Public Private Partnerships in Network and Information Security Education

Case studies

October 2014

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

For enquiries on EDUCATION refer to **Daria CĂTĂLUI**, editor of this report, using the following e-mails:

Contact

For contacting the authors please use stakeholderrelations@enisa.europa.eu

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

Acknowledgements

We would like to thank the following contributors who joined our effort with valuable insights from their own organisations and current work: **Karol KNIEWALD** — Cisco Systems; **Dr Martti LEHTO** — University of Jyväskylä**; Michael KAISER** — NCSA; **Loïc GUEZO** — Trend Micro; **Scott BUCK —** INTEL.

Catalogue number/ISBN/DOI/EN TP-04-14-676-EN-N 978-92-9204-089-5 10.2824/32322

Executive summary

This report focuses on the brokerage of best practices between the public and private sectors aimed at all members of the Network and Information Security Education community in Europe. ENISA is committed to taking the lead in encouraging the exchange of NIS best practices and it follows a strong community-building process for NIS Education stakeholders.

In this report we recommend reading the case studies with special attention to the methods used to build partnerships, the approach to working together and setting the right metrics. The case studies include: CISCO's networking Academy dedicated to professionals; Cybersecurity education in Finland describing academic programmes from universities and the link to the national cybersecurity strategy; The US National Cyber Security alliance and their approach on working together for achieving common results; Trend Micro's Internet Safety for Kids and Families Programme that shows the commitment towards community education; Intel's training programme and their integrating approach on education.

Furthermore, ENISA will use and share with communities the following recommendations:

1. EU and national policy makers should ensure that current education approaches are enhanced by a set of actions to improve cybersecurity know-how in the whole of society, and security should be incorporated as a supporting theme that plays throughout the computing curriculum;
2. Schools and institutes offering higher education should ensure that research and education programmes holistically integrate the perspectives of technology, information, organisations, business and people;
3. Educators should consider deploying a blended learning model, which combines classroom instruction with online curricula, interactive tools, hands-on activities and online assessments to provide immediate feedback;
4. Find better ways of working directly with the community in creative ways, advocacy work and empowering the users;
5. Use as a case study the Finnish model of Triple Helix Cooperation: business, academia and public authorities.

By closely monitoring current work, brokering best practices and planning in advance we participate in this process.

Stepping up the national effort on networks and information security education and training are the main priorities!

Table of Contents

1 Introduction

This report focuses on the brokerage of best practices between the public and private sectors. It is aimed at all members of the Network and Information Security ([1]) Education community in Europe. ENISA is committed in taking the lead in encouraging the exchange of NIS best practices and it follows a strong community-building process for NIS Education stakeholders.

In the 2013 report, Brokerage model for network and information security in education ([2]), after presenting case studies from Member States, we concluded with the following recommendations:

1. ENISA and EC should address Cybersecurity awareness at all levels in different arenas for sharing information;

2. Awareness organisations should pursue Public-Private partnerships in their educational efforts for digital users;

3. NIS in Education community members should target specific stakeholders with different methods and specific content.

The time has come to follow up on these recommendations and deliver on the results of the 2014 brokerage process.

Goal

In the context of this year's work on NIS Education, examples were identified by the community to deliver new material that will be consulted Europe-wide and inspire the way forward. The main goal is to set the proper context for enhanced public-private NIS education partnerships. The selection of case studies was done according to the collaborations we had on projects during the year.

Target audience

The target group is composed of educators, such as trainers, teachers and peers involved in formal education and non-formal education, including lifelong learning.

Structure of this document

This report is developed in three parts with the first part on the current status of NIS PPPs, the main part on case studies from organisations involved in NIS Education, and finally conclusions and recommendations for practitioners. The annexes offer more information on case studies and references on the online resources.

([1]) Referred in this report as NIS [Network and Information Security]
([2]) http://www.enisa.europa.eu/activities/stakeholder-relations/nis-brokerage-1/brokerage-model-for-network-and-information-security-in-education [accessed 7.7.2014]

2 Status of Public Private Partnerships in Europe

In this section the relevant references to public-private partnerships in Europe are provided and reasons are given as to why this model for NIS Education work is used.

> *'The measure of success for a PPP is the right people coming together to do the right things in the right way.'*

Despite the variety of PPPs present across the EU and internationally, a common framework has been developed which describes how these partnerships operate. The Good Practice Guide on Cooperative Models for Effective PPPs ([3]), published by ENISA in 2011, is a framework to provide a structure for understanding a range of diverse implementation approaches both for new PPPs and evolving PPPs. We recommend this study as background reading for a better understanding on PPPs.

> *PPP — An organised relationship between public and private organisations, which establishes common scope and objectives and uses defined roles and work methodology to achieve shared goals.*

2.1 Policy references on PPPs

The Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions — the Cybersecurity Strategy of the European Union: 'An Open, Safe and Secure Cyberspace' ([4]) represents the European public roadmap for cybersecurity actions. It describes the context, and at the same time, gives an indication of future actions that should be taken into consideration. It names actors like ENISA and the Member States and it empowers digital users by stating that cybersecurity is a shared responsibility:

> ***The growing dependency on information and communications technologies in all domains of human life has led to vulnerabilities which need to be properly defined, thoroughly analysed, remedied or reduced. All relevant actors, whether public authorities, the private sector or individual citizens, need to recognise this shared responsibility, take action to protect themselves and if necessary ensure a coordinated response to strengthen cybersecurity ([5])***.

Furthermore, regarding public-private partnerships it mentions the European Public-Private Partnership for Resilience ([6]) and the need in this context to:

> ***Develop informal and voluntary cooperation, including between public and private sectors, to boost security levels and exchange information and best practices ([7]).***

([3]) ENISA report 2011 http://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/national-public-private-partnerships-ppps/good-practice-guide-on-cooperatve-models-for-effective-ppps [accessed 17.7.2014]
([4]) http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf [accessed 8.7.2014]
([5]) Page 4 http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf [accessed 8.7.2014]
([6]) Launched via COM(2009) 149
([7]) Page 6 http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf [accessed 8.7.2014]

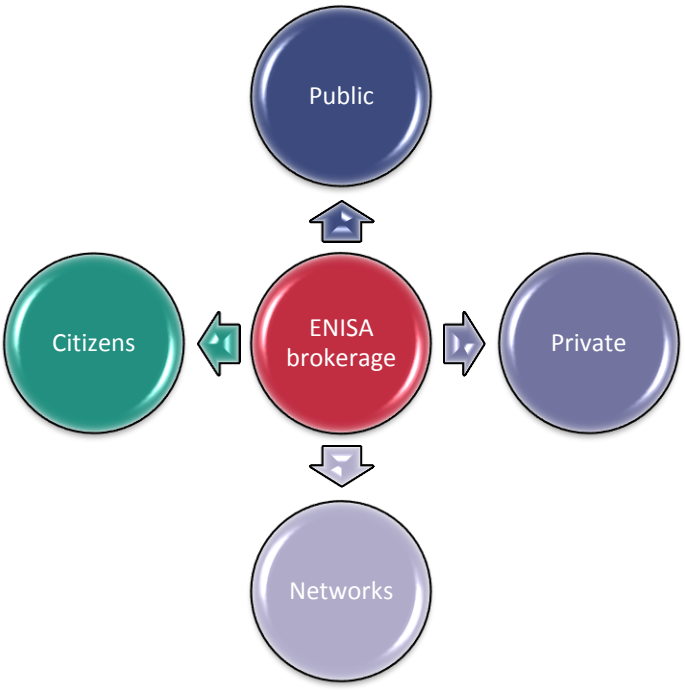
Stakeholders in NIS Education have a natural tendancy to work in partnerships and build initatives together, raising awareness in simple steps and furthering complex educational programmes. The policy document mentions the track record on this too:

> ***ENISA has been involved in raising awareness through publishing reports, organising expert workshops and developing public-private partnerships ([8]).***

The path forward is thus set and ENISA continues to believe that public-private partnerships are the main tool for efficient action.

