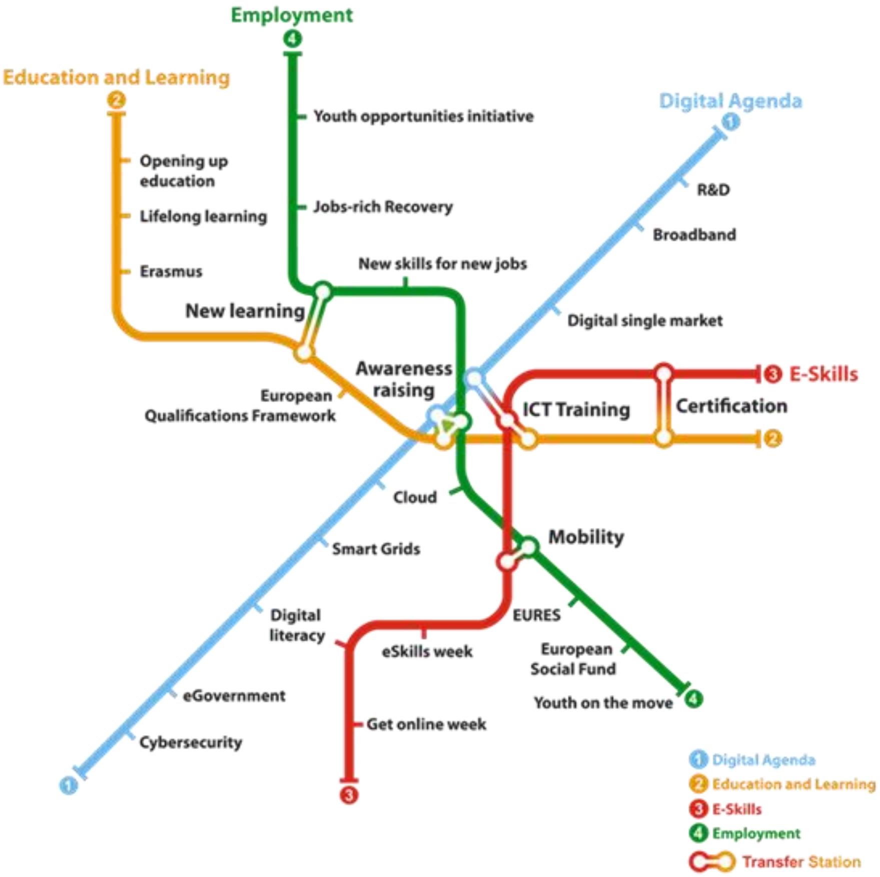


Roadmap for NIS education programmes in Europe

Education

October 2014

enisa

European Union Agency for Network and Information Security

www.enisa.europa.eu

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its Member States, the private sector, and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU Member States in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU Member States by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Authors

Bettina Berendt, KU Leuven, Belgium

Stefano De Paoli, Abertay University, Dundee, UK

Christopher Laing, Northumbria University, UK

Simone Fischer-Hübner, Karlstad University, Sweden

Daria Catalui, ENISA

Rodica Tirtea, ENISA

Contact

To contact the authors, please use stakeholderrelations@enisa.europa.eu.

For media enquires about this paper, please use press@enisa.europa.eu.

Acknowledgements

ENISA would like to thank the following people/teams for their feedback on this report: DG CONNECT team, Antonio Ramos - ISACA Madrid; ECDL; PRIPARE support action team; NIS Platform WG3.

Legal notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to (EU) Regulation No 526/2013. This publication does not necessarily represent state-of the-art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources, including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Copyright Notice

Catalogue number ISBN/DOI/EN TP-04-14-677-EN-N 978-92-9204-090-1 10.2824/32639

Executive summary

ENISA is one of the key stakeholders in Europe in the area of Network and Information Security (NIS). Given its positioning, ENISA is active in the area of education and awareness, using its knowledge to promote NIS skills and supporting the Commission in enhancing the skills and competence of professionals in this area. This document continues work from previous activities by suggesting training materials, scenarios and a way forward for implementing the EC roadmap for NIS education in Europe ([1]). In doing so, the Agency has recognised the heterogeneous landscape of Europe in this area.

This work was done in collaboration with educators for educators. The primary targets of this report are professors and trainers that have daily activities in NIS education. The secondary target of this report is policy-makers in the field of NIS education, those that make the decision on what enters the curricula and which new courses are adopted.

The report is structured in three parts. The first part maps the courses and materials available. The second part presents the gaps between existing training/certification schemes and market needs, including proposals of scenarios to narrow the existing gaps. Finally, a list of recommendations is presented for further steps and an open call from ENISA is available ([2]) in order to identify leading organisations best positioned to further work on the implementation:

- the authors suggest the creation of a Europass for NIS skills for the general public, very much in line with the model from CEDEFOP([3]);
- Deploying better continuing education programmes for teachers for enhancing the multiplier role they have. Solutions offered in scenario “Continuing Education for teachers”.
- European organisations and authorities should start developing NIS MOOCs. Section on MOOCs with examples.
- Developing a NIS course for health practitioners. Examples accessible in “Healthcare scenario”.
- Developing a Data Protection Officers (DPOs) course directed at lawyers and digital security specialists. Structure presented in “Data Protection Officers scenario”.
- Development of an EU information assurance training/education solution for the working realities of SMEs. Presented in “Small and Medium Enterprises scenario”.
- Development of an EU-based academic recognition for continuing professional development in digital forensics. Solutions accessible in “Digital Forensics scenario”.

Furthermore, we invite the reader to consult the tools developed through this project:

- ✓ the interactive map with NIS courses in Europe([4])
- ✓ the NIS quiz addressed to all users for updating knowledge([5])

([1]) Mentioned in the EU Cyber Security strategy page 8: http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf
([2]) In the news item announcing this report on ENISA webpage
([3]) About Europass: https://europass.cedefop.europa.eu/en/home
([4]) NIS courses in Europe: http://cybersecuritymonth.eu/references/universities
([5]) NIS quiz addressed to all users for updating knowledge: http://cybersecuritymonth.eu/references/quiz-demonstration

Table of Contents

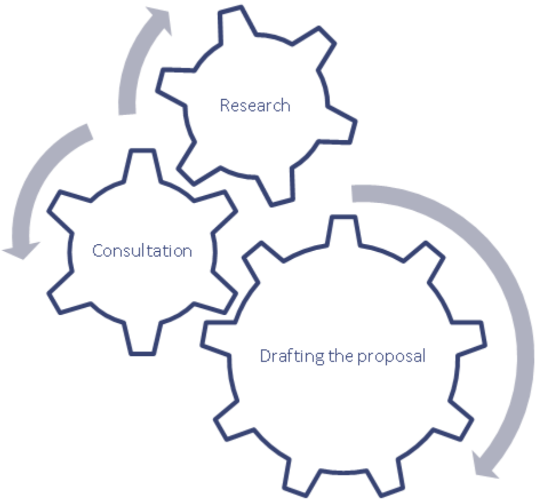
1 Introduction

The EU Cybersecurity Strategy 'An Open, Safe and Secure Cyberspace' ([6]) asks for the development of a roadmap for a 'Network and Information Security driving licence' as a voluntary certification programme to promote enhanced skills and competence of professionals.

ENISA has started the consultation process in order to involve the relevant stakeholders and guide the process in order to ensure quality results and the publication of a report. This report introduces the roadmap and its first steps that describe the certification ecosystem, relevant policies, stakeholders involved, and the gaps that need to be addressed with innovative solutions.

ENISA is well positioned to respond to the challenge, taking into consideration the brokerage that it has been achieving in the NIS environment in general and in NIS in Education in particular with the publication of annual reports ([7]) in these areas.

The process followed for preparing this current report included a research phase, a large consultation effort in order to involve all relevant stakeholders, and drafting the final document. The process is depicted in the image below:



1.1 Policy context and the perspective of this work

As mentioned in the introduction, the EU Cyber Security Strategy "An Open, Safe and Secure Cyberspace" suggests the development of a roadmap for Network and Information Security, as a voluntary certification programme to promote enhanced skills and competence of professionals. As we describe in this document, we are supporting this objective of the EU Cyber Security Strategy, by proposing an NIS /cybersecurity pass.

Furthermore, the EU Cyber Security Strategy acknowledges that cybersecurity can only be sound and effective if it is based on fundamental rights and freedoms. Any information sharing for the purposes

[6] http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1667
[7] NIS in Education reports http://www.enisa.europa.eu/activities/stakeholder-relations/nis-brokerage-1/brokerage-model-for-network-and-information-security-in-education

of cyber security, when personal data is at stake, should be compliant with EU data protection law ([8]) and take full account of the individuals' rights in this field.

The Strategy also acknowledges the need for a: “voluntary certification programme to promote enhanced skills and competence of IT professionals (e.g. website administrators)”, “training on NIS in schools”, “training on NIS and secure software development and personal data protection for computer science students” and “NIS basic training for staff working in public administrations”.

As such, our document has a broader perspective, from a general level of information security knowledge for training in schools, basic knowledge to public administration personal – that needs to understand security and data protection requirements –, up to specialized knowledge addressed to IT professionals – responsible for managing, designing or developing secure IT systems and applications that comply with data protection requirements.

1.2 Objectives

The main goals of this work are to define the roadmap and introduce steps that can be implemented in order to be in line with best practice in NIS education.

The objectives of the roadmap are:

1. Provide an initial market analysis of the courses and certification schemes available.

2. Identify gaps between available training courses, certifications and NIS education needs.

3. Suggest scenarios to narrow the gaps and provide best practices to organizations from all Member States.

4. Plan further actions based on the needs of NIS communities.

5. Identify and select partners to continue and disseminate the work.

Regarding potential strategies to exchange best practices, ENISA will use its existing NIS education communities to disseminate the work. e.g. the ECSM (European Cyber Security Month) community, the NIS in Education group, partner universities, etc.

Representatives of NIS organisations that will show interest in this report and that want to contribute should check the suitability of the proposed scenarios and suggest a way forward for implementation.

1.3 Target audience

This work has been prepared in collaboration with educators for educators. Professors and trainers that have daily activities in NIS education represent the primary target. The secondary target is represented by policy-makers in the field of NIS education, those that make the decision on what enters the curricula and which new courses are adopted.

Note that this report tackles not only IT administrators but a larger audience, including training and education solutions as already mentioned in the section dedicated to the perspective of this work.

([8]) More here http://ec.europa.eu/justice/data-protection/

1.4 Structure of this document

This report will unfold in three different parts: firstly, a mapping of the available courses and certifications schemes; secondly, a presentation and discussion of the gaps in current courses and certifications and the presentation of new scenarios whose goal is to offer a way forward to fill the identified gaps; and thirdly, a series of recommendations for further considerations.

We identified the topics of the scenarios by taking into account objectives of policy strategies, the policy context and provisions, the experience of the experts group, and the advice of the European Commission. For the purpose of this report we used desktop research and large consultation with representatives of different organisations part of the consultative group. We formed the consultative group as a result of a public announcement of this project.

In addition, the report benefits from the existence of some extra material:

1. A useful tool is the interactive map with NIS courses in Europe available on www.cybersecuritymonth.eu compiled with the help of by the NIS Platform WG3 group.
2. A NIS quiz addressed to all users for updating knowledge available on www.cybersecuritymonth.eu.

2 Mapping the available courses and materials

This part of the study provides the reader with an overview of existing education materials, curricula and courses. Furthermore, as the intention of this work is to provide way forward to address the existing gaps, in this part we provide some scenarios to address existing needs, such as the lack of proper data protection education for NIS professionals or for personal data processors.

2.1 Initiatives to gather information on existing certification and training programmes

2.1.1 Cyber Security Month programmes database

In the context of the European Cyber Security Month initiative, a database has been established where available courses and certification programmes linked to NIS and privacy/data protection are listed. This database of available courses and certifications programmes is not an exhaustive list. The data presented has come from work produced by the NIS Platform WG 3 members, whom we thank for their collaboration. Furthermore, the webpage allows educational institutions to add to the map courses, programmes and training that deal with Network and Information Security. We invite the reader to access the web address[9].

2.1.2 Privacy and security related educational information and reference material

PReparing Industry for Privacy by design by supporting its Application in REsearch (PRIPARE) ([10])

PRIPARE is a two-year FP7 support action ([11]) aimed at identifying and developing processes and tools capable of facilitating the widespread application of a Privacy and Security by Design methodology.

Recognizing the essential role of stakeholders' information and education about the risks, tools, best practices, rights, and responsibilities associated with digital security and privacy, PRIPARE provides educational information and reference material for the following set of stakeholders: general public, ICT educators, ICT practitioners, policy-makers, and governmental and non-governmental bodies acting for human rights protection. After a detailed analysis of stakeholder groups, their knowledge needs were identified ([12]) and project partners are currently producing and testing educational, information and reference material addressing these needs. Once validated, this material will be made available online ([13]) in modular format.

Stakeholder analysis for PRIPARE support action. Sub-groups of stakeholders within the large categories mentioned above have been identified and, for each one of these sub-groups, their informational/educational needs have been defined in terms of the learning outcomes that the educational material produced within the project should trigger. The general public was analysed on the basis of their level of vulnerability. Practitioners were considered in terms of their professional role, either managerial or development. The study of students' needs was based on the type of their degree (technical versus non-technical), the level of study (graduate, undergraduate), and career goals. Regarding policy and legal stakeholders, we have identified policy-makers and governmental bodies acting at different geographical levels (national, European, international) as well as non-governmental bodies, including NGOs, think tanks, civil society organisations, and legal professionals.

