Final Report ISES

Information Security Education   
and Solidarity Initiative

**From May 2014 to Dec 31, 2015**

UNESCO PP Project with Request No \*7290117321  
 with the title “Information Security Education and Solidarity Initiative”   
with the approved amount of 16’000 USD

**Bernhard M. Haemmerli  
ISES Project**

**Raymond Morel  
IFIP Special Advisor and ISES TC3 Chair**

**March 16, 2016 in Lucerne**

# Formal Report on ISES

## Abstract on Project Content and Goals

We reached all main aims of ISES:

* ☺ A worldwide partnership to build capacity and engage in digital equity.
* ☺ Identify critical technology gaps within the networks in developing & developed countries and how those loopholes can be closed (see ANNEX III).
* ☺ Establish new Cyber Models which are based on cultural, linguistic and institutional diversities (e.g. Africa, Asia & South America).
* ☺ Closing of the Digital and Knowledge Divide through knowledge sharing between Developing and Developed nations to fulfil strong prerequisite for success of ICT development; trust and confidence.
* Summary: we reached all aims of the proposal except the spread out to South Amerika (point 3)

In addition to the ISES proposal points of further reflection of the preliminary aims were all addressed, some more in-depth, some were dealt with more on the surface.

## Abstract on ISES events and activities for period 2014-2015

* ☺☺☺ additional not in goals: WISIS 2014 in Geneva: Special presentation on ISES
* ☺ TC 3:  Education to IFIP  GA,  Vienna, Austria, 12th and 13th of September 2014 by Bernard Cornu - TC3 chair +  THE ”TORUN VISION”.
* ☺ Task Force Meeting in (TBD) 4Q-2014 depending on the results of the proposal. This will be a working meeting to set out the real agenda and the real work in a global context.
* ☺ In 2 additional not in goals:015 ISES Meeting through video conferencing tools in first semester (TBD) with only a few people who want to engage from different regions with heavy point on IT security curriculum.
* ☺☺☺ additional not in goals: WISIS 2015 in Geneva: Full Workshop on ISES
* ☺ In 2015 IFIP Working Conference (WG 3.1 and 3.3), Vilnius, Lithuania, “Digital technologies, towards a new culture of learning: Computing for the next generation (DTCOL)”. Face to face meeting with ISES members and 1 or 2 paper presentations.
* ☺☺ 2015 a full Two (instead of one) stream in IFIP WCCE’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). This will be meeting face to face with engaged participants to discuss this project in perspective of a country to create community. A presentation of the work done for the whole year and to prepare for Phase 2.
* ☺☺☺ additional not in goals: Seville Spain: Seville, ICERI, November 2015

## Abstract on multiplier effects

In several dimensions, we had multiplier effects:

1. Annex 4: We could attract 57 members to cooperate with ISES
2. We were sending out questionnaires and received feedback
3. Spread out in 10 international presentation / workshops
4. We created an IFIP TC3 Taskforce on ISES which is by Raymond Morel
5. We could stimulate by new models, disclosed by expert for more ISES

## Abstract on Finances

1 Africa: Serah Francis 24.5%; 2 Nepal: Rajan Pant and Amibika Shrestha 37%; 3 India: Krishan Murali 33.8%; 4 Admin (Money transfer, other costs 4.7%): In total 14464 Euro (16’000 USD)

Western Expert were not paid out of UNESCO PP funds. All receipts are stored at both places for 5 years: Acris GmbH Prof. Hämmerli and IFIP Secretary Eduard Dundler.

## Conclusions

As expected, the project is very successful. But: every project leader would state this.

However, ISES can prove that all points of the submission were completed, and we covered even adding additional work packages in the frame of ISES project:

1. Four additional meetings
2. Disclosing new facts, e.g. that free of charge updates and virus control does not help in least developed countries, when the bandwidth costs are limiting.
3. Educational efforts in security are paramount: Except engaging in education and awareness, we cannot improve the situation.
4. Creating LDC ICT and security policy by copy past, does improve international compliance of LDC, but does not bring any progress. The important act is the discussion, which takes place to develop new thinking.
5. There are many low cost models, e.g. exchange of staff within sabbatical, tele support sessions etc. All this does work much better on individual level, but not very good on institutional level.

As always buy in with a new topic is hard: but the message ISES is very convincing, and daily more urgent, because more damage to society and poorest amongst us is happening. On behalf to this part of the population, we thank UNESCO PP for its support.

The state has the responsibility for national security, citizen welfare, economic growth, public health and a range of aspects that are fundamental to the prosperity and well-being of a country. The internet has become part of public and private life that it is now a vital component in almost all of these areas of state responsibility.

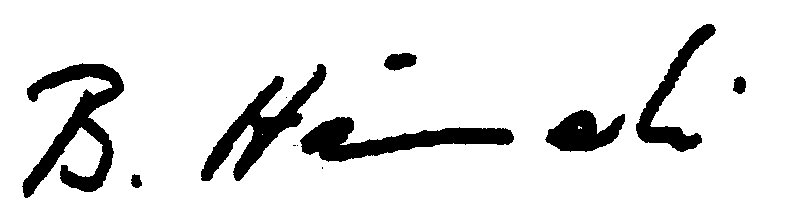
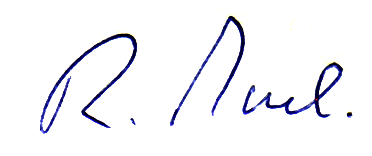
In response, governments are developing cyber strategies, policies and plans to address the enormous benefits an associated risks that come with the rise of internet connectivity. The question is what are the responsibility of nations in providing cybersecurity for individuals, organisations and its own operations. How can the government think about using cybersecurity to hel enable their country to benefit from the full potential of the internet. Important for governments:

1. Understand cybersecurity hierarchy of needs at a national level allows governments to take advantage of growing opportunities for the internet-enabled economy while improving risk management for existing and future cybersecurity threats

National Cyber Security Strategy and Policy is a good start, but with no resources and political will, many will not succeed. The society (governments, businesses, and individual users) need to change their mindset and adopt cultures that reflect the digital world. There is a variety of effective and low cost models that can be adopted and exchanged. The just concluded climate change conference in Paris demonstrated how nations can work together and come to an acceptable level of agreement. Cybersecurity is a concern for all and same can be down to make sure a minimum level of security is achievable by all nations.

* A worldwide partnership to build capacity and engage in digital equity.
* ☺ Identify critical technology gaps within the networks in developing & developed countries and how those loopholes can be closed (see ANNEX III).
* ☺ Establish new Cyber Models, which are based on cultural, linguistic and institutional diversities (e.g. Africa, Asia & South America).
* ☺ Closing of the Digital and Knowledge Divide through knowledge sharing between Developing and Developed nations to fulfil strong prerequisite for success of ICT development; trust and confidence.

We certify, that all means were correctly used for the ISES project and that the report depicts the work on ISES in the frame of the UNESCO PP Project with Request No \*7290117321 with the title “Information Security Education and Solidarity Imitative” with the approved amount of 16’000 USD and a transfer of 14464 Euro to IFIP account.

Prof. Dr. Bernhard M. Haemmerli Raymond Morel

# Table of content

[1 Formal Report on ISES 2](#_Toc447118056)

[1.1 Abstract on Project Content and Goals 2](#_Toc447118057)

[1.2 Abstract on ISES events and activities for period 2014-2015 2](#_Toc447118058)

[1.3 Abstract on multiplier effects 2](#_Toc447118059)

[1.4 Abstract on Finances 3](#_Toc447118060)

[1.5 Conclusions 3](#_Toc447118061)

[2 Table of content 5](#_Toc447118062)

[3 ISES Methods and Models 7](#_Toc447118063)

[4 Country Overview 8](#_Toc447118064)

[4.1 Example of Successful Cybersecurity Implementation 8](#_Toc447118065)

[4.1.1 UK Cyber Security Strategy (NCSS), 2014 8](#_Toc447118066)

[4.1.2 International Computer Driving Licence (ICDL)/ECDL 10](#_Toc447118067)

[4.2 India and Norway (by Krishna Murali) 12](#_Toc447118068)

[4.2.1 1.1 Methodology 12](#_Toc447118069)

[Figure 11: A 12](#_Toc447118070)

[4.2.2 What to measure– Phase 1 13](#_Toc447118071)

[4.2.3 How to Measure – Phase 2 14](#_Toc447118072)

[4.3 Norway and India: comparative study conclusions 15](#_Toc447118073)

[4.4 Kenya Cybersecurity Overview 16](#_Toc447118074)

[Cyber Security in Korea 19](#_Toc447118075)

[4.4.1 Cyber Security Policy in Korea - Mr. JaeSuk YUN 19](#_Toc447118076)

[4.4.2 IT Security in South Korea - Mr. JaeDok Shim 19](#_Toc447118077)

[4.5 Nepal 20](#_Toc447118078)

[4.6 University in Rwanda 21](#_Toc447118079)

[4.6.1 Measuring Outbound and Inbound max speed Sunday May 12 8:36 local time: 22](#_Toc447118080)

[4.6.2 One Year Later… 25](#_Toc447118081)

[4.7 Conclusion: 26](#_Toc447118082)

[5 Meetings and Workshops 27](#_Toc447118083)

[5.1 WISI 2015 Information Security Education & Solidarity ISES 27](#_Toc447118084)

[5.1.1 Outcome and Political demands 28](#_Toc447118085)

[5.1.2 Support Options: 28](#_Toc447118086)

[5.1.3 Final Conclusion 29](#_Toc447118087)

[5.1.4 Contact: 29](#_Toc447118088)

[5.2 Vilnius TC 3, WCC, July 2015 30](#_Toc447118089)

[5.2.1 General ISES Background Information: 30](#_Toc447118090)

[5.2.2 General ISES Goals: 30](#_Toc447118091)

[5.2.3 ISES Session Summary of Vilnius Meeting 30](#_Toc447118092)

[5.2.4 ISES initiator Goals and Background 31](#_Toc447118093)

[5.2.5 IT Security Challenges – a Case Study in Rwanda: 31](#_Toc447118094)

[5.2.6 Cyber Security in Kenya 32](#_Toc447118095)

[5.2.7 Cyber Security in Nepal: 32](#_Toc447118096)

[5.2.8 Mission Statement: 32](#_Toc447118097)

[5.3 Korea, October 2015 IFIP TC3 Working Conference "Opening our Future Together" 33](#_Toc447118098)

[5.3.1 ISES Session Summary of Daejeon Meeting 33](#_Toc447118099)

[5.3.2 Session One: Presentations 34](#_Toc447118100)

[5.3.3 Session Two: Panel Discussion 35](#_Toc447118101)

[5.4 Bibliography 39](#_Toc447118102)

[5.5 Seville, ICERI, November 2015 40](#_Toc447118103)

[5.5.1 Abstract: Policy and Implementation Issues for Information Security Education in Developing Nations 40](#_Toc447118104)

[6 Team and Contact List of Contributors 41](#_Toc447118105)

[7 Webpage 42](#_Toc447118106)

[8 Appendix I 42](#_Toc447118107)

[9 Appendix II: ISES - Questionnaire Findings 43](#_Toc447118108)

[9.1 Cyber-security challenges 43](#_Toc447118109)

[9.2 National Cyber Security Strategy/Policy 43](#_Toc447118110)

[9.3 Strategy/Policy implementation process 44](#_Toc447118111)

[9.3.1 (a) Capacity Building 44](#_Toc447118112)

[9.4 Cyber Security Strategy - Implemention Challenges 46](#_Toc447118113)

[9.4.1 Capacity Building 46](#_Toc447118114)

[9.4.2 Child Online Protection 47](#_Toc447118115)

[9.4.3 Successful models 47](#_Toc447118116)

[9.4.4 What needs improving 47](#_Toc447118117)

[9.4.5 Stakeholders 47](#_Toc447118118)

[10 Dissemination for next period 48](#_Toc447118119)

[10.1 UNESCO 48](#_Toc447118120)

[10.2 Corporate Social Responsibility Programs (ISO 26’000) 48](#_Toc447118121)

[11 Proposal UNESCO Participation Program 2016 / 2017 49](#_Toc447118122)

# ISES Methods and Models

We have One Net and we are living on One World, but we do as it is all over a different issue in each country. First world protects cyber space quite well, while leas develops countries LDC are suffering.

The cyber space is in principle gender neutral and offers both gender many opportunities to be active and gain from this new tool. The opportunities are at this time faster taken up by males than from females. However, gender reflection is very important, and also in LDC must this issue be addressed and females should be active in both, using the cyber space, and helping to secure cyberspace. Well-defined projects help to stimulate a gender balance, and also targeting female helping to care for security is very useful. The ISES project included females because they were performing well, but we had the intention to demonstrate a positive attitude in terms of gender balance.

ISES was active on all levels:

* Policy: to stimulate for more and better communicated policies
* Strategies: to translate policies into a viable strategy for implementation. In some cases policies were rather done in “copy-paste” way. Such policies need very long time for being translated into implementation.
* Concepts for implementation: several approaches were taken on technical, organisational and strategic level to foster implementation and to create better security. However, in many cases , when launching a new issue like ISES, personal relationship networks, personal contact, and interpersonal agreements work better. E.g the expert serving via skype or email for trouble management, CERT which makes education in Africa, professors which meet in conferences, and agreeing on collaboration.   
  Such stimuli and success are not created by systematic organisational approaches, but to let such approaches happen and serve the topic is the right attitude, if feasible even to give stimuli and support. Experts reports in such cases that they get a well-feeling, when they help, and this is a good incentive.
* Cyberwar is growing and is a huge issue by today. LDC needs protection for better sovereignty and protection of their intellectual and finical assets. It is the first world responsibility to engage.

