**Worldwide “Information Security Education & Solidarity”**

**ISES-Initiative**

Proposal for an IFIP TC 3 Task Force 2014-2017 on **ISES**

By Bernhard Hämmerli, Chairman of SI (Swiss Informatics Society), member of IFIP

**Prolegomenon**

In addition to our input in some action lines (AL) for statement and visions, there are at least three ways to use/consider the following proposed initiative:

1. **To continue to incorporate in AL c1/c2/c4/c5/C7 e-learning/C10/C11 some relevant fact linked with this initiative, or**
2. **To find/elaborate a cooperative mechanism for supporting from the WSIS facilitators the IFIP initiative, or**
3. **To reverse the way to achieve the goals by tacking at the WSIS facilitators level the initiative and asking IFIP tp put in action**

**The Challenge**

Internet is global, and we are electronically all interconnected: We face a Data Tsunami and an according explosion of world-wide stored and exchanged data: Nobody should be excluded from this innovation and to foster development of poor region it is an utmost important issue to participate in the next generation of data usage and exchange. The data sciences and its data engineering is crucial for inclusion of all regions in the digital society. Smart applications and technologies require smart citizen in a smart society or – as Prof. Seang-Tae Kim from South Korea, - smartizen. To manage lowering – or even closing – the gap between advanced and poor regions there is an all-over penetration of all societies and smartizen with access to devices and internet required. Unhappily poor regions are flooded today with cheap, partly used, but almost in any case insecure devices. Lack of knowledge, high prized security and protection software, missing knowledge on secure behaviour lead to inacceptable challenges in information security. And having security challenges in global net, means to have globally security changes. This means failure in Asia and Africa can have immediate impact on the first world: We depend on each other. Against this background, we need urgently to improve the security level in each single location, such that we reach as fast as possible minimum protection goal and standards all-over the world.

We know that information security depends on three key elements:

1. **User behaviour and protection**: If user do not protect their selves, or are not sufficiently informed on secure behaviour, it will not be possible to run a secure system.
2. **Accessibility of secure software and protection software** (internet security, virus control etc.) at no or reasonable cost in terms of local conditions.
3. **National efforts such as cyber laws, forensic capabilities, incident response capabilities, and exchange** and partnership procedures **to react in the international context** are needed for reaching minimum global protection level.

With our task force we will address topic 1 (Education) and elaborate for 2 (accessibility for internet protection) and 3 (international partnership) recommendations, such that we could reach a far more secure and better protected digital infrastructure in near future.

We strongly belief that our contribution is essential for the Millennium Development Goals MDG 2015+ as well as WSIS +10 and beyond

**Preliminary recent Action towards Solidarity Initiative**

In the World Conference on Computer in Education (IFIP WCCE 2013) in Torun, Poland, we had a session on information security education see Annex2 with contribution of experts see Annex 1:

* Frank Mockler, ECDL Foundation, an institution working on computer literacy, haven also a program on basics on information security,
* Tone Hoddø Bakås, working at Norwegian information security centre,
* Serah Francis, information security experts from Kenya,
* Adrian Kapczyński, senior expert, Poland
* Bernhard M. Haemmerli, president Swiss Informatics Society, Switzerland

The result demonstrated clearly the need for further action on information security education, as well as in European Member states as in developing and emerging countries. The initial policy requests (see Annex 2) have been confirmed and extended to the following issues:

1. **Recommendation 1**Introduce IT security competence to national regulations or guidelines referring to the teacher’s qualification profile, as post qualification and in the teacher’s curriculum.
2. **Recommendation 2**Education of IT Security should be mandatory at all levels of education.
(scholars, apprenticeship, high school, university)
3. **Recommendation 3**Implement recognised training programmes and certifications that benchmark the user’s levels of IT security skills and knowledge against a publicly expressed standard in the second and third tiers of national education systems.
4. **Recommendation 4**Promote security awareness on cyberspace to ensure secure online environment for conduting scholar, business, governmental and other activities by strengthening collaboration amongst all stakeholders and policy making.
5. **Recommendation 5**Demand the responsibility of all stakeholders, especially including parents, for their duties toward a worldwide secure ICT and internet operation.

**Or Recommendations as short version:**

1. **ICT-security competence (hands-on and background knowledge ) is core for all instructors and supervisors such as teacher and parents.**
2. **Apply ICT-security certification for all participants in the net.**
3. **Strengthen ICT-security by worldwide agreed standards and according policies on education, responsibility and digital forensics. This challenge is a global one!**

Furthermore it was pointed out, that in developing countries mobile internet devices are spreading out fast, but with no – or completely insufficient – internet security protection. The level of know how in information security is nearly zero and it is very likely and easy to victimise the population of developing countries. Actions on this issue are urgently requested.