([9]) ECSM http://cybersecuritymonth.eu/references/universities

([10]) **This section represents the contribution of the PRIPARE team.**

([11]) PRIPARE project public website: http://www.pripareproject.eu

([12]) PRIPARE project, deliverable D4.1 Educational Requirements to Foster Risk Management Culture (Draft — March '14), available at http://pripareproject.eu/research/

([13]) PRIPARE project repository: http://pripare.aup.edu/

Information Learning Modules of PRIPARE support action. The modules being produced respond to the knowledge needs identified in the stakeholder analysis phase, address privacy risks (c1-c5) and focus on privacy rights (e.g. OECD Privacy Guidelines, EU Data Protection Directive, EU ePrivacy Directive, etc.). Each module is implemented in the format best suited for communication of the specific content to the specific stakeholder group, ranging from standard slide presentations to crossword puzzles, from videos to infographics, from exercise series to structured references to academic literature, etc. Sets of modules can be compiled to create curricular structures, workshop material, individual lectures, awareness campaigns, etc. The complete list of modules is described in the PRIPARE deliverable 4.1[14]. Below are a few examples of modules for two of the stakeholders groups: the general public and the engineering practitioners.

Modules for the general public aim to raise awareness about Privacy by Design (PbD), the dangers of privacy violations and users' rights; they also explain the actions users may take in case of privacy infringement. They cover PbD in specific contexts, the tools for privacy protection, and methodologies for risk management. Modules for practitioners introduce PbD principles and concepts; themes include privacy context (the legal context as a source of privacy requirements for a software development process), risk management (what it is and its benefits for a software development process, privacy impact assessment as a risk management methodology applied to PbD), best practices (e.g. privacy patterns), technologies and solutions for privacy protection, and finally, the testing and validating of the outcomes of the PbD process. Other specific knowledge modules for engineering practitioners cover privacy patterns, privacy failures, Privacy Design Strategies, location privacy, anonymous cash, etc.

Modules Assessment in PRIPARE support action. Assessment work includes initiatives such as a seminar providing training on Privacy by Design to members from academia, EU research projects, and industry with a focus on technology ([15]), a round table with DPAs ([i]), and university courses. In a course designed by members of the PRIPARE consortium ([16]), it demonstrates how Privacy by Design may be effectively taught to a combined group of undergraduate and graduate students in the social sciences whose knowledge of technology is limited to their own user experience. The curriculum explores a new educational space at the theoretical intersection of human rights and digital technology while integrating a practical component that allows students to produce educational materials for stakeholder audiences; this merging of theory and practice provides our students with the opportunity to reflect on the convergence of law and technology. The curriculum incorporates Ann Cavoukian's set of seven guiding principles ([17]) as core learning objectives and uses the principles in contexts that are not limited to Privacy by Design, showing how they can effectively be applied to other contexts at the interface of human rights and digital technology. Each of Cavoukian's seven principles is addressed through the lens of a case study, with issues selected on the basis of their cross-cutting impact.

Regardless of whether the high level of user mistrust concerning privacy protection of digital information is justified, international human rights law and the robust Data Protection Regulation proposed by the European Commission require protection of online privacy. Educational materials for various types of stakeholders were produced in interaction with students. The focus is on the practical problem of how to best implement the right to privacy on a day-to-day basis. Providing an already mistrustful population with privacy-enhancing knowledge and tools is a seminal example of the mis en oeuvre of participatory action research methods. By transferring privacy principles to the larger

([14]) http://pripareproject.eu/resources/

([15]) See work-package 3 at http://pripareproject.eu/research/

([16]) Perry, S., Roda, C. Teaching Privacy by Design to Non-Technical Audiences. Cyber Security and Privacy (CSP) Forum 2014. Springer CCIS series, forthcoming.

([17]) Cavoukian, A.: Foundational Principles (Privacy by Design). (1997) Retrieved 22.5.2014 at http://www.privacybydesign.ca/index.php/about-pbd/7-foundational-principles/

domain of human rights and digital technology, students were able to view security and privacy protection as part of a larger exploration of how we are going to live in a digitally connected society. Only by privileging the broader perspective can we deliver on the promise of digital technology to enhance democratic dialogue and facilitate human lifestyles, and make sure that it is safe to use for the generations to come.

Expected Uses of the Material and Outcomes of PRIPARE support action. The Consortium of the project hopes that the information-educational material produced by the project will facilitate the dissemination and application of Privacy by Design principles and methodology. On one hand, the modules will increase stakeholders' familiarity with their privacy-related rights and responsibilities and with the current and potential technical solutions aimed at supporting the effective implementation of such rights and responsibilities. On the other hand, the modules will promote a mature reflection on the impact of privacy choices (both technical and regulatory) on societal structures such as businesses, industry, education, healthcare, transportation, etc. Overall, the educational material will disseminate the results and support the vision of the PRIPARE project to help 'forge sustainable links between the different privacy stakeholders (regulators, educators, engineers and standardisation organisms) in order to set the necessary common grounds on which to build trustworthy and privacy-respectful systems' ([18]).

2.2 NIS programmes for school education: an overview

School education is one factor used to reach the goal of helping minors to use the Internet in a 'safe' way and is widely perceived as an important component for improving cybersecurity ([19]). Reflecting on this perceived importance, a multitude of materials and associated activities such as training events and certification are being offered to teachers on the Web. The materials that we surveyed do not refer to a common theoretical or even terminological base ([20]). Therefore, we begin this section by proposing a structure on the basic concepts that will allow us to then overview and relate materials to one another. Based on this overview, we will make a proposal for a more comprehensive training programme in the scenario of Section 3.1.4.

THE BASIC CONCEPTS: CYBER RISKS AND SAFETY

In line with the well-known observation that doom scenarios do not have educational effects, the Internet/Web is introduced as a space full of opportunities but also of *risks*. In the following, we will call these *cyber risks*. The goal of the educational intervention is to turn this situation into a safe (or safer) space ([21]): thus, *safety* is implicitly defined to be a state in which these risks are mitigated. (As in other spaces with risk, a complete elimination is probably not possible, although this is not discussed explicitly.) The focus is on threats to the individual (here: the minor, the pupil) and on precautions that the individuals themselves can take to mitigate the risks. The effects that one person's privacy-related behaviour has on others mostly remain implicit: the Internet will be safer/better for all if all exhibit safe behaviour. Thus, cyber risks, the state in which they are mitigated and safety are conceived of similarly to, for example, road traffic.

[18] Nicolás Notario McDonnell, Alberto Crespo, Antonio Kung, Inga Kroener, Daniel Le Métayer, Carmela Troncoso, José María Del Álamo and Yod Samuel Martín. PRIPARE: A New Vision on Engineering Privacy and Security by Design. Cyber Security and Privacy (CSP) Forum 2014. Springer CCIS series, forthcoming.

[19] As an example, see the ENISA (2012) Report Collaborative Solutions for Network Information Security in Education. http://www.enisa.europa.eu/activities/stakeholder-relations/nis-brokerage-1/collaborative-solutions-for-network-information-security-in-education

[20] In fact, Vanderhoven et al. (2014) observe that most materials are not based on any theory and that only very few have been evaluated. Vanderhoven, E., Schellens, T., & Valcke, M. (2014). Educational packages about the risks on social network sites: state of the art. Procedia — Social and Behavioural Sciences, 112, 603-612.

[21] An example is the activities around the annual 'Safer Internet Day'; see below.

A TAXONOMY OF CYBER RISKS

The cyber risks typically discussed comprise (a) the risk of encountering inappropriate material which may comprise disturbing materials (violence, sexual content) or materials that can easily be misinterpreted especially by minors (false information, satire, etc.); (b) the risk of committing a criminal or otherwise sanctioned act oneself (copyright violations, plagiarism); and, increasingly, (c) a range of cybersecurity issues that typically involve violations of the pupil's own personal sphere or that of his/her friends ([22]). We use cybersecurity in the sense of 'the state of being protected from the criminal, unauthorised or otherwise undesired use of data, computer hardware or software' ([23]) and the notion that 'security' is a form of 'safety' that focuses on being protected against external threats ([24]). We do not regard (a) or (b) as cybersecurity issues because their focus is not on a personal sphere or a computational environment being intruded upon. However, it should be noted that the categories are not mutually exclusive. For example, pupil A may utter 'hate speech' (category b or verging on it) that deeply troubles pupil B (category a). Also, if pupil A cyberbullies pupil B, this may be both criminal and invasive of B's personal sphere (and damaging to A too). Within such a mixed set of problems, we will focus on their contribution to category (c) risks.

A TAXONOMY OF CYBERSECURITY RISKS

In the remainder of this section and in line with this report focus, we will concentrate on category (c), the cybersecurity issues deemed relevant for the school education of minors. The criterion of dividing (c) into sub-categories reflects the origin of the type of risk under consideration.

(c.1) *Contact risks* ([25]): abuses of data that identifies an individual

These risks comprise third parties (other people) communicating with the individual in undesired and often unexpected ways. Examples include cyberbullying and grooming ([26]). Such risks may be intensified by the frequency with which minors interact with strangers online ([27]). In general, a main reason leading to these risks is the abuse of identifying personal data given away voluntarily by the individual.

(c.2) *Invisible audiences* and *context collapse* ([28]) unintended/inappropriate audiences for data that profile an individual

[22] This top-level taxonomy is inspired by De Moor et al. (2008), reused by Vanderhoven et al. (2014).

[23] This combines the definition from the Oxford English Dictionary ('The state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this', http://www.oxforddictionaries.com/definition/english/cybersecurity) and whatis.com ('Cybersecurity is the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access. […]'. http://whatis.techtarget.com/definition/cybersecurity) Other definitions are broader still, highlighting only the protection aspect without detailing what to protect against, for example the definition by the International Telecommunication Union: 'Cyber security is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organisation and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment.' Definitions focusing on 'unauthorised' uses assume fully rational decision-makers. However, since privacy and security violations often occur after consent has been given only implicitly, or even after informed consent, we added 'or otherwise undesired'.

[24] http://www.dailywritingtips.com/safety-and-security/

[25] The term is due to De Moor et al. (2008) and Vanderhoven et al. (2014). De Moor, S., Dock, M., Gallez, S., Lenaerts, S., Scholler, C., & Vleugels, C. (2008). Teens and ICT: Risks and opportunities. Belgium: TIRO. Retrieved from http://www.belspo.be/belspo/fedra/TA/synTA08_en.pdf

[26] ENISA report on Grooming http://www.enisa.europa.eu/media/press-releases/new-report-cyber-bullying-online-grooming-18-protective-recommendations-against-key-risks

[27] Sharples, M., Graber, R., Harrison, C., & Logan, K. (2009). E-Safety and Web 2.0 for Children Aged 11-16. Journal of Computer Assisted Learning, 25(1), 70-84.

[28] The term is due to Boyd (2008), and the problem is widely discussed in the privacy literature. Boyd DM (2008) Taken out of context: American teen sociality in networked publics. ProQuest.

A second sub-class deals with the possible consequences of the permanence of information and its uses out of the context for which it was intended. Among other things, this may involve 'the wrong people getting a piece of information, maybe in the future'. In educational materials, this is usually projected to a few socially stereotyped behaviours and their assumed consequences: alcohol, (near-) nudity, and swearing are portrayed as 'risky information' (and thus, implicitly, their opposites as 'safe') with regard to impressions made on teachers, peers, and potential future employers (e.g. Moreno et al., 2009 ([29]); Vanderhoven et al., 2013 ([30])). The main reason leading to these risks is the decontextualised use, generally by peers or other people, of communication and profiling personal data given away voluntarily by the individual. A twofold strategy is recommended against these risks: (a) to use access control options ('privacy settings') judiciously when sharing *any* information and (b) to not share 'risky information' at all over social media, since even with carefully selected audiences, future (ab)uses cannot be predicted or prevented.

While this approach can be helpful, it is also problematic because of its often only implicit ethical judgements and the assumption of stable and predictable categories of 'risky information'. This may lead to the illusion that by simply not sharing *this* type of information (but sharing everything else), one can be 'safe'. The learning objective should not only be to avoid these risks, but also to appreciate and apply data minimisation as a general principle, to be aware that there can never be full certainty, and to use technology with a critical and informed perspective.

(c.3) Context collapse II: repurposing of data for commercial and other ends

Common notions of 'digital literacy' as a learning goal focus on knowledge and skills related to content risks and security risks (c.1) and (c.2). Other types of risks are currently covered less.

Some authors writing about school education analyse undesired uses of personal data by commercial entities (e.g. De Moor et al., 2008; Vanderhoven et al., 2014). These include the commercial misuse of personal data. Information can be shared with third companies via applications and user behaviour can be tracked in order to provide targeted advertisements and social advertisements ([31]). In addition to causing annoyance, profiling may also lead to *discrimination* in access to services, jobs, etc. A main reason leading to these risks is the decontextualised and repurposed use, by commercial entities, of personal data given away voluntarily by the individual.

(c.4) IT security risks include malware, phishing, pharming, or hacking. Some authors present empirical findings showing poor dealings with passwords among minors (sharing passwords with others, infrequently or never changing passwords, poor knowledge of what a strong password is ([32]). Reasons leading to these risks are the exploitation, by others, of weaknesses in computer software, hardware, and human naivety.

(c.5) Cybersecurity conflicts of interest in the fabric of society and democracy

The categories described so far (and most teaching materials) implicitly assume that safety, security and privacy are well-defined and generally agreed-upon values. However, as the privacy literature and current public debates show, this is not the case. Regarding protections against intrusions by peers (the main topic of categories (c.1) and (c.2), culture and education may work towards shared values of respect for other's spaces. However, this is less straightforward with regard to the relationships to

[29] Moreno, M. A., Vanderstoep, A., Parks, M. R., Zimmerman, F. J., Kurth, A., & Christakis, D. A. (2009). Reducing at-risk adolescents' display of risk behaviour on a social networking website: a randomized controlled pilot intervention trial. Archives of Paediatrics & Adolescent Medicine, 163(1), 35-41.

