undergraduate | IT Systems Engineering   |
| Germany | Universität Regensburg     | IT-Security I   | Undergraduate | Business Informatics   |

|         |   |   |                          |   |
|---------|---|---|--------------------------|---|
| Germany | Universität Regensburg                          | IT-Security II  | Undergraduate            | Business Informatics  |
| Germany | Universität Saarbrücken                         | Security and Privacy - A Beginner's Guide   | Undergraduate            |   |
| Germany | Universität Trier                               | Einführung in die Informationssicherheit (IT-Sicherheit I) / Introduction to Information Security (IT-Security I) | Undergraduate            | Computer Science, Business Informatics  |
| Germany | Universität Trier                               | System- und Netzwerksicherheit (IT-Sicherheit II) / System and Network Security (IT-Security II)                  | Undergraduate            | Computer Science, Business Informatics, Applied Mathematics   |
| Germany | Universität Bamberg                             | Informationssicherheit / Information and Security   | Undergraduate / Graduate | Computer Science  |
| Germany | Ruhr-Universität Bochum                         | Aktuelle Themen der IT-Sicherheit / Recent Topics in IT Security  | Undergraduate / Graduate | Applied Computer Science, IT Security/Information Technology  |
| Germany | Ruhr-Universität Bochum                         | Embedded Security   | Undergraduate / Graduate | Applied Computer Science, Electrical Engineering and Information Technology, IT Security/Information Technology |
| Germany | Ruhr-Universität Bochum                         | Sichere Hardware / Secure Hardware  | Undergraduate / Graduate | Electrical Engineering and Information Technology, IT Security/Information Technology                           |
| Germany | Ruhr-Universität Bochum                         | Projekt Netz- und Datensicherheit / Project Network and Data Security   | Undergraduate / Graduate | Applied Computer Science, IT Security/Information Technology  |
| Germany | TU Chemnitz                                     | Datensicherheit / Data Security   | Undergraduate / Graduate | Digital Manufacturing, Computational Science, Computer Science, Mathematics, etc.                               |
| Germany | Brandenburgische Technische Universität Cottbus | IT-Sicherheit in kritischen Infrastrukturen / IT-Security in critical infrastructures                             | Undergraduate / Graduate | Computer Science, eBusiness, Information and Media Technology   |
| Germany | TU Darmstadt                                    | Security, Privacy and Trust   | Undergraduate / Graduate | Computer Science (or related areas, such as electrical engineering)   |

|         |                       |   |                          |   |
|---------|-----------------------|---|--------------------------|---|
| Germany | Universität Dortmund  | Sicherheit: Fragen und Lösungsansätze / Security: Questions and Solution Approaches                     | Undergraduate / Graduate | Computer Science, Data Science  |
| Germany | TU Dresden            | Security and Cryptography II  | Undergraduate / Graduate | Computer Science, Media Computer Science  |
| Germany | TU Dresden            | Technischer Datenschutz / Technical Data Privacy  | Undergraduate / Graduate | Computer Science, Media Computer Science, Information Systems Engineering   |
| Germany | TU Dresden            | Komplexpraktikum Kryptographie und Datensicherheit / Practical course on Cryptography and Data Security | Undergraduate / Graduate | Computer Science, Media Computer Science  |
| Germany | TU Dresden            | Security and Cryptography I   | Undergraduate / Graduate | Computer Science, Media Computer Science, Computational Engineering, Computational Logic  |
| Germany | TU Dresden            | Kryptographische Grundlagen der Datensicherheit / Cryptographic Fundamentals of Data Security           | Undergraduate / Graduate | Computer Science, Media Computer Science  |
| Germany | Uni Erlangen-Nürnberg | Angewandte IT-Sicherheit / Applied IT-Security  | Undergraduate / Graduate | Computer Science  |
| Germany | Fernuniversität Hagen | Sicherheit im Internet I / Internet Security I  | Undergraduate / Graduate | Computer Science  |
| Germany | TU Hamburg-Harburg    | Software Security   | Undergraduate / Graduate | Computer Science/Engineering, Information and Media Technologies, Information and Communication Systems, Electromagnetic Theory |
| Germany | TU Hamburg-Harburg    | Network Security  | Undergraduate / Graduate | Computer Science/Engineering, Information and Media Technologies, Information and Communication Systems, Electromagnetic Theory |
| Germany | Universität Karlsruhe | Sicherheit / Security   | Undergraduate / Graduate | Computer Science  |