2.2 The future

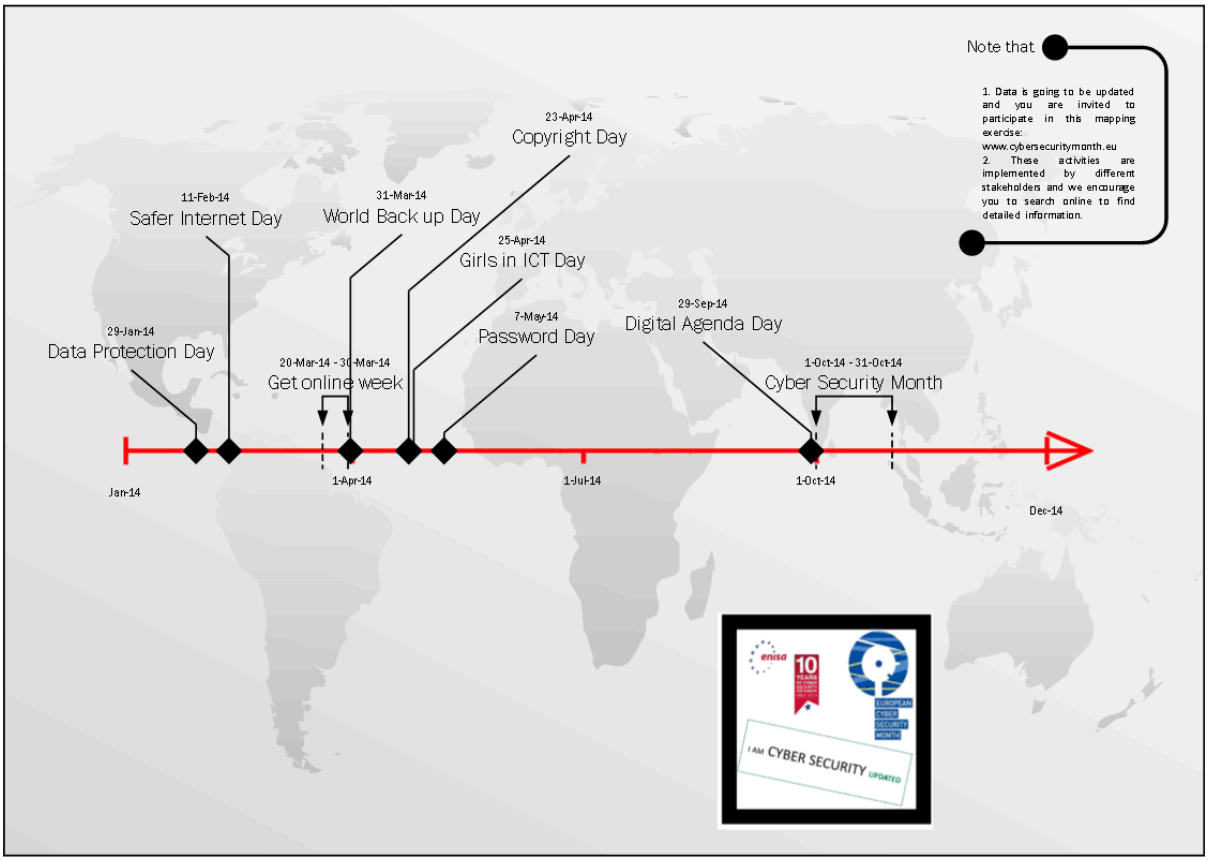
To facilitate implementation of these ideas we communicate an established model of cooperation and we monitor its results closely. This model, depicted in the graph below, shows ENISA's role and the partners with which we search to collaborate. Increasing the number of partners involved and bringing them together for common benefits is part of the daily work. We should add that in best practice the arrows exchange input both ways, in a bi-dimensional approach. Furthermore, for a mature dynamic model, exchanges should take place at all levels and connections should appear between all stakeholders involved. We benchmark future work according to all these criteria.



([8]) Page 8 http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf [accessed 8.7.2014]

2.3 Coalitions for eEducation

This year, ENISA launched an exercise(on its website) on collecting publicly available data on who is doing what in raising awareness on online security and its consequences. The map below depicts a snapshot of the current situation including international efforts by organisations such as the Council of Europe, Safer Internet Programme, UNESCO, International Telecommunication Union, Telecoms Centres, US Government, ENISA and European Commission. Readers are invited to participate to this world-wide open Wiki ([9]).



([9]) www.cybersecuritymonth.eu or e-mail to stakeholdersrelations [at] enisa.europa.eu

3 Case studies

This chapter presents current case studies from engaged public and private sector stakeholders. ENISA aims to increase its partnerships with more organisations and to identify and help disseminate their work so that it can be shared with the entire community. We recommend reading the case studies with special attention to the methods used to build partnerships, the approach to working together and setting the right metrics.

The case studies include:

- CISCO's networking Academy dedicated to professionals;
- Cybersecurity education in Finland, describing academic programmes from universities and the link to the national cybersecurity strategy;
- The US National Cyber Security Alliance and their approach on working together to achieve common results;
- Trend Micro's Internet Safety for Kids and Families Programme that shows the commitment towards community education;
- Intel's training programme and their integrating approach on education;

3.1 Cisco Networking Academy programme and cybersecurity education ([10])

Every year, hundreds of thousands of Networking Academy ([11]) students worldwide gain the skills needed to build, design and maintain computer networks, improving their career prospects while fulfilling the global demand for networking professionals. With 10 000 academies in 165 countries, the Networking Academy helps individuals to prepare for industry-recognised certifications and entry-level information and communication technology (ICT) careers in virtually every type of industry. Students develop foundational skills in ICT while acquiring vital 21st-century career skills in problem solving, collaboration and critical thinking.

The rapid growth of networks has created a global shortage of people who are qualified to implement and maintain networking solutions, especially in places where networks are being built to promote economic development. At the same time, people need access to better training and career opportunities to successfully compete in the global economy. The Networking Academy helps to address the growing demand for ICT professionals while improving career prospects in communities around the world.

Model, education content and tools

The Networking Academy uses a public-private partnership model to create the 'world's largest classroom'. Cisco partners with educational institutions, non-profit organisations, non-governmental organisations and community centres that provide classroom space, computer lab equipment and qualified instructors. Cisco provides online curricula, virtual learning tools, instructional support, teacher training and professional development opportunities for instructors.

Networking Academy courses are offered in multiple languages through a blended-learning model that combines classroom instruction with online curricula, interactive tools, hands-on activities and online assessments that provide immediate feedback.

The core Networking Academy courses are designed to help students to prepare for industry certifications and career paths. Industry certifications are highly respected by employers around the world and help to validate the skills needed to launch successful careers in networking and ICT.

([10]) Author Karol Kniewald, Area Academy Manager CEE / CIS, Cisco Systems
([11]) Established in 1997, the Networking Academy is Cisco's largest and longest-running Corporate Social Responsibility programme

Curriculum / course	Description	Industry certification
IT Essentials	IT Essentials covers the fundamentals of computer hardware and software and advanced concepts such as security, networking, and the responsibilities of an IT professional.	CompTIA A+
CCNA Routing and Switching	CCNA Routing and Switching provides a comprehensive overview of networking concepts and skills, from network applications to the protocols and services provided to those applications by the lower layers of the network, with an emphasis on practical application, work-force readiness and soft-skills development.	Cisco CCENT Cisco CCNA
CCNA Security	CCNA Security introduces the core security concepts and skills needed to install, troubleshoot and monitor a network to maintain the integrity, confidentiality and availability of data and devices.	Cisco CCNA Security
CCNP	CCNP teaches the advanced skills needed to install, configure, monitor and troubleshoot enterprise-sized networks and manage wireless, security and voice applications.	Cisco CCNP
Health Information Networking	Health Information Networking helps students to prepare for networking careers in the healthcare industry.	N/A
Entrepreneurship	The Entrepreneurship course is designed to supplement IT courses, teach critical business and financial skills, attitudes and behaviour, as well as helping to develop an entrepreneurial mindset.	N/A
Introduction to Cybersecurity	The Introduction to Cybersecurity course covers trends in cybersecurity and provides examples of the need for cybersecurity skills in various industries.	N/A
Introduction to the Internet of Everything (IoE)	The Introduction to IoE course discusses the Internet and its evolution to the interconnection of the people, processes, data and things that form the Internet of Everything.	N/A

Get Connected	The Get Connected introductory course focuses on basic connectivity to desktop and mobile devices and the Internet.	N/A
Voice Primer	Voice Primer provides an introduction to voice on a data network, known as Voice over Internet Protocol (VoIP).	N/A
Cloud Primer	Cloud Primer introduces cloud computing and the underlying delineating technologies in consolidation, virtualisation and automation.	N/A
Collaboration Primer	Collaboration Primer introduces enterprise collaboration with reference to the underlying delineating technologies in messaging, voice and video technologies.	N/A
NDG Linux Essentials	The Linux Essentials course teaches students the fundamentals of the Linux operating system and command line, as well as basic open-source concepts.	Linux Professional Institute (LPI) Linux Essentials Certificate of Achievement
Smart Grid Essentials	The Smart Grid Essentials curriculum provides an introduction to smart grid technologies for electro-technology students and employees in electro-technology professions.	N/A

Cybersecurity and network security courses

In the age of the Internet of Everything (IoE), the networked connections of people, processes, data and things create a greater need for a robust security infrastructure. The network is used for everything from storing an organisation's confidential data, to storing personal financial and health information. More connections make data more vulnerable to attacks, creating a growing need for individuals with cybersecurity skills.

The Introduction to Cybersecurity course covers trends in cybersecurity and provides examples of the need for cybersecurity skills in various industries.

The CCNA Security course provides a next step for individuals who want to enhance their CCNA-level skill set and help to meet the growing demand for network security professionals.

More details about courses are available in Annex A.

3.2 Activities in Finland ([12])

3.2.1 Cybersecurity Research and Education in Finnish Universities

Security and the cyber domain cover many walks of life and research subjects. A number of disciplines address themes associated with cybersecurity. For a long time now questions associated with cybersecurity have been studied in computer science and engineering, information systems science, information processing science and ICT technology, as well as automation science and engineering.