[30] Vanderhoven, E., Schellens, T., & Valcke, M. (2013). Exploring the Usefulness of School Education about Risks on Social Network Sites: A Survey Study. The Journal of Media Literacy Education, 5(1), 285-294.

[31] Debating, B., Lovejoy, J. P., Horn, A.-K., & Hughes, B. N. (2009). Facebook and online privacy: Attitudes, behaviours, and unintended consequences. Journal of Computer-Mediated Communication, 15(1), 83-108.

[32] Sharples et al. (2009), see above.

institutions (commercial entities as in category (c.3) or government entities). Individuals' and groups' rights to privacy vis-à-vis institutions may be legally protected, for example via data protection laws or fundamental rights such as informational self-determination (Germany) or the Fourth Amendment (U.S.A)[33]. However, other interests and rights held by the individual and/or others may conflict with these rights. These other interests and rights include contract freedom and the business model of financing a not-for-payment service by exploiting personal data, criminal investigations, or national security (for a critical discussion, see Solove, 2011 ([34])). Yet other rights such as freedom of speech are intimately tied up with privacy and security rights.

In other words, privacy and security are essential (and non-trivial) components of democracy and thus a necessary component of school education beyond informatics and also beyond the notion of digital literacy explained above. It is important to note that in this area of NIS education, the diversity of Europeans must be respected. Specifically, the nested identities of Europeans — as citizens of Europe but also of their respective country and maybe even region — implies that national laws and culture-specific histories and concepts, in particular of privacy, must be a focus of teaching in addition to pan-European or even global content. This would reflect the cultural diversity in the EU and the determining impact it has on education. Such diversity can occur at different levels.

Factors include national (or even personal) histories of regimes with intensive surveillance, such as in Germany or former communist states of Eastern and Central Europe, and likewise the histories of media coverage of and civic engagement against surveillance. School curricula themselves are a determining factor: is computer science being taught at all? (While it is well-entrenched in some European countries, it barely exists in others.) How much time can be allocated to a novel and cross-disciplinary content such as privacy/security education?([35]). Finally, "cultural variables" such as the relative focus on individualism vs. collectivism may affect the extent of learners' initiative and learning behaviour and therefore choices of didactic methods[36].

An overview of materials and training Events

In the following paragraphs, we give an exemplary overview of materials and training events, with a specific focus on European-level resources, and highlight their respective foci on selected categories of cyber risks/ cybersecurity risks. We also outline possible ways forward.

Basic requirements: ENISA has identified key points and success factors for teaching security in schools in the 2012 report 'Collaborative Solutions for Network Information Security in Education' ([37]). The report also contains descriptions and pointers to selected school projects, e.g. on the separation of digital identities (regarding risk category c.2). Key findings from the report are offered as downloadable posters that can be used for dissemination ([38]).

([33]) The right to informational self-determination was formulated in the German Federal Constitutional Court ruling on the Census of 1983: "[...] in the context of modern data processing, the protection of the individual against unlimited collection, storage, use and disclosure of his/her personal data is encompassed by the general personal rights of the German constitution. This basic right warrants in this respect the capacity of the individual to determine in principle the disclosure and use of his/her personal data. Limitations to this informational self-determination are allowed only in case of overriding public interest." This ruling has strongly influenced subsequent German and European data protection legislation. The Fourth Amendment of the US Constitution is "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." Surveillance and other privacy invasions are often regarded as breaches of the Fourth Amendment (e.g. Slobogin, C. (2008). Privacy at Risk: The New Government Surveillance and the Fourth Amendment. Chicago, IL: University of Chicago Press).

([34]) Solove, D. (2011). Nothing to hide. The false trade-off between privacy and security. Yale University Press.

([35]) As an example, see the observations recorded at HERE

([36]) e.g. M.S. Rosenberg, D.L. Westling, J. McLeskey (2008). Special Education for Today's Teachers: An Introduction, p. 63-64.]

([37]) https://www.enisa.europa.eu/activities/stakeholder-relations/nis-brokerage-1/collaborative-solutions-for-network-information-security-in-education

([38]) https://www.enisa.europa.eu/activities/stakeholder-relations/nis-brokerage-1/nis-in-education-infographics

Certification: The ECDL Foundation, a not-for-profit organisation of the European Professional Informatics Societies, offers the European Computer Driving Licence (ECDL), also known as the International Computer Driving Licence (ICDL). This is a computer literacy certification with several modules, one of which is IT Security ([39]), i.e. our category (c.4). Its focus lies on 'the secure use of ICT in daily life' and on 'managing data and information appropriately'.

ECDL/ICDL also recommends its certification for teachers, emphasizing the advantages of using ICT for teaching (e.g. creation of online content) and related and administrative tasks (e.g. online communication with students and parents, management of student data) ([40]).

Certification (accreditation) for institutions is discussed as a sub-point of European Schoolnet activities, to be discussed next.

European Schoolnet, a network of 31 European Ministries of Education, offers teaching materials and infrastructure for teacher collaboration, resources directly addressing pupils, activities and frameworks for pupil-/teacher-led activities, and a first step towards certification for schools as institutions:

- The **materials** collection *Insafe* in the Learning Resources Exchange: close to 300 resources on topics such as digital literacy, cyberbullying, safe searching, or privacy and personal information, with a focus on categories (a), (c.1), and (c.2) ([41]). Resource types vary, including lesson series descriptions and detailed materials, games, and interactive websites. Other materials have been created by the National Safer Internet Centres ([42]). Their foci resemble those of *Insafe* materials.
- **Infrastructure**: the European networking platform ([43]) for teachers.
- **Activities** framework: the annual Safer Internet Day ([44])
- **Institutional accreditation**: 'The eSafety Label offers an Assessment Form covering the broad range of actors who can impact, within and beyond the school walls, the level of eSafety of an educational institution. Based on a school's results, an Action Plan is drawn up to increase the level of eSafety, which might lead the way towards eSafety Label Accreditation […] ([45]). Sample questions indicate that the notion of 'eSafety' used covers (at least) selected aspects of IT security (c.4) such as protection against malware, and of privacy, such as having a school policy about taking photographs of and by pupils (c.2).
- **Incentive schemes**: ENISA and European Schoolnet created an award for 'Teaching online safety and citizenship' in schools ([46]) with the 2010 winner project focusing on contact risks (category c.1 above) and online games.

Teaching materials and training events on IT security: e-skills UK, the United Kingdom's sector skills council for the IT industry, offers teaching resources with a view to attracting pupils to cybersecurity careers. It offers various basic 20-30 minute modules on issues and methods mostly of category (c.4) such as phishing, hacking, digital forensics, and cross-curricular resources ([47]). More advanced

[39] http://www.ecdl.org/programmes/index.jsp?p=2928&n=2944

[40] 'ICT skills enable teachers to use technology more effectively in the teaching process, thus achieving educational goals more efficiently, and in doing so saving time, and increasing productivity in the classroom'. http://www.ecdl.org/index.jsp?p=100&n=330

[41] http://lreforschools.eun.org/web/guest/insafe

[42] Examples are http://www.saferinternetday.org/web/finland/home and http://www.klicksafe.de/ueber-klicksafe/die-initiative/project-information-en/

[43] http://www.etwinning.net

[44] http://www.saferinternetday.org/

[45] http://www.esafetylabel.eu/web/guest/esafetyschool

[46] https://www.enisa.europa.eu/media/press-releases/enisa-european-schoolnet-new-prize-for-teaching-of-online-safety-in-schools

[47] http://www.bigambition.co.uk/secure-futures/resources/

materials, partially in the form of (hacking) games, are available for A-Level students [48]. Similar initiatives, especially hackathons etc. focusing on spotting pupils with cybersecurity talents, are now emerging across Europe (for example, see the presentations at the 2014 ENISA Workshop on Cyber Security Issues in Europe [49]).

Teaching materials and training events about the economic and democratic issues of privacy and security: In spite of the growing perception of the importance of these issues (for example, see the sections on tracking and the monetisation of personal data in the 2012 ENISA report) and the presence of good work in the privacy literature, this is hardly covered in today's teaching materials. Exceptions include materials and lesson plans developed in the context of the interdisciplinary SPION ('Security and Privacy in Online Social Networks') project: from the short treatments of economic risks in the privacy manual [50], via its extension and evaluation in Vanderhoven et al [51]., to the lesson series 'If you're not paying for it, you're the product' [52] that explores the cybersecurity risk categories (c.3) and (c.5) in detail and in their interrelationship, and the teacher training workshop based on it [53].

Additional teaching forms: ISC2 (International Information Systems Security Certification Consortium), a membership body of certified information and software security professionals that is best known as a certification body (e.g. CISSP, accredited by ANSI as ISO Standard 17024:2003), offers one-hour presentation visits of volunteer security practitioners at schools [54]. Target groups are pupils aged 7-10 or 11-14 and parents. Judging from the content that is available online, content is a combination of issues from the categories (c.1), (c.2), and (c.4) (cf. The 'Safe and Secure Online Top 10 Tips' [55]).

Conclusions

In summary, this overview shows that:

- There is an abundance of materials and programmes for helping European teachers learn about and teach cybersecurity;
- While some cybersecurity risks and remedies are covered well (especially contact risks and invisible audiences / context collapse, with IT security being well-covered but only partially so for school purposes), others are touched on rarely (commercial risks such as the repurposing of personal data) or very rarely (privacy, security, and democracy);
- The non-uniform use of terms such as 'safety' and 'security' and various derivatives of these words, and the lack of definitions or theoretical underpinnings, may make it difficult for teachers to perceive, explore, and teach the field in a structured fashion. The risk is that lesson plans become a rather arbitrary collection of 'do's and don'ts' that seem unrelated and do not support deep learning, reflection, and transfer skills.

In the scenario described in Section 3.1.4, we will propose a way to improve on this situation.

[48] http://www.behindthescreen.org.uk/projects/cyber-security-advanced/

[49] https://www.enisa.europa.eu/activities/identity-and-trust/whats-new/cyber-security-chalenges-in-europe-workshop

[50] http://www.spion.me/publication/spion-deliverable-922-first-version-of-privacy-manual-for-educational-users-at-the-microlevel

[51] The various publications are aggregated and summarised in Vanderhoven, E. (2014). Raising risk awareness and changing unsafe behaviour on social network sites: A design-based research in secondary education. PhD Thesis, University of Ghent, Belgium, 2014.

[52] Berendt, B., Dettmar, G., Demir, C., & Peetz, T. (2014). Kostenlos ist nicht kostenfrei. LOG IN 178/179, 41-56. Links to teaching materials and English summary at http://people.cs.kuleuven.be/~bettina.berendt/Privacy-education/

[53] http://www.hyfisch.de/Fachgruppe/tagung13/ws1_2014

[54] https://www.isc2cares.org/Internet-security-for-kids-teachers/

[55] https://www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/SSO-Top-Ten-Tips.pdf: '1. Keep passwords private. 2. Think before you send. 3. Respect yourself and others. 4. Report bullying. 5. Keep all settings private. 6. Always log off. 7. Never meet an online only friend alone. 8. Tell someone if something makes you feel uncomfortable. 9. Keep personal information private. 10. Use these tips for smartphones too!'

2.3 NIS education roadmap and MOOCs

One of the goals of this report is also to provide an initial non-exhaustive map of NIS Education opportunities. A current trend in education is the emergence of MOOCs – Massive Online Open Courses [56]. MOOCs are a new way of delivering online education and cater for a wide audience, although there is debate on this. MOOCs are currently being used also to deliver NIS education, however the current status of MOOCs in this specific area is quite fragmented. In this section we provide an initial overview on the status of NIS MOOCs, also focusing on two key relevant aspects: a MOOC on the subject of Cybersecurity funded and supported by the UK Government as part of its Cybersecurity policy and a MOOCs platform launched by the EU Commission which can offer relevant opportunities within the EU context. Courses resemble university courses in terms of content and breadth, but the delivery model, assessment and peer collaboration is different from traditional university courses. MOOCs are delivered via tailored online platforms. In most cases they are free and open to access, but the platforms could be both commercial and non-commercial. They are often delivered by elite universities from Europe and the U.S. and hence there is the promise for top level education for a wider audience. However, MOOCs have so far seen a high level of enrolment coupled with a low level of completion [57]. However, it needs to be noted that, according to some commentators, the completion rate should not be considered as the key metric for MOOCs viability, and other benefits come from access to high quality material, peer collaboration, and learning experiences [58]. Data also shows that students completing MOOCs often already possess bachelor degrees [59]. This could be a relevant aspect to consider when the audience for this project module is mainly composed of IT professionals or teachers (i.e. professionals already possessing bachelor degrees) that would seek to obtain further training in specialised areas (e.g. NIS), via a MOOC module.