|         |                         |   |  |   |
|---------|-------------------------|---|--|---|
| Germany | RWTH Aachen             | Selected Topics in IT-Security  |  |   |
| Germany | RWTH Aachen             | Selected Topics in IT-Security and Cryptography   |  |   |
| Germany | Ruhr-Universität Bochum | Betriebssystemsicherheit / Operating System Security  |  | IT Security/Information Technology  |
| Germany | Ruhr-Universität Bochum | Systemsicherheit I + II / Systems Security I + II   |  | Applied Computer Science, Electrical Engineering and Information Technology, IT Security/Information Technology |
| Germany | Ruhr-Universität Bochum | Netzicherheit I + II / Network Security I + II  |  | Electrical Engineering and Information Technology, IT Security/Information Technology                           |
| Germany | Ruhr-Universität Bochum | Praktische Aspekte der Cybersicherheit / Practical Aspects of Cyber Security  |  | IT Security/Information Technology  |
| Germany | Ruhr-Universität Bochum | XML- und Webservice-Sicherheit / XML and Webservice Security  |  | Applied Computer Science  |
| Germany | TU Chemnitz             | Praktikum Theoretische Informatik und Informationssicherheit / Practical Course Theoretical Computer Science and Information Security |  | Computer Science, Applied Computer Science  |
| Germany | TU Darmstadt            | Secure, Trusted and Trustworthy Computing   |  |   |
| Germany | TU Darmstadt            | Embedded System Security  |  |   |
| Germany | TU Darmstadt            | Practical Lab on Smartphone Security  |  |   |
| Germany | TU Darmstadt            | Physical Layer Security in Drahtlosen Systemen / Physical Layer Security in Wireless Systems  |  |   |
| Germany | TU Darmstadt            | Praktikum Sichere Mobile Netze / Practical Course on Secure Mobile Networks   |  |   |
| Germany | TU Darmstadt            | Ausgewählte Themen der Netzicherheit / Selected topics of Network Security  |  |   |

|         |                       |   |  |                  |
|---------|-----------------------|---|--|------------------|
| Germany | TU Darmstadt          | Mining Facebook   |  | Computer Science |
| Germany | TU Darmstadt          | Praktikum Smartphone Sicherheit für Android Applikationen / Practical Course Smartphone Security for Android Applications |  |                  |
| Germany | TU Darmstadt          | Implementierung in Forensik und Mediensicherheit / Implementation in IT-Forensics and Multimedia Security                 |  |                  |
| Germany | TU Darmstadt          | Security and Privacy in Information Technology  |  |                  |
| Germany | TU Darmstadt          | Sicherheit von SDN / Security of SDN  |  |                  |
| Germany | TU Darmstadt          | Cryptography, Privacy and Security  |  |                  |
| Germany | TU Darmstadt          | Building and Breaking Comply Software Systems   |  |                  |
| Germany | TU Darmstadt          | Implementing Secure & Reliable Software   |  |                  |
| Germany | TU Darmstadt          | Security and the Cloud - The Issues and Metrics   |  |                  |
| Germany | TU Darmstadt          | Smart Grid Informatics and Trustworthiness  |  |                  |
| Germany | TU Darmstadt          | Cloud Security  |  | Computer Science |
| Germany | Universität Freiburg  | Sicherheit in BPM / Security in BPM   |  | Computer Science |
| Germany | Universität Freiburg  | IT-Sicherheit / IT-Security   |  | Computer Science |
| Germany | Universität Freiburg  | Security and Risk Management  |  | Economics        |
| Germany | Universität Freiburg  | Privacy and Security in der Informationsgesellschaft / Privacy and Security in the Information Society                    |  | Computer Science |
| Germany | Universität Freiburg  | Sicherheitstechnologien der Informationsgesellschaft / Resilient Business Process Management                              |  | Computer Science |
| Germany | Fernuniversität Hagen | Parallelverarbeitung und IT-Sicherheit / Parallel processing and IT Security  |  | Computer Science |