Models we found in our discussions are

* Sabbatical expert going to LDC (less preferred: LDC multiplier in Developed World)
* Good material after replacement is shipped to LDC
* Webpage support
* Model templates for reproduction: e.g. INES case
* Intro: Stakeholder: Expert, Media, Education, Policymakers
* Education and Knowledge: Agreed sharing and support.
* Solidarity  
  - Remote support for LDC peer schools  
  - Stimulate Partnerships
* BCM / DRP: will be important for the next period

# Country Overview

## Example of Successful Cybersecurity Implementation

(by Serah Francis)

Different countries are at different maturity stages of cybersecurity but lessons could be learnt from more mature models on best practices for developing and implementing cybersecurity strategies and policies. Examples of two models: Implementation of the UK National Cybersecurity Strategy and ICDL/ECDL educational programme used in many countries across the world.

### UK Cyber Security Strategy (NCSS), 2014

The UK Cyber Security Strategy was first published in 2011[[1]](#footnote-1). Since then, the strategy has been revised and the budget increased from 650 million pounds to 860 million pounds. The UK NCSS was developed after the government conducting a national Security Risk Assessment (NSRA) and prioritizing what was seen as areas of national security risk in both domestic and abroad[[2]](#footnote-2). By doing this the government was able to analyses the key security risks the country is facing now and likely to face in the future and the current state of preparedness of each risks. The outcome enabled them to determine which risks were higher priority and need to be addressed. With this information the UK government set clearly what it wants to achieve, ways in which to achieve and devoted some resources to achieve those goals.

The countries vision is “for the UK in 2015 to deliver huge economic and social value from a vibrant, resilient and secure cyberspace, where actions, guided by core values of liberty, fairness, transparency and the rule of law, enhance prosperity, national security and a strong society”. The strategy has four objectives: making the UK one of the most secure places in the world to do business in cyberspace; more resilient to cyberattack and better able to protect our interest in cyberspace; cyber security knowledge, skills and capability. The strategy is based on a risk-based approach, working with partners and balancing security with freedom and privacy.

To achieve the above objectives, the government set out some inputs to facilitate implementation of the strategy:

* building relationship with its international cooperation
* reduce vulnerabilities in government systems
* encouraging cyber security professionals in to public institutions, e.g ethical hackers
* maintaining a robust legal framework
* raise public and business awareness
* support private sector in taking opportunities that cyberspace offers

The government hoped to increase the number of experts with specialized cyber knowledge and skills in the country and for that reason half of the first 650 million pounds assigned to cybersecurity went towards enhancing building capability. Since it’s establishment the UK National Cyber Security Strategy has achieved a lot (See Figure 2 below)[[3]](#footnote-3).

**Figure 1**: UK National Cybersecurity Strategy, 2014

Achievements To Date

|  |
| --- |
| OBJECTIVE 1  **MAKING THE UK ONE OF THE MOST SECURE PLACES IN WORLD TO DO BUSINESS ONLINE**   * 750 organizations in CISP: The Cyber-security information Sharing Partnership for industry & Government * Cyber Essentials: 5 critical controls to protect businesses from common cyber threats * Cyber security exports £ 1.040bn in 2013, 22% increase on 2012 & for 2 billion target by 2016 * Guidance: ‘10 steps to Cyber Security’ & small business version   **AND TACKLING CYBER CRIME**   * National Cyber Crime Unit in the National Crime Agency: 30live domestic & International operations disrupt serious cybercrime * 9 cyber units in each of the Regional Organized Crime Units: over 85 live operations * HMRC’s cyber team: more than £100m fraud prevention this year   OBJECTIVE 2  **A UK IS MORE RESILIENT TO CYBER ATTACK AND BETTER ABLE TO PROTECT OUR INTERESTS IN CYBERSPACE**   * CERT-UK: new Computer Response Team for national incidents international CERT liaison * GCHQ working to detect & defend against cyber threats * All local authorities & councils on the Public Service Network   OBJECTIVE 3  **A UK HELPING TO SHAPE AND OPEN, VIBRANT AND STABLE CYBERSPACE THAT SUPPORTS OPEN SOCIETIES**   * Ongoing series of ‘London Process’ global conferences shaping the debate on cyberspace * 15 international visits to the UK hosted by FCO * 30 international Cyber Security Capacity Building Fund projects   OBJECTIVE 4  **A UK THAT HAS CYBER KNOWLEDGE, SKILLS AND CAPABILITY IN NEEDS**  **SCHOOLS**   * Cyber security in computer science GCSE   **APPRENTICESHIPS**   * 200 Tech Partnership entry-level jobs, first HMG & industry apprenticeship frameworks   **CAREERS & PROFFESSIONALISM**   * Initiatives for computer science students & graduates: * Cyber Security Challenge & Cyber Growth * Partnership: mentoring & ‘cyber camps’ * Campaign via Graduate Prospects website, * Virtual hub for those joining in the field   **HIGER EDUCATION**   * 4 Higher Education Academies * 6 Master’s degrees in in General Cyber * Security certified by GCHQ   **RESEARCH**   * 3 Research Institutes * 11 Academic Centres of Excellence in Cyber Security Research * 2 Centres of Doctoral Training * 66 PhDs from 2017   **WIDER EDUCATIONAL SUPPORT**   * 24,127 sign-ups for first round of Open University’s Massive * Open Online Course “Introduction to Cyber Security”   **AWERENESS RAISING**   * Cyber Streetwise campaign: Over 2 million more adults use safer online. |

The most notable improvements of the strategy implementation, is on improved capabilities to counter cybercrime, and support on research and development. The UK continue to improve the skills and capabilities as the need be. Awareness raising, working with partners both nationally and internationally is very important. The government has established websites for both end-users and SMEs which can be used by all around the world. These are lessons other countries can learn and apply where applicable. This year, the UK government also provided an international Cyber Capacity Building Fund for projects aimed to assist developing countries. The UK NCSS can be a good case study for those who are just starting to develop NCSS or others who want to enhance their strategy or policies. All progress and review reports can be viewed at www.gov.uk.

### International Computer Driving Licence (ICDL)/ECDL

ICDL programme is a worldwide certification offered in most countries and has more than 13 million candidates participating in different programs. The aim of the program is to promote digital skills as the key enabler or effective use of ICT for all. The programme offers from basic, standard to advance ICT skills[[4]](#footnote-4).

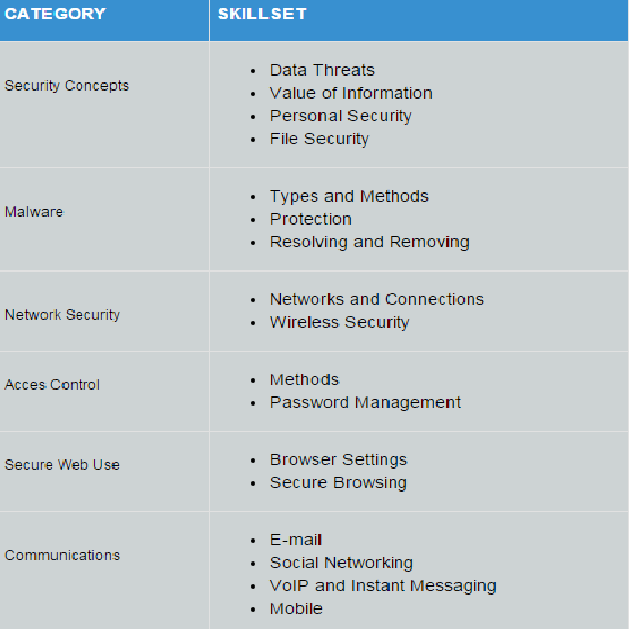
The IT Security module `sets out concepts relating to the secure use of ICT in daily life and skills used to maintain a secure network connection, use the Internet safely and securely, and manage data and information appropriately (See Figure 2). The course is flexible and is offered online but the tests are carried out in test centres across the world. The course provides sample test to evaluate IT security knowledge and prepare for the tests.

In many countries, especially in developing world, the government has endorsed ICDL as an entry-level job certification e.g. Kenya, Uganda, Zimbabwe. The course is available through National Operators who also engage with private and public sector (e.g. Ministry of Education). In some occasions governments will offer training for their employees as a one off course. The IT Security model is not very popular in developing countries due to lack of awareness and skilled trainers.

In some developed countries like South Korea, the program is fully funded by the government and offered as an extra curriculum in both primary and higher education. 60 universities in Korea has adopted ICDL (IT Security Module included) as a required certification.

ICDL is an example of an international standard successful model which could be included as part or extra school curriculum in many developed and developing countries from early school education. Public and private organization could also adopt the program too. Developing countries could benefit more if the full program was adopted and funded, as many in those countries are still digital illiterate. Although many countries have endorsed the course as a national certification, only those who can afford to meet the cost can benefit.

**Figure 2:** ICDL ‘ IT Security Module’



## India and Norway (by Krishna Murali)

First, we present the methodology of the study and then we take conclusions.

### 1.1 Methodology

In this part, we present the methodology for Measuring Information Security Maturity in Norwegian and Indian MSME’s with special focus on people actor.

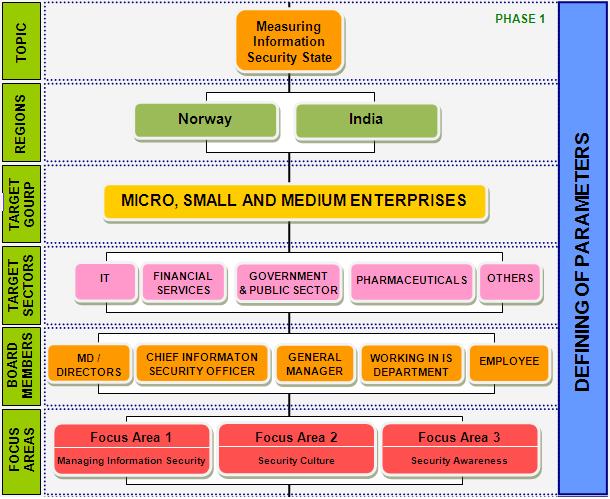
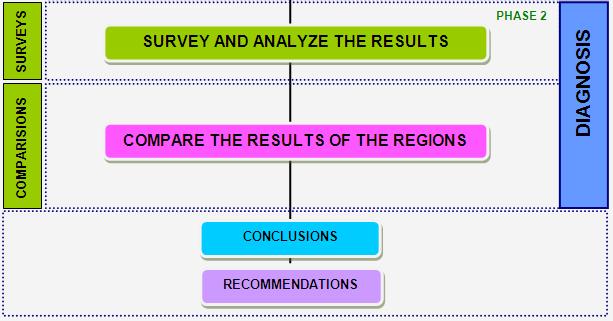


Figure 11: A **Methodology for measuring information security maturity in Norwegian and Indian MSME’s with special focus on people factor.**

**The Methodology has two phases in the measurement process:**

### What to measure– Phase 1

In phase one, the parameters like target regions, target groups, board members and focus areas are defined for measuring information security maturity levels.

The developed methodology is now used in measuring the information security maturity in Norwegian and Indian MSME’s targeting the survey participants from IT, Financial Services, Government & Public Sector, Pharmaceuticals and other industry sectors as the main target sector participants.

Normally defining focus areas is based on the requirement of different regions and target groups measurement requirements, but in this report in order to measure the maturity levels of the Norwegian and Indian MSME’s with special focus on people factor, we have used managing information security, security culture and awareness as the main focus areas for the preparation of questionnaire.

Figure 12: Focus areas on Information Security

The questionnaire developed was prepared based on the survey questionnaire prepared by Deloitte[[6],](file:///C:\Users\zahaemme\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\47DF9SXM\KRISHNA%20Methodology.docx#_8_Bibliography) Detecon [3] ,Devoteam Consulting [[4]](file:///C:\Users\zahaemme\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\47DF9SXM\KRISHNA%20Methodology.docx#_8_Bibliography) ,Data Security Council of India cooperation[[8]](file:///C:\Users\zahaemme\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\47DF9SXM\KRISHNA%20Methodology.docx#_8_Bibliography),Ernst& Young[[6],](file:///C:\Users\zahaemme\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\47DF9SXM\KRISHNA%20Methodology.docx#_8_Bibliography) Dr. Thomas Schlienger of Tree Solution [[7]](file:///C:\Users\zahaemme\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\47DF9SXM\KRISHNA%20Methodology.docx#_8_Bibliography) ,Forrester Research [[19]](file:///C:\Users\zahaemme\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\47DF9SXM\KRISHNA%20Methodology.docx#_8_Bibliography), European Network and Information Agency [[11]](file:///C:\Users\zahaemme\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\47DF9SXM\KRISHNA%20Methodology.docx#_8_Bibliography) ,KPMG[[22]](file:///C:\Users\zahaemme\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\47DF9SXM\KRISHNA%20Methodology.docx#_8_Bibliography) and Price water coopers [[29]](file:///C:\Users\zahaemme\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\47DF9SXM\KRISHNA%20Methodology.docx#_8_Bibliography) for measuring information security state in large enterprises with focus on people,processes and technology. Mainly questions from “Survey from Information Security Culture [“[12],](file:///C:\Users\zahaemme\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\47DF9SXM\KRISHNA%20Methodology.docx#_8_Bibliography)Ernst Young 2009 [[16]](file:///C:\Users\zahaemme\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\47DF9SXM\KRISHNA%20Methodology.docx#_8_Bibliography) ,“ Awareness Raising Quiz templates for parents, end users and SME “[[18]](file:///C:\Users\zahaemme\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\47DF9SXM\KRISHNA%20Methodology.docx#_8_Bibliography) by ENISA and “The State of SMB IT Security Market and Emerging Trends: 2009 to 2010 [“[31]](file:///C:\Users\zahaemme\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\47DF9SXM\KRISHNA%20Methodology.docx#_8_Bibliography) are used to prepare the questionnaire .The questionnaire prepared was mainly focusing on the people factor as people or employees in these organizations are those who maintain the technology, manage day to day security processes, influence the environment or manage security of their organizations. So it is important to focus on above people factors to understand the maturity levels of Norwegian and Indian MSME’s.