In working issue 3 international security partnership, FIRST (Forum of Incident Response and Security Teams, [www.first.org](http://www.first.org), premier organization and recognized global leader on this issue) has made in Africa a workshop in October in 2013 to educate experts in forensics and incident response, The conducting expert Margrete Raaum from Norway (FIRST board director) is willing to support our initiative

**Worldwide Information Security Education and Solidarity Initiative**

Information Security Education and Solidarity seems to be the utmost important issue to reach a more secure global internet. For this reason we want to create a working group starting in 2014 with the goal

to have a ready to approve ISES **Declaration on Information Security Education and Solidarity**

for the IFIP WCCE 2017 in Dublin Ireland.

For reaching this goal we ask the board of IFIP for:

* Approval of the Initiative, such that ISES can act on the initiative on behalf of IFIP TC3,
* To start an according working group with initially around 10, later maximum size of 30 experts,
* To act according the proposed agenda (milestones) below and facilitate up to seven in person meetings for finding consensus
* An estimated budget is actually in preparation

**We kindly ask IFIP to approve the Worldwide Information Security Education and Solidarity Initiative with the goal of a Declaration on Information Security Education and Solidarity (ISES).**

**Draft Agenda / Roadmap of the ISES taskforce**

**Roadmap and Milestones**

* Each year during WSIS Forum
* In addition some events are planned in IFIP circles such as :
	+ In 2014 a exploratory workshop during KEYCICT in Potsdam <http://ifip-education.ning.com/events/ifip-wg-3-1-wg-3-2-wg-3-3-conference-key-competencies-in>
	+ In 2015 a full stream in IFIP WCC’2015 at Daejeon among the 4 pillars of the congress (New IT-oriented jobs for near future, Seoul accord and related topics, IP3 (IT professionalism and certification) related topics, K-12 creative IT Education)
	+ In 2016 International Hearing (location to be fixed)
	+ In 2017 one of the main stream during IFIP WCCE’2017 in Dublin
	facilitate presentations and strategic dialogue on the
	**Declaration on Information Security Education and Solidarity (ISES)**
* Interleaved events with other multi stakeholder and reinforcement of the regional cooperation

We will start initially with a small group ca. 10 experts, and will grow in numbers as the project demands. Discussions should remain in groups, and the core group should not extend 35 expert. In hearings of course, we expect to facilitate strategic dialogues with larger audience.

We will use electronic communication and in person meetings only, if necessary to drive the process forward.

**Annex**

Annex 1: CV of Initial Experts for the Initiative
Annex 2: Submission to WCCE Poland 2013 for a Strategic Workshop

**Annex 1: CV of Initial Experts:**

## Biographies

##

|  |  |
| --- | --- |
| Internetbild1 | **Bernhard Hämmerli** is Professor at University of Applied Sciences Lucerne and at University College Gjovik. He is President of the Swiss Informatics Society and CEO of Acris GmbH, a consulting company in CIP, IT - and Information Security. He built up two master programs: Information Security and IT-Network Manager. Furthermore, he contributed to CIP development in Governments, EU-level and Research. He is with Javier Lopez chair of Critis Steering Committee.  |
|  | **Tone Hoddø Bakås** have been working in Norwegian Centre for Information Security (NorSIS) for seven years. NorSIS are raising awareness threats, making people aware of important security measures and are working to improve security culture in Norwegian small and medium businesses, as well as the inhabitants. She is project Manager for the National Security Month in Norway.  |
|  | **Serah Francis from KEnya** is a Student at Gjøvik University College, Norway. Currently, doing a Master Thesis on ICT and IT-Security Strategy and implementation in Kenya. Previously, worked as a Training Coordinator, developing in-house workshops on ICT for small businesses and a System Analyst in different organisations. Holds a MSc in Forensic Computing and BSc in Business Information Systems from University of Derby, UK. |
|  | **Adrian Kapczyński** is a lecturer and project manager with over 15 years of professional and academic experience acquired in the field of information security. Currently holds the positions of assistant professor at Silesian University of Technology in Gliwice and Academy of Business in Dabrowa Gornicza. Since 1998, he is gathering professional experience in developing and customizing sophisticated security solutions for two polish companies: AutoID Poland and Infoprotector. At Polish Information Processing Society, he is holding the position of president of the board of PIPS Silesian Chapter, as well as being a member many associations. |
|  | **Frank Mockler** is Head of Programme Standards at ECDL Foundation, the certifying authority of the leading international computer skills certification programme – ECDL / ICDL. He has almost 20 years’ experience in electronic publishing, instructional design, and curriculum development. Frank is a member of the CEN Workshop on ICT Skills and is a graduate of Trinity College Dublin and the University of Essex |