Traditionally, universities have dedicated separate departments to information technology, the information processing sciences and to automation science and engineering. In addition to these, research has been intensified in big data, cloud services, usability and embedded systems, among others, which also include perspectives on cybersecurity.

The Finnish Cybersecurity Strategy states that:

> ***'As a small, capable and collaborative country Finland has excellent chances of rising to the vanguard in cybersecurity. We have an extensive knowledge base and strong expertise and a long tradition of close public-private cooperation, built on trust, as well as intersectional collaboration.'***

In support of continuously improving the competence and awareness of the actors of society, inputs will be made to developing, utilising and training common cybersecurity and information security instructions. Inputs into R & D and education will be increased, as well as action to improve cybersecurity know-how in the whole of society.

<u>Cybersecurity Research and Education in Universities and Research Centres</u>

Aalto University

Aalto University is working towards a better world through top-quality research, interdisciplinary collaboration, pioneering education, surpassing traditional boundaries and enabling renewal.

([12]) Author Researcher, Dr Martti Lehto, Department of Mathematical Information Technology University of Jyväskylä

Cybersecurity research and education has been carried out in the School of Electrical Engineering and the School of Science.

Cybersecurity research at Aalto University is wide-ranging. The School of Electrical Engineering has extended its research to societal and technical topics. In addition to risk analysis, modelling, security considerations in diverse systems and questions related to cybersecurity in public administration, the legislative perspective is also covered.

At Aalto University cybersecurity is always studied in conjunction with an application schema, rather than as a major subject or programme. Although information networks are the key application schema, it is possible to include information security studies as a minor subject along with any field of technology.

The research themes are Network Security, Vulnerability Analysis, Intrusion Prevention/Detection Systems, Cloud Technology Security, SCADA Security, Legal Aspects in a Cyber World, Internet Security, Smart Grid Security, Risk Analysis and Cyber Competences in the Public Sector.

University of Helsinki

The University of Helsinki is the most comprehensive research institution of higher education, edification and intellectual regeneration in Finland. Precise reasoning is one of the focus areas. This focus area encompasses mathematics and information sciences, as well as their applications in other fields.

In the Faculty of Science (Department of Computer Science and Department of Physics) the cybersecurity research themes are Secure Systems, Mobile Security, Trust Management, Data Security and Usability, Internet of Things, Network Protocols, Big Data, Security of the Distributed Systems, ICT-applications and Cryptology.

The Faculty of Science themes for cybersecurity advanced studies (80 ECTS) are Information Security, Cryptography and Network Security, Software Security and Mobile Platform Security.

University of Jyväskylä

The University of Jyväskylä is a nationally and internationally significant research university and an expert on education that focuses on human and natural sciences. The University is Finland's leading expert in teacher education and adult education, as well as the major exporter of education. One main technology focus area is human-centred information and communication technology.

The Faculty of Information Technology responds to the challenges in research and education brought by the development of information technology and digitalisation. The Faculty holistically integrates the perspectives of technology, information, organisations, business and people into its research and education.

Information Security (Master of Science: 120 ECTS) is based on two sub-programmes: the technology profile and the organisation security profile. The aim of the Master's degree programme in Cybersecurity is to provide solid skills in the kinds of demanding management and development tasks that require comprehensive awareness in cybersecurity. The studies comprise an entity which addresses the cyber world and its security from societal, functional, systemic and technological perspectives.

The Cybersecurity Research areas are Anomaly Detection, Advanced Persistent Threat (APT), Big Data Security, Cyber Defence, Critical Infrastructure Protection, Cybersecurity and Human Aspects,

Cybersecurity Investments, Cybersecurity Management, Cybersecurity Situation Awareness, Identity Protection, Secure Services and Security Economics.

National Defence University

The National Defence University is a training institution responsible for educating the future leaders of Finland's armed forces. The National Defence University offers undergraduate, Master's and doctorate studies and research programmes in the area of military science.

Military science is a multi-disciplinary and complex collection of subjects that study wars, crises, other threats to security and the means for preventing these. In today's world, military science must comprehend military security and defence from a wide security framework perspective. At the National Defence University, the main research interest is above all future threat scenarios and the development of the national defence system.

Different departments of the National Defence University engage in cybersecurity research. The Departments of Strategic and Defence Studies, Leadership and Military Pedagogy as well as Tactics and Operations Art bring different approaches to the field of research. The Department of Military Technology especially studies the possibilities of compiling a situation picture of critical infrastructure.

University of Oulu

The University of Oulu is a multi-disciplinary science university with international operations. The university operates in eight major fields: humanities, education, economics, natural sciences, technology (incl. architecture), medicine, dentistry and health care, distributed in six faculties. Focus areas of the university are: Biosciences and Health, Information Technology, Cultural Identity and Interaction, Environment, Natural Resources and Materials.

Research on information security at the Department of Information Processing Science at Oulu University's Faculty of Information Technology and Electrical Engineering concentrates on research areas such as secure coding, digital water-marking and biometric identification.

The Department of Computer Science and Engineering runs an associated degree programme, which includes information security studies. The degree programme at the Department of Information Processing Science also includes information security studies. Cryptography and encryption techniques can be studied at the Department of Mathematical Sciences.

Tampere University of Technology

Tampere University of Technology is primarily a research university, which specialises in technology and architecture. Technology is the key to addressing global challenges. The University combines a strong tradition of research in the fields of natural sciences and engineering with research related to industry and business.

The Cybersecurity Research areas are Cloud Computing Security, Identity and Access Management, Key Management, Cryptographic Protocols, Secure Programming and SCADA Security.

The syllabus for information security, studied as a minor subject, includes programmes, network, management and cryptology. The Department of Automation Science and Engineering has integrated information security into its basic studies of systems, and automation into the studies of information systems. The cyber-security approach has been set out from the following perspective: 'information security, communications technology, software technology and the methods of software engineering as tools used in generating reliable automation'.

University of Turku

The University of Turku is an internationally competitive university, the operation of which is based on high-quality multi-disciplinary research. High-level research creates the basis for the university. The strategy of the University of Turku has identified information security as one of four research areas that are in an advanced stage of development. Turku University provides a multi-disciplinary research environment in information security, bringing together experts in information technology, mathematical cryptography and information systems science.

Research topics include *inter alia* cryptology, information security and data protection in mobile communications, software security, security in embedded systems, network security and human aspects of information security as well as information security and guaranteeing business continuity management.

Master's Degree programme in Information Security and Cryptography (120 ECTS) has two tracks: Cryptography and Data Security and Networked Systems Security. The Cryptography and Data Security major subject educates future experts of the field that have strong and broad knowledge on mathematical aspects of cryptography and data security. The students learn to assess the strengths and weaknesses of cryptographic solutions based on a deep understanding of the underlying theory. The Networked Systems Security major subject gives its students profound and substantial education and expertise in the networked systems security and technology field.

Technical Research Centre of Finland

The Technical Research Centre of Finland (VTT) is a globally networked multi-technological applied research organisation. VTT provides high-end technology solutions and innovation services. Research activities at VTT encompass forecasting future technological and market development trends, creating novel know-how, providing customers with new development impulses, developing technologies and concepts, applying technologies and enhancing technology transfer and utilisation.

VTT focuses its research spearheads on specific areas, which will be undergoing major business transitions or radical technology changes. VTT's research vision is directed by two major trends: digitalisation and sustainable development. Information digitalisation guides not only information and communication technology, but also the development of all its application areas. Sustainable development, on the other hand, requires taking environmental aspects into account in products and services as well as production processes.

The VTT Technical Research Centre of Finland studies and develops suitable methods for the purpose of sustaining information security in software-intensive systems and products and serving the needs of the ICT industry. The main research topics in this field are: information security analysis methods, securing software security, monitoring and guaranteeing information security in operational systems, and information security metrics.

Finnish Defence Research Agency

The Finnish Defence Research Agency is a military institution under the authority of Defence Command Finland and provides advanced research, development, testing and evaluation services for the Finnish Defence Forces. The Defence Research Agency is a multi-disciplinary research and development organisation bringing together research and development activities related to military, behavioural, social and natural sciences under one roof.

The Electronics and Information Technology Division focuses on research into electronic defence applications. The division researches Radio-frequency Sensor and Electronic Warfare Systems, Cyber Defence and C4-Systems. The main Cyber Defence research areas are vulnerabilities and cryptology.