Based on the focus areas, 19 questions and answer choices were developed in different formats like single choice & multiple choice answers, rating scale and matrix of choices

|  |  |
| --- | --- |
| **S.No** | **Section Subjects** |
| 1 | Managing Information Security |
| 2 | Security Culture |
| 3 | Security Awareness |
| 4 | Background Information of Respondents |

**Table 4: Questionnaire Structure**

In normal measurement process, the above subject areas are individual focus areas for measurement. But in this study, we use all the above focus areas and subjects for knowing the MSME’s maturity levels. Further related questions on each subject areas are asked. This process of defining the parameters for measurement in phase 1 is as a step-by-step approach, which is a simple representation of a measurement process.

### How to Measure – Phase 2

The second phase of measurement process is to analyze the actual information security maturity in Norwegian and Indian SME’s defined as “diagnosis” phase. The questionnaire is now sent directly to the security custodians or individuals through emails with an online link to answer the questionnaire. The participants here are basically from the senior management or middle management or operational level positions who are caretakers, decision makers of IT and Information Security issues or employees in these organizations.

The MSME’s (target groups) in this measurement are contacted with support of NorSIS [28] and personal contacts. Survey with Indian MSME’s is done with cooperation of Institute of Electronic Governance, State Government of Andhra Pradesh, India [33] and personal contacts. Invitation Letters are sent to these MSME’s through emails with a request to participate in the survey. In addition to these emails, associations, governmental agencies and friends are contacted requesting them to support for the survey by asking them to forward this invitation to friends and cousins working in various MSME organisations for their participation.

After analyzing the results from the online survey in phase 2. A comparison study is made to compare the similarities and differences in two regions (Norway and India) with respect to information security Maturity in different industry sectors and sizes of companies. Later recommendations are recommended to the target groups to improve the information security maturity levels based on the conclusions.

The methodology is sustainable and can be applied over and over. It is fairly easy to use and output is given in a quantitative manner that is easy to understand. In general, the methodology provides a number of opportunities to beneﬁt from

* The methodology not only will measure the information security maturity in Norwegian and Indian MSME’s and focus areas, but helps to define the diagnosis parameters like target regions, target groups and sectors, target levels, focus areas, analyzing and interpretation of results in a step by step simple process and for further enhancing the methodology.
* By applying the methodology at regular intervals, the change in maturity levels can be measured and an index of maturity levels can be constructed. This will assist MSME management to measure the change in maturity levels over a period time and to take corrective action if necessary.

## Norway and India: comparative study conclusions

1. The security culture, awareness and managing information security is at a very good level in Norwegian financial service enterprises.
2. Information Security Maturity levels in Norwegian MSME’s is high compared to Indian MSME’s with respect to managing of information security and awareness.
3. MSME’s in Norway and India are having dedicated, non-dedicated staff and outside experts to manage information security, but managing information security is not similar in both the regions. Information Security is well managed in Norwegian MSME’s with having qualified staff for managing information security. Whereas information security is not managed well in Indian MSME’s due to lack of qualified experts or employee non seriousness. It is recommended that Information security management should be improved in Indian MSME’s by recruiting qualified security persons for managing information security through proper implementation of security policies, accessibility to employees and measuring them and taking measuring to protect computer & electronic data.
4. Norwegian and Indian MSME’s have different drivers for creation of security policy. An analysis of drivers for creation of security policy in India shows that there is not given much importance for Indian legislative regulations and standards. Indian government should put in effort to identify the weakness in the legislative regulations and make the legislative regulations more visible and standards stronger. So that Indian MSME’s make information security as their top priority security goal achieving their business objectives and managing information security well in their organizations.
5. The Norwegian and Indian MSME’s top management is convinced that information security is important for achieving the business objectives, but revealed also some main weaknesses in security culture in like Employee Non Seriousness, lack of right people to run the awareness activities in house, organization culture and fear and resistance to change from employees. These weaknesses should be improved. Most effort should be to put on Training & Education for employees who are not serious and fear & resistance to change with run people to run awareness activities. Also making the security experts more visible will also positively influence the security culture of Norwegian and Indian MSME’s.
6. The Norwegian and Indian MSME’s have different priorities of elements covered in the security awareness and training programs. A detailed analysis of elements covered showed that more effort should be out on improving the security awareness in Indian MSME’s with respect to incidence reporting and direct & frequent updates/alerts on current threats to their organization. The different regions also different proportions of budget allocated for information security awareness. A detailed analysis shows that Indian MSME’s are having more proportion of budget and plan to spend more in 2010-11 for security awareness compared to Norwegian enterprises. But the weaknesses in Indian enterprises with respect to the security culture, awareness and managing information security shows that that their of right people to run the awareness activities and for managing information security. Qualified staff and well-established budget plan is recommended for the Indian MSME’s with improving the security awareness with their organizations.
7. Overall, the information security maturity levels in Norwegian MSME’s is good compared to Indian enterprises with respect to the managing of information security, security culture and awareness.

## Kenya Cybersecurity Overview

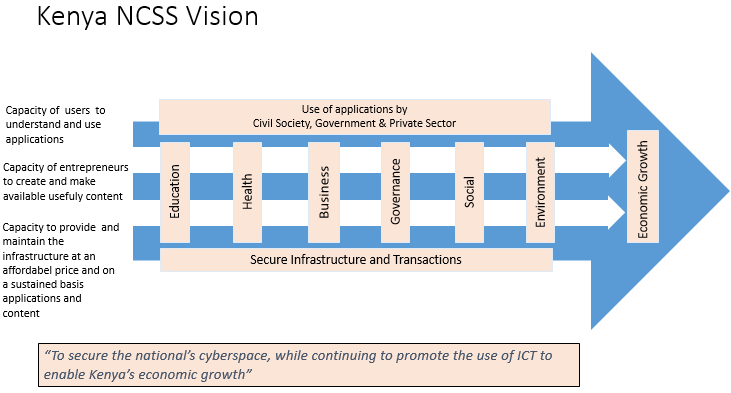
(by Serah Francis)

Kenya is one of the East African countries with a population of 45 million people as of July 2014 estimate. One of the African countries where ICT sector is playing a major role in generation of social and economic development. Through its ICT Master Plan 2014-2017, the Government of Kenya (GoK) has recognized that ICT is an important tool to improve the livelihood of Kenyans and is backed with a commitment to ensuring the availability of accessible, efficient, reliable, affordable services as well as promote anti-corruption in government and industry[[5]](#footnote-5) . By focusing on ICT developments, the GoK hopes to provide a high quality life to all its citizens by 2030.

Kenya’s such efforts to utilize ICT provides a dramatic increase in the delivery of services and sharing information across organization, social and geographical borders. A good example where the country is making a huge investment is in Smart County Projects, where the county governments need to build or improve delivery of services including health, education, revenue collection, human resource management among others[[6]](#footnote-6) . These projects include capacity building, information centres, connectivity infrastructures, communication systems, and strategic information system to name a few. Business and the tech community are also supporting the Kenyan youth to be innovative and have the exposure to the global market through technology `hubs` and incubators in the country. The introduction of The East African Marine System (TEAMS) initiative contributed to increasing internet penetration, and growth of e-government and e-commerce service, setting Kenya as technology hub in the global market. As well, the business community are using internet services for business opportunities. Many organizations are steadily embracing cloud computing, outsourcing services, Enterprise Resource Planning (ERP) automation and Bring Your Own Device (BYOD) just to mention a few.

However, the increase dependency on digital information systems has also seen an increase on cyber threat, where cyber criminals continue to exploit ICT vulnerabilities in Kenya. Report suggests that in 2013 the number of cyber threat attacks detected in Kenya cyberspace grew by 108% to 5.4 million attacks compared to 2.6 million attacks detected in 2012 [[7]](#footnote-7). A report by the Ministry of ICT noted that Kenya is losing an estimated Kenya Shillings 2 billion ($ 23.3 million) annually through cybercrime [[8]](#footnote-8) . The country had 29.2 million internet users by March 2015 compared to 21.7 million same time last year. Due to fast internet connection, increase internet penetration, growth of e-services and changing threat landscape, the country was becoming a high risk of cyber threats and attacks.

In response to these risks, in July 2014 the GoK developed a National Cybersecurity Strategy as a plan of action with activities set to contribute to the security of its cyberspace[[9]](#footnote-9). The government vision is to `secure the national`s cyberspace, while continuing to promote the use of ICT to enable Kenya`s growth`(Figure 3) .



The hope is that, with the help of NCSS, the country will be able to bring the security to a minimum level and also show the world it's commitment to cybersecurity. Implemented properly, the strategy has the potential to generate significant economic development gains for the country, by promoting users and investors’ confidence and tapping into global business opportunities.

The strategy strategic objectives are to:

* Develop comprehensive governance structures and policies
* Raise awareness in public and private sectors
* Expand cyber security education to build the Kenyan workforce
* Foster information sharing and collaboration both nationally and internationally.

The strategy outlines the increasing need to protect the critical information infrastructure and citizens, educate and train the Kenya public and workforce, develop comprehensive governance framework, enhance legislation and work with businesses and international bodies. This provides a road-map in securing the nation`s cyber infrastructure against existing and emerging threats.

One year after the first Kenya National Cybersecurity Strategy was established in Kenya, many experts argue that things have not improved and the rate of computer crime has risen. Kenya is becoming a cashless society and cybercrime will continue to rise if serious measures are not taken to secure the internet infrastructure. Most of the crime is targeted to financial sector through Kenya’s banking fraud syndicates, which is a collaboration of banking staff and the cyber-criminals. There is shortage of information security skills in the country and security awareness is very low. Although the government is trying through the national computer response team (KE-CIRT) to educate users on the risks of being online, a lot need to be done to improve the awareness.

As well as the above mentioned challenges, Kenya has no specific legislation on cybercrime. The Kenya Communications Act (Amendment Act 2009) has been enacted to deal with cybercrime. Meaning that some cybercrimes are not covered by the Act and this could lead to criminals being charged for the wrong crimes or never charged. The police and judicial departments are not well trained to handle digital evidence nor does the government has a specific digital forensic lab. The country does not have any official recognized national cybersecurity framework for implementing international recognized cybersecurity standards, or a certification framework for certification and accreditation for national agencies and public sector professionals. The certification and accreditation for cybersecurity standards is done by other entities who might not be fully equipped with skills required for cybersecurity. Same might happen with organisations hiring rogue professionals. The country does not have any official recognized research and development (R&D) program/projects for cybersecurity and no specific agency to deal with IT security awareness for users in the country. There is no specific Child Online Protection legislation neither institution support/reporting mechanisms for the same.

On the positive side, the government is showing some effort in certain areas. The Information and Communication Technology Authority (ICT Authority) under the ministry of Information Communication and Technology was established in August 2003 to manage the ICT and ICT Security functions in the country. The country already has a functioning KE-CIRTs which also facilitated the launching of the Public Key Infrastructure, although critics argue that the agency is understaffed. The government has endorsed International Computer Driving License (ICDL) programme as the entry level computer certification designed to demonstrate competence in computer use and is working with academics and businesses to develop a cyber security curriculum for high education. The ICDL ‘IT Security module’ could be promoted to create awareness among users and workforce in the country. The first Cyber security training program was introduced last year at the University of Nairobi through the ICT Authority and private partners. The GoK is working with the East African countries to harmonize and improve legislation with the help of ITU-IMPACT. In August 2015 the government launched a campaign on Child Online Protection at an annual conference for Kenya Primary Schools Head Teachers Association (KEPSA) and was supposed to last for 3 months.

A ‘Draft Policy Framework for the Critical Infrastructure Protection’ has just been published by the government of Kenya and ‘The Critical Infrastructure Protection Bill, 2015’ is already in parliament waiting to be passed. A critical infrastructure protection unit will be established to provide leadership in the implementation of the policy in partnership with private sector owners. Three sectors namely; Transport, Energy and Petroleum has been defined as the Kenya’s critical infrastructure needing protection. The government already faces challenges such as weak laws and skilled workforce. It is hoped that the new bill will facilitate collaboration and information sharing between all stakeholders and improve the protection of critical infrastructure in Kenya.

Cyber Security in Korea

**(both paragraphs are also included in the conference overview,   
reported by Raymond Morel)**

### ****Cyber Security Policy in Korea - Mr. JaeSuk YUN****

Mr. YUN discussed ICT environment in Korea, trends on cyber-attacks, cyber security policy and implementation.  The government of Korea has been very active in promoting cybersecurity for some time, due to security threats from outside the country.  Mr. YUN pointed out that a multistakeholder approach led by KISA (Korea Internet and Security Agency) with support from the government has led to the successful implementation of Cyber Security Policy of Korea.  With this success Korea is able to share its model with interested countries.  Already, the country is cooperating with developing countries in areas such as sharing know-how on incident response, providing cyber security system, training & business opportunities and consulting about cyber security policy & strategy. He also explained how Korea is playing its part in global arena by supporting cyber capacity building for developing countries and sharing practical cyber security knowledge and experience through their practical global cybersecurity center for development & cybersecurity alliance for mutual partnership (CAMP).