MOOCs could hence constitute an interesting avenue for NIS education and a way of delivering NIS Education modules to large audiences. This is an approach that can be potentially embraced by interested stakeholders. In particular, there are two aspects in this perspective that could contribute to the interests in MOOCs. Firstly, among Member States for instance, the UK is actively looking at MOOCs as part of its Cyber Security Strategy. In a document titled '*The National Cyber Security Strategy Our Forward Plans* [60]*'*, there is an indication that the government is investing in MOOCs as part of its plan to increase NIS training and in particular: '*the Open University is developing a Massive Open Online Course (MOOC) on cyber security to be run for the first time by summer 2014. The course has the potential to reach 200,000 students, including internationally. The MOOC is intended to run over an eight week period and will be presented four times a year for three years. The goal is to help raise awareness of cyber security among a mass audience as well as providing a high-quality course which will make the subject accessible to non-specialist learners and encourage those with an interest in the subject to study further*'. The Open University MOOC on Cyber Security has opened for registration in September 2014 and lecturing started in October of the same year. In the perspective of the NIS education roadmap, results of this MOOC (in terms of reached audience, attendance, and awareness raising) could offer indication for future diverse implementations of NIS modules via MOOC platforms. A second relevant aspect to consider is that the EU Commission is also looking at this delivery model with a focus on using MOOCs to bridge gaps in digital and IT skills. The Commission has

[56] See for an exhaustive review. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/240193/13-1173-maturing-of-the-mooc.pdf

[57] See, for instance, completion data from MIT and Stanford. http://www.edtechmagazine.com/higher/article/2014/02/harvardxs-and-mitxs-mooc-data-visualized-and-mapped

[58] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/240193/13-1173-maturing-of-the-mooc.pdf

[59] http://theinstitute.ieee.org/ieee-roundup/opinions/ieee-roundup/low-completion-rates-for-moocs

[60] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/265386/The_National_Cyber_Security_Strategy_Our_Forward_Plans_December_2013.pdf

already taken steps for '*launching a network of providers of MOOCs related to web and apps skills* [61].' European Commission Vice President Neelie Kroes, responsible for the Digital Agenda, said: '*By 2020, 90 % of jobs will need digital skills. That is just around the corner, and we aren't ready! Already businesses in Europe are facing a shortage of skilled ICT workers. We have to fill that gap, and this network we are launching will help us identify where the gaps are.*' [62] In addition to this, a pan-European MOOC platform [63] was launched by the Commission, financed through the Lifelong Learning Programme. This platform now hosts a number of MOOCs, some related to IT skills (e.g. computer programming, network architecture), but currently no course is directly related to NIS education.

MAPPING MOOC COURSES

The following is a non-exhaustive list of MOOCs in the area of NIS courses. Few of these are or were delivered by European universities and institutes with the majority being delivered by U.S. universities. This might be an aspect to consider in a pan-European perspective and offer a further recommendation for action with more NIS MOOCs delivered by European entities.

Title	URL	Provider	Platform
Public Privacy: Cyber Security and Human Rights	https://iversity.org/courses/public-privacy-cyber-security-and-human-rights	The Hague Institute for Global Justice	Iversity
IT Security	http://www.opencourseworld.de/pages/coursedescription.jsf?courseId=485951	Technischen Universität Darmstadt	OpenCourseWorld
Malicious Software and its Underground Economy: Two Sides to Every Story	https://www.coursera.org/course/malsoftware	University of London	Coursera
Information Security and Risk Management in Context	https://www.coursera.org/course/inforiskman	University of Washington	Coursera
Cybersecurity	https://www.coursera.org/specialization/cybersecurity/7?utm_medium=catalogSpec	University of Maryland	Coursera
Internet History, Technology, and Security	https://www.coursera.org/course/insidetheinternet	University of Maryland	Coursera
Usable Security	https://www.coursera.org/course/usablesec	University of Maryland	Coursera
Building an Information Risk Management Toolkit	https://www.coursera.org/course/inforisk	University of Washington	Coursera
Industrial cybersecurity	https://formacion-online.inteco.es/en/web/advanced-course-in-industrial-cybersecurity	INTECO	INTECO
Introduction to Cyber Security	https://www.futurelearn.com/courses/introduction-to-cyber-security	The Open University	FutureLearn

[61] http://europa.eu/rapid/press-release_IP-14-335_en.htm
[62] http://europa.eu/rapid/press-release_IP-14-335_en.htm
[63] http://www.openuped.eu/

3 Identifying gaps between available training courses, certifications and NIS job market needs

This section aims to describe the identified gaps between available training courses, certifications, and NIS needs. Furthermore, scenarios will be suggested to provide best practices to organizations from all Member States with the hope that, together with the consultative group, we may plan further actions based on the needs of NIS communities and identify partners to continue, implement, and disseminate the work.

3.1 Recommending NIS education scenarios for a pan-European Level

The scenarios were developed by following an agreed-on template with publicly available information from universities, institutions, and other projects.

The scenarios are put forward for wider debate and dissemination in order to achieve a truly consultative process. This can be considered as the theoretical part, phase one of the initiative, with a phase two to follow for implementation by public-private partnerships or single organisations that have the will and resources to put the scenarios into practice.

The scenarios can be implemented as activities for continuing professional development for professionals from the respective scenario’s target group(s). We would like to emphasize that these scenarios should be viewed as frameworks for concrete implementations. For example, concrete implementations should be adapted to their specific contexts (such as the duration of the course). Also, these scenarios can, by definition, only portray the area at the time at which this report was written. Given the rapid developments in the NIS area (in terms of technology, vulnerabilities, user behaviour and concerns) and also evolving legal frameworks, concrete implementations of the scenarios should strive to keep materials and course contents up-to-date.

3.1.1 Continuing Education for Teachers Scenario

Security and Privacy: Continuing Professional Development (CPD) for School Teachers	
Summary	According to a 2012 ENISA Report ([64]), '*Cyber security is generally in the hands of specialists who implement technical solutions. Citizens and SMEs (Small and Medium Enterprises) are left out of this action despite the fact that a thorough awareness of end users about cyber security is the first line of defence against cyber threats. As such, these players must be provided with the skills to protect their devices, their data, and their online identity*'. The Eurobarometer survey on cyber security ([65]) revealed that '*Most EU citizens do not feel very or at all well informed about the risks of cybercrime (59 %) while 38 % say they are very or fairly well informed. There is a clear link between being well informed and feeling confident online*'. The same survey also discovered socio-demographic variations, for instance, access to the Internet or type of crime in which citizens of different ages are victims. Among other categories of citizens, children and young adults deserve particular attention. On average, children start using the Internet at the age of 7. Together with quality content, they need to be provided with appropriate skills and awareness for ensuring their safety online. This scenario aims to close the gap identified in the 2012 ENISA report. It suggests an intervention on a specific target group whose multiplier role means that having increased capacities in terms of transferable NIS education skills could have a wide and lasting impact on EU society and its citizens, and in particular on children and young adults: **school teachers**. This target group is interesting not only because of their role as societal multipliers. Teachers are also a target group specifically interested in continuing professional development and 'life-long learning'. With informatics topics in particular, many school teachers face the challenge that pupils consider themselves more knowledgeable 'about computers', 'about social media', etc. than the teachers. To meet this challenge, it is particularly important that school teachers display and express well-founded, structured knowledge and reflection. In addition, a school itself is an environment in which practical measures can be tested and institutionalised (such as the responsible dealings with personal data of pupils, teachers, and other personnel). To the extent that teachers can be agents of change in this way, they can set examples for effective action orientation. In sum, we therefore consider developments of training activities for the target group of school teachers a possible blueprint for life-long learning activities which can also be used for other citizens.

([64]) http://www.enisa.europa.eu/activities/cert/other-work/eisas_folder/eisas-large-scale-pilot, p.1.
([65]) http://ec.europa.eu/public_opinion/archives/ebs/ebs_404_en.pdf

Target audience	School teachers of computer science and with other specialisations who want to offer courses on privacy and security for children and teenagers. This mix of participants is essential for our concept of security/privacy education being an overarching topic: neither only technical nor only social. Ideally, the courses will stimulate collaboration between teachers across traditional boundaries of their subjects. According to a Eurydice report, '*education on online safety (OS) is included in the school curriculum in 24 countries/regions'* ([66]), but the EU Kids Online Report remarks that '*in many countries, teachers provide little in the way of safety awareness and training to guide pupils' Internet use, though the range and adoption of new initiatives is now spreading*.' ([67]) Therefore, school teachers are those IT professionals that can be most effective as multipliers in today's society for broad segments of the population that will, in their own professional training later, not necessarily themselves receive privacy/security training but whose actions will determine privacy/security outcomes: i.e. those pupils who will not become IT professionals themselves or who will become IT professionals but will only have a narrow technological focus in their professional context experience.
Main stakeholders involved	• ECDL Foundation • ISC • SANS • European Schoolnet, eTwinning • National and regional teacher (training) associations
Current status	See Section 2.3.

Recommendations for Implementation

Objective: to reduce the gap between the need for NIS security skills in the wider EU society with a direct intervention on a key target group — school teachers. School teachers are those IT professionals that can be most effective as multipliers in today's society for broad segments of the population. This objective can be achieved by developing appropriate NIS education training modules targeted at teachers' needs and competences. We outline how these could be based on existing modules.

Implementation aspects:

- *Duration and other factors of context adaptation:* The duration of the course could differ from a standard smaller-scale professional development course spanning one or two full days to a more in-depth extension of qualification involving weekly meetings of 2-3 hours over a year or more. The requirements for duration of teacher CPD activities as well as the incentives given to teachers in the form of recognition for their job requirements, vary across European countries. We recommend an exploratory questionnaire concerning the breadth and depth of such a training among the target group in order to determine an

[66] http://eacea.ec.europa.eu/education/eurydice/documents/thematic_reports/121EN.pdf

[67] Livingstone, S, and Haddon, L (2009). EU Kids Online: Final report. LSE, London: EU Kids Online. (EC Safer Internet plus Programme Deliverable D6.5).
http://www.lse.ac.uk/media@lse/research/EUKidsOnline/EU %20Kids %20I %20 %282006-9 %29/EU %20Kids %20Online %20I %20Reports/EUKidsOnlineFinalReport.pdf, p. 21.

appropriate duration. Context adaptation should also take into account the participants' local legal and cultural context as explained in Section 2.3 of this report.

- *Continuing Professional Development:* Within a teacher's career, this can be a one-time CPD activity. This would most likely be the model if the course is of short duration. If the course is a longer-term qualification and, resources permitting (see 'basic structure'), it should be made possible for participants to update their knowledge by re-taking updated individual modules. In addition, other interested persons can use the online materials.

- *Specific properties of this course, added value compared to existing offers:* As detailed in Section 2.3, there are a multitude of offers on regional, national and European levels of materials, lesson plans, etc. for teachers of primary and secondary education on various notions of '(e)safety', 'security', 'privacy', etc. However, in spite of individual topics being covered well, the underlying notion(s) of these terms are often not explained, ethical assumptions are not questioned and often remain implicit, action orientation remains limited, and possible conflicts between different notions of 'security' (etc.) are neither identified nor discussed. This leads to fragmented knowledge and skills that are ill-suited to developing, let alone teaching, comprehensive security knowledge and skills. An additional shortcoming is that the privacy practices of teachers and schools are rarely discussed, although these are required for teachers to set a credible example. This course addresses this challenge by (1) devoting a full module to clarifying and discussing the different notions of 'security' and related terms; (2) including modules on each of these notions; and (3) in each module, and specifically in the additional module 6 on collaboration and continuing learning, also addressing teachers' own practices and possibilities for improving them. These modules can reuse materials from the existing stock; cf. the mapping between materials and risk types provided in Section 2.3 and used in the module descriptions.

- *Training* and *training the trainers*: All modules should help teachers in their own qualifications but also be a basis for their educational activities. Therefore, participants should be given ample opportunity to discuss their own teaching practice and to receive concrete ideas (case studies) as well as concrete materials that they can use or even full lesson series. Many such examples are included in the overview in Section 2.3.

Curriculum proposal: *basic structure:* The curriculum consists of six modules. Resources permitting, modules could be updated and revised in version numbers. Materials of previous instantiations of the course are made available online.

- Module 1: Different notions of 'security': safety, e-safety, security, cybersecurity, security and privacy, IT security and national security, 'good and bad hackers', etc.: untangling a conceptual mess and the inherent as well as the illusory conflicts and trade-offs between the different notions
    - This presents an overview and synopsis of the issues dealt with in modules 2-6, and invites participants' reflection and critical discussion of the course structure.

- Module 2: 'Security' in the sense of 'protection against inappropriate content and undesired audiences and contacts' with a special focus on problems affecting children and teenagers
    - This module focuses on cyber(security) risk types and 'content risks' (c.1) and (c.2). Course participants learn about problems that affect children and adolescents in particular but not only them (e.g. posting to 'inappropriate audiences' and/or sharing

- ‘inappropriate content’). Thus, the learning goal is also digital literacy for adults, including a reflection on (and possibly change of) one’s own behaviours.
    - Recommended specific topics in this module include: content risks, safe searching, contact risks (cyberbullying, grooming, etc.), and audience management (privacy settings).

- Module 3: ‘Security’ in the sense of ‘protection of personal data and privacy ’
    - This module focuses on cybersecurity risk type (c.3). Participants receive a comprehensive overview of privacy and data protection issues. Technical, computational, legal, and social aspects are covered with a special focus on helping participants develop lesson plans tailored to their subject and time constraints.
    - Recommended specific topics in this module include: basics of data-based web business models, interest conflicts between companies and users, tracking and anti-tracking tools and PETs, basics of data mining tasks and methods, data protection legislation, and practice.

- Module 4: ‘Security’ in the sense of ‘IT Security’
    - This module focuses on cybersecurity risk type (c.4). Participants learn theoretical foundations and practical skills. The goal is twofold: first, to learn (and be able to teach) protection measures for daily life; second, to help course participants create a secure IT environment at their schools which may include technical as well as social institutional arrangements. The module also deals with appropriate ways for pupils to participate in these measures. This module is key in that it shows to pupils, teachers, and school management that security is not something the individual can achieve alone. Joint efforts that can lead to ‘security accreditation’ for the school as an institution are described ([68]).
    - Recommended specific topics in this module include: basic safety measures such as dealing with passwords, communications and encryption, malware, social engineering such as phishing, network security, hacking, and secure data management.

- Module 5: ‘Security’ in the sense of ‘protection of fundamental rights and democracy’
    - This module focuses on cybersecurity risk type (c.5). In this module, the manifold relationships between IT, security, privacy, and society are discussed.
    - Recommended specific topics in this module include: ‘big Data’ and data mining; informational self-determination and free speech rights, surveillance, and chilling effects; privacy, transparency, and accountability; and ‘post-privacy’.