|         |                         |  |  |  |
|---------|-------------------------|--|--|--|
| Germany | Fernuniversität Hagen   | Sicherheitsgerichtete Echtzeitsysteme / Safety-related real-time Systems   |  |  |
| Germany | Fernuniversität Hagen   | IT-Sicherheit Konzepte, Standards, Verfahren und Anwendungen / IT Security Concepts, Standards, Proceedings and Applications |  |  |
| Germany | Universität Hamburg     | Verteilte Systeme und Informationssicherheit / Distributed Systems and Information Security                                  |  |  |
| Germany | TU Hamburg-Harburg      | Introduction to Security   |  |  |
| Germany | TU Hamburg-Harburg      | IT Security Risk Management  |  |  |
| Germany | Universität Karlsruhe   | Asymmetrische Verschlüsselungsverfahren / Asymmetric Cipherring Methods  |  |  |
| Germany | Universität Karlsruhe   | Seitenkanalangriffe in der Kryptographie / Side Channel Attacks in Cryptography  |  |  |
| Germany | Universität Karlsruhe   | Beweisbare Sicherheit in der Kryptographie / Verifiable Security in Cryptography   |  |  |
| Germany | Universität Karlsruhe   | Symmetrische Verschlüsselungsverfahren / Symmetric Cipherring Methods  |  |  |
| Germany | Universität Magdeburg   | Biometrics and Security  |  |  |
| Germany | TU München              | Sichere mobile Systeme / Secure mobile systems   |  |  |
| Germany | TU München              | IT-Sicherheit / IT-Security  |  |  |
| Germany | TU München              | Practical Course Web Application Security  |  |  |
| Germany | Universität Rostock     | Rechnernetze und Datensicherheit / Computer Networks and Data Security   |  |  |
| Germany | Universität Rostock     | Datensicherheit / Data Security  |  |  |
| Germany | Universität Saarbrücken | Language-Based Security  |  |  |

|         |   |   |                   |  |
|---------|---|---|-------------------|--|
| Germany | Universität Saarbrücken                 | Security  |                   |  |
| Germany | Universität Saarbrücken                 | Hot Topics in Security & Privacy  |                   |  |
| Germany | Universität Saarbrücken                 | Privacy Enhancing Technologies (PETs)   |                   |  |
| Germany | LMU, TU, Uni Augsburg                   | IT-Security   | master-level      | computer science   |
| Greece  | University of Piraeus                   | Digital Systems Security  | Graduate (MSc)    | Computer Science/Computer Engineering/Information Systems/Communication Systems                        |
| Greece  | University of the Aegean                | Information & Communication Systems Security                                    | Graduate (MSc)    | Computer Science/Computer Engineering/Information Systems/Communication Systems                        |
| Italy   | Università degli Studi di Milano        | Computer and network security (Sicurezza dei Sistemi e delle Reti Informatiche) | Undergraduate     | Computer Science   |
| Italy   | Università degli Studi di Milano        | Information Security  | Graduate (master) | Computer Science - Security  |
| Italy   | University of Modena and Reggio Emilia  | Master on "Information security and Legal disciplines"                          | Graduate          | Computer science, Computer engineering, Law  |
| Italy   | University of Modena and Reggio Emilia  | Master on "Digital forensics"   | Graduate          | Computer science, Computer engineering   |
| Italy   | University of Modena and Reggio Emilia  | Master on "Cyberdefence"  | Graduate          | Computer science, Computer engineering   |
| Italy   | Politecnico di Milano                   | Security Specialist   | Graduate          | Computer Science   |
| Italy   | Università degli Studi di Milano        | Computer and network security (Sicurezza dei Sistemi e delle Reti Informatiche) | Undergraduate     | Computer Science   |
| Italy   | Università degli Studi di Milano        | Information Security  | Graduate (master) | Computer Science - Security  |
| Italy   | UCBM Univerity CAMPUS BioMedico di Roma | Master in Homelaand Security  | Post-graduated    | Economic, Law, Risk Management, Cybersecurity, Physical Security, Technologies, Complex Systemn Design |
| Italy   | University of Catania                   | Internet Security   | Undergraduate     | Computer Science   |
| Italy   | University                              | Computer Security   | Graduate          | Computer Science   |
| Italy   | University of Padua                     | Computer and Network Security   | Graduate          | Computer Science   |