### ****IT Security in South Korea - Mr. JaeDok Shim****

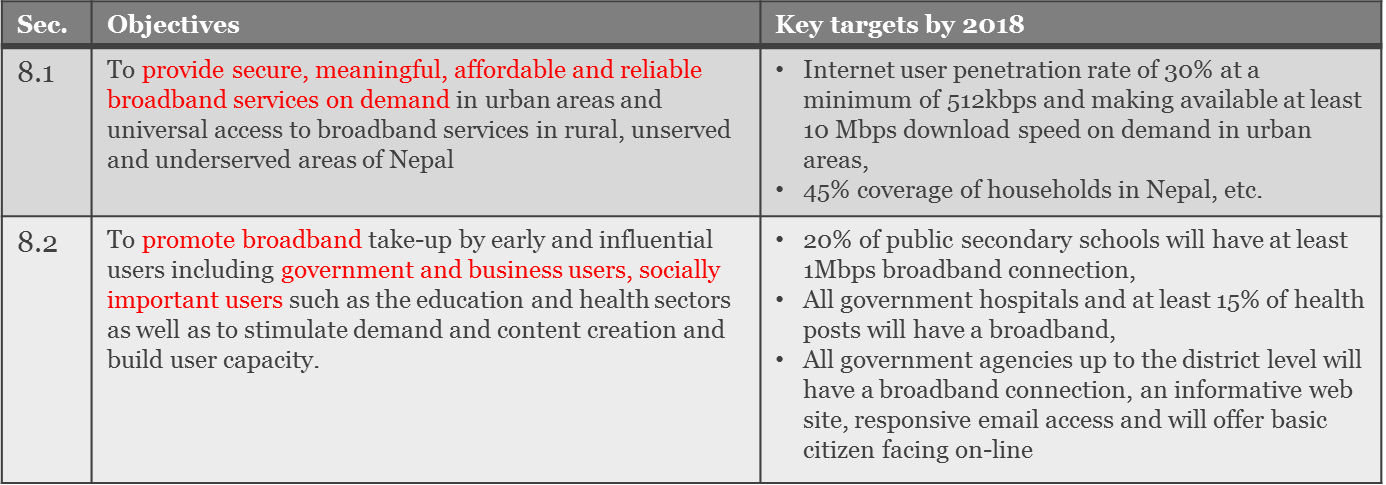
Mr. Shim explained the importance of Knowledge and Skills and especially in IT Security.  He pointed out that ICDL is a worldwide certification offered in most countries.  The aim of the program is to promote digital skills as the key enabler of effective use of ICT.  He explained that IT Security module sets out concepts relating to the secure use of ICT in daily life and skills used to maintain a secure network connection, use the Internet safely and securely, and manage data and information appropriately.  The course is available through National Operators who also engage with private and public sector (e.g. Ministry of Education).  The course is widely used and in some countries, the program is funded by the government and offered as an extra curriculum in both primary and higher education.  This is an example of a successful model of building knowledge and experience in IT security.

## Nepal

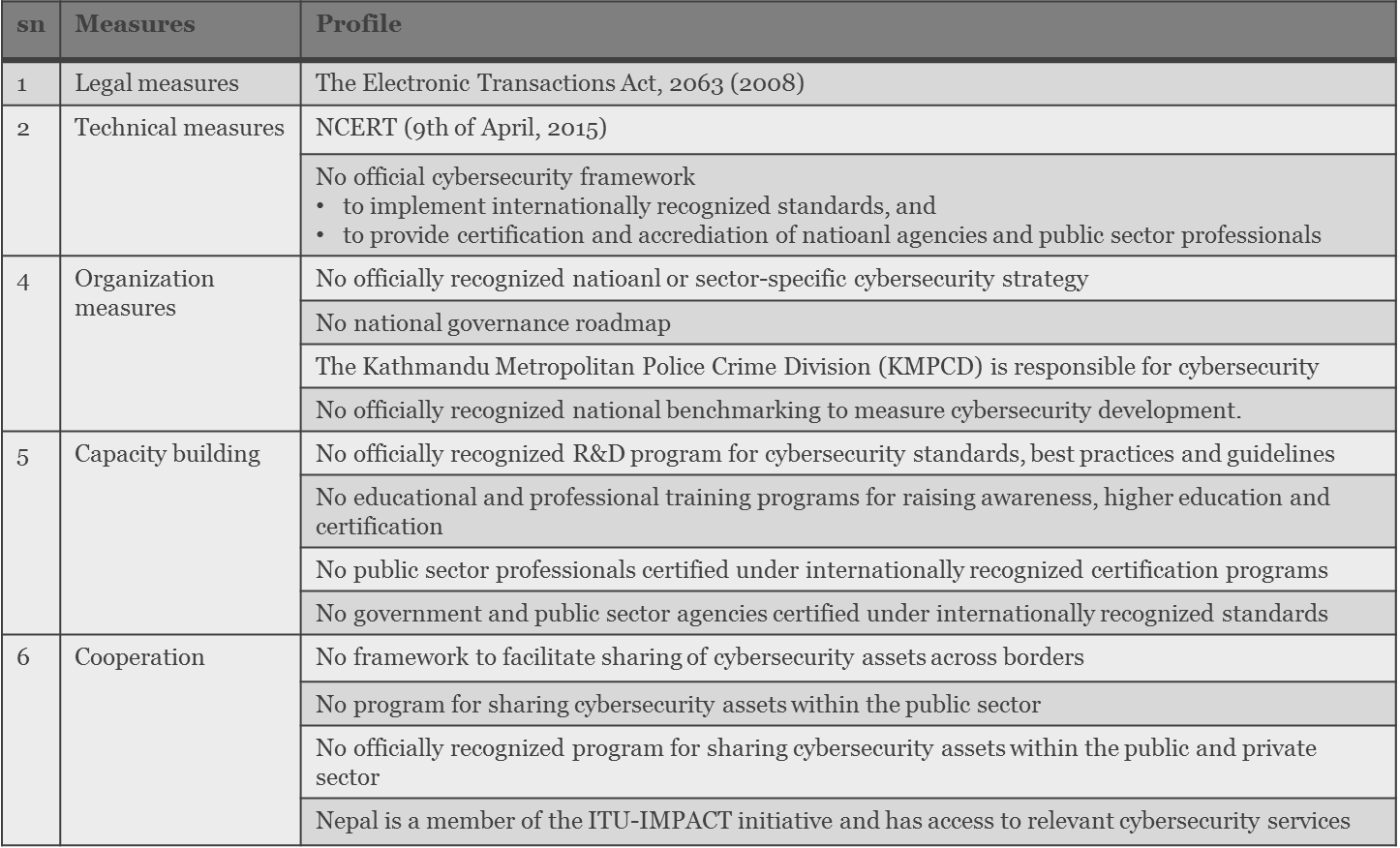
By Ambika Shrestha

Types of Cyber crimes experienced in Nepal has many facettes:

* + ATM pin steal
  + Cloning of ATM Card
  + Hacking
  + Financial fraud in Internet banking
  + Phishing
  + Social networking related crime

Based on this fact was in May 2015 a national CERT created, and the following objectives defined for 2018:  
  


Cyber crime is handled by Nepal police and Kathmandu District court has been put in charge for cyber crimes.

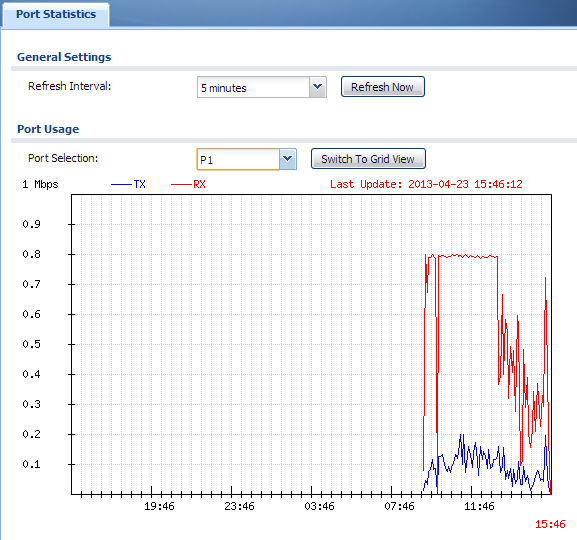


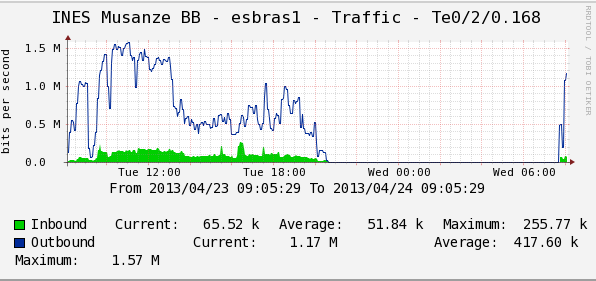
## University in Rwanda

**By Konrad Marfurt**

**Bandwidth-Problems at INES Ruhengeri  
(May 2013, updated July 2014)**by Prof. Konrad Marfurt, Lucerne Business School, Switzerland

When I started my term as a visiting professor at INES Ruhengeri I was confronted with some networking problems the most significant being a “very slow internet connection”. Lacking adequate equipment we had to wait for more than a month until we got a router/security gateway from the lab at my home university in Switzerland. Once they were installed the main problem was evident:

  
Figure 1: MTN’s bandwidth cut at 0.8 Mbps

  
Figure 2: MTN’s traffic statistics for the same time slot

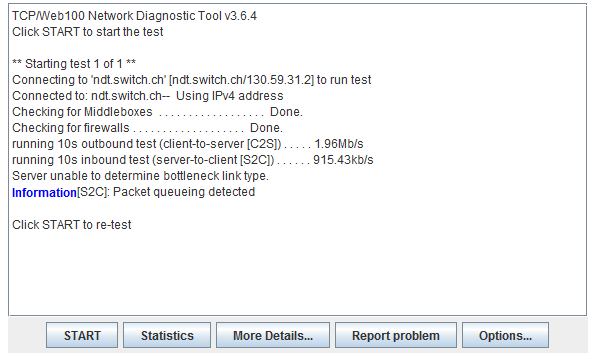
Apparently MTN Rwanda or its regional provider (in case MTN do not operate the connection to South Africa themselves) cannot provide a backbone connection with the bandwidth leased to INES (2 Mbps in the current contract). The results of figure 1 were reproduced many times with the same result: the statistical distribution is cut off when INES’s demand for bandwidth exceeds 0.8Mbps.

Unfortunately it was impossible to discuss the matter with MTN’s technical support. They seemed not even to understand the problem (maybe they didn’t want to) and advised our staff to “open several parallel youtube connections” in order to increase our bandwidth consumption although it was already at its (0.8 Mbps) limit with dozens of active workstations connected. On Friday May 10th they sent a technician who was supposed to prove that the problem was on our side and not on MTN’s. He conducted a speed test with iperf to the next hop which unsurprisingly showed a clean 2 Mbps connection to the next hop which is behind a fiber optic cable. Unfortunately MTN’s technicians in Kigali refused to run a 10 Mbps test which would very likely have succeeded, too. We assume this because in low traffic timeslots we had been able to establish *uplink* speeds to CERN, Geneva, of up to 3.75 Mbps (which is a really good result on public connections with 17 hops) but never downlink speeds exceeding 1 Mbps. At least MTN’s network engineer could be assured on location at INES that our equipment was working properly and our bandwidth measurements are perfectly accurate. He was kind enough to arrange another IP address for our connection (without the overhead of a PPPoE layer) to MTN’s local network in Musanze district. He also could satisfy himself on the fact that the bandwidth cut does not take place between INES and the first hop but at MTN’s own backbone connection, most likely before Rwanda Internet Exchange RINEX (196.223.12.1 visible in Table 2). ***We are still hoping that MTN will resolve this issue in the near future because it is definitely not good practice to sell more bandwidth to their customers than they can provide.***

In the following sections we shall point out the current situation.

### Measuring Outbound and Inbound max speed Sunday May 12 8:36 local time:

For a first test we used NDT at CERN Geneva (located in the academic network in Switzerland):

  
Figure 3: connection speed test between INES Ruhengeri and NDT at CERN, Geneva, Switzerland

This is an interesting result: although the server is at a bird’s flight distance of 6’500 km (the real distance covered being more than twice that because packets are routed via South Africa and LINX in London) we get an uplink speed of 1.96 Mbps. The downlink speed is at 915 kbps which shows that the bandwidth control implemented by MTN or its regional provider only cuts inbound traffic. Table 1 documents the path of the packets in this speed test:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| maximum of 30 hops |  | Tracing route to 130.59.31.2 |  |  |
| 1 | <1 ms | <1 ms | <1 ms | 192.168.1.1 |
| 2 | 4 ms | 3 ms | 3 ms | 41.186.33.61 |
| 3 | 5 ms | 5 ms | 5 ms | 41.186.50.54 |
| 4 | 187 ms | 241 ms | 187 ms | 196.44.31.86 |
| 5 | 238 ms | 205 ms | 205 ms | 209.212.111.83 |
| 6 | 185 ms | 185 ms | 219 ms | 209.212.111.200 |
| 7 | 186 ms | 187 ms | 187 ms | 209.212.111.187 |
| 8 | 199 ms | 199 ms | 199 ms | 195.50.122.181 |
| 9 | 220 ms | 219 ms | 219 ms | 4.69.139.88 |
| 10 | 204 ms | 203 ms | 203 ms | 4.69.153.125 |
| 11 | 219 ms | 219 ms | 219 ms | 4.69.143.110 |
| 12 | 213 ms | 214 ms | 212 ms | 4.69.161.86 |
| 13 | 217 ms | 217 ms | 217 ms | 4.69.161.101 |
| 14 | 220 ms | 219 ms | 219 ms | 4.69.134.49 |
| 15 | 220 ms | 219 ms | 220 ms | 4.69.137.81 |
| 16 | 205 ms | 203 ms | 203 ms | 213.242.73.74 |
| 17 | 215 ms | 215 ms | 215 ms | 130.59.31.2 |

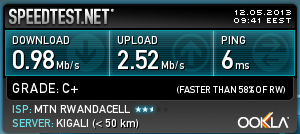
Table 1: route from INES Ruhengeri to NDT at CERN Geneva (Switzerland)

One could now argue that it is not appropriate to measure the quality of MTN’s internet connections in Rwanda using a server in a European Lab for Nuclear Physics. Although we contacted MTN several times they were not able to provide us with a test server outside their local network in Rwanda (e.g. at their home base in South Africa (which would be for example 196.44.31.86) at hop 4 in Table 1.