- Module 6: ‘Security’ in the sense of ‘protection against procrastination’
    - In this module, practical skills are introduced and exercised to enhance the sustainability of learning outcomes.
    - Recommended specific topics in this module include: methods for networking (e.g. joint teaching projects on the European level as supported by etwinning.net or its national analogues) as well as successful initiatives that foster student-centric learning (such as recent editions of the Safer Internet Day).

([68]) This discussion of accreditation and seals should, however, also discuss failures in the past (e.g. Rifon, N.J., LaRose, R., & Choi, S.M. (2005). Your privacy is sealed: Effects of web privacy seals on trust and personal disclosures. Journal of Consumer Affairs, (39):339-362). It should be made clear that security is never perfect and that having a seal or accreditation should not lead to an illusory sense of safety.

Estimated results: School teachers across EU Member States are trained, awareness is raised, and the level of online safety for young generations is enhanced. Institutional change is encouraged. There is also potential for having a long-term and lasting impact on the wider EU society in a pan-European perspective.

Means to achieve the goals (didactical elements): A means to implement the curriculum proposal is the pedagogic perspective of the *Communities of Practice* in which learners '*engage in joint activities and discussions, help each other, and share information. They build relationships that enable them to learn from each other*'. Therefore, learning becomes a social process taking place in communities of learners that build a shared repertoire of practices: '*They develop a shared repertoire of resources: experiences, stories, tools, ways of addressing recurring problems—in short, a shared practice. This takes time and sustained interaction*' ([69]). European platforms such as etwinning.net could be used to coordinate and support follow-up activities that bring together teachers, pupils, and other relevant stakeholders from different European countries.

The suggested approach considers offline courses with the target audience (teachers) coming together (for short or long periods) for a collective learning experience and sharing their experiences among colleagues, possibly across diverse countries, and learning from each other and the diverse contexts. This approach could also have a positive impact on the perspective to 'treat security education as a global issue' ([70]), fostering a pan-European perspective on transferring NIS education from teachers to pupils.

The **practical implementation** of this approach focuses on linking (sometimes abstract) concepts with real-life settings and impact. It includes: lectures for overview and structure; case studies, joint development of 'stories' about privacy + security that structure a lesson series and their components: informatics-centred exercises, cross-subject exercises, balance between knowledge, and skills and attitudes development; concrete exercises with participants drawing on techniques such as programming, data analysis, and role plays; lessons learned from empirical evaluations of security-related teaching materials such as the adequacy of simulated (rather than authentic) scenarios, the importance of individual reflection in a domain heavily influenced by peer pressure, etc. can be used ([71]).; discussion of existing modules and lesson series and their applicability (or need for adaptation) in course participants' teaching practice.

These offline courses can be accompanied by structured collaborations on a platform such as etwinning.net where teachers already organise joint courses, share their experiences, and carry out further collaborative projects across borders. These continuing activities are key for ensuring *continuing* professional development in the fast-changing area of security/privacy, and they also embody a *blended learning* approach (offline courses plus online activities on the teacher platform) needed for deriving maximum advantage from different media and interaction modi.

Means and incentives for stakeholders: According to a Eurydice report ([72]), continuing professional development for teachers has gained importance in Europe and is considered a professional duty in a majority of Member States. The same report notices that CPD activities could contribute to promotions and that this is an incentive for teachers to undertake such activities. NISDL training deliverers can leverage this need for teachers and tailor NISDL modules that would contribute to

[69] Wenger, E. 2007. Communities of Practice. A Brief Introduction. [online] Available from: http://wenger-trayner.com/theory/

[70] http://ecesm.net/sites/default/files/Dev %201.2. %20- %20v1.1.pdf

[71] Vanderhoven, E. (2014). Raising risk awareness and changing unsafe behaviour on social network sites: A design-based research in secondary education. PhD Thesis, University of Ghent, Belgium, 2014.

[72] http://eacea.ec.europa.eu/education/eurydice/documents/key_data_series/151EN.pdf

the teachers' CPD. This is linked with the observation that NIS educational activities for children in Europe is usually jointly delivered by the ICT teacher and other teachers ([73]).

As mentioned in Section 2.3, ECDL already addresses teachers with a broader vision to consider them key actors for a multiplier effect for IT security skills for citizens. This could constitute an incentive for the creation of a tailored NISDL module for teachers. Furthermore, as noted before, ECDL already has a module on IT security; this could also constitute a training of interest for the target audience.

A further incentive for stakeholders relates to education on online safety being widely included in the school curriculum in several EU Member States (see 'Target audience' above). Thus, teachers can be offered training that they can transfer in their classes, in line with the goal of bringing security and privacy education to schools.

Evaluation methods and metrics: Evaluation methods should include qualitative and quantitative aspects. It would be possible to measure the number of school teachers (both in Europe as a whole and in each Member State) entering CPD activities in the area of NIS education. This could offer knowledge for targeted actions (in each Member State and in a pan-European perspective). It will also offer information to stakeholders implementing NIS education modules in terms of where conduct further targeted interventions and filled market gaps.

Qualitatively, teachers should be offered opportunities for self-assessment both in terms of how NIS education training contributed to CPD as well as in terms of knowledge and skills acquired. This will help teachers identify further training needs and opportunities. This evaluation will also offer relevant information for stakeholders implementing NIS education modules as to where there is a direct demand and gaps to fill.

To assess the continuing use of materials and activities for self-directed continuing professional development, learning analytics such as those defined for the eTwinning platform (Berendt et al., 2013) ([74]) could be employed.

Participants will also want to think about success metrics for their own courses. One option is to test knowledge and transfer abilities of pupils by exams ([75]). Further metrics will be characterised by an *absence*: an absence (or reduction) of regrets concerning behaviour in social media ([76]), an absence of incidents of cyberbullying among pupils, an absence of hacking attacks on the school's infrastructure, etc. Such success metrics are, to the best of our knowledge, not yet existent for education; measures from IT Security and penetration testing could serve as inspiration.

[73] http://eacea.ec.europa.eu/education/eurydice/documents/thematic_reports/121EN.pdf

[74] Berendt, Bettina; Vuorikari, Riina; Littlejohn, Allison; Margaryan, Anoush. Learning analytics and their application in technology-enhanced professional learning, Littlejohn, Allison; Margaryan, Anoush (eds.), Advancing Technology Enhanced Learning, Routledge Taylor & Francis Group, 2013.

[75] E.g. Berendt, B., Dettmar, G., Demir, C., & Peetz, T. (2014). Kostenlos ist nicht kostenfrei. LOG IN 178/179, 41-56. Links to teaching materials and English summary at http://people.cs.kuleuven.be/~bettina.berendt/Privacy-education/

[76] Yang Wang, Gregory Norcie, Saranga Komanduri, Alessandro Acquisti, Pedro Giovanni Leon, and Lorrie Faith Cranor. 2011. 'I regretted the minute I pressed share': a qualitative study of regrets on Facebook. In *Proceedings of the Seventh Symposium on Usable Privacy and Security* (SOUPS '11). ACM, New York, NY, U.S.A, Article 10. http://doi.acm.org/10.1145/2078827.2078841

3.1.2 Healthcare Scenario

Information Security for Healthcare Professionals	
Summary	Several reported incidences in the healthcare sector have shown that many healthcare providers do not live up to the legal requirements for security, safety and data protection, often due to a lack of a security culture. As such we propose this scenario/module: "Information Security — Information Security Management in Practice', 7, 5 ECTS. The principal basis for the content of the education is a Swedish framework (SVISA framework) [77] for the deployment of an information security management system (ISMS) supplemented with other material from information security standards (ISO/IEC 27000), regulations, and research. The SVISA framework was developed by the project SVISA led by the Swedish Civil Contingency Agency (MSB). The course is given in 6 blocks of 2 days and, between these blocks, practical task assignments being conducted at the participants' regular jobs.
Target audience	Participants come from different areas of health care organisations and have their backgrounds as clinical staff, business analysts, and/or IT professionals.
Main stakeholders involved	The course is given by Skövde University, the Computer Science Department, on behalf of Västra Götaland County in Sweden. One of the course coordinators is Dr Rose-Mharie Åhlfeld who is an IT security researcher and university teacher. Also, information security professionals working in the health care sector of Västra Götaland County have been involved when the course was designed. A similar course could also be held by other universities in cooperation with other health care providers provided that they have a similarly qualified team consisting of IT security and privacy researchers and IT security professionals from the health care area.
Recommendations for implementation	
Objective and estimated results	The course has the objective to apply the SVISA framework with the expected result that participants from the health care sector will gain knowledge and understanding, skills and abilities, judgment, and an approach to implement an information security management system (ISMS).
Incentives for stakeholders	There are special legal requirements for safety, security, and privacy in the healthcare sector (e.g. pursuant to the Swedish Patient Data Act) as well as ethical obligations of the medical profession to keep patient data confidential and safe. In Sweden, there are special incentives for healthcare providers to have such an educational programme in place with the aim of increasing the security knowledge and awareness of their clinical staff, business analysts, and/or IT professionals, and successively establishing a security culture in their organisations.

[77] MSB (2014). SVISA framework - MSB's method support for deployment of information security management systems. Available: https://www.informationssakerhet.se/sv/Metodstod/

Means to achieve the objective	The course consists of lectures, reports, seminars/group discussions, and workshops. It includes an introduction and the following six blocks, including both theoretical and practical elements: Block 1 — Business analysis, Block 2 — Risk analysis, Block 3 — Gap analyses, Block 4 — Identify security measures and processes, Block 5 — Develop and improve guidelines and instructions, Block 6 — Follow up and improve information security. The theory part is based on standards for the introduction of ISMS (ISO/IEC 27000 family) as well as the latest research in order to provide in-depth knowledge of the field. The practical part has its basis in the ISMS of the participants' working environment in order to practically train them to implement the management system at the operational level. For this, students have to conduct and apply practical application assignments undertaken in the student's working environment for providing the skills and ability to apply ISMS in practice.
Metrics	The course examination consists of two parts where the results from the first three blocks are presented at a seminar at half-time and the remaining data from blocks 4-6 are presented in the final seminar at the course's conclusion. The students also have to submit a final report.
Evaluation	The students were present in the final report to include both reflections about the course content and design. In the currently ongoing course there are no written reflections, but the oral feedback so far has been clearly positive. Two aspects were considered to be particularly valuable: the practical link of the education with the student's work and the seminar components where students get a lot of input and feedback from each other. Furthermore, the course organisers report that a key success factor of the education has been the student group composition consisting of professionals from the healthcare sector with different backgrounds and the motivation for dedicated, creative discussions that have been extremely valuable and rewarding. The observations and comments from the participating parties of the time that the course was hold were input for a SWOT-Analysis for the course.

3.1.3 Data Protection Officers Scenario

Data Protection Officer Education	
Summary	Data Protection Officer Education, 7.5 ECTS. Data protection officers (DPOs) designated by data controllers or processors play an important role according to the European Data Protection Legal Framework. The proposed EU General Data Protection Regulation (GDPR) requires that data protection officers, pursuant to Art. 35, shall have expert knowledge of data protection law and practices, and the ability to fulfil the tasks referred to in Article 37. This includes the task to 'monitor the implementation and application of this Regulation, in particular as to the requirements related to data protection by design, data protection by default and data security' as well as the task to 'monitor the performance of the data protection impact assessment by the controller or processor'. The educational programme proposed here aims to educate lawyers and IT security specialists on privacy law and privacy technologies for achieving the qualifications required for data protection officers. Different specialisations should be offered for lawyers and for information security specialists.
Target audience	Students should already have a degree in law or computer science, or a related subject with an academic and/or practical specialisation in IT security.
Main stakeholders involved	This programme can be offered by universities with a research or educational profile in privacy or other qualified institutes/organisations.
Current status	Dedicated programmes for educating data protection officials have already been offered to Computer Science students by the Hochschule Ulm since the early 1990s ([78]). In addition to this, courses on privacy and privacy-enhancing technologies (PETs) have been offered by several European universities such as Karlstad University and the Royal Institute of Technology in Sweden ([79]), KU Leuven ([80]), or other universities ([81]). EuroPriSe GmbH offers 2+ days' of international expert workshops addressing legal or technical privacy professionals with in-depth knowledge in data protection and privacy ([82]). It specifically introduces the EuroPriSe privacy seal certification scheme, provides training evaluation, and focuses on privacy use cases with the objective to provide participants with the opportunity to qualify to become EuroPriSe evaluation experts.

([78]) http://www.hs-ulm.de/Fakultaet/Informatik/Zusatzqualifikationen/Datenschutzbeauftragter/

([79]) http://www.csc.kth.se/~buc/PPC/syllabus/

([80]) PETs: Privacy and Big Data (http://onderwijsaanbod.kuleuven.be/syllabi/e/H00Y2AE.htm); various aspects of privacy: Interdisciplinary Privacy Course (http://people.cs.kuleuven.be/~bettina.berendt/teaching/ Privacy12/)

([81]) See the list of courses created by NIS Platform Working Group 3 https://ec.europa.eu/digital-agenda/en/news/nis-public-private-platform- %E2 %80 %93-call-expression-interest

([82]) https://www.european-privacy-seal.eu/ws/EPS-en/Expert-Admission-Workshops

	Data protection officers should also possess the privacy expertise expected from EuroPriSe evaluators, especially as privacy seal certification schemes should be encouraged by the European Commission pursuant to Art. 39 GDPR.

Recommendations for implementation

The **objective** of the proposed educational programme is to provide lawyers or IT security specialists with the qualification for becoming or assisting DPOs in organisations handling personal data. The qualification required for DPOs comprises expertise in both data protection law and privacy technology. As a **result**, participants will have knowledge of both domains. They will be able to evaluate a design or product, highlight problems, and suggest improvements. They will be able to communicate with other DPOs and experts from both the legal and the IT side.