**Annex 2:** Submission to WCCE Poland 2013 for a Strategic Workshop

**On Teaching/Learning Information Security: Multi-Country Overview**From Philosophy and Ethics to Implementation

**Bernhard M. Haemmerli, Frank Mockler, Tone Hoddø Bakås, Serah Francis and Adrian Kapczyński**

**Abstract:** Teaching Information Security is raising awareness, creating attitude and anchoring in behaviour. More than 20 years of experience in this topics lead to specific structure how to educate. Today, we need to address the ethical and philosophical questions to reach engagement and insights, educate the daily routine on base line IT- and information security protection. Furthermore, public initiatives such as “Information Security for Kids” and Awareness raising from Norwegian information Security Centre NorSIS demonstrate supportive measures from non-government organizations NGO. A look towards Africa at the example Kenya will complete the view on needs in different cultures and how these interdepend.

**Overview:** We intend to give a broad overview on successful practice in information- and IT-security education by advanced institution in Europe. First, we communicate the results of a study of the Swiss Academy on Engineering Science on the topic sustainable use of data. Thereby a lot of very basic questions arise on what it means to have non-deleteable data in the information age, and where courage ends and stupidity starts. Also privacy issues will be discussed. Seven major issues will be presented and the findings of those.
Second we will introduce European Computer Driver Licence ECDL-security course with the aim to enable the computer user (rather than IT professionals) to identify and protect themselves and their organisation from common security challenges when using ICT. Upon completion of the module, the candidate shall be able to understand the key concepts relating to the importance of secure information and data, physical security, privacy and identity theft, to protect a computer, device or network from malware and unauthorised access, to understand the types of networks, connection types and network specific issues including firewalls including secure use of the Internet, to understand security issues related to communications including email and instant messaging, and to backup and restore data appropriately and safely, and securely dispose of data and devices.
Third, we will demonstrate what Norwegian Information security Centre has developed within 10 years of operation. The focus of this presentation will be on Awareness, ID-theft and service of helping people to delete information and pictures on the Internet. After an overview on the activity fields the focus will be twofold: First Norsis presents success and lessons learnt by doing awareness. Also it will be pointed out, how general awareness for citizen and businesses will impact teachers and scholars and students. Second the campaign “information security for kids” and “Delete Me” will be presented and experience on impact and effect will be given.

Forth, the istuation on information security 3education and awareness in Poland, as an advanced example of the new Member states of EU will be presented and analysed.

Fifth, the IT Security awareness on Information Security Strategy for developing countries is presented with Kenya as a case study. This study will analyse the situation in Kenya by defining ICT Strategies, Legal framework, Level of ICT Skills and IT Security Awareness. The results will be compared with other international Cyber Security Strategies and any issues will be discussed and a list of improvement proposed.

After those presentations lasting for around 60 minutes, we will start with a discussion on request to policy makers. Upfront we will prepare hypotheses which will be discussed with the experts and the audience. The intention is to develop a position statement which should serve IFIP to start an initiative on information security education.

Moderation: Prof. Dr. Bernhard Haemmerli, Lucerne University of Applied Sciences and Arts, President Swiss Informatics Society, Leader of the Security topic Platform of Swiss Academy of Engineering Sciences

Participants: Presenters/Experts + WCCE’2013 participants

**Initial request to policy:**according these lines we will facilitate a debate. In case of acceptance the discussion issues will be shaped and fine-tuned.

1. It is important to raise awareness for Information security at schools equally as today first aid; traffic awareness and other important topics risk are taught.
2. Children will be next generation managers. To come better in information security it is important to reach the children, and engage with according political support for this purpose.
This is justifiable because children learn easy are ready take care of information security. Furthermore several programs have demonstrated that children are sufficiently mature for decision making on posting to social media.
3. Implement recognised training programmes and certifications that benchmark the user’s levels of IT security skills and knowledge against a publicly expressed standard in the second and third tiers of national education systems.
4. Introducing IT security competence to the national regulations or guidelines referring to the teacher’s qualification profile.
5. Organise awareness campaigns targeted at parents of primary schools pupils to highlight the need for IT security education from the moment a child first interacts with IT.

**More in-depth about the presentations**

**Bernhard M. Hämmerli, Lucerne University of Applied Sciences and Arts, President Swiss informatics Society**

Recently a brochure within the Swiss Academy on Engineering Science on the topic sustainable use of data will be used at the 30 year celebration of Swiss Informatics Society for inspiring with philosophical and ethical questions 150 scholars (10-12 grades). With this activity the society wants to attract more students for informatics and IT curriculum. The discussion domains will be prepared with presentation and question will be very fundamental to inspire a dialogue.