|             |  |   |               |   |
|-------------|--|---|---------------|---|
| Luxembourg  | University of Luxembourg in collaboration with CRP Henri Tudor | Master in "Information Systems Security Management" | Master        | Computer science  |
| Netherlands | Eindhoven University of Technology                             | Cryptography I                                      | Graduate      | Information Security Technology   |
| Netherlands | Eindhoven University of Technology                             | Verification of Security Protocols                  | Graduate      | Information Security Technology   |
| Netherlands | Eindhoven University of Technology                             | Information Security Technology                     | Graduate      | Information Security Technology   |
| Netherlands | Eindhoven University of Technology                             | Hacker's Hut  | Graduate      | Computer Science & Engineering, Information Security Technology, Service Design and Engineering |
| Netherlands | Eindhoven University of Technology                             | Cryptography II                                     | Graduate      | Information Security Technology   |
| Netherlands | Eindhoven University of Technology                             | Physical Aspects of Digital Security                | Graduate      | Information Security Technology   |
| Netherlands | Radboud University Nijmegen                                    | Hardware Security                                   | Graduate      | Computing Science, Information Security Technology  |
| Netherlands | Radboud University Nijmegen                                    | Privacy Seminar                                     | Graduate      | Computing Science, Information Security Technology  |
| Netherlands | Radboud University Nijmegen                                    | Law in Cyberspace                                   | Graduate      | Computing Science, Information Science, Information Security Technology                         |
| Netherlands | Radboud University Nijmegen                                    | Software Security                                   | Graduate      | Computing Science, Information Security Technology  |
| Netherlands | Radboud University Nijmegen                                    | Security in organisations                           | Graduate      | Computing Science, Information Science, Information Security Technology                         |
| Netherlands | Radboud University Nijmegen                                    | Software & Web Security 1                           | Undergraduate | Computer Science  |
| Netherlands | Radboud University Nijmegen                                    | Software & Web Security 2                           | Undergraduate | Computer Science  |
| Netherlands | University of Twente   | Security and Privacy in Mobile Systems              | Graduate      | Computer Science, Information Security Technology   |

|             |                                 |  |                       |  |
|-------------|---------------------------------|--|-----------------------|--|
| Netherlands | University of Twente            | Secure Data Management                               | Graduate              | Computer Science, Information Security Technology  |
| Netherlands | University of Twente            | Network Security                                     | Graduate              | Business Information Technology, Computer Science, Electrical Engineering, Telematics, Information Security Technology |
| Netherlands | University of Twente            | Cyber Crime Science                                  | Graduate              | Computer Science, Information Security Technology  |
| Netherlands | Vrije Universiteit Amsterdam    | Computer and Network Security                        | Graduate              | Computer Science, Parallel and Distributed Computer Systems  |
| Netherlands | Vrije Universiteit Amsterdam    | Advanced Topics in Computer and Network Security     | Graduate              | Parallel and Distributed Computer Systems  |
| Norway      | University of Oslo              | Security in distributed systems                      | Graduate              |  |
| Norway      | University of Oslo              | Security in operation systems and software           | Graduate              |  |
| Norway      | University of Oslo              | Information Security                                 | Undergraduate         |  |
| Norway      | University of Oslo              | Intrusion detection and firewalls                    | Graduate              |  |
| Norway      | University of Oslo              | Unassailable IT-systems                              | Graduate              |  |
| Norway      | NTNU - Trondheim                | Wireless Network Security                            | Second degree level   |  |
| Norway      | NTNU - Trondheim                | ICT-Security Evaluation                              | Doctoral degree level |  |
| Norway      | NTNU - Trondheim                | Information Security                                 | Second degree level   |  |
| Norway      | NTNU - Trondheim                | Software Security                                    | Second degree level   |  |
| Norway      | NTNU - Trondheim                | Cryptographic Protocols and Their Applications       | Doctoral degree level |  |
| Norway      | NTNU - Trondheim                | Cryptography   | Second degree level   |  |
| Norway      | Gjøvik University College (GUC) | Introduction to Information Security                 | Undergraduate         | Information Security   |
| Norway      | Gjøvik University College (GUC) | Introduction to Information Security Risk Management | Undergraduate         | Information Security   |
| Norway      | Gjøvik University College (GUC) | Data Communication and Network Security              | Undergraduate         | Information Security   |