Table1 of Cybersecurity Research Areas in Finnish Universities:

	Aalto Univ.	Univ. of Helsinki	Univ. of Jyväskylä	Defence Univ. and PVTT	Univ. of Oulu	Tampere Technical Univ.	Univ. of Turku	VTT
Anomaly detection			X					X
APT analysis			X					X
Authentication, authorisation and identity management (IAM)						X		X
Big data security	X		X					
Cloud service security	X				X	X		X
Computer Security	X		X		X			
Cryptography	X	X		X	X	X	X	X
Cyber defence			X	X				
Cyber security, legal aspects	X							
Critical infrastructure protection	X		X	X		X		X
Cyber security and human aspects			X		X		X	
Cyber security investments			X					
Cyber security management			X					
Cyber security situation awareness	X		X	X				X
Data mining and analysis and cyber security		X	X					

Dos/DDos attack protection	X		X					
Incident analysis and management								X
Identity and access management	X					X		
Identity protection			X					
Industrial Control System (ICS) security	X				X			X
Information assurance		X						X
Information security		X	X		X	X		
Intrusion detection	X		X					X
Intrusion prevention/Detection systems, IPS/IDS	X		X					
IoT security	X	X			X	X		X
Mobile security		X	X			X	X	
Network security and monitoring	X	X	X			X	X	
Privacy	X							X
Risk analysis	X							X
SCADA security	X		X	X		X		X
Secure services			X				X	X
Secure System Design	X		X		X	X		
Security architectures and communication protocols	X	X		X				X

Security economics			X				X	X
Security information visualisation and interpretation			X	X				X
Security metrics and data aggregation			X					X
Security standardisation								X
Security testing					X			X
Smart grid security	X					X		X
Software security		X	X		X		X	
Systems security	X	X			X	X	X	
Threat, vulnerability and dependency analysis	X		X	X			X	X
Trust management	X	X	X			X		X

3.2.2 Master's Degree studies in Cybersecurity at the University of Jyväskylä

The University of Jyväskylä is a nationally and internationally significant research university and an expert on education that focuses on human and natural sciences. **The Faculty of Information Technology** plays a key role in developing one of the University's core fields, human technology. One of the Faculty's primary strengths is its ability to view IT broadly, integrating various perspectives and identifying the joint effects of different phenomena. This is combined with internationally recognised research in the strategic areas, as well as with active societal interaction.

The Faculty of Information Technology responds to the challenges in research and education brought by the development of information technology and digitalisation. The Faculty holistically integrates the perspectives of technology, information, organisations, business and people in its research and education as well as in its cooperation with interest groups.

According to Finland's Cybersecurity Strategy, ensuring the security of society is a key task of the government authorities and the vital functioning of our society must be secured in all situations. Cybersecurity Strategy states that strategic guidelines are needed in support of continuously improving the competence and awareness of the actors of society; inputs will be made into developing, utilising and training common cybersecurity and information security instructions. Inputs into R & D and education will be increased, as well as action to improve cybersecurity know-how in the whole of society.

The Ministry of Employment and the Economy has selected five themes for the Innovative Cities (INKA) programme 2014–20. The purpose of the programme is to accelerate major projects that create new business and international competitive advantages through cooperation between cities and the state. Jyväskylä was assigned a national coordinator role in Cybersecurity. The vision of the Cybersecurity Theme is that Finland will become an internationally recognised global forerunner in cybersecurity business and the awareness of cyber threats. The University of Jyväskylä has very important role coordinating the national Cybersecurity Research and Education in this programme.

We build on the present Triple Helix cooperation: business, academia and public authorities.

Cybersecurity Master's Degree Studies

The Cybersecurity Master of Science education is a joint programme for both departments of the Faculty of Information Technology: The Department of Computer Science and Information Systems (CSIS) and the Department of Mathematical Information Technology (MIT). The Cyber World and its security are examined from a social, functional, systemic and technological point of view during courses.

The extent of the Master's degree programme is 120 ECTS credits. The objective of a cybersecurity education is to create strong know-how in the demanding management and development tasks implied in the total control of cybersecurity.

The aim of the Master's degree programme in Cybersecurity is to provide solid skills in the kinds of demanding management and development tasks that require comprehensive awareness in cybersecurity. The studies comprise an entity which addresses the cyber world and its security from societal, functional and technological perspectives.

A graduate in Cybersecurity is able to define cybersecurity risks in information, data networks, computer systems, telecommunication networks and SCADA-systems. She or he knows the different threat models of the cyber world, and knows the functional and technological solutions which are related to the prevention of threats.

She or he has good readiness to design and to carry out cybersecurity strategies, and to lead the functional and technological planning and development of cybersecurity that meets the requirements of an organisation. A graduate is able to adapt the newest technologies to the cybersecurity issues and is able to produce real-time plans and solutions.

The Cybersecurity Master of Science programme has two sub-programmes. In the CSIS department the knowledge profile is cybersecurity in organisations and the typical job for graduated students is Chief Information Security Officer, CISO.

In the MIT department the knowledge profile is cybersecurity technology and the typical job for graduated students is Chief Security Technology Officer, CSTO.

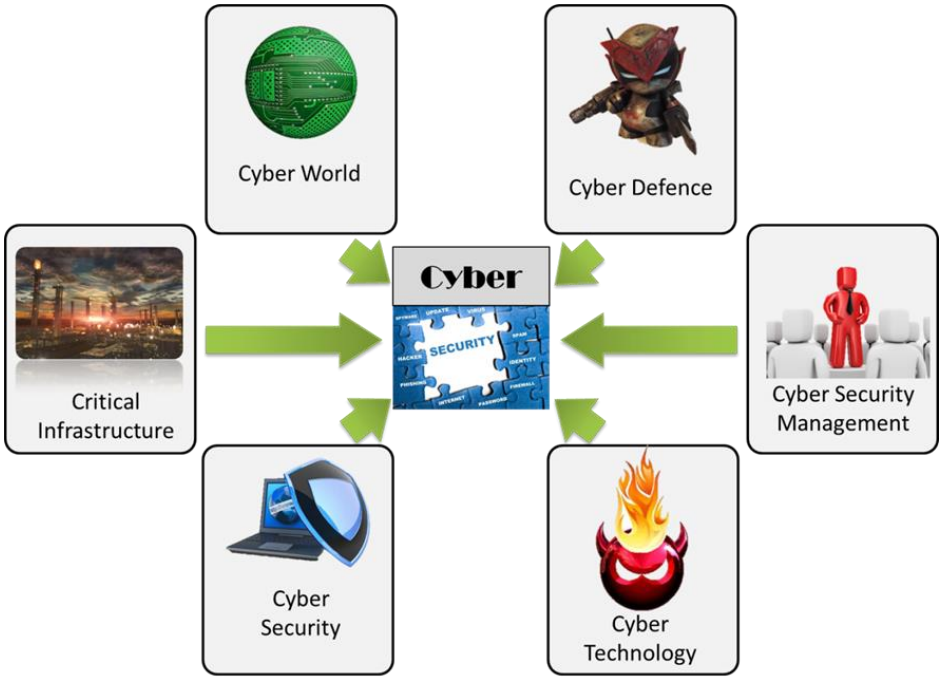
We have identified 17 cybersecurity competence areas in the Cybersecurity Master's programme:

Competence areas	**Courses covered the competence areas**
1. Introduction to cybersecurity	Course 1: Cyber world and security, Course 2: Society and information security
2. Operating system security	Course 1: Operating system security 1 Course 2: Operating system security 2
3. Network security	Course 1: Network security
4. Software security	Course 1: Software security
5. Database security	Course 1: System vulnerabilities
6. Web security	Course 1: Network security
7. Anomaly detection	Course 1: Anomaly detection Course 2: Advanced anomaly detection Course 3: Advanced persistence threat
8. Cryptology	No course
9. Information assurance	In progress
10. Information security management	Course 1: Information security management Course 2: Advanced course on information security management

11. Secure system design	Course 1: Secure systems design
12. Critical infrastructure (CIP) and information infrastructure protection (CIIP)	Course 1: Cyber security and critical infrastructure protection
13. Cyber war and cyber conflicts	Course 1: Introduction to cyber conflict Course 2: Cyber defence strategy analysis Course 3: Cyber attack response and protection
14. Cyber business	In progress
15. Compliance and legal issues	Course 1: Cyber world and international law
16. Digital forensics	No course
17. Human aspects of cyber security	Course 1: Information privacy

The Master of Science education is carried out as a whole in which the time is used for different projects (management, company projects, research projects, Master's thesis) in addition to the traditional multi-disciplinary two-year course. The Cybersecurity courses have also been designed for people in their working life.

In the academic year 2013–14, there were approoximately 25 students in the Cybersecurity Master's programme. The goal is to achieve about 40 students. We have both young B.Sc. students who will continue their studies in this programme and students from working life to complete their diploma to Master's degree level. Study goals and individual curricula are established through personal study plans in which the students agree on the mandatory and elective studies and optional content, established by the faculty and the departments for the Master's degree programmes. All students have their own personal study plans; the plans may recognise expertise acquired through previous work experience.



3.3 US — The National Cybersecurity Alliance ([13])

Public Private Partnership

STOP. THINK. CONNECT. and National Cybersecurity Awareness Month

The National Cyber Security Alliance (NCSA) was founded in 2001 shortly after the terrorist attacks in New York City and Washington. It was formed by a group of visionary industry leaders from Microsoft, Computer Associates, AOL, Cisco, Symantec and McAfee that came to the realisation that not enough was being done to educate the public about protecting themselves and their shared digital assets, including risks to networks and critical infrastructure.

From the very beginning the guiding principles included that all the industry partners, even though they might compete in other ways, had a shared interest in a safer, more secure and trusted Internet and that success would be achieved by working closely with government, which also shared a stake and interest as well.

Today, the NCSA's mission is to educate and therefore empower a digital society to use the Internet safely and securely at home, work and school, protecting the technology that individuals use, the networks they connect to, and our shared digital assets ([14]). NCSA activities are funded by contributions from its industry Board Members and the Department of Homeland Security. Current NCSA Board members are: ADP, AT&T, Bank of America, Comcast, EMC, ESET, Facebook, Google, Intel, Leidos, McAfee, Microsoft, Symantec, Verizon and VISA.

The public private partnership is based on a few key concepts:

- No one entity is solely responsible for protecting the Internet, requiring us to work together;
- To help all Internet users to be safer and more secure requires effort on an enormous scale and no government agency can reach everyone or provide all the resources necessary on its own;
- Everyone benefits when Internet users know how to protect themselves and their business interests;
- The infrastructure of the Internet is complex and distributed between industry and government, requiring a way to work together towards common goals.

Target audiences have always included home computer users and families, the education system, and small and medium-sized businesses. Programmes have evolved over the years but now are focused on four initiatives: Cyber Security Awareness Month (October), the STOP. THINK. CONNECT. campaign, Data Privacy Day (January 28) and Re: Cyber (for CEOs and corporate governance).

STOP. THINK. CONNECT.

([13]) Author: Michael Kaiser, Executive Director NCSA
([14]) http://www.staysafeonline.org/about-us/

The NCSA model is to harmonise around messaging and the calendar and to engage a broad array of stakeholders to communicate those core messages. In addition, the NCSA counts on stakeholders to participate actively in core programmes, such as STOP. THINK. CONNECT. and the National Cyber Security Awareness Months so messaging and education reaches as many people and organisations as possible.

STOP. THINK. CONNECT. reflects that operating philosophy. In the United States, the Alliance had many companies, government and organisations actively engaged in helping people to use the Internet safely and more securely. However, the education and awareness landscape was cluttered with numerous pieces of advice about how to stay safe, a great deal of technical advice that users didn't understand and significant fear-based messaging that encouraged users not go online.

In 2009 President Obama's Cyberspace Policy recommended that, 'The Federal government, in partnership with educators and industry, should conduct a national cybersecurity public awareness and education effort.' ([15]) In response, in an unprecedented initiative, the NCSA along with the Anti-phishing Working Group ([16]) brought together twenty-five companies and seven government agencies to explore the possibility of building a national education and awareness campaign. The group readily agreed to take on the task and over the next fourteen months worked in close collaboration and by consensus to conduct research and develop a suite of messaging to be available and used by all.

The work was recognised as the national message when President Barack Obama declared STOP. THINK. CONNECT. the national cybersecurity awareness campaign during his Presidential Proclamation of National Cyber Security Awareness Month in 2010.

An excerpt of the proclamation reads:

'Together with businesses, community-based organisations and public- and private-sector partners, we are launching a National Cybersecurity Awareness Campaign: 'STOP. THINK. CONNECT.' Through this initiative, Americans can learn about and become more aware of risks in cyberspace, and be empowered to make choices that contribute to our overall security.' ([17])

Rather than originate from only one place, by design, the campaign uses the relationships that already exist between companies, government and education institutions and NGOs to reach their core audiences more quickly. In addition, any organisation developing materials is encouraged to share them with others that are participating in the campaign. Because the campaign is based on research that was done collectively and in partnership, the NCSA has found that adoption by others has been fairly rapid.

Some outcomes to date include:

- More than 150 partners signing a licence to use the STOP. THINK. CONNECT. message ([18]). The campaign is used by companies (large and small), police departments, education institutions and government.
- The campaign has been used in the subway and public transport systems in major US cities, including Washington, Boston and Chicago ([19]).

([15]) http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf
([16]) www.apwg.org
([17]) http://www.whitehouse.gov/the-press-office/2010/10/01/presidential-proclamation-national-cybersecurity-awareness-month [accessed on 17.7.2014]
([18]) Partial list http://www.stopthinkconnect.org/get-involved/partner-program/our-partners
([19]) http://stopthinkconnect.org/resources/landing/

- Companies working together including Microsoft creating television ads for the campaign ([20]) that were then shown by AT&T and Verizon on their cable networks.
- Many companies have started including STOP. THINK. CONNECT in their core messaging ([21]).
- Campaigns have been developed around specific areas of advice such as Keep a Clean Machine, which encourages users to make sure that all software is up to date ([22]).
- Some companies — Campbell Soups, Merck, Warner Brothers Pictures — have started to use the materials in their internal awareness campaigns for employees.
- Leading organisations, such as the Better Business Bureau have begun to incorporate the campaign into their public facing work ([23]).
- Materials have been developed for the classroom and the NCSA has partnered with a couple of companies and the Department of Homeland Security to bring assemblies to schools ([24]).

STOP | THINK | CONNECT™

International expansion

While originally envisioned to start in the United States, the campaign has grown internationally very quickly. This quick uptake of the message reflects the simple universality of the message combined with the increasing desire by people across the globe to reap the benefits of the Internet by using it safely and more securely. The NCSA and APWG have signed Memorandums of Understanding with regional organisations including the Organisation of American States and APCERT to encourage their members to join the campaign, and directly with countries, such as Public Safety Canada and Paraguay. Additionally NGOs in India, Spain and Australia have signed on as well.

With help of companies and local partners, STOP. THINK. CONNECT. materials are now available in Spanish, French, Brazilian Portuguese and Japanese ([25]).

National Cyber Security Awareness Month (NCSAM)

Developed by the Department of Homeland Security and NCSA and first celebrated in 2004, the National Cyber Security Awareness Month has grown in size, scope and reach.

The theme for the last few years has been 'our shared responsibility', and reflects the role that every Internet user plays in staying safer and more secure online.

In many aspects the NCSAM is a grassroots campaign. Companies, organisations and educational institutions from around the country participate in a variety of ways reaching their customers, citizens

([20]) https://www.youtube.com/v/gnEykE9_6v0
([21]) http://www.stopthinkconnect.org/get-involved/partner-program/how-partners-use-stop-think-connect
([22]) www.stopthinkconnect.org/keepacleanmachine
([23]) http://www.bbb.org/blog/2014/06/6-tips-for-protecting-your-identity-online-during-Internet-safety-month/
([24]) http://stopthinkconnect.org/resources/landing/
([25]) http://www.staysafeonline.org/ncsam/about

or students. The NCSA maintains a web portal with tip sheets, graphics, ideas for activities, event listings and champions that want to express their support for the month ([26]).

In 2013, the 10th anniversary of NCSAM, was a tremendous success. A snapshot of the results is as follows:

- 3 130 online articles/print articles/blogs were written about the month — an increase of 193 % (1 067 in 2012);
- Total potential media impressions (includes multiple pick ups or releases and articles) reached 7 885 570 070 — an increase of 255 % (2 220 322 790 in 2012);
- Total tweets using #NCSAM were over 16 000 - an increase of 56 % over 2012 and had over 100 000 000 impressions and was used in over 85 countries;
- The NCSA's Twitter handles @stopthnkconnect, @staysafeonline and the #chatSTC (Twitter chat series hash tag) had over 43 000 000 impressions;
- The governors of all 50 US states issued proclamations in support of the month;
- Facebook sponsored the live stream of the National Cyber Security Awareness Month Launch event in Boston;
- More than 340 companies, organisations, government entities and schools became champions of the month, a 49 % increase from 2012.

Annex B presents the areas of work for the 2014 National Cyber Security Month in the US.

([26]) http://www.staysafeonline.org/ncsam

3.4 Trend Micro's Internet Safety for Kids and Families Programme — ISKF ([27])

The ISKF programme was launched in 2008 and aims to raise awareness and provide education to parents, teachers and youth on Internet safety issues. The global programme is designed to do this through partnerships, volunteering, grants and donations.

The programme's vision is to extend Trend Micro overall corporate vision of creating a world safe for the exchange of digital information to the world's youngest citizens. Its mission is to help kids, families and schools to use technology safely, responsibly and successfully. The programme's strategy to achieve this mission has four pillars:

- **EDUCATE:** Promote online safety, digital literacy and digital citizenship;
- **INNOVATE:** Use Trend Micro expertise, technology and resources when and where applicable;
- **COLLABORATE:** Team with experts for their knowledge and to raise awareness together;
- **EMULATE:** Practice what Trend Micro preaches. Lead by example.

What the programme encourages and actively promotes is **Youth advocacy**: Empowering youth to be safe, responsible and successful online and to have a role in their own safety and success and **Parent advocacy**: Providing parents and teachers with the resources to help young people be safe, responsible and successful online. The overall programme goal is to help audiences to be aware of the risks presented by the Internet and technology, but it goes beyond just discussing safety. It attempts to help people to use technology in ways that are productive for themselves and for others.

Global impact and outreach to date

Trend Micro feels strongly about making sure programmes like the ISKF programme are in fact making a difference with the intended audience. Measuring this type of impact is a challenge for every organisation. Trend Micro measures its global activities and outreach to students, teachers, parents and guardians in addition to a more important measurement/barometer: the feedback and behaviour changes communicated to the company from the communities where the ISKF programme is active. A few interesting numbers about the ISKF programme can be found in ANNEX C.

Partnerships and coalition-building

The topic of Internet safety, digital literacy and digital citizenship spans numerous issues: ranging from online social interactions to data theft to respecting laws. Trend Micro is collaborating with multiple organisations who share the same goals of making the Internet safe for young people so that their combined efforts and expertise can bring the most valuable information and advice to the greatest number of people. These organisations share the ISKF vision and have made a lot of positive strides towards that end. They also believe in promoting the positive aspects of the Internet to children and families while educating them on the risks and how to avoid them. They are enthusiastically supporting the team's efforts and have contributed and advised on so much along the way. With its resources and ability to reach a wider audience, the team hopes to further the good work they started years ago.

In order to achieve its mission, the team is working closely with organisations of all kinds — non-profit, for-profit and governmental — as the company believes that the issues are wide-ranging and require collaboration with a number of experts in multiple countries. To name a few: the National Centre for Missing and Exploited Children, the Family Online Safety Institute, Connect Safely, Childnet International, MOIGE, INHOPE, EducAid, Twitter, Yahoo!, PTO Today, Webwise and the UK

([27]) Author Aurélia RENAUD, Trend Micro

government's Cyber Streetwise campaign. ISKF volunteers from all around the world have built strong local relationships with organisations, government bodies and non-profits to further the ISKF mission.

Some specific ways in which Trend Micro collaborate with other organisations include: co-developing or financially supporting education materials designed for kids, parents or schools; getting input into the design of products developed by the company that can directly protect families and kids; working with organisations such as the National Centre for Missing and Exploited Children and INHOPE to help stop the distribution of child sexual abuse material online; public speaking in the form of panels or presentations; promoting each other's expertise and education materials to the respective audiences and providing consultation to each other in the areas of the respective core competencies.

ISKF education and advocacy activities include:

- Engaging directly with schools and communities to educate;
    - Talking Internet safety to parents/guardians and teachers;
    - A competition with a difference: **What's Your Story** is an internationally acclaimed competition for young people now running in eight countries worldwide. It is a powerful way for young people to raise awareness within their school/community and they become advocates of their own online message. It is also an educational activity for families because everyone can view and rate entries online. Trend Micro strongly believes that young people can promote a safe, responsible and successful online world. **What's Your Story** is a competition for children 8 years and upwards. They submit a two-minute film or poster under the announced Internet Safety theme. They upload their entries to the website for public viewing and voting (each country has a unique website). Entries with the highest views and votes are shortlisted for final decision with independent judges.
- Global/local events and campaigns;
- Global/local partnerships;
- Global/local sponsorships;
- Social media engagement ([28]).

([28]) Blog http://internetsafety.trendmicro.com/ Web www.trendmicro.com/internetsafety

3.5 INTEL approach: Security — the ever-present 'leitmotif' for tomorrow's engineers ([29])

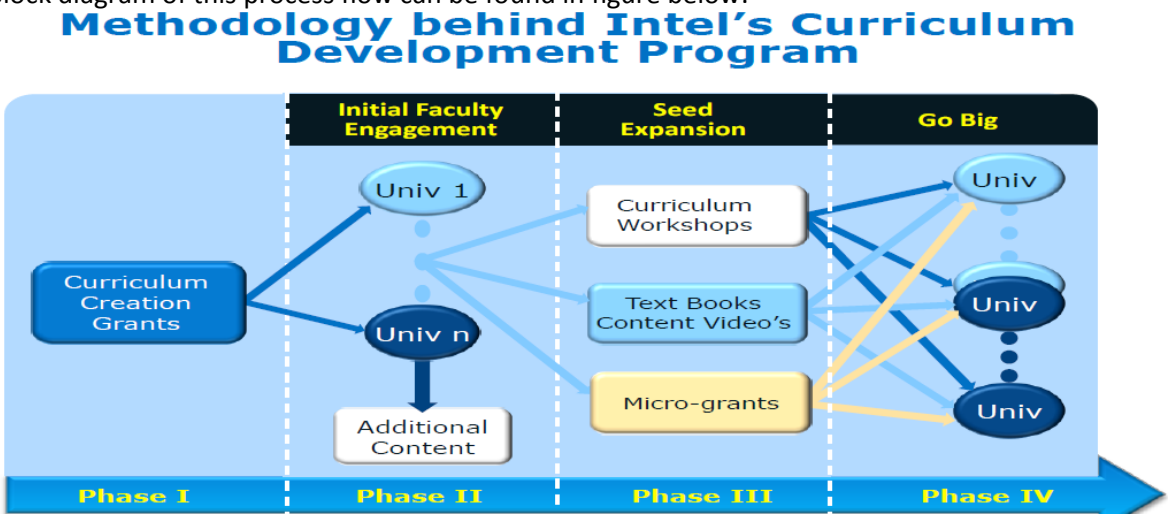
Intel's observation is that many technologists, even world-class engineers, are unprepared to think about and deal with the security issues raised as they develop solutions. They do not know how to systematically address these problems or assess their importance. Because of this, INTEL hypothesise that a security curriculum needs to be developed in a multi-disciplinary framework that puts security features into the context in which they will be used. Security is supplemental to core features in a technology and is rarely the principal aim of most developers, but it arises at every level of a system design. They believe that security needs to become a *leitmotif* that every engineer learns to think about at any level of a system design. Thus, designed-in-security is an important principle for any technology development process. Accordingly, the goal is to incorporate security as a supporting theme that plays throughout the entire symphony of the computing curriculum. They want every computing and engineering student to have basic knowledge about security and be able to recognise specific aspects of designed-in security wherever they may arise within a system's architecture. In order to do this, the student needs to be able to understand some of the basic models for thinking about security issues.

Intel's Approach

The goal of Intel's University Security Curriculum Initiative is to develop a pipeline of students who understand security challenges. By raising awareness of Intel's philosophy of designed-in security and providing funding support to develop security curriculum content, Intel hopes that its activities will be seen by fellow industry partners and help to amplify this message to institutes, faculties and computing/engineering students at all levels of its importance. By working with key faculties, Intel seeks to identify opportunities to develop modules or whole courses that will provide benefits to the academic community and be included in diverse course syllabi. Through these efforts, Intel provides motivation to encourage a culture of faculty collaboration to embrace the incorporation and dissemination of security content. Intel seeks to identify novel approaches and methodologies for cybersecurity education and reaches out to a diverse set of academic partners that have created content to advance student cybersecurity learning. The initial focus of this programme is to stimulate undergraduate education which Intel believes requires a multi-faceted approach. First, the programme seeds the development of security content to build a repository of the elements of security curriculum which it hosts on its Security website. Second, the programme looks at different delivery vehicles to disseminate the awareness of security concepts through books, games, contests and videos. Intel believes that a flexible approach is required to produce students with the needed abilities. Next, students need to develop critical thinking skills; the programme hosts workshops to bring together faculty, industry and government agencies that foster a security curriculum community. The goal of these workshops is to share course materials and labs which provide those hands-on experiences and inspire students to adapt their learning to an ever-changing world. Finally, the programme looks to provide insight into understanding the demand in the cybersecurity labour market through its partnership with fellow industry partners. Intel believes that institution decisions towards academic courses, faculties and programmes will be influenced by the anticipated needs of the labour market for security-trained students.

([29]) Author: Scott Buck, INTEL Higher Education Programme

A block diagram of this process flow can be found in figure below:



Repository of course modules

Intel's Security Curriculum Programme looks to build a security repository of content with a balanced approach. In practice, security requires the utilisation of three elements: mitigation, vulnerability analysis and validation. First there is a modelling effort to capture a threat model. Second the threat model is used to propose mitigations. Finally there is an analysis and validation stage, to determine how well the proposed mitigations address the threats.
Consequently, the security curriculum elements for this programme are grouped into three dimensions: vulnerability analysis — identify what system threats exist; mitigations — identify how to defend against the identified threats; and validation — verify that the mitigations address the threats identified. Through the programme's engagements with faculties, it appears that most students have some knowledge about mitigations, but know little about threat modelling or validating mitigations against a threat model. The programme seeks to address these findings by supporting curricula that will improve students' understanding of these elements. Using this approach the programme has sought out and continues to identify faculties in Europe that provide content in these groups. Available course modules in ANNEX D.

Looking at privacy

This year Intel launched a new initiative in privacy to extend and complement the security curriculum initiative. The privacy initiative will seek to engage universities in the area of multi-disciplinary privacy education. The mission of this programme is to develop a pipeline of capable students who understand multi-disciplinary privacy challenges, can help to create privacy-aware technologies and a privacy-friendly ecosystem. To meet the scope of this mission, the programme is sponsoring faculty teams (e.g. a technologists, economists and policy professionals) that can leverage each of their respective strengths to develop comprehensive content. The output from these teams will be multi-disciplinary curricula content that will contain elements of privacy technologies, user requirements, user psychology and legal, economic and policy frameworks for privacy. The privacy initiative will seek to engage faculties in privacy topics that are cross-cutting i.e.: data protection; privacy policies and regulations; legal frameworks for privacy, economics of privacy; regional differences in privacy; usability and user adoption, information usage models. But the programme also has a technology focus i.e.: privacy-preserving protocols and architectures; re-identification and other privacy attacks; privacy by design; user-controlled privacy models; and

privacy support in low-power devices. The first funded faculty team under this new initiative was with MIT Professor Daniel Weitzner (Law/Internet public policy) with co-authors Hal Abelson (Computer Science) and Michael Fischer (Anthropology) for multi-disciplinary, cross-cultural perspectives on information privacy. The objective of this work is to develop curriculum content aimed at providing CS undergraduates with a cross-disciplinary and cross-cultural perspective on privacy. Additionally, this grant ties in collaborations with universities in Brazil, UK and the Netherlands.

In conclusion, the above-funded faculty and their content areas are important topic areas and students with those skills would be desired by the industry. Intel's Security/Privacy Curriculum Initiative focuses on stimulating the formation of an academic community to develop and share content knowledge, which addresses student learning needs by providing the foundation for needed skills and the tools of tomorrow.

4 Conclusions

This report has highlighted some optimal measures for working in public-private partnerships for network and information-security education. It also provides an example of ENISA's role in brokerage between stakeholders and achieving coordination.

To conclude, we take the opportunity to emphasise some of the learning points from these case studies, points that we will use and share with our communities. All these should be tackled by universities around Europe, supported by national authorities from Member States together with ENISA and EC, but also interested stakeholders from industry.

1. EU and national policy makers should ensure that current education approaches are enhanced by a set of actions to improve cybersecurity know-how in the whole of society, and security should be incorporated as a supporting theme that plays throughout the computing curriculum;
2. Schools and institutes offering higher education should ensure that research and education programmes holistically integrate the perspectives of technology, information, organisations, business and people;
3. Eductaors should consider deploying a blended learning model, which combines classroom instruction with online curricula, interactive tools, hands-on activities and online assessments to provide immediate feedback;
4. Find better ways of working directly with the community in creative ways, advocacy work and empowering the users;
5. Use as a case study the Finnish model of Triple Helix Cooperation: business, academia and public authorities.

The priority for this area of work can be read in the EU Cybersecurity Strategy and also in the key impact indicators for NIS Education at ENISA, namely:

Stepping up the national effort on network and information security education and training are the main priorities!

References

All references were accessed during the period June–October 2014.

Related ENISA papers

[1] ENISA report 2014: http://www.enisa.europa.eu/activities/stakeholder-relations/nis-brokerage-1/brokerage-model-for-network-and-information-security-in-education and report 2011 http://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/national-public-private-partnerships-ppps/good-practice-guide-on-cooperatve-models-for-effective-ppps

Legislation

[2] EU Cybersecurity strategy http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en

Other sources

[3] Blog http://internetsafety.trendmicro.com/ Web www.trendmicro.com/internetsafety

[4] http://www.staysafeonline.org/about-us/

[5] http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

[6] www.apwg.org

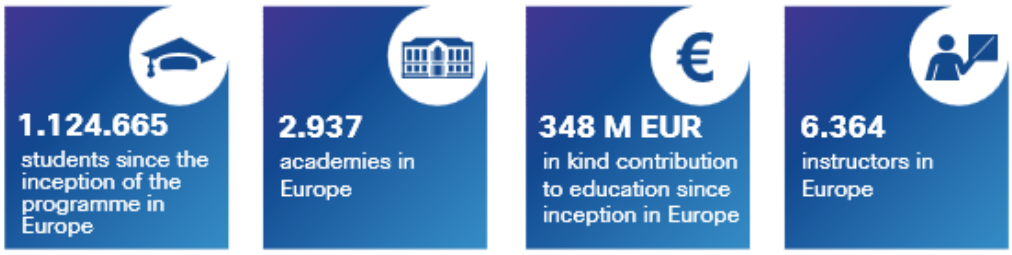
[7] www.staysafeonline.org

[8] www.netacad.eu

Annex A:

Impact of the Networking Academy Programme in Europe

Every year, the Networking Academy teaches thousands of students in the European Union the skills needed to design, build, manage and secure computer networks, helping to enhance their career prospects and fill the global demand for networking professionals. Present in 28 EU Member States, the Networking Academy is one of the pillars of Cisco's Corporate Social Responsibility policy. Since its launch in Europe in 1997, the programme has trained more than one million students.



More info about Networking Academy in Europe at www.netacad.eu

Introduction to the cybersecurity course

The Cisco Networking Academy Introduction to Cyber Security course covers trends in cybersecurity and career opportunities available in this field. Cybersecurity refers to the people, products and processes that protect electronic data from those with malicious intent. This course introduces students to a variety of networking professionals who discuss the exciting and growing industry of cybersecurity. The course modules define cybersecurity, explain why it is important and introduce some of the products and processes used to secure data.

The course offers the following:

- Recorded presentations and panel discussions created by cybersecurity professionals and industry experts;
- Activities that reinforce learning;
- Links to articles and websites to help you explore cybersecurity on your own;
- Quizzes to check your understanding of the information presented;

Students who complete the Introduction to Cybersecurity will be able to perform the following tasks:

Module	Learning Objectives
The Cybersecurity Industry	• Explain the importance of cybersecurity in the global economy • Explain why cybersecurity is a growing profession
Malware and How to Protect Yourself	• Explain the characteristics and operation of malware. • Explain how hackers use unsuspecting individuals to propagate malware
Overview of Cybersecurity in Finance and Telecommunications	• Explain why cybersecurity is critical to the banking industry • Explain why cybersecurity is critical to the telecommunications industry
Cisco Security Solutions	• Explain Cisco's approach to cybersecurity. • Explain the behavior-based approach to cybersecurity
Defending Against Global Threats	• Explain the characteristics of cyber warfare. • Explain how Cisco's Security Intelligence Operations (SIO) tracks and responds to a global threat
Strategic and Architectural Cybersecurity Planning	• Explain trends in the cyber threat landscape. • Explain the framework of the Enterprise Security Architecture
Vulnerabilities and Solutions	• Explain why cybersecurity is critical to the medical devices industry. • Explain the components of cloud security
Will Your Future Be in Cybersecurity?	• Explain the opportunities for pursuing network security certifications

CCNA Security course

The Cisco Networking Academy CCNA Security course provides a next step for individuals who want to enhance their Cisco CCENT certification-level skill set and helps to meet the growing demand for network security professionals. The curriculum provides an introduction to the core security concepts and skills needed for the installation, troubleshooting and monitoring of network devices to maintain the integrity, confidentiality and availability of data and devices.

CCNA Security offers the following:

- Provides an in-depth, theoretical overview of network security principles, as well as the tools and configurations available;
- Emphasises the practical application of skills needed to design, implement and support network security;
- Supports the development of critical thinking and complex problem-solving skills through hands-on labs;
- Promotes the exploration of networking security concepts through Cisco Packet Tracer simulation-based learning activities, and allows students to experiment with network behaviour;
- Includes innovative assessments that provide immediate feedback to support the evaluation of knowledge and acquired skills;

Students who complete CCNA Security will be able to perform the following tasks:

Chapter	Learning Objectives
1. Modern Network Security Threats	Describe the security threats facing modern network infrastructures
2. Securing Network Devices	Secure Cisco routers
3. Authentication, Authorization and Accounting	Implement AAA on Cisco routers using a local router database and external ACS
4. Implementing Firewall Technologies	Mitigate threats to Cisco routers and networks using ACLs
5. Implementing Intrusion Prevention	Implement secure network design, management and reporting
6. Securing the Local Area Network	Mitigate common Layer 2 attacks
7. Cryptographic Systems	Implement the Cisco IOS firewall feature set
8. Implementing Virtual Private Networks	Implement the Cisco IOS IPS feature set
9. Implementing Cisco the Adaptive Security Appliance (ASA)	Implement a site-to-site VPN
10. Managing a Secure Network	Implement a remote access VPN

ANNEX B

In 2014, the overall theme remains our shared responsibility and weekly themes will be:

Week 1: 1–3 October 2014
Theme: STOP. THINK. CONNECT.
Week 1 aims to raise online safety awareness among all Americans and reinforce STOP. THINK. CONNECT. and the simple measures that everyone should take to be safer and more secure online.
Week 2: 6–10 October 2014
Theme: Secure Development of IT Products
Building security into information technology products is key to enhanced cybersecurity. Security is an essential element of software design, development, testing and maintenance. The software that we use every day on our phones, tablets and computers may have vulnerabilities that can compromise our personal information and privacy. This week will target these stakeholders and educate others about what to do and look for in products.

Week 3: 13–17 October 2014
Theme: Critical Infrastructure and The Internet of Things
The Internet underlies nearly every facet of our daily lives and is the foundation for much of the critical infrastructure that keeps our nation running. The systems that support electricity, financial services, transport and communications are increasingly interconnected. The Internet of Things — the ability of objects and devices to transfer data — is changing the way that we use technology. Week Four highlights the importance of protecting critical infrastructure and properly securing all devices that are connected to the Internet.
Week 4: 20–24 October 2014
Theme: Cyber Security for Small and Medium-Sized Businesses and Entrepreneurs
Small and medium-sized businesses are an important part of our nation's economy, but they often do not see themselves as a target for a cyber attack. Strong cybersecurity practices are vital within these organisations. Entrepreneurs are recognising the cybersecurity field as a burgeoning marketplace. This week will focus on what emerging and established businesses can do to protect their organisations, customers and employees, as well as cybersecurity as a business opportunity using tools such as the DHS C^3 Voluntary Programme.

Week 5: 27–31 October 2014
Theme: Cyber Crime and Law Enforcement
This week will help to draw awareness to, and educate law enforcement officers about, how to assist their communities in combating cyber crime and educate the general public with ways to protect themselves from becoming a victim of identity theft, fraud, phishing and other crimes.

More information can be found at: www.staysafeonline.org

ANNEX C

310 Trend Micro qualified and trained Internet Safety advocates worldwide who dedicate their personal time to Internet safety education.

3 000 events hosted worldwide focusing specifically on education directly with students, teachers, parents and guardians.

225 000 parents/guardians and teachers have attended Internet Safety evenings worldwide.

60 000 students and parents/teachers have engaged in our **What's Your Story** Competition worldwide.

55 000 students have attended our Internet Safety programmes worldwide.

40 partnerships worldwide, working together with partners closely aligned to ISKF mission and vision.

Feedback and Testimonials:

'Thank you so much! We learned very important info and had great discussions! Thank you!'

Sharonville Elementary, Cincinnati, OH, USA

'**This programme really helps me to think about safety and I now have a great opportunity to create some family rules at home.'**Parent @ Security Summer Seminar for kids and families, Tokyo, Japan

*'All the classes showed a considerable interest in the lessons carried out, following with attention to both explanations proposed, presentations and movies. Many students asked specific questions. Each student was given a booklet for further study or as a reminder. Overall, the initiative was very interesting, precise and careful and the assessment can only be very positive. The increasingly valuable collaboration between schools and local resources in order to constantly improve the provision of training for the benefit of all the participants should be emphasised. Trusting in continuity over the years of this particular project, we express gratitude and appreciation to the organisers for the valid proposal, for their efforts, for the materials received and for their ongoing support.' **Dirigente Scolastico, Scuola Media Statale Peyron, Italy***

'**Social networking plays such a big part in young people's lives and this is what attracted us to '**What's Your Story'.** It is very relevant and very real to young people everywhere. We really do need to raise more awareness about online safety and responsibility and are very proud that our film will be used as future educational material too.'**Siobhan Fitzgerald, (teacher) & overall winner of What's Your story, Ireland

***'**The **What's Your Story** competition gives young people the opportunity and the space to consider how their Internet use affects them personally. Webwise.ie is very proud to be associated with an initiative that encourages children to be creative and to express themselves freely on topics that are of great importance to them. In the context of ubiquitous Internet access, it is vital that we implement strategies such as this that focus on empowerment, prioritising critical thinking and engagement.'*

Simon Grehan, National Centre for Technology in Education, Dublin City University, Ireland.

ANNEX D

Available Course Modules

Below are course overviews from funded faculties:

Dusko Pavlovic (Royal Holloway, University of London), Social and economic processes for information security

The course provides content to inform future security professionals, on one hand, about the economic tools that address some of the needs for quantitative methodologies; and on the other hand about methods to include security into economic and business analyses. The need for such methods is increasingly felt among the security practitioners and stakeholders. This course brings together some methods normally taught to the students of economics, with some methods normally taught to the students of computer science.

Angela Sasse (University College London), Usable Security through Serious Games

The approach for engaging this faculty was teaching material to develop a game 'Serious Game — for our 'People and Security'. This game is to help students understand the complex interactions between technical and human elements in an organisation, business processes and information security policies and mechanisms, and information security risks and organisational strategies for making a profit. The aim is to enable students to identify information security risks in a specific organisational context, and manage them in a way that fits with the organisation's business goals, processes and culture. Additionally, this game helps students to learn about complex interactions (by showing hidden costs, and the side and downstream effects of deploying security mechanisms), and increases student motivation because the game adds fun and competitive elements. Students will play parts of the game in single-player mode to acquire the basic concepts, but the application to specific organisational scenarios will be a multi-player game.

Michael Huth (Imperial College London) Integrating Security Protocols into the Curriculum

The teaching materials developed in this area of security were based on protocol design and validation, which students can then use in order to acquire skills and competencies in modelling and analysing such protocols through the active use of bespoke formal methods tools.

Ingrid Verbauwhede (KU Leuven), Secure Embedded Circuits and Systems

We developed a set of courses focused on Secure Embedded Circuits and Systems. Here a traditional circuit designer typically has to balance three optimisation goals: area, throughput and power/energy consumption. However making the implementation of cryptographic algorithms and components physically secure adds a fourth optimisation goal. The circuit implementation also has to resist physical attacks, both active and passive attacks. The curriculum also contains hands-on experiments and lab sessions to introduce students to the challenges that they will be facing in developing new embedded ICT circuits/systems.

N. Asokan (University of Helsinki) Mobile Platform Security

The faculty created two new courses on security technologies for advanced Computer Science students. Software Security: the motivation behind this course, when the industry recruits new CS graduates to work on software projects, they usually need to provide in-house training on selected software security aspects. The objective of this course was to expose students to

Software security methodologies that are widely used in the industry. The next course was Mobile (Platform) Security: The objective of this course was to provide students with the background necessary to carry out graduate-level research in mobile platform security.

Aleksy Schubert (University of Warsaw), Constructing Trusted Code Base
The support to this faculty created a new course on security technologies for advanced Computer Science students. Constructing Trusted Code Base (TCB): The objective for this course was to provide students with the basic information concerning the TCB and contemporary methods to construct such software and combine it with hardware platforms. Further, material was provided to students with an understanding of the main cryptographic schemes currently in use and the associated challenges in applying these schemes.

Jean-Pierre Seifert (TU Berlin), Embedded System Security Course Development
This course looks at integrated course modules on embedded system security and addresses areas such as common software security problems and what are their underlying causes. Further it will bring students' attention to techniques, guidelines and principles, and tools to prevent or detect security problems such as buffer overflows, integer overflows, SQL injection, XSS and race conditions. They will develop skills and techniques to prevent or detect problems including threat modelling, check lists and coding standards, static analysis tools, code reviews, typing, static analysis, language-based security (or platform-based security), security middleware, runtime monitoring, information flow analysis, programme verification and proof-carrying code.

Looking at Privacy
This year Intel launched a new initiative in privacy to extend and complement the security curriculum initiative. The privacy initiative will seek to engage universities in the area of multi-disciplinary privacy education. The mission of this programme is to develop a pipeline of capable students who understand multi-disciplinary privacy challenges, can to help create privacy aware technologies and privacy-friendly ecosystem. To meet the scope of this mission, the programme is sponsoring faculty teams (e.g. a technologists, economists and policy professionals) that can leverage each of their respective strengths to develop comprehensive content. The output from these teams will be multi-disciplinary curricula content that will contain elements of privacy technologies, user requirements, user psychology, and legal, economic and policy frameworks for privacy.The privacy initiative will seek to engage faculties in privacy topics that are cross-cutting i.e.: data protection; privacy policies and regulations; legal frameworks for privacy, economics of privacy; regional differences in privacy; usability and user adoption, information usage models. But the programme also has a technology focus i.e.: privacy-preserving protocols and architectures; re-identification and other privacy attacks; privacy by design; user-controlled privacy models; and privacy support in low-power devices.The first funded faculty team under this new initiative was with MIT Professor Daniel Weitzner (Law/Internet public policy) with co-authors Hal Abelson (Computer Science) and Michael Fischer (Anthropology) for multi-disciplinary, cross-cultural perspectives on information privacy. The objective of this work is to develop curriculum content aimed at providing CS undergraduates with a cross-disciplinary and cross-cultural perspective on privacy. Additionally, this grant ties in collaborations with universities in Brazil, UK and the Netherlands.In conclusion, the above-funded faculty and their content areas are important topic areas and students with those skills would be desired by industry. Intel's Security/Privacy Curriculum Initiative focuses on stimulating the formation of an academic community to develop and share content knowledge, which addresses student learning needs by providing the foundation for needed skills and the tools of tomorrow.

Catalogue number/ISBN/DOI/EN TP-04-14-676-EN-N 978-92-9204-089-5 10.2824/32322

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