1. IT Security: How national government protect the citizen?
Cyber defence projects and Information sharing centre and privacy (Why can national government protect us not completely, and why are base line protections not sufficient?)
2. Trust and confidentiality: (crypto is only a small part. Moreover it deals on data classification, applying classification, dealing with authorization and rights, and why access rights are not always sufficient protection?
3. Long term archiving, storing data, decaying of data, lifelong data. (Why are temporal data different from long term data? Why is the handling of long term data so challenging?)
4. Data: Discussion on how data are perceived differently during history, in various cultures and groups.
Example 1: A risky picture in a social network may lead into troubles, when entering a traditional Arab country.
Example 2: Assuming a critical statement was made in Germany in 1929, 1939 and 1949. At least in period this could lead into jail or even to end deadly. The difference between today and these times is that such critical remarks remain stored in the systems, and can be recalled any time: What do those facts mean for us? How should we behave, that we remain courageous and open as well as avoiding stupid vulnerabilities.
5. IT and crime: What are threats for citizen and the infrastructure of a nation?
6. Data organization: What are good practises? How we structure reasonably? Can we rely on search engines?
When we should – or have to delete data? And are data really deleted, when we delete them?
7. Open government data (OGD) & public data: (Which are data are public, which one private. How we can OGD data be evaluated, and how we can get access to OGD? Which conclusion we can take from those data?

**Frank Mock**

**Background: Developing core IT security skill in students – ECDL Foundation’s IT Security module**

Growing concerns about security when using technology point to the need for a structured approach to knowledge and skills development among students. Students are often seen as intuitive users of technology, but they may not apply good security practice, or they may not by fully aware of the threats posed to their personal data and information. Important security concepts are transversal, and can be introduced in the context of different learning activities. But the importance of security can be emphasised by developing specific interventions. ECDL Foundation’s IT security module is intended for people in different contexts, including education, who spend a considerable amount of time online or using a computer. It helps to protect both themselves and their data from a range of fraudulent or malicious activities. Specifically, it covers topics including security concepts, malware, network security, secure web use, communications, and secure data management. These topics are not only essential for students as they manage their own work but are also important in preparing them to be safe online citizens and effective knowledge workers.

**ECDL IT Security** **Module** has been developed to enable the computer user (rather than IT professionals) to identify and protect themselves and their organisation from common security challenges when using ICT.

Upon completion of the module, the candidate shall be able to:

1. Understand the key concepts relating to the importance of secure information and data, physical security, privacy and identity theft
2. Protect a computer, device or network from malware and unauthorised access
3. Understand the types of networks, connection types and network specific issues including firewalls
4. Browse the World Wide Web and communicate on the Internet securely
5. Understand security issues related to communications including email and instant messaging
6. Backup and restore data appropriately and safely, and securely dispose of data and devices.

ECDL / ICDL certification programmes is the international standard in end-user computer skills.  ECDL / ICDL certification programmes consist of modules which define the skills and competencies necessary to be a proficient user of a computer and common computer applications. Each ECDL / ICDL module provides a practical programme of up-to-date skills and knowledge areas which are validated by a test.  Currently, there are 13 ECDL / ICDL modules in total.

**Tone Hoddø Bakås
Norsis: Awareness Raising and Information Security**

Norwegian Centre for Information Security (NorSIS) is part of Norway’s focus on information security. The centre aim to make information security a natural part of everyone’s daily life. Our primary target group is the small and medium sized enterprises as well as the public citizen. Our ambition is to provide services for every part of the society.

 NorSIS will try to reach its objectives through raising awareness about information security through training and information and compilation and creation of guidelines and tutorials concerning information security topics. We have conferences, campaigns and several projects to reach the public.

Slettmeg.no ("deleteme.no") is a service from Norwegian Centre for Information Security (NorSIS). The aim of this service is to help people who experience privacy violations online. The service was launched in March 2010. Slettmeg.no offers advice and guidance to people of all ages who find offending material about themselves on the Internet. Offending material might be photos published without permission, fake profiles on different Internet services, incorrect personal information or harassment.

Norway has seen an increasing activity of ID theft and fraud with people's ID. We have seen trends from abroad switching over to Norway such that qualified attacks directed to several players lead to new issue on corporate agendas. Norwegian centre for information security (NorSIS) put the spring of 2007, identity theft on their agenda after visiting Canada (CIPPIC). In the autumn of 2007 we began work to establish the preliminary study of ID-theft. Since then ID-theft has been an important work program for NorSIS.

**Full CV of Experts**:at disposal