|        |                                 |   |               |                      |
|--------|---------------------------------|---|---------------|----------------------|
| Norway | Gjøvik University College (GUC) | Introduction to security Plannin and Incident Handling  | Undergraduate | Information Security |
| Norway | Gjøvik University College (GUC) | Software Security   | Undergraduate | Information Security |
| Norway | Gjøvik University College (GUC) | Ethical Hacking and Penetration Testing   | Undergraduate | Information Security |
| Norway | Gjøvik University College (GUC) | Introduction to Cryptology  | Undergraduate | Information Security |
| Norway | Gjøvik University College (GUC) | Digital Forensics   | Undergraduate | Information Security |
| Norway | Gjøvik University College (GUC) | Cryptology I  | Graduate      | Information Security |
| Norway | Gjøvik University College (GUC) | Applied Information Security  | Graduate      | Information Security |
| Norway | Gjøvik University College (GUC) | Legal Aspects of Information Security   | Graduate      | Information Security |
| Norway | Gjøvik University College (GUC) | Socio-technical Security Riks Modeling and Analysis 1   | Graduate      | Information Security |
| Norway | Gjøvik University College (GUC) | Foundations of Information Security   | Graduate      | Information Security |
| Norway | Gjøvik University College (GUC) | Cryptology II   | Graduate      | Information Security |
| Norway | Gjøvik University College (GUC) | Software Security Trends  | Graduate      | Information Security |
| Norway | Gjøvik University College (GUC) | Security as Continuous Improvement  | Graduate      | Information Security |
| Norway | Gjøvik University College (GUC) | Security Management Dynamics  | Graduate      | Information Security |
| Norway | Gjøvik University College (GUC) | Security Planning and Incident Management   | Graduate      | Information Security |
| Norway | University of Stavanger         | Risk Analysis and Risk Management   | Graduate      |                      |
| Spain  | Almeria                         | Especialista en Seguridad Informática, IT Security specialist   | Postgrad      | Computer science     |
| Spain  | Leon                            | MASTER PROFESIONAL EN TECNOLOGÍAS DE LA SEGURIDAD, Proffesional master in Security Technology   | Postgrad      | Computer science     |
| Spain  | UOC, URiV, UAB                  | MISTIC: Máster interuniversitario de seguridad de las tecnologías de la información y de las comunicaciones, Interuniverstity master in | Postgrad      | Computer science     |

|        |  |   |          |                                 |
|--------|--|---|----------|---------------------------------|
|        |  | technology and communication security   |          |                                 |
| Spain  | Deusto   | Diploma de especialización en Seguridad de la información, IT security speclaization  | Postgrad | Computer science                |
| Spain  | UAX  | Máster Universitario en Ingeniería de Seguridad de la Información y las Comunicaciones, Communications and information security                                 | Postgrad | Computer science                |
| Spain  | UAM  | Máster en Auditoría, Seguridad, Gobierno y Derecho de las TIC, master in IT audit Security governance and law   | Postgrad | Computer science                |
| Spain  | Uc3M   | Máster Universitario en Ciberseguridad, Cybersecurity master  | Postgrad | Computer science                |
| Spain  | UDIMA  | Máster en Dirección de Seguridad de la Información. Information security direction  | Postgrad | Computer science                |
| Spain  | UE   | MÁSTER UNIVERSITARIO EN SEGURIDAD DE TECNOLOGÍAS DE LA INFORMACIÓN Y DE LAS COMUNICACIONES, master in technology and communication security                     | Postgrad | Computer science                |
| Spain  | UNIR   | máster universitario en seguridad informática, IT security  | Postgrad | Computer science                |
| Spain  | UNED   | MÁSTER EN SISTEMAS DE GESTIÓN DE SEGURIDAD INFORMÁTICA, IT security systems governance  | Postgrad | Computer science                |
| Spain  | UPM  | DIRECCIÓN Y GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN, Information security governance   | Postgrad | Computer science                |
| Spain  | CEU  | Máster Internacional Universitario en Protección de Datos, Transparencia y Acceso a la Información, Data protection, transparency and information access master | Postgrad | Law                             |
| Spain  | CEU  | Máster en Seguridad de la Información, Information security master  | Postgrad | Computer science                |
| Spain  | Centro Universitario de Tecnológica y Arte Digital (U-TAD) | Master Indra en Ciberseguridad  | Graduate | Computer Science, Cybersecurity |
| Sweden | Chalmers   | Computer Security   | Graduate | computer science                |