Means and incentives for stakeholders: Knowledge transfer from universities to industry and society is gaining increasing importance throughout Europe, not only in the form of joint research projects but also in the form of training programmes offered for non-university members. Incentives can be monetary (participation fees), knowledge transfer *to* society, and also the knowledge transfer *from* participants and possible joint follow-up projects. In this way, academics and practitioners gain new ways of engaging in and shaping societal debates and developments. Universities that already offer such training events ([83]) could help others realise this potential by sharing their expertise on organisation, benefits, and challenges.

The advantages of reciprocal knowledge transfer may be sufficient incentive for voluntary forms of the proposed course. These may then be offered at irregular intervals within well-suited environments that are typically non-permanent such as externally funded projects, and/or with different specialisations in each iteration. If, in contrast, the training events are to offer not only education and university-based certification of attendance and/or completion, but also an official certification, they form a new task for universities that will typically go beyond their normal teaching tasks and capabilities, and additional means and incentives are needed. Public funding that covers actual costs should be provided to ensure that sufficient and qualified teaching resources can be devoted to the courses.

Curriculum proposal and means to achieve it (didactical elements): The educational programme consists of four parts.

The first part, for all participants, offers a basic introduction to privacy and data protection law (incl. the concepts of privacy, data protection, and related rights and obligations, OECD Privacy Guidelines, EU Data Protection Directive, EU e-Privacy Directive, GDPR, national data protection laws as well as the tasks and responsibilities of DPOs, etc.) basic IT security concepts, privacy-enhancing technologies (incl. basic concepts for anonymous communication and application protocols, anonymisation of databases, and privacy policy languages), Privacy Impact Assessment and privacy by design.

In the second part, different specialisations are offered for lawyers and IT security specialists. The legal specialisation will teach more details of privacy legislation and will train the legal evaluation of systems and products. The technical specialisation provides more technical details of PETs (e.g. mixes, Tor, blind signatures, zero knowledge proofs, anonymous credentials, k-anonymity and differential privacy, P3P, PPL, privacy and identity management, transparency, and control tools) and provides training events on the technical evaluation and certification of PETs.

([83]) See the list of courses created by NIS Platform Working Group 3.

The third part is complementary to the second part: Here, the objective is to teach the two participant groups an understanding of the other's conceptualisations. The objective of this part is a deep understanding of privacy by design (PbD). Care will be taken to highlight typical pitfalls such as the merely additive combination of data types, transfer, storage, and use from an 'offline' version of the application task with technological safeguards such as encryption. This can be illuminated with case studies of problematic or even failed PbD such as ELENA, the German Electronic Proof of Earnings ([84]). The case studies will serve as important didactical elements in teaching the mixed audience key elements of the others' conceptual models of data protection and privacy. The reason for this is that both designers and critics (such as DPOs with the task of overseeing or auditing a privacy-by-design process or product) can often determine whether a system truly has 'privacy built in' if they have (a) a formal model of requirements (both of the application task to be solved and of the privacy requirements), (b) an understanding of the purpose and what its minimal data requirements are, and (c) state-of-the-art IT security. ([85]).

Based on this understanding, the fourth part concludes the programme with practical Privacy Impact Assessment and privacy by design assignments and a privacy seal evaluation assignment. Both will be conducted jointly by groups of students with technical and legal backgrounds. The assignments should include learning methods such as role-plays that are appropriate for also highlighting the difficulties of conflicting privacy requirements and their treatment in design.

Evaluation methods and metrics: The education programme is passed if the practical assignments have been solved successfully and an oral or written test has been passed.

Oral and anonymous written course evaluations and reflections by students will be required after different course elements (i.e. after the introduction, specialisations (part 2) and integration (part 3), and after each assignment).

[84] Schaar, P. (2010). Privacy by Design. Identity in the Information Society, 3:267-274; and digital courage e.V. (2011). Datenkrake ELENA erledigt. http://www.foebud.org/datenschutz-buergerrechte/arbeitnehmerdatenschutz/elena/datenkrake-elena-erledigt/

[85] Gürses, S., Troncoso, C., & Diaz, C. (2011). Engineering Privacy by Design. In Conference on Computers, Privacy & Data Protection (CPDP 2011); and Deng, M., Wuyts, K., Scandariato, R., Preneel, B., & Joosen, W. (2011). A privacy threat analysis framework: supporting the elicitation and fulfilment of privacy. Requirements Engineering Journal, 16(1), pp. 3-32.

3.1.4 Small and Medium Enterprises Scenario

Training for Small and Medium Enterprises (SMEs)	
Summary	Small and medium enterprises (SMEs) have become targets of malicious online activities and the level of cybercrime faced by SMEs is increasing ([86]) [87] ([88]). This and the apparent lack of knowledge on and awareness of the problem, could have a serious impact on the continuing economic development of the EU — especially as the vast majority of all European businesses are, in fact, SMEs. Unfortunately, as reported by a recent workshop on cybersecurity training ([89]), private sector companies such as SMEs, and to a lesser degree public sector organizations, are either unable or unwilling to fund information assurance and security training. In addition, those SMEs that are actively looking to improve their knowledge and understanding of information security are forced down the ISO 270001 route which, in most cases, is unnecessary and unobtainable. It is this lack of knowledge, awareness, an over bureaucratic certification process, and of course the lack of funding that are the key aspects of this problem. The intention is to develop and deliver (via stakeholders — see below) a low-cost mini ISO 270001 suitable for the working realities of SMEs.
Target audience	SME owners and employees
Main stakeholders involved	• Academic institutions (e.g. universities, polytechnics, colleges of further education) • Certification bodies (e.g. IASME, (ISC)2, ISACA, SANS, etc.,) • Regional business associations (e.g. Federation of Small Businesses, European Business Support Network, etc.,) • Regional development Organisations (e.g. Northumberland Community Development Network, Association of Regional Development Agencies, etc.,) • Regional & national government Organisations (e.g. Warning, Advice & Reporting Points, International Cyber Policy Unit, Information Commissioner's Office, ENISA, Action Fraud, etc.,) • NGOs (e.g. Business Crime Reduction Centre, Scottish Business Resilience Centre, The Analogies Project, Cloud Security Alliance, etc.,) • Law enforcement agencies (e.g. NCA, Europol, etc.)
Current status	This section of the scenario offers a list of materials, initiatives, and training that illustrate the current status of implementation of this scenario with regard to the target user (SMEs) in Europe. The list is not exhaustive and is meant to provide an initial and reasoned overview: • ENISA ([90]) has developed NIS training material for SMEs

([86]) Hayes, J., & Bodhani, A. (2013). Cyber security: Small firms under fire. *Engineering & Technology*, *8*(6), 80-83.
([87]) http://www.fsb.org.uk/frontpage/assets/fsb_cyber_security_and %20_fraud_paper_2013.pdf
([88]) http://www.iiea.com/ftp/Publications/Cybersecurity_How %20Cybercrime %20Affects %20your %20Business-IIEA_2013_compressed.pdf
([89]) http://www.copura.de/cnf/workshopreport
([90]) https://www.enisa.europa.eu/publications/archive/training-material-SMEs

- European Project INSEMOT — Information Security Modular Training for SMEs (LifeLong Learning Programme) [91]
- ISACA [92]
- SANS Institute
  - Security Awareness for SMEs [93]
  - Free Webcast for SMEs [94]
- UK government's Centre for the Protection of National Infrastructure [95], initiative on securing the data and network infrastructures of small and medium enterprises (SMEs)
- Cyber Essentials Scheme: Cyber Essentials [96] is a UK government-backed, industry-supported scheme to help organisations protect themselves against common cyber attacks
- IASME [97]: information assurance management standard for SMEs

Recommendations for implementation

- **Objective:** to develop (taken advantage of the experience with the UK model) an EU Information Assurance training/standard/certification for SMEs (EUIASME).
- **Proposed curriculum:**
  - Assessing Risks
  - Policy & Compliance
  - Identifying Assets
  - People Management
  - Physical & Environmental Protection
  - Access Control
  - Operations Management
  - Malware Intrusion Detection
  - Systems Monitoring & Protection
  - Backup & Restore
  - Incident Response Management
  - Disaster Recovery & Business Continuity

- **Estimated results**: While ISO27001 is comprehensive, it is also extremely challenging for a small company to achieve and maintain. An EUIASME training/standard/certification would offer a new, easily accessible and sustainable route for SMEs. In essence the EUIASME standard (following its UK counterpart) will be developed as per the ISO27001 but specifically tailored for small companies, while still demonstrating baseline compliance with the international standard.

- **Encouraging participation:** The biggest problems facing acceptance by SMEs, will firstly be their reticence (it's just another EU bureaucratic hurdle we have to jump over), and secondly, how much it will cost. It is suggested that economic incentives for companies (in

[91] https://www.insemot.eu/en/
[92] http://www.isaca.org/Journal/Past-Issues/2012/Volume-6/Documents/12v6-SME-Cybersecurity.pdf
[93] https://www.securingthehuman.org/programs/sme
[94] https://www.sans.org/webcasts/practical-threat-management-incident-response-small-medium-sized-enterprise-98260
[95] www.cpni.gov.uk
[96] https://www.gov.uk/government/publications/cyber-essentials-scheme-overview
[97] https://www.iasme.co.uk/

the same way as UK government cybersecurity vouchers [98] are used. In addition, there are a group of SMEs that are required to undertake continuing professional development (CPD Points). They are lawyers, accountants, solicitors, etc., and CPD points are a mandatory element of their continuing professional recognition. In addition, this group could also be considered as 'enablers', that is, they also have a client base, which in all probability would also be SMEs.

- **Stakeholder incentives**: starting from top to bottom:
  - Academic institutions: The majority of UK higher education institutions will have some form of business engagement/outreach programme targeted at local and regional businesses; offering various business development activities, which will include SMEs. The incorporation of the information assurance certification would have added value for business support and development activities.
  - The remainder (apart from certification bodies — see below) are all (certainly within the UK) committed to the cause. This includes regional business associations because they must be seen doing something, and regional development organizations, government organizations, and NGO and law enforcement agencies because they are all 'on message' and follow central government directives.
  - The certification bodies: All their standards and certifications (CISSP, CISM, and CISA), have been directed at large national and multi-national organisations. However, they have recently realized that SMEs represent an untapped and potentially quite profitable sector. This group represents the key to the success of the project. If we are able to progress an EU standard (EUIASME) that these organisations can develop, deliver, and then certify, then I suspect they would only be too happy to get involved.

    Evaluation methods and metrics: A mix of quantitative and qualitative measures will be used. For example, quantitative metrics could be based on the number of SMEs undertaking this specific training; in the UK, the Federation of Small Business (FSB) estimate that 20 % of SMEs have undertaken some form of security training. This metric could have a further differentiation, e.g. per sector (finance, manufacturing, etc.), per country and at an EU general level. This will offer information about the impact of the action and indication where there are gaps and market needs. In addition, participants could also be offered qualitative opportunities for self-assessment with further identification of existing gaps and training opportunities to fill the identified gaps.

[98] https://www.gov.uk/government/news/support-for-small-businesses-to-tackle-record-levels-of-cyber-attacks

3.1.5 Digital Forensics Scenario

Digital Forensics Certification	
Summary	Given the current increases in cybercrime, it is suggested that many EU organisations need highly skilled and professional individuals able to resolve the problems with the collection, preservation, and analysis (e.g. digital integrity and continuity of evidence) of cybercrime activities within an organisational environment. In addition, such individuals will need to assist the organisation in developing a tactical (e.g. incident response) and strategic approach to the investigation of cyber criminal activities. Such individuals must also consider the legal, social, and ethical issues when undertaking an investigation within a work-based environment. Therefore, a European work-based postgraduate certificate in digital forensics investigations is proposed — the following sections will outline its structure and implementation.
Target audience	Public & Private Sector Organisations
Main stakeholders involved	Academic institutions (e.g. universities, polytechnics, colleges of further education) Law enforcement agencies (e.g. NCA, Europol, etc.)
Current status	This section of the scenario offers a list of initiatives and training that illustrate the current status of implementation of this scenario with regard to the target user in Europe. The list is not exhaustive and is meant to provide an initial and reasoned overview: **Commercial (Software Vendor) Organisations:** EnCase ([99]) is a suite of digital forensics developed by Guidance Software that is designed for digital forensics, cybersecurity, and e-discovery. In addition to the product, Guidance Software also provides training which can result in the award of an EnCase Certified Examiner qualification ([100]). NB This requires attending classroom sessions. Access Data ([101]) also provides vendor specific training on its suite of software products (e.g. Digital & Mobile Forensics, Litigation & E-Discovery, Cyber Security). As with EnCase, Access Data also offers Certified Examiner certification. In addition they also offer academic institutions 'ready-made' digital forensics courses. **Commercial (Training Providers) Organisations:** In the UK, companies such as FireBrand ([102]) offer a number of digital forensics courses. Again, this requires attendance at classroom sessions. While at an

[99] https://www.guidancesoftware.com/training/Pages/encase-forensic-training-series.aspx?cmpid=nav
[100] https://www.guidancesoftware.com/training/Pages/ence-certification-program.aspx?cmpid=nav
[101] http://www.accessdata.com/
[102] http://www.firebrandtraining.co.uk/courses

	international level, the SANS Institute [103] has a number of digital forensics certifications (non-vendor specific) [104]. In addition, the SANS Technology Institute [105] offers various degrees [106] in cybersecurity. However, new enrolments on these programmes are normally limited to 100 per year.

Recommendations for implementation

Objective: to develop a work-based distance learning digital security postgraduate certificate offered by various academic partners across the EU.