The only feasible solution was to use Rwandatel’s Server in Kigali (at 196.12.157.204) which offers speed tests within the speedtest.net project (based on ping-based traffic with tools like iperf etc):

  
Figure 3: user interface of the speedtest.net project

The results of our test taken at the same time as the test above (time difference in figure 4 is due to the fact that speedtest.net uses Eastern African time which is 1 hour ahead) are not surprising:

  
Figure 4: speed test between INES Ruhengeri and Rwandatel in Kigali

The tests show the same effect (bandwidth cut on incoming traffic) on a much shorter route:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| maximum of 30 hops |  | Tracing route to 196.12.157.204 |  |  |
| 1 | <1 ms | <1 ms | <1 ms | 192.168.1.1 |
| 2 | 5 ms | 3 ms | 3 ms | 41.186.33.61 |
| 3 | 5 ms | 5 ms | 5 ms | 196.223.12.1 |
| 4 | 5 ms | 5 ms | 5 ms | 196.12.157.204 |

Table 2: route between INES Ruhengeri and Rwandatel Kigali

The traffic is routed from MTN’s server at hop 2 to RINEX at hop 3 and the speedtest.net server at hop 4. We would like to point out that it is very likely that between hops 2 and 3 is the point where the bandwidth is cut. Without help from MTN it will be quite difficult to proof this but there is some evidence:

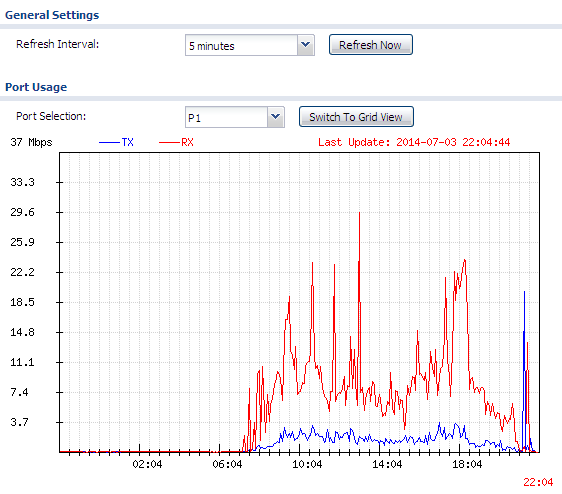
|  |  |
| --- | --- |
| MTN Johannesburg | MTN Capetown |
| 196.31.4.71: | 41.208.11.215: |

Table 3: speed tests between INES Ruhengeri and MTN servers in Johannesburg and Cape Town

As you can see from the figures in Table 3 the pattern is similar when we use MTN’s speed test servers in Johannesburg and Cape Town. Unfortunately we have no control over the route to these servers and MTN not being cooperative on this issue did so far not provide us with a speed test server in their network on a closer route.

### One Year Later…

In February 2014 INES signed a contract with a new local internet provider: Broadband Systems. They provide 20 Mbps at roughly the same price as MTN’s 2 (real 0.8) Mbps. There is no bandwidth cut:

  
Figure 5: Traffic Statistics with new internet provider

Note that the maximum download traffic is now around 30 Mbps and there is no plateau visible.

The speedtests are more encouraging now:

|  |  |
| --- | --- |
| Broadband Systems Kigali (local provider) | SIG Telekom Geneva, Switzerland |
| 57.5 Mbps down / 25.8 Mbps up: | 14.7 Mbps down / 6.1 Mbps up: |

Table 4: speed tests between INES Ruhengeri and servers in Kigali and Switzerland

## Conclusion:

ISES covered in the first phase already many countries and identified a large variety of methods and models.

Surprises as e.g. bandwidth challenges (e.g. prize and availability) disables even well meant approaches from global software companies. Updates of system software and virus scripts are just too expensive.

ISES managed to be recognized as a valid and necessary activity. Outreach was good within conferences, but more work needs be done for creating more impact.

The big credo is that we need to continue ISES, with:

**More Countries,**

**More Diversity of Models**

**Implementation level exchange**

**Increase international support**

**More presence and visibility**

**If we manage to perform the above action points, security will develop globally, for the good of all of us.**

# Meetings and Workshops

## WISI 2015 Information Security Education & Solidarity ISES

**ISES is a debate and a dialogue on information security status, strategies and models, depicting world’s diversity and transforming today’s situation in a better and more secure future cyber space. A discussed action plan will result from this workshop.**

**Keywords:** Information Security Awareness / ICDL/ECDL / Education / Policy /   
 Strategy / Teaching / Learning / Citizen

**Organiser: Prof. Dr. Bernhard M. Hämmerli, past-President Swiss Informatics Society  
 IFIP Member**

**Supporters:** Konrad Marfurt, Professor, Lucerne-Switzerland; Frank Mockler, ECDL Foundation, director information security certification, Ireland; Serah Francis, topic matter expert, Kenya (project Lead ISES for July 14-Dec. 14);

**Form:** Workshop with four introduction-presentations and following debate.

**General Background (Preparatory Action):**

* Initial ISES Meeting at WCCE 2013 in Torun July 2013
* Contribution to different Action Lines of WISIS+10 October 2013
* Accepted Activity Proposal of ISES to IFIP TC3 January 2014
* Accepted Activity Proposal of ISES to IFIP Board February 2014
* Presentation at WISIS+10 High Level Meeting July 9, 2014 in Geneva
* Finalization of a IFIP Project for the UNESCO Coordination Programme 2014/15 by August 31, 2014

**Presentations**

* Prof Hämmerli presented the global context picture of Least Developed Countries LDC with a description of the stakeholder’s option. LDC Governments can just stimulate global players to provide internet and cell access in their countries by giving license and regulations. Best is to have competition (e.g. three providers) which will regulate market price.   
  The operators go for a high risk business and will design their tariffs accordingly highwhich leads to slower development and fewer access for citizens.   
  Citizens have to pay around 10% of average GDP/person per month for receiving a voucher for 500 Mbytes of data transfer. The choice - whether to make a security update or go for an email / Facebook sync - is always on email / Facebook.
* Prof Marfurt reported on a 3-months stay at INES University in Ruanda. He demonstrated how good measurements and negotiations with the providers may substantially improve internet access and security. Security is improved by having one local update copy which can be used to update all 200 PC of the university without consuming extra bandwidth for downloads. Internet Access was improved by showing that you didn’t get, what you paid for - even with a 6 month negotiation phase. It ended up with tenfold speed. Furthermore, add blockers and low data rate web design as e.g. in mobile apps or 20 year old websites in developed world improve also access by factors. And he inspired that spending sabbatical in LDC is just a great experience.
* Frank Mockler (ECDL Foundation Ireland) presented the concept of ECDL / ICDL for all programs and elaborated details of ECDL Foundation’s IT Security program. International standards for the computer users and their security behaviour are very important as a tool for developing crucial competences in individuals and by extension societies. Implementation of ECDL Foundation programmes is through local partners and organisations, and operational details, such as pricing, vary depending on national norms. ECDL Foundation has a real commitment to setting a global standard and providing all countries, including those in the developing world, access to its certifications, including IT Security.
* Serah Frances, ISES driver, presented on the situation in Kenya, as an example of an LDC. Kenya recently accepted master plan on information technology with a strategy for information security. However, in the rating and international comparison of information (security) policy and strategy, not all aspects are covered and understandable. Furthermore, there is a long way from writing on paper to action. Both – on document level and on implementation level much work must be done in near future to improve the situation. Furthermore, Serah presented actual figures on the threat landscape in Kenya and the enormous – partly life critical – losses citizen suffer, and others (most out of country) profit from. To stabilize the economy security in the cyberspace is an utmost important issue for further growth and trustworthy development.

### Outcome and Political demands

* A worldwide partnership should be established to build capacity in this field i.e. Technical, Legal & Policies
* Critical technology gaps within the networks in developing countries and how those loopholes can be closed should be identified.
* For developing nations, ICT is a key component in improving the quality of life and participation in global economics activities. Failure to recognize the above could limit their economic and social goals, widening the gap between the rich and the poor.
* An attack on one unsecured system could affect the rest of cyberspace.
* Current cyber models appear not to be working, and we need to consider secure, vigilant and resilient cyber models that can manage risks and drive innovation in the cyber world.
* Cyber models should also be based on cultural, linguistic and institutional diversities.
* People and culture play a bigger role in managing cyber risks and their engagement would help in understanding the security and privacy challenges on cyberspace.
* Such models could minimise emerging cyber threats globally and increase trust on cyberspace and especially in emerging economies where ICT plays an important part in the future economy, and where cyber security is at an early stage.
* Developed Countries and LDC are globally linked and interdepend on each other in cyber security

### Support Options:

* **LDC Government level:  
  -** Insist that only secure technology can be delivered to LDC  
  - Insist that security software is made available for free or at acceptable local prices and kept up to date despite local bandwidth limitations  
  - Stimulate solidarity – instead of additional fences between LDC and High Tech
* **First World Government:**- Create support program for security in LDC  
  - Stimulate global corporation to ethical standards for delivering secure systems  
  - Stimulate engagement and cooperation with LDC
* **First World Educational Institutions and Universities:**- Create common projects for improvement  
  - Support education and awareness efforts by knowledge  
  - Support forensic capacities in LDC  
  - Promote faculty sabbaticals in LDC  
  - Provide student exchange programs

**ISES needs a support network with more experts for**

* Knowledge transfer
* Technology transfer
* Political visibility and political pressure (Number of Supporters)

**More experts should be part of ISES network and support because**

* It is right and good to do it (Ethical Motivation)
* It protects also first worlds network (mutual dependence)

**Formal Request to the IFIP TC3 Board**

Approve a Task Force for ISES which collaborates with Taskforce CS in Education and the IFIP Project Digital Equity. Annually contribution at WISIS Forum with a thematic workshop is planned. Contribution to WCC 2015 and a stream for WCCE 2017 in Dublin should be an integrated part of the project.

### Final Conclusion

It is enriching for us interacting on different levels and contributing to a better (ICT) world, and contributing to meaningful initiative.

### Contact:

* Serah Francis, ISES Driver, [serahm2@gmail.com](mailto:serahm2@gmail.com)
* **Prof. Konrad Marfurt, Hochschule Luzern – Wirtschaft,** Institut für Wirtschaftsinformatik, Fachvorstand Technologiemanagement, T direkt +41 41 228 4118

[konrad.marfurt@hslu.ch](mailto:konrad.marfurt@hslu.ch) , Zentralstrasse 9, Postfach 2940, CH 6002 Luzern

* **Prof. Bernhard Hämmerli**, Bodenhofstrasse 29, CH-6005 Lucerne, Switzerland, T: 0041 79 541 7787, [bmhaemmerli@acris.ch](mailto:bmhaemmerli@acris.ch)
* **Frank Mockler,** [frank.mockler@ecdl.org](mailto:frank.mockler@ecdl.org)

## Vilnius TC 3, WCC, July 2015

**Information Security Education & Solidarity (ISES):  
Sharing Strategies, Implementation, and Experience: Stimulation new Action**Session July 2, 2015 14:30-17h, room 218b Parliament Building Vilnius.

### General ISES Background Information:

The Internet is global. Is security in the global net a local issue? One for all, all for one: We are connected and by demonstrating Information Security Solidarity from rich countries, we also foster least developed countries’ information security: in return rich countries benefit from fewer attacks: we remain all connected!   
In support of the millennium development goals of a more wealth and gender balanced future and in preventing conflicts in these respect we engage for information security.

### General ISES Goals:

The main aim of ISES is to provide a platform for discussion on ICT Security by experts from different countries and different advancement. The current situation in different countries is discussed openly in terms of ICT security, strategies and implementation. The debate and dialogue on IT security models applied by least developed and wealthy nations creates inspiration for new action and mutual support: the resulting actions should improve ICT security readiness and lead to global minimum security standards compliance.

### ISES Session Summary of Vilnius Meeting

General Findings:

1. **ICT** or **Information Security Policy and Strategy** is a good start, but not the completion.  
   International pressure on all countries to create and approve ICT security policies and strategies is quite high. Under this pressure some countries can make also a copy paste approach for quick advancement in information security policies and strategies. However, in agencies and parliament non-anchored documents do not implement fast and might not be funded with according means.
2. Knowing that limited means only are available for implementing information security a variety of effective and low cost models should be collected. Three such models were presented:

* Rwanda: Swiss Professor makes sabbatical at the private university INES and boosts the internet forward. Additionally, after leaving the professor maintains remote support for INES ICT staff.
* Kenya: Expert Serah Francis has educated herself in Norway in information security management and is engaging for information security strategy and implementation in Africa generally and more specifically in Kenya.
* Nepal: Ambika Shrestha Chitrakar PHD Student in Norway makes an analysis of Nepal’s information security and concludes with a call for international support.

1. The audience required to detail out multi stakeholder models for boosting information security in the poorest countries. It is utmost important that all options are collected including seeding knowledge in the poorest countries, attracting support from rich countries (north south support), and creating opportunities for state-of-the-art education for experts from least developed countries. More specifically promotion of information security should address:

* More aggressive approach in terms of education.
* Collecting policies cyber security, including specific guidelines for kids.
* Blocking pages because for the protection of kids should be feasible, when Providing open access, e.g. when tablets are given to scholars or students

The audience agreed that further activities are a “must” and must be driven by financial support but also most importantly by the mindset of solidarity.

Refinement of these thoughts will be done in Daejeon IFIP conference, as well as speeding up the collection of model and state-of-the-art world-wide by questionnaire.

### ISES initiator Goals and Background

By Bernhard Hämmerli

The goals, mission statement and general background as mentioned above were presented. Additionally, a focal point was pointing out idealistic support models as well as engaging deeper in the solidarity mind set, for the good of both: more secure advanced world and a better future of the least developed countries. The journey just started and there is an enormous effort to take for succeeding in an acceptable and balanced situation.