|                |  |   |           |                       |
|----------------|--|---|-----------|-----------------------|
| Sweden         | Chalmers                               | Network Security  | Graduate  | computer science      |
| Sweden         | Chalmers                               | Language-based security                                     | Graduate  | computer science      |
| Sweden         | Chalmers                               | Cryptography  | Graduate  | computer science      |
| Sweden         | Chalmers                               | ICT Support for Adaptiveness and Security in the Smart Grid | Graduate  | computer science      |
| Sweden         | Linköping University                   | Software Security   | Undergrad | Computer science      |
| Sweden         | Linköping University                   | Information Security, Second Course                         | Undergrad | Computer science      |
| Sweden         | Linköping University                   | Information Security, Introduction                          | Undergrad | Computer science      |
| United Kingdom | Cardiff Metropolitan University (UWIC) | Information & Communication Technology Management           | Graduate  | Technology Management |
| United Kingdom | Cardiff University                     | Computer Science with placement                             | Graduate  | Computer Science      |
| United Kingdom | Cardiff University                     | Information Security & Privacy                              | Graduate  | Computer Science      |
| United Kingdom | City University, London                | Information Security and Risk                               | Graduate  | Information Systems   |
| United Kingdom | Coventry University                    | Forensic Computing  | Graduate  | Computer Science      |
| United Kingdom | Cranfield University                   | Cyber Defence and Information Assurance                     | Graduate  | Computer Science      |
| United Kingdom | Cranfield University                   | Forensic Computing  | Graduate  | Computer Science      |
| United Kingdom | De Montfort University, Leicester      | Cybersecurity   | Graduate  | Computer Science      |
| United Kingdom | Edge Hill University                   | Information Security and IT Management                      | Graduate  | Computer Science      |
| United Kingdom | Edinburgh Napier University            | Advanced Security and Cybercrime                            | Graduate  | Computer Science      |
| United Kingdom | Edinburgh Napier University            | Advanced Security and Digital Forensics                     | Graduate  | Computer Science      |
| United Kingdom | Essex University                       | Computer Networks and Security                              | Graduate  | Computer Science      |
| United Kingdom | Glasgow Caledonian University          | IT Security   | Graduate  | Computer Science      |
| United Kingdom | Glasgow Caledonian University          | Network Security  | Graduate  | Computer Science      |
| United Kingdom | Heriot-Watt University, Edinburgh      | Advanced Internet Applications                              | Graduate  | Computer Science      |
| United Kingdom | Imperial College London                | MSc in Computing (Secure Software Systems specialism)       | Graduate  | Computer Science      |