Proposed Curriculum: It is suggested that the programme could make use of the knowledge, understanding, and/or skills specified by the UK Skills for Justice: National Occupational Standards (NOS) [107]: SFJ CO1: Identify and secure electronic evidence sources, SFJ CO2: Seize and record electronic evidence sources, SFJ CO3: Capture and preserve electronic evidence, SFJ CO4: Investigate electronic evidence, SFJ CO5: Evaluate and report electronic evidence, SFJ CO6: Conduct Internet investigations, SFJ CO7: Conduct network investigations, SFJ CO8: Conduct covert Internet investigations, SFJ CO9: Take first response actions in investigations involving digitally related evidence, SFJ CO10: Provide single point of contact services for investigations into digitally related crime, SFJ CB1: Gather and submit information that has the potential to support policing objectives, SFJ DB4: Collate and provide papers for individual court/tribunal cases, SEM BIT4: Leading workplace organisation activities, SEM BIT24: Leading the application of Six Sigma methodology to a project, SEM BIT27: Leading the application of Six Sigma metrics to a project, SEM BIT29: Leading the carrying out of capability studies. See Appendix A for NOS Learning Module.

The programme consist of the following modules:

Principles of Digital Forensics Investigations: focusing on the principles and techniques of identifying and securing electronic evidence sources, including the capture and preservation of digital evidence. The module will also introduce the types of investigations that can be undertaken, and how to evaluate and report digital evidence.

Digital Forensics Investigation Strategy: In this module, individuals will evaluate current issues in digital forensics investigations in the light of their company's management, strategic, and operational perspectives after which they will be able to provide a single point of contact when investigating a digital related crime, take appropriate first responder actions, and prepare all necessary documentation related to the digital crime.

Workplace Digital Forensics Project: In this module, individuals are required to identify and successfully lead a workplace digital forensics project. The individual will be accountable for the development and management of the project, and will ensure that the project provides sufficient opportunities for personal, professional, and organisational development.

Estimated results: It is anticipated that the enhancement of the technical and business skills of IT staff will help in raising the general business community's awareness of cybercrime, and by improving the conditions for business growth and successes, will ultimately benefit the EU. In addition, the provision of a formal academic qualification (as opposed to vendor driven certification) for practitioners will enhance the IT industry sector. Furthermore, the work-based

[103] http://www.sans.org/
[104] http://www.giac.org/certifications/forensics
[105] http://www.sans.edu/
[106] http://www.sans.edu/cyber-security-degrees
[107] http://nos.ukces.org.uk/Pages/index.aspx

learning approach will help embed expertise into organisations and pull together practitioners able to disseminate digital forensics intelligence across Europe.

Encouraging participation: Given that the programme is envisaged as being a work-based learning programme with expert speakers delivering their sessions via e-learning platforms such as Blackboard or via video streaming and podcasting, participants will not need to take time from their work. This should prove beneficial to their concerned organisations. In addition, the programme provides opportunities for participants to develop new and highly relevant technical and managerial skills, enhancing their career prospects and encouraging their continuing professional development.

Stakeholder Incentives

Academic institutions: For example, the majority of UK higher education institutions will have some form of business engagement/outreach programme targeted at local and regional businesses; offering various business development activities. Assuming that European institutions have similar programmes, the incorporation of the information assurance certification would provide added value to business support and development activities.

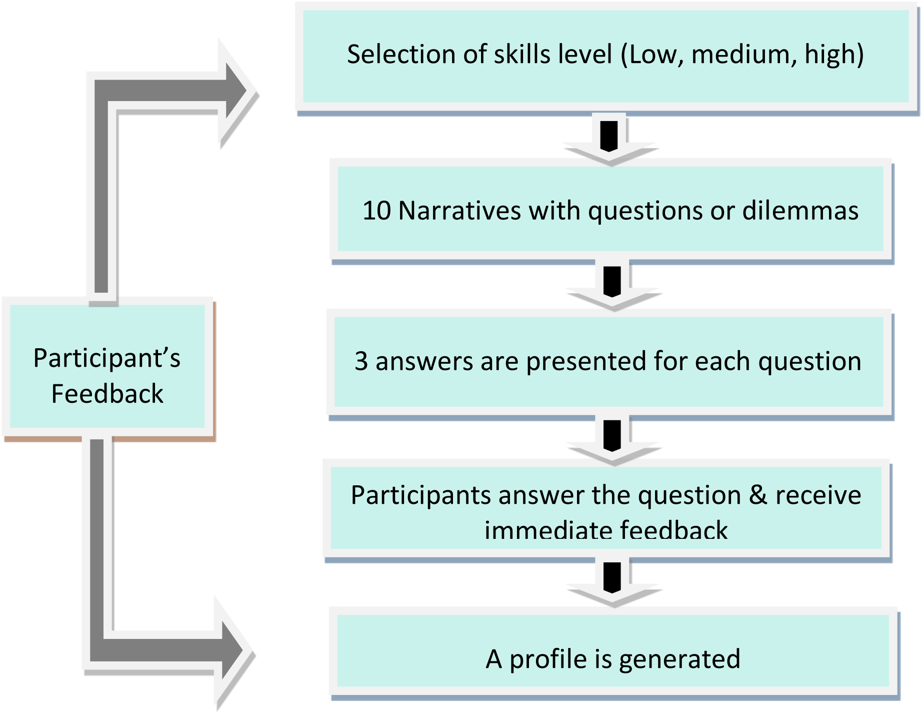
Law enforcement agencies: Anything that helps to reduce the impact of cybercrime and helps with the detection and investigation of such activities will be welcomed by the majority of law enforcement. In addition, we may find that such agencies would also like their own digital forensics investigators to hold this academic qualification.

Evaluation methods and metrics: A mix of quantitative and qualitative measures will be used. For example, quantitative metrics could be based on the number of organisations undertaking this specific training. This metric could have a further differentiation, e.g. per sector (finance, manufacturing, etc.), per country, and at an EU general level. This will offer information about the impact of the action and indication where there are gaps and market needs. In addition, participants could also be offered qualitative opportunities for self-assessment with further identification of existing gaps and training opportunities to fill the identified gaps.

3.2 Developing a pilot application on NIS self-assessment

ENISA has developed a self-assessment quiz as part of its NIS education activities. The audience for this quiz is the broad public and the quiz is intended to combine an entertaining activity with a serious goal: offer an opportunity for participants to familiarise themselves with some of the key themes of NIS education and some of the ENISA recommendations, including material developed in recent years by ENISA through its work. Some questions are also directly connected to the concepts introduced in the first part of this report.

During the work of the expert team, several models for a quiz and delivery options were considered. ENISA, together with the experts, agreed that the quiz should be a simple way to measure some of the participants' skills related to NIS but should also offer a way for participants to identify knowledge and skills gaps and offer information on how to bridge these gaps. Furthermore, the experts agreed that the quiz should contain opportunities for the participant to offer his/her own suggestions. The quiz, therefore, is not just a way for the public to self-assess some of their skills, but it is also an opportunity to offer their voice and discuss their own NIS challenges. Therefore, there is a form where the participants can input their expectations about the quiz at the beginning of it. At the end of the quiz, a further opportunity asking what could have been done differently is offered to participants. This material will, at a later stage, be analysed and assist ENISA in its activities in the NIS education area for the general public, including improving the existing quiz and the development of further quizzes. Following the input form, at the beginning of the quiz, participants are required to select their level of confidence about NIS: from low to medium to high level. Depending on the initial choice the quiz offers increasingly more difficult questions for testing own skills and knowledge.


Selection of skills level (Low, medium, high)
10 Narratives with questions or dilemmas
3 answers are presented for each question
Participants answer the question & receive immediate feedback
A profile is generated
Participant's Feedback

The quiz contains 10 NIS questions and in total, together with input forms, it should take approximately 10 minutes to complete. Each question starts with a short narrative and then a dilemma or a direct question. For each answer (either correct or not) there is then a short explanation/discussion with some further suggestions. A profile will be generated based on the overall result of the quiz. The profile can be one of the following:

1. Beginner: with limited number of correct answers. This profile signals limited level of skills or knowledge of NIS (according to the quiz and the difficulty level selected by the participant).
2. Intermediate: good number of correct answers. This profile has a reasonable level of skills and knowledge of NIS (according to the quiz and the difficulty level selected by the participant).
3. Advanced: high number of correct answers. This profile has an excellent level of skills and knowledge of NIS (according to quiz and the difficulty level selected by the participant).

For each generated profile further indications are being offered in terms of documentation and material to consult with particular attention to ENISA reports. At the low and medium levels there is also the suggestion for attempting the next confidence level quiz.

The application is available on the website www.cybersecuritymonth.eu from October 2014 as a pilot with a possibility of renewal after the first evaluation.

Existing Self-Assessment Quiz

Some of the NIS education stakeholders offer self-assessment quizzes. In most cases they are intended as preparation tests for certifications (e.g. CISM, CISA) or modules (ECDL IT Security). Therefore, they have different goals compared to the ENISA NIS quiz which has a more general goal of signalling relevance of certain subjects and to make relevant suggestions. The following is a list of the existing relevant NIS self-assessment quizzes offered by the stakeholders:

- **ISACA — CISM-CISA Self-Assessment Exam ([108]):** ISACA has a self-assessment quiz (multiple-choice) whose goal is to prepare candidates for the certification exams.- The self-assessment is made against the learning material and it is meant to be used in preparation for the exam.
- **ECDL IT Security Module ([109]):** ECDL Foundation has a sample test (multiple-choice) for self-assessment and the IT Security Module. The quiz allows testing knowledge about the content for the ECDL IT Security Module.
- **ISC (studISCOPE)**: Has a test that allows 'enabling security staffs and individuals to assess their knowledge of the (ISC) ² CBK®, taxonomy of information security topics that serves as the foundation for all (ISC) ² certifications' ([110]).
- **SANS Cyber Talent Skill Assessment Quiz:** This quiz measures skills against the 'Global Information Assurance Certification (GIAC). SANS Cyber Talent Assessments can provide benchmarks across many information security domains including communications security, internet security, networking concepts and operating systems security' ([111]).

([108]) http://www.isaca.org/Certification/CISM-Certified-Information-Security-Manager/Prepare-for-the-Exam/Pages/CISM-Self-Assessment.html; http://www.isaca.org/Certification/CISA-Certified-Information-Systems-Auditor/Prepare-Exam-old/Pages/CISA-Self-Assessment-New.html
([109]) http://www.ecdl.org/programmes/index.jsp?p=2928&n=2944
([110]) https://www.isc2.org/cbk/Default.aspx; https://www.expresscertifications.com/ISC2/
([111]) https://www.sans.org/press/sans-cybertalent-assessment-quiz-finds-a-winner.php

4 Recommendations

To conclude with, we would like to underline some key messages of this current work below:

- While there is an abundance of cybersecurity materials and programmes for helping European teachers, unfortunately, such materials often make use of terms such as ‘safety’ and ‘security’ in an inconsistent manner. Consequently, this lack of standard usage may limit the ability of teachers to understand, explore, and hence teach cybersecurity basics in a structured manner, resulting in lesson plans becoming a collection of ‘do’s and don’ts’, that do not support deep learning and any form of reflection on that learning by the student. By deploying better continuing education programmes for teachers we advocate for enhancing the multiplier role they have. The scenario presented suggests an intervention on this specific target group whose multiplier role means having increased capacities in terms of transferable NIS education skills that could have a wide and lasting impact on EU Society and its citizens.
- Massive Online Open Courses (MOOCs) may offer opportunities for the distance learning delivery of network and information security modules to large audiences. Furthermore, this approach could be easily adopted by interested stakeholders. Consequently, it is felt that more emphasis should be placed on NIS and that European Institutions should start to develop NIS MOOCs. In addition, any future pan-European MOOC initiatives should consider including ‘NIS for Dummies’ modules within the programmes portfolio. To sum up, we advocate for: more NIS MOOCs developed by European organisations over ‘traditional’ platforms where, at the moment, most of them are developed by U.S. universities; that pan-European MOOC initiatives should consider basic NIS modules in their portfolio.
- By developing a course for health practitioners, participants from the health care sector could gain knowledge and understanding, skills and abilities, judgment, and an approach to implement an information security management system (ISMS).
- For IT-security educational programmes for practitioners:
  - There should be a practical link of the education with the participants’ work and the security challenges that the participants face at their work places. Especially practical assignments during this course should be designed accordingly to address this requirement.
  - It is also beneficial to have seminar discussions with groups consisting of students coming from different disciplines and having different professional backgrounds, representing people that typically should cooperate in implementing security and creating a security culture in an organisation.
- The development of the Data Protection Officers (DPOs) course directed at lawyers and digital security specialists would help ensure that both groups have an understanding of data protection laws and privacy technologies. Since participants will have knowledge of both domains, technical specialists will be better able to evaluate a design or product, highlight problems, and suggest improvements from a legal perspective, while a lawyer may be able to do the same, but from a technical perspective.
- The development of an EU information assurance training/education solution for the working realities of SMEs may prove extremely useful in the fight against cybercriminal activities directed at European SMEs.
- The rising increases of digital crime directed at European private and public organisations suggest that EU organisations require individuals skilled in digital forensics investigations and the collection and presentation of digital evidence of the crime. The development of an EU-

based academic recognition for continuing professional development in digital forensics may help in the provision of those skilled investigators.

Furthermore, we invite the reader to consult the tools developed through this project:

1. The interactive map with NIS courses in Europe available on www.cybersecuritymonth.eu compiled by the NIS Platform WG3 group. One can also add a new reference simply by using the 'ADD' button.