### IT Security Challenges – a Case Study in Rwanda:

By Prof Konrad Marfurt

The case study demonstrates that proper funding and support with hardware and network technology are just one first step - but not sufficient. Government and non-government Institutions are doing their best to provide schools with electricity and network connections. But this is just the first step. The next step is educating local staff, teachers and students to use ICT in appropriate ways without putting oneself in danger. Implementing a firewall concept is one thing. In good projects it is usually part of the initial setup; in “not-so-good” projects it is not considered because the projects end with the delivery and installation of hardware. ISES is meant to turn “not-so-good” projects into good ones by offering initial training to local staff and faculty and maintain a relationship after that which includes remote support, exchange of students’ knowledge, internet-related projects with cooperation on faculty- and students-levels. The case study showed that INES’s ICT infrastructure was quite good and didn’t need more than $2’000 in hardware improvement; the three man-months of support were of much higher value changing an erratic internet connection into a high-speed connection which now allows remote support from Swiss schools’ network labs to INES. “Solidarity” means to maintain this kind of peer-to-peer cooperation when the installation projects are completed and constantly enable students, staff and faculty in the North and in the South to cooperate in the future.

### Cyber Security in Kenya

By Serah Francis

For developing world, ICT is a key component in improving the quality of life and participation in global economies. It provides opportunities for people with basic services such as e-banking, e-health, e-commerce and e-learning, services they may not have been able to access were it not from the internet. To minimize emerging cyber threats globally and increase trust in cyberspace we require reliable and secure information infrastructure with guaranteed accessibility, availability, dependability and continuity of services. Recent reports on cybercrime in Africa, shows that Africa is not immune to cyber risks and this could impact the technological growth, thus excluding many Africans from the benefits of being online. Collaboration between security services of public, private sector in Kennya as well as international organization is urgently needed to promote secure use and protection of digital devices at local and national level.

### Cyber Security in Nepal:

By Ambika Shrestha Chitrakar

Cyber space does not have any boundary and its usage is rapidly increasing, even in least developed and developing countries like Nepal. Nepal even being one of the poorest countries in the world, the usage of cyber space among young generation is rapidly increasing. Cyber space and its applications have made our daily life much easier than before but they also bring cyber security related challenges. Cyber security is totally a new field in Nepal and we do not have any computer security related education even after more than one and a half decades of experience in computer science education. Most of the younger people are not aware of possible cyber threats and therefore they heavily use cyber space. Nepal lack skills in computer security, and does not have any official cyber security strategy. NCERT (Nepal Computer Emergency Response Team) has been recently formed with 7 members on 9th of April 2015. When the world is struggling with harmonizing the cyber security strategy, Nepal is in its initial stage. Nepal has also experienced some cyber threats and there is immediate necessity of a proper formal cyber security strategy. Cyber security is a global issue and there should be balance in its strategy over the whole world in order to strengthen it. In current context, Nepal needs international collaboration and support for capacity building in cyber security and for developing internationally harmonized cyber security strategy. Possible ways to do so could be by providing cyber security related awareness, education, experience sharing, and computer security related training.

|  |
| --- |
| **Information Security Education & Solidarity (ISES):**  **The way to balance wealth and gender** |

### Mission Statement:

The Internet is global. Is the security in the global net a local issue? One for all, all for one: We are connected and by demonstrating Information Security Solidarity from rich countries, we foster least developed countries as well as the rich countries: we all connected!

## Korea, October 2015 ****IFIP TC3 Working Conference "Opening our Future Together" inside WCC’2015 (World Computer Congress)****

ISES Participation on 5th October, 2015, in Daejeon, Korea

**Speakers:**

         Mr. JaeSuk YUN representing Korea

Mr. JaeDok Shim, representing ICDL Korea

M. Rajan R. Patan, representing Nepal

Serah Francis, representing Kenya

Mr. Penmetsa Murali Krishna, representing India

 Moderator: Raymond Morel, IFIP GA and TC3

=====================================================

### ****ISES Session Summary of Daejeon Meeting****

**General Findings:**

Information Security is becoming a global concern for all governments worldwide.  This was highlighted by experts from different countries.  Most countries have recognized the urgency of developing ICT security policies and strategies but successful implementation requires huge commitment and support from the government and all stakeholders.  Lack of funding, commitment, shortage of skills and awareness are just some of the things hindering successful implementation of policies.  Advanced countries are already implementing and reviewing their strategies and policies but least developed and developing countries are still lagging behind.  Developing a cyber security strategy or policy does not change anything in terms of improving cybersecurity but the real change comes when a government has been able to put the plan into action and have measurements and tools for continues assessment and evaluation.  For example, user awareness, R & D, and professional skills development in information security should be every government top priority when allocating funds but research shows that very few countries have dedicated budget for IT security.

### ****Session One: Presentations****

The speakers presented current situation in different countries in terms of cybersecurity policy and strategy development and implementation, with an example of how technology trends are pushing enterprises to implement mobile devices without clear policies on how to address the risks.  In addition, an education model (ICDL) applicable to all users and workforce both in government and private sector was presented as an example of successful educational model.

#### ****Cyber Security Policy in Korea - Mr. JaeSuk YUN****

Mr. YUN discussed ICT environment in Korea, trends on cyber-attacks, cyber security policy and implementation.  The government of Korea has been very active in promoting cybersecurity for some time, due to security threats from outside the country.  Mr. YUN pointed out that a multistakeholder approach led by KISA (Korea Internet and Security Agency) with support from the government has led to the successful implementation of Cyber Security Policy of Korea.  With this success Korea is able to share its model with interested countries.  Already, the country is cooperating with developing countries in areas such as sharing know-how on incident response, providing cyber security system, training & business opportunities and consulting about cyber security policy & strategy. He also explained how Korea is playing its part in global arena by supporting cyber capacity building for developing countries and sharing practical cyber security knowledge and experience through their practical global cybersecurity center for development & cybersecurity alliance for mutual partnership (CAMP).

#### ****IT Security in South Korea - Mr. JaeDok Shim****

Mr. Shim explained the importance of Knowledge and Skills and especially in IT Security.  He pointed out that ICDL is a worldwide certification offered in most countries.  The aim of the program is to promote digital skills as the key enabler of effective use of ICT.  He explained that IT Security module sets out concepts relating to the secure use of ICT in daily life and skills used to maintain a secure network connection, use the Internet safely and securely, and manage data and information appropriately.  The course is available through National Operators who also engage with private and public sector (e.g. Ministry of Education).  The course is widely used and in some countries, the program is funded by the government and offered as an extra curriculum in both primary and higher education.  This is an example of a successful model of building knowledge and experience in IT security.

#### ****IT Security in Nepal: Issues and Challenges - Mr.  Rajan R. Pant****

Mr. Rajan pointed out the current status of IT Security: available infrastructure, threats and challenges. He pointed out that internet penetration is growing in Nepal and with this, security threats are increasing.  He also pointed out challenges faced by Nepal in the area of Information Security such as lack of Cyber security policy, relevant skills, user awareness, specific cyber laws and lack of urgency from the government among others. With the theme SECURE YOU, SECURE YOUR NATION, Mr. Rajan explained how he is helping his country to be secure. He explained how he has established an organization, Information Technology Emergency Response Team Nepal (ITSERT-NP - [www.itsert-np.org](http://www.itsert-np.org/)) and its role towards the information security. He has also introduced classes for students, training for teachers, guideline for parents and warnings for users in Nepal.  He hopes the program will continue offering more support to many users.  He emphasised that awareness and education is the best way to make sure many are aware of information security.

#### ****Cyber Security Issues & Challenges in Kenya - Serah Francis****

Ms Serah Francis discussed on the current status on Cybersecurity in Kenya.  She highlighted that there is still a growing concern on the increasing cyber threats in Kenya in spite of the government launching the National Cyber Security Strategy last year.  She explained that the government is facing challenges on implementing the policy due to lack of resources, IT security skills and IT Security Awareness in the country among other things.  She pointed out that through education and solidarity, countries can help each other in Policy making, legal and regulatory frameworks, designing of Cyber Security Curriculum in academic institutions, designing affordable and accessible training through e-learning and to identify critical technology gaps within the networks in developing countries and how those loopholes can be closed.

#### ****The State of Mobile Security in India -  Prof. Murali Krishna, Penmetsa****

Mr. Krishna presented the findings about the present state of Mobile security in India. He presented his findings on the technological trends, economic trends, socio culture trends and proposed recommendations based on his findings for improvements. From his first findings, he emphasized the need for development of mobile security policies for organization on acceptable and non-acceptable use of applications. Secondly, he recommended organizations to develop BYOD (Bringing your own device) strategy with security functions like password entry, remote lock & wipe and biometrics.  Finally, he recommended the need to create mobile security awareness program on use, compliance to policies, loyalty, controls and accountability.

### ****Session Two: Panel Discussion****

The panel felt that there is a need to involve more countries in ISES (Information Security Education & Solidarity) to get a clear world view and to share their experiences on cybersecurity. Cyber security is not a one countries or individual problem, all is responsible. The participants felt that Information Security is a clear cut in all entities of IFIP and that there need to be a way on how all can share ideas and experiences.

The questionnaire was discussed and the full report on response should be analysed on the next conference in Seville in November 2015.  Raymond to pass and discuss the questionnaire with General Assembly next few days. Mr. Rajan stressed on implementation of different programs of ISES in different countries.  For this purpose, he offered to distribute the questionnaire through Computer Emergency Response Teams (CERTs) in different countries to understand the status of information security of those countries to guide us on future plan and objectives.  Mr. Raymond explained on the objective and goals of ISES and since we are coming to the end of the year the committee should start preparing the full report for the whole year. Prof. Krishna stressed the need for defining long term objective for project ISES initiative and steps that need taken for the achievement of the objective.

We are promoting information security education by conducting different awareness programs as recommendations provided by speakers and moderator.  Next step is to build a website with sufficient information related to information security to support our initiation of ISES.

#### ****Cybersecurity challenges in developing countries - Findings****

Cybersecurity is one of the most serious economic and national security challenges the world is facing today.  Recent media coverage about hacks, data breaches and theft of personal information doesn’t go unnoticed and many governments have taken steps of developing cybersecurity strategies to coordinate measures to protect their critical infrastructure and citizens.  Most National Cybersecurity Strategies will have some similar key areas due to the nature of cyberspace.  These key areas include legal measures, technical measures, organisation measures, capacity building and cooperation.  Comparing these key areas of a country is important to intensify a country’s effort to cybersecurity and to identify the gaps and shortcomings of the strategy.

Unfortunately, most of the National Cybersecurity Strategies don’t live to their expectations. Some   strategies are unclear and relatively weak when describing detailed action plans in different areas.  Furthermore, many fail to mention the key stakeholders, their responsibilities and how they work together.  Cybersecurity is a clear cut in many areas of the government agencies and therefore it is important to mention how the strategy integrates to other areas, but many cybersecurity policies fail to do so.  In most cases Cybersecurity strategy or policy is not seen as a core strategy like ICT or defense strategy and therefore, no separate budget is allocated to the process, meaning that many actions could be overlooked due to lack of resources. Evaluation and control metrics to measure performance are not mentioned on many of the cybersecurity strategies.  Without these measures a country will not be able to tell whether the strategy is a success or not.  Some would argue that cybersecurity is a sensitive issue and therefore not everything should be put on public domain.  Unfortunately, this can create problem when it comes to assessing the readiness and cyber commitment of a country, in case of foreign investment. The Governments is also responsible to act to address the growing cyber threats and attacks, hence promoting public confidence and trust in the use of cyberspace. The process of developing a strategy is always the easy part – implementing the plan is always a challenge. National Cybersecurity is no exception: the environment has to be right with key elements and proper funding.

In many developing and least developed countries, cybersecurity has gone from a concern to an issue of pressing concern.  This is because these countries are investing large amounts of money to improve digital technology with less attention paid to securing or responding to any attacks on cyberspace. Meaning that most systems and networks in those regions could be vulnerable and exposed to cyber threats and attacks.  Africa is becoming an attractive target for home-grown young hackers who want to commit economic fraud and also international criminals wanting to take advantage of the ineffective laws and political instability.  The region accounts for 4% of total security incidents worldwide and this figure is expected to rise due to improved internet infrastructure and falling prices.  Research has shown that developing nations have poorly secure networks, lack of cyber laws and short of well-trained IT security experts both in private and government agencies. The level of ICT mutuality is still very low compared with other nations in the world and IT Security Education and Awareness is almost non-existence in mainstream academic institutions. Successful development and implementation of a National Cyber Security plan, requires professionals with skills covering all the cybersecurity domains to champion the initiative. Although most of the above mentioned challenges are not only unique to developing countries, there are several factors why many are concerned on the state of cybersecurity in developing countries. Below is a summary of some of the challenges facing policy implementation in developing and least developed countries;

* + Lack of Cybersecurity Strategies/Policies and legal & regulatory framework in some countries
  + Inadequate fund allocation to cybersecurity ecosystems
  + Lack of information security awareness and persistent information security culture
  + Insufficient computer literacy and lack of local digital contents especially in rural areas
  + Inadequate standards and maturity models for cybersecurity
  + Lack of a Child Online Protection Framework
  + Lack of basic awareness, information security professionals and skills within government
  + Lack of specific sector policies e.g. education
  + Resistance to change, especially in public sector
  + Reliance on imported hardware and software
  + Lack of sector specific R&D programs/projects, especially in education
  + Lack of appropriate national and global organizational structure to deal with cyber incidents

In addition, increasing level of internet penetration through mobile devices and fast broadband in developing countries is thought to contribute to increasing attacks from various malicious online agents. To remain competitive on the global market developing countries need to show their commitments in securing the cyberspace.  Kenya is an example of a developing country that want to emerge as an ICT hub in East Africa and as such has tried to respond to cyber security threats by emulating other countries.   In 2014, the Kenya government developed the National Cybersecurity strategy which aims to define the country’s cybersecurity vision, goals and objectives to secure the nation’s cyberspace while continuing to promote the use of ICT to enable economic growth. Unfortunately, the country has not been able to respond to growing cyber risks in the country. Experts in the region argue that the problem has even gotten worse.  Developing a national cybersecurity strategy is one thing but not supporting implementation plans and funding, could be detrimental to their success. Lack of effective cyber laws and regulations, skills shortage, raising awareness, national and international collaboration and organization structure as well as protecting children online are all key elements that cannot be ignored when we think of cybersecurity ecosystem. A Multi-layered approach consisting of all the above is required in order to fight cybercrime and if countries want to remain competitive in the global market.

Few countries in developing world have established CERT/CIRTS but their effects on whether they can respond to cyber threats in a timely and coordinated manner is yet to be felt.  Many are not well funded and they lack qualified experts and tools.  Many countries are not member of other initiatives like FIRST and have not signed or ratified with Budapest Convention.  Members of FIRST share information and good practices as well as taking advantage of the training offered by FIRST.

Many in developing countries lack very basic security skills like using a password or dealing with emails and as such, criminals take advantage of these poor security practices to steal personal data. Unlike most of the developed world, cybersecurity education is at its infant stage and in some countries none at all. The shortage is being felt across all organisations but the most felt is the government, financial institutions, SMEs and NGOs.  In many countries there no government funded IT security courses and IT Security certification offered by organisations such as SAN or ISACA are very expensive for the locals.  The few experts in the continent are recruited by the private sector as they offer higher financial rewards.  In most cases, cybercrime incidents are never solved due to lack of Computer skills and expertise.  In many countries the government there no government computer forensic labs.

Legislation and regulatory framework are key elements of cybersecurity. Unfortunately, existing frameworks in most developing countries are only partly sufficient or not sufficient at all. For example, Kenya has been criticized for lack of effective laws and skills shortage in law enforcement. Lack of awareness among the parliamentarians can delay legislation process. Lessons can be learnt from countries like Estonia or UK in terms of developing laws and regulations to govern cybersecurity. In some areas of the law, other countries could pick what is relevant to their situation instead of reinventing the wheel. A good example is the UK Computer Misuse Act. The U.K. Computer Misuse Act 1990 is an example of comprehensive legislation on computer crime while the U.S. Federal Information Security Management Act of 2002 is also a comprehensive legislation on cybersecurity compliance and the E.U. Directive 95/46/EC on the “protection of individuals with regard to the processing of personal data and on the free movement of such data” is a partial regulation in the Europe uniquely related to cybersecurity among other things.

Although some countries are experiencing fast broadband, the infrastructure needs upgrading. Old software like Window XP is still in large use even though Microsoft ceased its support. Many cannot afford to upgrade their devices or virus scanner and are not aware of automatic updates or of free downloads offered by supplier’s e.g free VG virus scanner from Microsoft.  In some parts of Africa, internet is still very expensive compared with their earning and when it comes to using broadband they would rather use the few hours they have purchased on social media or email than updating their devices. Many are not aware of the security threats posed by not protecting their devices.  There is also widespread use of pirated software.

One of the most threat to many firms especially in financial institution in Africa is inside threats. There no regulations for reporting cybercrime in most developing countries and therefore, most  organisations prefer to deal with the problem from within.  There is lack of trust on the legal system in cases where cyber laws are in place and fear of reputation.  Countries do not have national databases for criminals, making it easy for those employees who commit crime to move from one place to another committing similar crimes.  In most situations, even when cases are taken to court, many end up not facing judgment due to lack of enough evidence. Lack of digital investigating tools and training in many law enforcement agencies also plays a part. Many firms are ill prepared to detect, prevent and investigate any security information breaches, costing them millions of dollars annually arising from corporate theft and information security breaches.

The increasing use of social networking sites such as Facebook, Twitter in Africa for example, increases the mobile device vulnerabilities.  Criminals are using data stealing apps and other attacks to steal personal data stored on mobile devices. Millions of internet users in Africa use their mobile devices both for work and private use, thus storing large amounts of data leaving them vulnerable to cyber criminals who want their personal details and that of their companies to steal trade secrets.

Developing countries should also learn how to regulate the IT market to avoid being a dumping place of unnecessary cheap hardware and software and to create a market for local talents. There is a need of a political commitment at the highest level of government so that they can support and assist in creating awareness to their people. There is a high risk of digital divide if urgent measures are not taken, to educate, train and raise awareness on information security especially for minority and vulnerable people. Cultural differences can also hinder development in countries where most people can only speak their native language. Most security awareness initiatives are concentrated in urban areas leaving rural areas behind.

Developing and least developed countries are still a long way in having an effective mature cybersecurity ecosystem compared to developed countries due to Infrastructure, legal and policy loopholes and failure from some countries not doing anything about it.  If countries are to achieve their millennium targeted goals, adoption of appropriate legislation, effective institution structure and global partnership are needed to deal with cybersecurity.  It is evident that capacity building cuts across all areas of cybersecurity. Therefore, security information awareness is important to draw attention to the society on the security issues surrounding them. Education and training give people skills to manage their devices and have relevant skills to be able to carry out their jobs. Last but not least, without R&D, countries miss out on innovation.

## Bibliography

(1)   ENISA Website, National Cybersecurity Strategies in the World. <https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world>

 (2)   ABI & ITU, Global Cybersecurity Index & Cyberwellness Profile 2015. <https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-E.pdf>

**(3)** Luiijf, et al, Nineteen National Cyber Security Strategies, [International Journal of Critical Infrastructure Protection](http://www.researchgate.net/journal/1874-5482_International_Journal_of_Critical_Infrastructure_Protection) (Impact Factor: 1). 01/2013; 9(1):3. DOI: 10.1504/IJCIS.2013.051608

**(4) ENISA 2014, An evaluation framework for Cyber Security Strategies.** <https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/an-evaluation-framework-for-cyber-security-strategies-1>

 (5)   GoK 2014, Kenya National Cybersecurity Strategy. <https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/KE_NCSS.pdf>

 (6)   WSIS Forum, Outcome Document, ISES Session, 25-29th May 2015, Geneva Switzerland

 (7)   Europol, The Internet organized Crime Threat Assessment (iOCTA) 2014. [www.europol.europa.eu/content/internet-organised-crime-threat-assesment-iocta](http://www.europol.europa.eu/content/internet-organised-crime-threat-assesment-iocta)

 (8)   Kigen et al, “Kenya Cyber Security Report, “Rethinking Cyber Security: An Intergrated Approach,” TESPOK & Serianu Ltd, 2014.

## Seville, ICERI, November 2015

### Abstract: Policy and Implementation Issues for Information Security Education in Developing Nations

By Serah Francis, Gjovik University College (Norway) and Konrad Marfurt Lucerne, University of Applied Science (Switzerland)

**Keywords:** ICT Security Education, Education in Developing Countries, Global Solidarity, Information Security Policies.

The increasing ubiquitous of the ICT has changed the way the society operates. When used effectively, ICT has provided people not only with access to information but also opportunities to participate in the global economy. Unfortunately, dissemination of ICT presents a wide range of social and ethical issues like online safety and security, misuse of information etc. It is important that users are equipped with appropriate knowledge and skills to operate their devices securely. Therefore, countries should address the issue of Information Security to minimize the risk and bring it to acceptable level while still exploiting the opportunities offered by ICT.

An in-depth analysis has shown that effective implementation of information security and especially education is not adhering to paper based requests from government policies and strategies. The lack of cyber laws/regulations, shortage of ICT security skills and poorly secured networks are just some of the challenges affecting policy development and implementation. There is an urgent need for action within all key stakeholders to promote and adopt a proactive approach towards responsible and safe use of ICT: providing security education environment at sufficient high level is thereby key for further improvement.

The issue of securing the cyberspace is important to all nations including developing and least developed countries because cyber insecurity has international ramifications. An attack on one vector could affect the rest of the cyberspace. The fact that criminals can commit crime anonymously with minimum effort, and minimum risk of being caught makes cybercrime the favourable tool for many criminals and also a great concern to all. North-South collaboration and support is needed in promoting cyber-security and especially maintaining the concept of solidarity in information security education. Failure to act now means that we are allowing cyber criminals to take over our networks for their use.

The current situations in cyber-security in Kenya, Rwanda and Nepal are presented and models of clever low cost implementation for awareness and educational purposes are shared. The term cyber-wellness (in regard to legislation/regulations, national curriculum, and other educational initiatives) is defined and analysed in the three countries. Furthermore, cyber-wellness is compared with advanced countries to identify the gaps. Literature analysis, questionnaire field research and workshop discussions have identified relevant gaps, but also hope: effective implementation models on strong education and solidarity will assist policy makers and other stakeholders in developing and integrating ICT security in curricula at all stages.

This paper discusses current ICT security policy implementation issues in education and how this can be improved by sharing knowledge and successful implementation models.

The research and development is made in the frame of the “Information Security Education and Solidarity Initiative (ISES)”, a project sponsored by UNESCO Participation Programme submitted through Technical Committee No. 3 “Education” of the International Federation on Information Processing (IFIP).

# Team and Contact List of Contributors

**Information Security Education and Solidarity (ISES) Initiative Members - 2015**

1. Prof. Dr. Bernhard Hammerli; [bmhaemmerli@acris.ch](mailto:bmhaemmerli@acris.ch" \t "_blank)
2. Prof. Konrad Marfurt; [konrad.marfurt@hslu.ch](mailto:konrad.marfurt@hslu.ch)
3. Frank Mockler; Frank.mockler@ecdl.org
4. Serah Francis; [Serah.francis@hig.no](mailto:Serah.francis@hig.no)
5. Raymond Morel; [Raymond.Morel@unige.ch](mailto:Raymond.Morel@unige.ch)
6. Tone Hoddø Bakas; [Tone@norsis.no](mailto:Tone@norsis.no)
7. Adrian Kapczynski; [akapzynski@gmail.com](mailto:akapzynski@gmail.com)
8. Jacub Christoph; Jakub.christoph@ecdl.org
9. Dr. Adenisa Simon; [sinaronke@yahoo.co.uk](mailto:sinaronke@yahoo.co.uk" \t "_blank)
10. Prof. Dr. Lim Tong Ming; [tongming@sunway.ed.my](mailto:tongming@sunway.ed.my)
11. Angela Lee Slew Hoong ; [angelal@sunway.edu.my](mailto:angelal@sunway.edu.my)
12. Dr Arthur Tatnall; [Arthur.tatnall@vul.edu.au](mailto:Arthur.tatnall@vul.edu.au)
13. Hermogenes Nzang Esono (Hermes); [hermesn2003@gmail.com](mailto:hermesn2003@gmail.com)
14. Anthony Gioko; [gioko@akam.ac.ke](mailto:gioko@akam.ac.ke)
15. Stephen Ibaraki; [sibaraki@cips.ca](mailto:sibaraki@cips.ca)
16. Pascal Mbonyiyeze ; [mbonpascal@yahoo.fr](mailto:mbonpascal@yahoo.fr)
17. Prof. Saito Toshinori; [t-saito@kyoiku-u.jp](mailto:t-saito@kyoiku-u.jp)
18. Gregory Kuhlmann; [Gregory.Kuhlmann@t-online.de](mailto:Gregory.Kuhlmann@t-online.de)
19. Prof Rolf Romeike; Rolf.romeike@unige.ch
20. Prof. Niki Davis; Niki.davis@cantebury.ac.nz
21. Francis W. Sitati; sitati@cck.go.ke
22. Turid Aarseth; Turid.aarseth@himolde.no
23. Anne Karin Wallace ; Anne.k.wallace@himolde.no
24. Kurt Haering; khaering@bluewin.ch
25. Fredy Schwyter; f.schwyter@atr.ch
26. Enos Kiforo Ang’ondi; kiforoenos@yahoo.com
27. Prof. Marie Iding; miding@hawaii.edu
28. Seiji Isotani; sisotani@icmc.usp.br
29. Hermogenes Nzang Esono (Hermes); [hermesn2003@gmail.com](mailto:hermesn2003@gmail.com)
30. Turid Aarseth ; Turid.aarseth@himolde.no
31. Anne Karin Wallace ; Anne.k.wallace@himolde.no
32. Peter Micheuz; Peter.micheuz@uni-klu.ac.at
33. Adriana Sobreira Tones; adriana@escolaparque.g12.br
34. Maria NievesFlorentin Nunex; florentin@uni.edu.py
35. Dr. Sebastian H.D. Fledler; fuieldler@tlu.ee
36. Terje Valjataga; Terje.valjataga@tlu.ee
37. Prof. Junusz Morbitzer; janmor@up.krakow.pl
38. Vassela Ilieva; Vessel.ilieva@abv.bg
39. Murali Krishna Penmetsa; krishna@krimsh.com
40. Shirisha Penmetsa; Shirisha.penmetsa@gmail.com
41. Rajan Pant; rajanpant@outlook.com
42. Nicholas Mavengere; mavengere@gmail.com
43. Ousmane Ndiaye; [Ousmane.ndiaye@artp.sn](mailto:Ousmane.ndiaye@artp.sn)
44. Pasi Mafuta Nova; [pasimafuta@gmail.com](mailto:pasimafuta@gmail.com)
45. Ambika Shretsha; Ambi.shrestha@gmail.com
46. Margret Mukira; mmukira@yahoo.com
47. Jane Njuru; jnjuru@mku.ac.ke
48. Mr. Suroor Mohsin Al Harbi; [salharbi@moi.gov.ae](mailto:salharbi@moi.gov.ae)
49. Cecilia G. Mamelodi-Onyadile; [cmonyadile@sadc.int](mailto:cmonyadile@sadc.int)
50. Thadei Msumanje; Msumanje@yahoo.com
51. Stewart James Kowalski; Stewart.kowalski@hig.no
52. Jeffy Mwakalinga; jeffy@ling.su.se
53. Zdena; [Zdena.liotta@gmail.com](mailto:Zdena.liotta@gmail.com)
54. Bjoern Stockleben; [Miroslava.cernochova@pedf.cuni.cz](mailto:Miroslava.cernochova@pedf.cuni.cz)
55. Seetam; [Seetam@utas.edu.au](mailto:Seetam@utas.edu.au)
56. Peter Doe; [Peter.doe@utas.edu.au](mailto:Peter.doe@utas.edu.au)
57. Miroslava Cernochova; [Miroslava.cernochova@pedf.cuni.cz](mailto:Miroslava.cernochova@pedf.cuni.cz)

# Webpage

Webpage [www.ISES-int.org](http://www.ISES-int.org) under construction (Konrad Marfurt)

# Appendix I

At NTNU Science and technology Centre Trondheim, Norway, were two master thesis may on the topic:

* Information security comparison of Norway and India with focus on SEM: master thesis by Murali Krishna
* Information Security Policy and Strategy in Kenya: Masterthesis Serah

On top of those two thesis was for the ISES project a questionnaire designed and evaluated

(see next page).

# Appendix II: ISES - Questionnaire Findings

**Abbreviation: P = Answering Person**

## Cyber-security challenges

Majority of the respondent felt that internet users have insufficient digital skills to recognize potential threat and how to protect their personal or company’s data as well as their devices. IT literacy and basic understanding of fundamentals of computer science concepts can be challenge to many users. Lack of user awareness goes across the board - from typical users to people in high places such as politicians and bank managers. This result to weak passwords, unpatched devices, visiting harmful websites, identity theft, cyber bullying, fraud etc. The increasing connection of users and devices with weak systems make cyberspace a safe haven for cybercriminals.

One respondent felt that Internet users from low social economic demographics are very susceptible to online scams.

Businesses are also to blame for realising software’s with bugs –  **P1:** (*"There is a dangerous contradiction between cyber-security and business interests of some companies (most importantly, Microsoft, but also Apple and Google move that way). Ignorant people are the best customers and technological monocultures are the best ways to make profit - yet both lead to security nightmares (e.g. computer viruses have always been 99% Microsoft phenomenon). Fortunately, both risks are possible to leverage on national/governmental and international (treaty) level."*)

The exposure of violent, sexual materials on Internet towards young children pose a great threat - concern to some of the responders.

## National Cyber Security Strategy/Policy

Evidence showed that most countries have acknowledged cybersecurity as an urgent issue but most are still at their early stages in putting preventative measures in place. However, some countries (mainly in developed countries) have already developed a National Cybersecurity Strategy or Policy. For many of the National Cybersecurity or Strategies their deployment are yet to be felt when it comes educating and training the users.

Most developing countries have a long way to go, and without having proper measures to secure their infrastructure, some are opting to limit the option of the internet freedom for the sake of security*.*

Countries are at different level of maturity on cybersecurity. Some have cybercrime bills waiting to be passed while others are still at the initial stages of drafting cyber laws. Due to government in some countries wanting to adopt egovernment, short courses are offered to government staff e.g ICDL and others however the training does not continue for long.

Some developed countries are offering help to least developed countries in cybersecurity

Most countries in developing countries have a long way to go and without having proper measures to secure their infrastructure they are opting to limit the option of the internet freedom for the sake of security*.*

***P14****:(“I don't aware of any government Policy about cyber-security in Central Asia. Last week the Government of Tajikistan closed Facebook and other social network sites in Tajikistan due to security issues.”)*

## Strategy/Policy implementation process

### (a) Capacity Building

**Awareness Raising**

In some countries CSIRTs are responsible for educating and creating necessary awareness through their websites and carrying out trainings in schools and government agencies e.g. Sri Lanka CERT, Rwanda Rw-CSIRT. In other countries security awareness campaigns are done by government partnership with other private organisations, academics and non/governmental organisations. This is being done though mass media (TV, Interviews on TV & Radios) publishing books, and through government and businesses websites e.g. banks. Some of these campaign are not long lasting but one off event. In the “Cybersecurity Strategy of the European Union”, ENISA is to propose a roadmap Network and Information Security driving licence” for all its members and to encourage businesses to promote cybersecurity at all levels. Few governments are trying to work with academic institutions with the government funding IT security models e.g. ECDL. In Zimbabwe for example the Computer society of Zimbabwe is making an effort to promote security awareness and hope to carry out training for relevant stakeholders.

The research shows IT security awareness is still lacking in most countries and where it is done the scheme do not apply to all users across the board.

***P7: (“****Until recently less effort have been made to build capacity on cyber security including users and workforce. There is a very big gap if we consider security awareness to users despite the fact that every organization are transforming the way they operate or do their business using internet technology without putting much effort. It’s very dangerous as I can learn from what is being practiced in our country. Security education is vital if the government wishes to create health security to the community.”)*

**(ii) ICT Security Education in Schools**

In most countries ICT curriculum does not cover IT security education and training. There are no national standards to integrate IT security education in normal educational systems. In Europe, through the “European Strategy for a Better Internet for Children” the Member States (MS) are advised to include online safety in school curricula. EC also to assist in developing a specific module within Europass for digital competence industry.

In Sri Lanka, ICDL, Sri Lanka CERT, National Child Protection Authority and Microsoft Sri Lanka, all collaborates to conduct awareness sessions for schools, educational institutions and Sunday schools.

P20: (“*Capacity building and creating awareness to the community is very important. Currently there is no cyberwellnes in ICT education in Tanzania. This is from family, primary level education to universities. Its normal to find a university with ICT programmes but none in security. This area needs a lot of research if we are to keep our people safe.”)*

While some countries are trying to amend their ICT curriculum to include aspects of Cyber bullying and Safety, things seem to move very slowly.

Many respondents feel that information security fundamentals should be part of school curricula.

**(iii) Security Education in higher education**

In many developing countries IT security is not available in high academic institution. Even where it is being taught, the course is part of the Computer Science courses rather than a standalone course. In some countries higher education courses in information security are only found in private institutions. E.g. Strathmore College university in Kenya just launched an MSC in Information Security

ICLD IT security model seems to be the only course offered in many schools and higher education institutions in the world.

***P6:*** *(“It seems that here in Germany we are still believing in the concept of "digital natives" that grow up with IT and a comprehensive understanding falls into place.”)*

Lack of IT security professional is also hindering introduction of Information Security courses in some countries

Industry standard certification such as CCNA, MCSE, CISSP are offered in many countries*.*

**(b) Child Online Protection**

(i) Legislation

In most countries the respondents were not sure of the legislation. Some think that there may be some policies in place but not effectively adopted. Even for the few countries who responded there is the issues of technicality and personnel capacities. There is lack of awareness in this area.

(ii) Reporting mechanisms of incidents

In most countries they have Child Protection hotlines but when it comes to Child Online Protection reporting mechanism, here is always a challenge on handling of incidents and investigation. Many respondents felt that very few people are aware of where or how to report cases in different countries and even when reported very little is done due to lack of resources in many countries.

As mentioned above on legislation awareness of reporting mechanisms and the law is lacking in many countries.

## Cyber Security Strategy - Implemention Challenges

### Capacity Building

|  |
| --- |
| * Lack of knowledge to government officials * Education and training * Resources * Lack of legislation * Lack of sponsorship in building capacity of trainers and professionals to champion awareness raising * Lack of government-led initiatives (with funding) to support any campaign. * Low capacity for both individuals understanding of the issue, as well as technical constraints. * Regional/geographical isolation. * Ineffectiveness of implementation of the policies * The lack of capital, difficulties in balancing the national expenditure for common demands in life and new facilities (i.e. computers, modems), the maintenance procedure * Developing and adopting the strategy was relatively easy; however, implementing it needed resources that could not be allocated and maintained with time. * the need to work on grassroots level (ordinary users * Proper training of ICT officials, trainers, teachers. Constantly evolving IT security threats * The contradiction between cybersecurity needs and business interests. * Capacity building due to financial constraint from governments and businesses. * Lack of knowledge or appreciation of ICT. Government not embracing and implementing laws to curb cyber security issues. * Child Online Protection – is not enough resources and attention to this as well |

|  |
| --- |
|  |

### Child Online Protection

There was very few response on this questions.

* The respondent felt that parents do not have enough digital knowledge to control their children.
* Both parent and children should be well trained. Trainings should be based on the national standards.
* Training could be done through community support for parents.
* Sponsorship needed.

**P1: (“***The constant underfinancing of educational sector has led to the situation where most teachers are underpaid and overworked, leaving them with neither skills or interest to handle cyber security incidents (in fact, those in charge are often the most ignorant). The legislation is mostly adequate, the practical implementation is often lacking*”.)

### Successful models

* Some countries are starting to recognize human aspects of security and are working with ordinary users to raise awareness.
* In Europe there are a number of awareness raising activities e.g. Safer Internet Day, European awareness network Insafe etc.
* In many countries people are not aware of what the government is doing, so not much have been achieved in this area.
* Increased number of schools that are being proactive in awareness campaigns.
* Passing of the bills, which is raising awareness at the highest levels.
* Proactive foreign policy positions on key issues of Information Development.

### What needs improving

Knowledge and Awareness

Legislation

Capacity building for all stakeholder

Regional Coordination to share knowledge and information

### Stakeholders

**All Stakeholders:**

Ministry of ICT

Government agencies

Policy makers

Educators

Teachers & Parents

ICT business sector

ICT Professionals

Politicians

NGOs

# Dissemination for next period

This part describes which activities must be taken to the next phase of ISES.

## UNESCO

The project team did not sufficiently communicate with local UNESCO offices. Therfore for the next phase we want:

* Join local UNESCO Conferences
* Regional Head Office: Connect and get program to connect. Deliver our report in persons  
  What they have in the program 2016/17: Is there a good opportunity to connect for Events / Workshops / Conferences …

## Corporate Social Responsibility Programs (ISO 26’000)

The project team made some attempt to connect to major player and get some funding for LSD projects. However, we were running out of time. Typical organisation we can ask are:

Companies with Corporate Social Responsibility programs, which might be useful in the context of ISES e.g. for HW / SW / Funding:

* Microsoft
* Intel
* Samsung
* Huawei (Steward Kowalski)
* HP
* Cisco
* GAFA (Google, Amazon, Facebook, Apple)

Associations, which might be useful in the context of ISES

* ISACA
* CIRT / FIRST (Bernhard asks Margrete)
* Central Banks
* Government Agencies

Thereby, logos of IFIP, UNESCO, and ENISA (if possible) could be used for Website and communication.  
In addition a professional ISES Logo must be designed.

# Proposal UNESCO Participation Program 2016 / 2017

ISES addresses issues of SDG / WITT4 and is in line for supporting both goals. See also:

* UNESCO Strategy 2014-2021
* UN Sustainable Development Goals SDG
* Action Line WISIS (ITU / UNESCO)

We present to coincidence of ISES with the SDG goals in the matrix below:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **SECURITY** | **EDUCATION** | **ECONOMY** | **DIGITAL EQUITY** |  |
| ISES supports Trust and Confidence as its central target | ISES targets security education as one of the main means for awareness | ISES supports economy, because losses of cybersecurity will eat up the revenue in LDC otherwise. | Equity is ISES target to balance out between first world and LDC | **TRUST & CONFIDENCE** |
| Empowerment is the ISES keyword for creating a responsible security behaviour. | Education is the mean for empowerment. | ISES encourages international companies, to support LDC | All gender and all nations should have equal security standards: this is one of the main goal of ISES. | **DIGITAL RESPONSABILITY** |
| Without according information security, sustainable development in LDC will not happen. | Traditionally, education is the premium mean to create a sustainable difference. | Continues effort for continuous growth is one of the best stimuli. This can happen only, when the digital assets are secure. | An opportunity is to use smart brains at both places, in first world and LDC.  ISES is stimulating this. | **SUSTAINABLE DEVELOPMENT** |

1. ENISA (2011) The UK Cyber Security Strategy: Protect & Promoting the UK in a digital world. Website: <https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/cyber-security-strategy-of-the-united-kingdom>. (Accessed, December 2015) [↑](#footnote-ref-1)
2. HM Government (2010) A strong Britain in an age of uncertainty: The National Security Strategy [↑](#footnote-ref-2)
3. HM Government (2014) The UK Cybersecurity Strategy Report on Progress & Forward Plan. Website: <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/386093/The_UK_Cyber_Security_Strategy_Report_on_Progress_and_Forward_Plans_-_De___.pdf>. (Accessed, December 2015) [↑](#footnote-ref-3)
4. ECDL Foundation, Website: http://www.ecdl.org/ [↑](#footnote-ref-4)
5. ICTAuthority. (2014) ICT Masterplan 2017: Towards a digital Kenya. Kenya Education Network (KENET). Website: <https://www.kenet.or.ke/node/132>. (Accessed, December 2014) [↑](#footnote-ref-5)
6. ICT Authority (2014) Shirikiana government shared secivices. Website: <http://counties.icta.go.ke/>. (Accessed, December 2014) [↑](#footnote-ref-6)
7. Kimani K., Mwangi M., Shiyayo B., Kigen P., Muchai C. Kenya Cyber Security Report 2014: “An Integrated Approach: Processes, Intelligence & Monitority”( Page 12). Serianu Limited. Website: http://www.serianu.com/downloads/KenyaCyberSecurityReport2014.pdf (Accessed, December 2014). [↑](#footnote-ref-7)
8. Carolyne G. Cyber crime in Kenya. Ministry of Information, Communications and Telecommunication. Website: <http://www.information.go.ke/?p=770> (Accessed, December 2014) [↑](#footnote-ref-8)
9. ENISA(2014) Kenya National Cybersecurity Strategy. Website: <https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/KE_NCSS.pdf>. (Accessed, December 2014). [↑](#footnote-ref-9)