|                |   |  |          |                  |
|----------------|---|--|----------|------------------|
| United Kingdom | Kings College (University of London)          | Computing and Security                                   | Graduate | Computer Science |
| United Kingdom | Kingston University                           | Network and Information Security with Management Studies | Graduate | Computer Science |
| United Kingdom | Kingston University                           | Network and Information Security                         | Graduate | Computer Science |
| United Kingdom | Lancaster University                          | Cyber Security   | Graduate | Computer Science |
| United Kingdom | Leeds Metropolitan University                 | Digital Forensics & Security                             | Graduate | Computer Science |
| United Kingdom | Liverpool Hope University                     | Networks and Security                                    | Graduate | Computer Science |
| United Kingdom | Liverpool John Moores University              | Computer Network Security                                | Graduate | Computer Science |
| United Kingdom | London Metropolitan University                | Computer Forensics and IT Security                       | Graduate | Computer Science |
| United Kingdom | London Metropolitan University                | Computer Networking with Security                        | Graduate | Computer Science |
| United Kingdom | London Metropolitan University                | Network Management and Security                          | Graduate | Computer Science |
| United Kingdom | Loughborough University                       | Communication Networks, Security and Forensics           | Graduate | Computer Science |
| United Kingdom | Loughborough University                       | Internet Computing and Network Security                  | Graduate | Computer Science |
| United Kingdom | Middlesex University                          | Computer and Network Security                            | Graduate | Computer Science |
| United Kingdom | Middlesex University                          | Electronic Security and Digital Forensics                | Graduate | Computer Science |
| United Kingdom | Newcastle University                          | Advanced Computer Science                                | Graduate | Computer Science |
| United Kingdom | Newcastle University                          | Computer Security and Resilience                         | Graduate | Computer Science |
| United Kingdom | Nottingham Trent University                   | Internet and Security                                    | Graduate | Computer Science |
| United Kingdom | Oxford University                             | Software Engineering                                     | Graduate | Computer Science |
| United Kingdom | Robert Gordon University                      | Information and Network Security                         | Graduate | Computer Science |
| United Kingdom | Royal Holloway, London (University of London) | Information Security                                     | Graduate | Computer Science |
| United Kingdom | Sheffield Hallam University                   | Information Systems Security                             | Graduate | Computer Science |
| United Kingdom | Staffordshire University                      | Computer Networks and Security                           | Graduate | Computer Science |
| United Kingdom | University College (University of             | Information Security                                     | Graduate | Computer Science |

|                |                                  |  |          |                     |
|----------------|----------------------------------|--|----------|---------------------|
|                | London)                          |  |          |                     |
| United Kingdom | University of Bath               | Internet Systems and Security                      | Graduate | Computer Science    |
| United Kingdom | University of Bedfordshire       | Computer Security and Forensics                    | Graduate | Computer Science    |
| United Kingdom | University of Bedfordshire       | Computer Forensics and IT Security                 | Graduate |                     |
| United Kingdom | University of Birmingham         | Computer Security                                  | Graduate | Computer Science    |
| United Kingdom | University of Bradford           | Internet, Computer and System Security             | Graduate | Computer Science    |
| United Kingdom | University of Central Lancashire | IT Security  | Graduate | Computer Science    |
| United Kingdom | University of Derby              | Information Security                               | Graduate | Information Systems |
| United Kingdom | University of East London        | Information Security and Computer Forensics (ISCF) | Graduate | Computer Science    |
| United Kingdom | University of Glasgow            | Information Security                               | Graduate | Computer Science    |
| United Kingdom | University of Glasgow            | Information Technology                             | Graduate | Computer Science    |
| United Kingdom | University of Gloucestershire    | Computing (Information Security)                   | Graduate | Computer Science    |
| United Kingdom | University of Greenwich          | Computer Forensics and the Law                     | Graduate | Computing and Law   |
| United Kingdom | University of Greenwich          | Information Security and Audit                     | Graduate | Information Systems |
| United Kingdom | University of Greenwich          | Computer Forensics and Cyber Security              | Graduate | Computer Science    |
| United Kingdom | University of Greenwich          | Network and Computer Systems Security              | Graduate | Computer Science    |
| United Kingdom | University of Kent               | Computer Security                                  | Graduate | Computer Science    |
| United Kingdom | University of Kent               | Networks and Security                              | Graduate | Computer Science    |
| United Kingdom | University of Leicester          | Security and Risk Management                       | Graduate | Law                 |
| United Kingdom | University of Manchester         | Computer Security                                  | Graduate | Computer Science    |
| United Kingdom | University of Northampton        | Computing (Internet Technology and Security)       | Graduate | Computer Science    |
| United Kingdom | University of Plymouth           | Computer and Information Security                  | Graduate | Computer Science    |
| United Kingdom | University of Plymouth           | Network Systems Engineering                        | Graduate | Computer Science    |
| United Kingdom | University of Portsmouth         | Communication Network Planning and Management      | Graduate | Computer Science    |

|                |   |   |               |                     |
|----------------|---|---|---------------|---------------------|
| United Kingdom | University of Portsmouth                | Computer Network Administration and Management      | Graduate      | Computer Science    |
| United Kingdom | University of Portsmouth                | Forensic Information Technology                     | Graduate      | Computer Science    |
| United Kingdom | University of Portsmouth                | Computer and Information Security                   | Graduate      | Computer Science    |
| United Kingdom | University of Salford                   | Information Security                                | Graduate      | Information Systems |
| United Kingdom | University of South Wales               | Computer Systems Security                           | Graduate      | Computer Science    |
| United Kingdom | University of South Wales               | Computer Forensics                                  | Graduate      | Computer Science    |
| United Kingdom | University of South Wales               | Computer Systems Security                           | Graduate      | Computer Science    |
| United Kingdom | University of Southampton               | Corporate Risk and Security Management              | Graduate      | Business Studies    |
| United Kingdom | University of Surrey                    | Security Technology and Applications                | Graduate      | Computer Science    |
| United Kingdom | University of the West of England (UWE) | Network Systems includes Securing Networks          | Graduate      | Computer Science    |
| United Kingdom | University of Westminster               | Computer Forensics                                  | Graduate      | Computer Science    |
| United Kingdom | University of Wolverhampton             | Cybersecurity and Digital Forensics                 | Graduate      | Computer Science    |
| United Kingdom | University of York                      | Cyber Security                                      | Graduate      | Computer Science    |
| United Kingdom | Warwick University                      | Cyber Security and Management (CSM)                 | Graduate      | Computer Science    |
| United Kingdom | The Open University                     | Digital Forensics (M812)                            | Graduate      | Computer Science    |
| United Kingdom | The Open University                     | Information Security (M811)                         | Graduate      | Computer Science    |
| United Kingdom | The Open University                     | Network Security (T828)                             | Graduate      | Computer Science    |
| United Kingdom | University of Kent                      | Advanced MSc in Computer Security                   | Post Graduate | CS                  |
| United Kingdom | University of Kent                      | Advanced MSc in Networks and Security               | Post Graduate | CS                  |
| United Kingdom | University of Kent                      | Advanced MSc in Information Security and Biometrics | Post Graduate | CS, Biometrics      |

## Appendix 3. List of secondary sources evaluated

1. *Cybersecurity Curricula in European University*. Final report, 2003. Available at: [www.fondazionerosSELLi.it/DocumentFolder/Cyber\\_Final.pdf](http://www.fondazionerosSELLi.it/DocumentFolder/Cyber_Final.pdf)
2. MARTIN C. LIBICKI, DAVID SENTI, JULIA POLLAK. *H4CKER5 WANTED*. An Examination of the Cybersecurity Labor Market. Rand Corporation Security Research Division, 2014
3. *An overview of international cyber-security awareness raising and educational initiatives: Research report commissioned by the Australian Communications and Media Authority*. May 2011.
4. Andrew McGettrick *Toward Curricular Guidelines for Cybersecurity: Report of a Workshop on Cybersecurity Education and Training*. Association of Computer Machinery, August 2013.
5. IBM Center for Applied Insights. *Cybersecurity education for the next generation: Advancing a collaborative approach*. 2013.
6. Tempus. *Report on EU practice for cyber security education*. 2013.
7. Michael Locasto, Sara Sinclair. *An Experience Report on Undergraduate Cyber-Security Education and Outreach*. 2009.
9. *BIS Skills Report* {correct citation needed}

## Bibliography

---

<sup>i</sup> Available at: [www.fondazionerosSELLi.it/DocumentFolder/Cyber\\_Final.pdf](http://www.fondazionerosSELLi.it/DocumentFolder/Cyber_Final.pdf)