2. NIS quiz addressed to all users for knowledge update, available on www.cybersecuritymonth.eu.

As a final conclusion the authors suggest the idea of creating a Europass [112] for NIS Skills for the general public, very much in line with the model of the Europass Language Passport [113]. Skills can be self-assessed for certain NIS areas (e.g. privacy, general security) and according to an established self-assessment frame. A 'NIS Europass' could facilitate, for example, jobseekers in applying for jobs across Europe and could facilitate employers in assessing prospective candidates. Clearly the development of this passport will require appropriate research and the need to work directly with key stakeholders delivering NIS education for the public, work to be followed in the future by interested organisations.

[112] http://europass.cedefop.europa.eu/en/home
[113] http://europass.cedefop.europa.eu/en/documents/european-skills-passport/language-passport

References

ENISA

- European Cyber Security Month www.cybersecuritymonth.eu
- ENISA's NIS in Education reports http://www.enisa.europa.eu/activities/stakeholder-relations/nis-brokerage-1/brokerage-model-for-network-and-information-security-in-education
- ENISA training material: https://www.enisa.europa.eu/publications/archive/training-material-SMEs and EISAS http://www.enisa.europa.eu/activities/cert/other-work/eisas_folder/eisas-large-scale-pilot

OTHER STUDIES

- Cavoukian, A.: Foundational Principles (Privacy by Design). (1997) http://www.privacybydesign.ca/index.php/about-pbd/7-foundational-principles/
- Vanderhoven, E., Schellens, T., & Valcke, M. (2014). Educational packages about the risks on social network sites: state of the art. Procedia — Social and Behavioural Sciences, 112
- De Moor, S., Dock, M., Gallez, S., Lenaerts, S., Scholler, C., & Vleugels, C. (2008). Teens and ICT: Risks and opportunities. Belgium: TIRO. Retrieved from http://www.belspo.be/belspo/fedra/TA/synTA08_en.pdf
- Sharples, M., Graber, R., Harrison, C., & Logan, K. (2009). E-Safety and Web 2.0 for Children Aged 11-16. Journal of Computer Assisted Learning, 25(1)
- Moreno, M. A., Vanderstoep, A., Parks, M. R., Zimmerman, F. J., Kurth, A., & Christakis, D. A. (2009). Reducing at-risk adolescents' display of risk behaviour on a social networking website: a randomized controlled pilot intervention trial. Archives of Paediatrics & Adolescent Medicine, 163(1)
- Vanderhoven, E., Schellens, T., & Valcke, M. (2013). Exploring the Usefulness of School Education about Risks on Social Network Sites: A Survey Study. The Journal of Media Literacy Education, 5(1)
- Debating, B., Lovejoy, J. P., Horn, A.-K., & Hughes, B. N. (2009). Facebook and online privacy: Attitudes, behaviours, and unintended consequences. Journal of Computer-Mediated Communication, 15(1)
- Slobogin, C. (2008). Privacy at Risk: The New Government Surveillance and the Fourth Amendment. Chicago, IL: University of Chicago Press
- Solove, D. (2011). Nothing to hide. The false trade-off between privacy and security. Yale University Press
- M.S. Rosenberg, D.L. Westling, J. McLeskey (2008). Special Education for Today's Teachers: An Introduction
- Vanderhoven, E. (2014). Raising risk awareness and changing unsafe behaviour on social network sites: A design-based research in secondary education. PhD Thesis, University of Ghent, Belgium, 2014
- Berendt, B., Dettmar, G., Demir, C., & Peetz, T. (2014). Kostenlos ist nicht kostenfrei. LOG IN 178/179

ONLINE resources

- EU Cyber Security strategy http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf
- Europass https://europass.cedefop.europa.eu/en/home
- EC Data Protection http://ec.europa.eu/justice/data-protection/
- PRIPARE project public website: http://www.pripareproject.eu
- Definitions of cybersecurity http://www.oxforddictionaries.com/definition/english/cybersecurity http://whatis.techtarget.com/definition/cybersecurity
- http://www.dailywritingtips.com/safety-and-security/
- ECDL http://www.ecdl.org/programmes/index.jsp?p=2928&n=2944
- Teaching about privacy in schools http://people.cs.kuleuven.be/~bettina.berendt/Privacy-education/index.pdf
- INSAFE http://lreforschools.eun.org/web/guest/insafe
- Safer Internet http://www.saferinternetday.org/web/finland/home
- Klick Safe http://www.klicksafe.de/ueber-klicksafe/die-initiative/project-information-en/
- http://www.etwinning.net
- Safer Internet Day http://www.saferinternetday.org/
- E Safety label http://www.esafetylabel.eu/web/guest/esafetyschool
- http://www.bigambition.co.uk/secure-futures/resources/
- http://www.behindthescreen.org.uk/projects/cyber-security-advanced/
- SPION http://www.spion.me/publication/spion-deliverable-922-first-version-of-privacy-manual-for-educational-users-at-the-microlevel
- http://www.hyfisch.de/Fachgruppe/tagung13/ws1_2014

MOOC section

- https://www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/SSO-Top-Ten-Tips.pdf

- https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/240193/13-1173-maturing-of-the-mooc.pdf
- http://www.edtechmagazine.com/higher/article/2014/02/harvardxs-and-mitxs-mooc-data-visualized-and-mapped
- http://theinstitute.ieee.org/ieee-roundup/opinions/ieee-roundup/low-completion-rates-for-moocs
- http://europa.eu/rapid/press-release_IP-14-335_en.htm
- http://www.openuped.eu/

SCENARIOS sections

- http://ec.europa.eu/public_opinion/archives/ebs/ebs_404_en.pdf
- http://eacea.ec.europa.eu/education/eurydice/documents/thematic_reports/121EN.pdf
- Livingstone, S, and Haddon, L (2009). EU Kids Online: Final report. LSE, London: EU Kids Online. (EC Safer Internet plus Programme Deliverable D6.5) http://www.lse.ac.uk/media@lse/research/EUKidsOnline/
- Rifon, N.J., LaRose, R., & Choi, S.M. (2005). Your privacy is sealed: Effects of web privacy seals on trust and personal disclosures. Journal of Consumer Affairs, (39):339-362
- EACEA http://eacea.ec.europa.eu/education/eurydice/documents/thematic_reports/121EN.pdf
- Berendt, Bettina; Vuorikari, Riina; Littlejohn, Allison; Margaryan, Anoush. Learning analytics and their application in technology-enhanced professional learning, Littlejohn, Allison; Margaryan, Anoush (eds.), Advancing Technology Enhanced Learning, Routledge Taylor & Francis Group, 2013.
- Yang Wang, Gregory Norcie, Saranga Komanduri, Alessandro Acquisti, Pedro Giovanni Leon, and Lorrie Faith Cranor. 2011. ‘I regretted the minute I pressed share’: a qualitative study of regrets on Facebook. In Proceedings of the Seventh Symposium on Usable Privacy and Security (SOUPS ‘11). ACM, New York, NY, U.S.A, Article 10. http://doi.acm.org/10.1145/2078827.2078841
- http://www.hsulm.de/Fakultaet/Informatik/Zusatzqualifikationen/Datenschutzbeauftragte
- https://www.informationssakerhet.se/sv/Metodstod/
- http://www.csc.kth.se/~buc/PPC/syllabus/
- PETs: Privacy and Big Data http://onderwijsaanbod.kuleuven.be/syllabi/e/H00Y2AE.htm)
- Interdisciplinary Privacy Course (http://people.cs.kuleuven.be/~bettina.berendt/teaching/ Privacy12/)
- List of courses created by NIS Platform Working Group 3 https://ec.europa.eu/digital-agenda/en/news/nis-public-private-platform- %E2 %80 %93-call-expression-interest
- https://www.european-privacy-seal.eu/ws/EPS-en/Expert-Admission-Workshops
- Hayes, J., & Bodhani, A. (2013). Cyber security: Small firms under fire. Engineering & Technology, 8(6)
- http://www.fsb.org.uk/frontpage/
- http://www.iiea.com/ftp/Publications/
- http://www.copura.de/cnf/workshopreport
- https://www.insemot.eu/en/
- http://www.isaca.org/Journal/Past-Issues/2012/Volume-6/Documents/12v6-SME-Cybersecurity.pdf
- https://www.securingthehuman.org/programs/sme
- https://www.sans.org/webcasts/practical-threat-management-incident-response-small-medium-sized-enterprise-98260
- www.cpni.gov.uk
- https://www.iasme.co.uk/
- https://www.guidancesoftware.com/training/Pages/encase-forensic-training-series.aspx?cmpid=nav
- http://www.accessdata.com/
- http://www.firebrandtraining.co.uk/courses
- http://www.giac.org/certifications/forensics
- http://nos.ukces.org.uk/Pages/index.aspx
- https://www.isc2.org/cbk/Default.aspx
- https://www.expresscertifications.com/ISC2/
- http://nos.ukces.org.uk/PublishedNos/SFJCO1.pdf

Annex A: NOS Learning Module

Title	Post Graduate Certificate: Digital Forensics Investigations
Target Group	This programme is aimed at individuals who are involved in preventing e-crime, specifically those individuals who are responsible for the forensic monitoring of an organisation's IT security This programme may relate to a criminal or civil investigation, or to due diligence and internal discipline
Type of Programme	P/T course + self-study
Link to NOS	SFJ CO1: Identify and secure electronic evidence sources ([114]) SFJ CO$_2$: Seize and record electronic evidence sources ([115]) SFJ CO3: Capture and preserve electronic evidence ([116]) SFJ CO4: Investigate electronic evidence ([117]) SFJ CO5: Evaluate and report electronic evidence ([118]) SFJ CO6: Conduct Internet investigations ([119]) SFJ CO7: Conduct network investigations ([120]) SFJ CO8: Conduct covert Internet investigations ([121]) SFJ CO9: Take first response actions in investigations involving digitally related evidence ([122]) SFJ CO10: Provide single point of contact services for investigations into digitally related crime ([123]) SFJ CB1: Gather and submit information that has the potential to support policing objectives ([124]) SFJ DB4: Collate and provide papers for individual court/tribunal cases ([125]) SEM BIT4: Leading workplace organisation activities ([126]) SEM BIT24: Leading the application of Six Sigma methodology to a project ([127]) SEM BIT27: Leading the application of Six Sigma metrics to a project ([128]) SEM BIT29: Leading the carrying out of capability studies ([129])<)NF>(
Objective	To produce highly skilled and professional individuals able to resolve problems with the collection, preservation and analysis (e.g. digital integrity and continuity of evidence) of cyber crime activities within an organisational environment.
Learning outcomes	At the end of this programme participants will be able to demonstrate that they can design, deliver, and evaluate procedures used to: • Identify and secure electronic evidence sources • Seize and record electronic evidence sources • Capture and preserve electronic evidence sources • Investigate electronic evidence sources

[114] http://nos.ukces.org.uk/PublishedNos/SFJCO1.pdf
[115] http://nos.ukces.org.uk/PublishedNos/SFJCO2.pdf
[116] http://nos.ukces.org.uk/PublishedNos/SFJCO3.pdf
[117] http://nos.ukces.org.uk/PublishedNos/SFJCO4.pdf
[118] http://nos.ukces.org.uk/PublishedNos/SFJCO5.pdf
[119] http://nos.ukces.org.uk/PublishedNos/SFJCO6.pdf
[120] http://nos.ukces.org.uk/PublishedNos/SFJCO7.pdf
[121] http://nos.ukces.org.uk/PublishedNos/SFJCO8.pdf
[122] http://nos.ukces.org.uk/PublishedNos/SFJCO9.pdf
[123] http://nos.ukces.org.uk/PublishedNos/SFJCO10.pdf
[124] http://nos.ukces.org.uk/PublishedNos/SFJCB1.pdf
[125] http://nos.ukces.org.uk/PublishedNos/SFJDB4.pdf
[126] http://nos.ukces.org.uk/PublishedNos/SEMBIT4.pdf
[127] http://nos.ukces.org.uk/PublishedNos/SEMBIT24.pdf
[128] http://nos.ukces.org.uk/PublishedNos/SEMBIT27.pdf
[129] http://nos.ukces.org.uk/PublishedNos/SEMBIT29.pdf

	• Evaluate and report electronic evidence • Conduct Internet investigations • Conduct network investigations At the end of this programme participants will be able to demonstrate that they can: • Contribute to the development of an organisation’s legal & ethical obligations to the nature and variety of computer crime • Contribute to the development of an organisation’s awareness of the nature and variety of computer crime • Contribute to the improvement of an organisation’s IT security

Content/Syllabus	• Admissibility of electronic evidence • Digital evidence controls • Processing incident scenes • Electronic evidence collection and preservation • Forensic examination of digital and electronic media • Internet & network investigations • Writing investigation reports • Legal and ethical issues with electronic evidence
Learning strategy	Training session led by facilitator and work-based independent study
Learning support	Kruse, W.G., & Heiser, J. G., (2002) Computer Forensics: Incident Response Essentials, Addison Wesley Britz, M. J., (2004) Computer Forensics and Cyber Crime; an Introduction, Pearson Prentice Hall Slade, R.M., (2004) Software Forensics, Collecting Evidence from the Scene of a Digital Crime, McGraw Hill Phillips, A., Enfinger, F., & Nelson, B., (2004) Computer Forensics and Investigations, Course Technology Bainbridge, D., (2004) Introduction to Computer Law, 4th Edition, Pearson Education Limited Casey, E., (2004) Digital Evidence & Computer Crime, 2nd Edition, Elsevier Academic Press Schneier, B., (2000) Secrets & Lies, Wiley Publishing Inc. Mitnick, K., & Simon, W., (2005) The Art of Intrusion, Wiley Publishing Inc.

Catalogue number ISBN/DOI/EN TP-04-14-677-EN-N978-92-9204-090-1 10.2824/32639

ENISA
European Union Agency for Network and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office
1 Vass. Sofias & Meg. Alexandrou
Marousi 151 24, Athens, Greece

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu