POLICY AND IMPLEMENTATION ISSUES FOR INFORMATION SECURITY EDUCATION IN DEVELOPING NATIONS

Serah Francis[1], Konrad Marfurt[2]

[1] *Gjovik University College (NORWAY)*
[2] *Lucerne University of Applied Science (SWITZERLAND)*

Abstract

The increasing ubiquitous use of 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, the widespread use of ICT presents a wide range of social and ethical issues from online safety to security and misuse of information. 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 an acceptable level whilst 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 responsible and safe use of ICT.

The issue of how to secure 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 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, we are allowing the 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 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 for effective implementation models on strong education and solidarity to assist the policy makers and other stakeholders in development and integration of ICT security in education curriculum 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).

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

1 INTRODUCTION

1.1 General Remarks

The world has become reliant on technology thus improving lives of millions of people through information and communication technologies (ICTs). People continue to move away from using conventional ways of doing things to computerized techniques such as e-banking, e-learning, e-health, e-business, e-government and socialization. With an estimate of two thirds of the world’s population

online, the full potential of the digital economy has yet to be realized. Unfortunately, the continuous growth and wide spread use of technology has the downside to it. The report “Comprehensive Study on Cybercrime” by the UN office on Drugs and Crime’s argues that cybercriminals no longer require complex skills or techniques to conduct cybercrime, and that developing countries subcultures of young men who engage in computer fraud have emerged, many of whom have been involved in cybercrime in late teenage years [1].

The issue of securing cyberspace is important to all nations including developing and developed countries because cyber insecurity has international ramifications. Therefore, improving resilience capabilities requires investment by political, economic, and social forces through law enforcement and regulatory department, educational institutions and ministries, private sector operators and developers of technology, public partnerships, national and international cooperation [2]. This requires a structured strategy or policy outlining the vision, priorities, principles and approaches which a country has to take to protect its systems and networks as well as the society from cyber threats. Many countries in the world have developed and published their National Cybersecurity Strategies but most have failed to address some key elements such as analysis of the cost planned activities, performance and monitoring measures, assessment of the risks and cost of mitigating them [3]. 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.

Most countries in the developing world are yet to develop their cybersecurity strategies or policies and for those who have done so, implementing them is an additional challenge. The next section points out the issues affecting policy implementation.

1.2 Policy and Strategy Implementation Issues

The following table summarizes issues that were raised as a result of earlier literature review, question field research, and workshop discussions with participants from different parts of the world.

Table 1: Implementation Issues

– 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

The table shows that there is still a lot to be done and nations need to work together if the minimum level of security is to be reached. There is also an increasing demand of experts with relevant skills to assist policy makers in making the right decisions on what needs to be protected and how it needs to be done, especially in developing countries. Different countries are at different levels of cybersecurity maturity but raising awareness through government led initiatives can go a long way in changing people’s habits on how to behave online and also attract more people to the industry. This is key, especially for the younger generation who are new to the industry, who rather than entering the industry become hackers for the wrong reasons.

2 FIVE CRITERIA FOR CYBERWELLNESS

2.1 Overview

Cybersecurity Strategy or Policy attempts to provide a framework with "a set of action based upon a national vision to achieve a set of objectives that contribute to the security of the cyberspace" [2]. The strategy should state clearly how these objectives will be achieved and which stakeholders ensure that those objectives are achievable. For example, in a case where a cybercrime is committed in a different country the law enforcement agencies have to collaborate with different agencies within and outside the country. Effective structures must be in place if the criminals will be apprehended. The country where the crime is committed must have proper resources and experts in that area of investigation. In addition, it must have signed an extradition treaty with the country where the criminal is residing. Without an effective legal and regulatory framework, proper skills specific to cybersecurity, cooperation, national and international organization structures, apprehending such criminals could be difficult [4]. Moreover, sharing information across the border could minimize the spread of threats and attacks and also give warning to those who want to commit crimes in multiple countries thinking they won't be caught. Without performance and evaluation measures, it is difficult to know if a country is making any progress or not [5]. Cybersecurity is clear cut in all sectors and therefore, it requires collaboration from the law enforcement and justice departments, education institutions and ministries, private sector operators and developers of technology, public-private partnerships and intra-state-cooperation as well as individual users. Technology keeps evolving over time, so it would be naive to expect the exact state of review for each country. We also have to keep in mind that Cybersecurity is a sensitive issue and some governments might not want to publish their documents online.

The Global Cybersecurity Index (GCI) and Cyberwellness framework provides five criteria with indicators to gauge the level of commitment for each nation [6].

Table 2: Criteria for cyberwellness

– Legislation
– Technichal Measures
– Organizational Measures
– Capacity Building
– Cooperation

We shall illustrate these criteria with five relevant examples from different countries in the following subsection. The following section will contain three case studies from developing countries with focus on education and child online protection.

2.2 Australia (Legislation)

Australia is rated number 3 in the global ranking index, and first for Good Practices in legal measures in Asia region. The National Cybersecurity for Australia was established in May 2012 [7]. One of its strategic priorities is "to maintain an effective legal framework and enforcement capabilities to target and prosecute cybercrime" [7]. To achieve its objective, the government of Australia took measures and enacted several legislations and regulation relating to cybersecurity.

Table 3: Australian Legislation Relating to Cybersecurity

• Cybercrime Legislation Amendment Act 2012, No.120, 2012
• Australian Cybercrime Online Reporting Network and the Cybercrime Strategic Framework
• Australian Communications and Media Authority (ACMA) responsible for enforcing the spam Act 2003
• The Australian competition and Consumer commission (ACC) provide advice about scams and how to report them
• Australian Federal Police (AFP) High Tech Crime Operations (HTCO) responsible for investigating high tech crime
• Australian Securities and Investment Commission (ASIC) investigating spams relating to financial services such as phishing

Organised crime costs Australia around $10 to $15 billion each year, and so Australia had a reason of wanting to create and enhance its legal framework. In addition, the government is also undertaking other measures such as providing Australia legal professionals with requisite level of technological knowledge and understanding, among other things.

2.3 Estonia (Technical Measures)

The first Estonia Cyber Security Strategy was developed in 2008 – a year after the country had experienced a massive DDoS attack which shut down services to major websites and communication disrupted across the country. After this attack, Estonia needed to increase its technological capabilities that could protect its critical and vital services to reduce the risk of being attacked again. Since then the strategy has been reviewed and an updated version was published in 2014 [8]. The main goal of the new strategy is "to increase cybersecurity capabilities and raise the population's awareness of cyber threats, thereby ensuring continued confidence in cyberspace". Also after the DDoS attack, the country got a lot of attention from IT security companies wanting to expand their businesses and now it has a very high level of information security competence and awareness. So, the government has taken the following measures to ensure the reliability of services and infrastructure in the country.

Table 4: Govt. Measures to Ensure Cybersecurity in Estonia

- Compulsory Information Security Standard (ISKE) for state and local government organisations to handle databases/registers
- Definition of a Three-level Baseline System: three different sets of security measures for three different security requirements
- The Estonia e-Government and IT infrastructure system uses 2048-bit encryption to power its Electronic-ID, digital signature and X-road-enabled systems
- Estonia implemented a national PKI (Public Key Infrastructure)

2.4 Japan (Cooperation)

Japan ranks 5th in the international ranking and best for good practice in terms of Cooperation in Asia Pacific. Japan International Strategy on Cybersecurity Cooperation – j-initiative for Cybersecurity was developed in October 2013 through the Information Security Policy Council [9]. The Cybersecurity Cooperation Strategy objective is "to actively strengthen cooperation and mutual assistance internationally so as to ensure safe and reliable cyberspace". Japan is accomplishing this goal by collaborating with other countries through sharing of information and technical capabilities. So far, Japan has already signed an agreement with Asian Pacific region and provides secretariat function for the Asia Pacific Computer Emergency Response Team (APCERT). The government has international cooperation with US, EU, Israel and South America to promote policy consultation and information sharing. Elsewhere, Japan is a member of the Forum of Incident Response and Security Teams (FIRST) and collaborates with the UN Group of Governmental Experts (UNGGE) on Developments in the Field of Information and Telecommunications in the Context of International Security. It is also member of G8, OECD, APEC, NATO, ASEAN etc. In view of the above, it would seem that Japan is working towards its main objectives of strengthening cooperation.

2.5 United Kingdom (Capacity Building)

In 2011, the UK set aside 860 million pounds to support the National Cyber Security Strategy 2011 for four years running from 2011 to 2015 [10]. Part of that budget was to tackle cybersecurity skills shortage by educating general public and businesses on cybersecurity awareness. Since then, the government has collaborated with several organizations and academic institutions and as a result several initiatives have been launched.

Table 5: Cybersecurity Initiatives in the UK

- "GetSafeOnline" was developed to assist general population with cyber issues
- "10 Steps to Cyber Security" is a one stop place where organisations can get guidance on how to protect themselves in cyberspace.
- The government is sponsoring 30 PhDs and the Department for Business to 48 PhDs through two centres doctor training.

- Cybersecurity training for the civil service, law enforcement and the military has already been rolled out.
- A cybersecurity challenge which aims to groom young cyber specialists is already up and running.
- The Communicatons-Electronics Security Group (CESG) is the Information Security arm of Government Communications Headquarters (GCHQ), definitive voice on the technical aspects of Information Security in Government
- The UK has established a set of Academic Centres of Excellence in Cybersecurity Research and complementary Research Institutes e.g. Oxford Internet Institute that includes capacity building centre

Capacity building is necessary across all sectors of cybersecurity ecosystem and therefore, with clear set objectives and resources a country can work towards having a society built on knowledge, skills and capability to fight cyber security. This is what UK is trying to achieve and can be a good lesson for others. The country is number 4 in global ranking and it is on the top for good practices on Capacity Building in Europe.

2.6 Korea (Organizational Measures)

Korea is ranked 5th in global ranking and the best in good practice on Organisation measures in Asia Region [6]

The Korea National Cyber Security Measures is responsible for the national security of Korea.

The Personal information protection normalization plan provides a national governance roadmap for cybersecurity in Korea.

The National Information Security Index provides the national benchmarking for information security level of the private sector and individual users.

The National Information Security Index Ministry of Science, ICT and Future Planning and is the national benchmarking for private cybersecurity development.

3 THREE CASE STUDIES FROM DEVELOPING COUNTRIES

3.1 Kenya

3.1.1 Kenya's Cybersecurity Strategy

The country is increasingly becoming dependent on computer networks and information infrastructure due to faster internet connectivity rates. In 2013, Kenya had 33.6M mobile subscribers (82.6% penetration) and 26.1M Internet users (64.3%). Unfortunately, the increasing dependency of the Internet has also brought some risks. In the same year, the rate of cybersecurity attacks in Kenya had increased by 108% from 2.6M to 5.4M attacks [11]. Every government has a role to play in protecting its ICT infrastructure and promoting the use of ICTs by its citizens. There was a need for the Government of Kenya (GoK) to coordinated national structure in order to improve and enhance its cybersecurity policy, legal and regulatory frameworks. This would support national priorities of ICT growth and critical information infrastructure protection. In response, Kenya developed a National Cybersecurity Strategy with a vision "to secure the national's cyberspace, while continuing to promote the use of ICT to enable Kenya's economic growth*"* [12].

Table 6: Main Focus of Kenya's Cybersecurity Strategy

- Enhance the nation's cybersecurity posture in a manner that facilitates the country's growth, safety, and prosperity
- Build national capability by raising cybersecurity awareness and developing Kenya's workforce to address cybersecurity needs
- Foster information sharing and collaboration among relevant stakeholders to facilitate an information sharing environment focused on achieving the strategy's goals and objectives

- Provide national leadership by defining the national cybersecurity vision, goals, and objectives and
- Provide national leadership by defining the national cybersecurity vision, goals, and objectives and coordinating cybersecurity initiatives at the national level.

One year after the first Kenyan National Cybersecurity Strategy was established in Kenya, experts in the country argue that things have not improved and the rate of computer crime has risen. 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. The government is lacking experienced security professional to counter cyber threats. Information security awareness is very low although the government is trying through the national computer response team (KE-CIRT/CC) to educate users on the risks of being online. Kenya is becoming a cashless society and cybercrime will continue to rise if serious measures are not taken to secure the internet infrastructure.

3.1.2 Kenya's Cyberwellness

The Kenya Communication Acts (Amendment Act 2009) has been enacted to deal with cybercrime in Kenya.

Kenya does not have any official recognized national cybersecurity framework for implementing internationally recognized cybersecurity standards, or a certification framework for certification and accreditation for national agencies and public sector professionals. The Ministry for information, Communications and Technology is responsible for the overall national cybersecurity strategy.

Kenya does not have an officially recognized research and development (R&D) program/projects for cybersecurity. There is no specific agency to deal with IT security awareness for users in the country. KE-CIRT/CC is working with various stakeholders to promote educational and professional training programs for raising awareness with the general public. The University of Nairobi, through C4DLab, supported by ICT Authority (ICTA) is offering a Cyber Security training program for 3 days. Some public universities already run IT security modules as part of their overall IT or Computer Science program. The Kenya government has endorsed International Computer Driving License (ICDL) programme as the entry level computer certification designed to demonstrate competence in computer use.

Kenya does not have a specific Child Online Protection legislation. Specific legislation on cybercrime has been enacted through the following instruments: Sexual Offense Act, Children Act, Information and Communication Act.

In addition to the above national legislation, Kenya has ratified to the following international conventions, "Convention on the Rights of the Child" articles 16, 17(e) and 34(c) and the "Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography" articles 2 and 3.

In August 2015, the government of Kenya in partnership with other organisations launched a campaign on Child Online Protection through the ICT regulator, Communication Authority of Kenya (CA). The campaign was launched at the Kenya Primary Schools Head Teachers Association (KEPSA) Annual conference held this year and it is expected to last for 3 months. Unfortunately, there are no mechanisms for reporting incidents related to child online protection, any reports are handled by child protection agencies or the police.

3.2 Nepal

Internet services were first introduced in 1993 and almost all big cities had Internet facilities before the earthquake in April 2015. During the period 2013/2014, Nepal internet penetration rate had risen to 33.15% from 18.94% in 2011/2012. Through their national broadband policy (2013/2014) the government of Nepal's objective was to provide secure, meaningful, affordable and reliable broadband services to government agencies, health and education sectors. The government has yet to develop a Cybersecurity Strategy or Policy and effective legal measures to protect the country's internet infrastructure and its online users. A lot of things have changed after the earthquake, meaning that the government of Nepal and all stakeholders have a complex work ahead and help is needed from the International cooperation to assist in building the infrastructure.

Nepal ranks number 25 in the global ranking index.

The country does not have any specific policy or legislation on cybercrime. Any cybercrime is handled through Electronic Transaction Act. The Kathmandu Metropolitan Police Crime Division (KMPCD) is the agency responsible for cybersecurity [6].

As a least developed country Nepal has been getting support on cybersecurity from the cybersecurity execution arm of ITU (ITU-IMPACT) through the project “Enhanced Cybersecurity in Least Developed Countries”.

Nepal has a high demand of computer science education due to thrilling outsourcing industry in software development. Like many other developing countries, Nepal is short of specialist skills on cybersecurity which leaves most of the systems and network open to abuse. The lack of awareness is dangerously high. Software piracy is a big problem in the Asian region, Nepal included. The country has been a victim of cybercrimes such as ATM pin steal, cloning of ATM cards, Hacking, Financial fraud in Internet banking, Phishing and Social network related crime. The Number of reported Cybercrimes rose from 34 in 2012-2013 to 65 in 2014-2015.

3.3 Rwanda

Rwanda internet penetration is 25.5% in 2015 compared to 7% in 2011. The growth has been contributed by the large investment by the government on ICT. The country ranks one of the best for good practices in capacity building in Africa and number 11 in global ranking.

Rwanda does not have an officially recognized national cybersecurity policy but the Specialized Cyber Security Division is the official recognized agency for implementing a national cybersecurity strategy. However, there is a draft National Security Policy which was waiting for approval and further dissemination according to the world internet stats. Legislation on cybercrime has been enacted through the Law on Electronic Message, signature and Draft ICT bill Transaction. The country has no recognized certification and accreditation agencies.

The country has an official Computer Incident Response Team (Rw-CSIRT) and collaborates with other agencies in Africa and outside Africa e.g. Korea KISA and ITU. It is an active member of East Africa Community (EAC) and African Union (AU) [6].

The government of Rwanda is very active in capacity building. Under the BSc Information Security Program, different Information Security Course Modules are offered in IT or Computer Engineering in higher education. Cybersecurity awareness is promoted for internet users in Rwanda. Rwanda has 80 public sector professionals certified under international recognized certification. In 2008, the government of Rwanda launched One Laptop per Child (OLPC) project. The project is still ongoing.

Rwanda is the regional centre for ICDL Africa and has recognized ICLD certification programs for Government employees, teachers, students and general population. Recently, the government has offered ITU to establish a regional centre for cyber security in the country.

The country has a specific legislation on child online protection enacted through Article 211, 229 and 230 of the Organic Law instituting Penal Code and acceded in several conventions on the Rights of the Child but no reporting mechanisms.

4 DISCUSSION

There is no doubt that Kenya, Nepal and Rwanda as part of developing and least developed countries are lagging behind in some aspects of cybersecurity. Developing Cybersecurity Strategies or policies is one thing but not supporting their 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 if these countries want to be part of the global economy.

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. A good example for capacity building initiatives is the UK. The country has allocated millions of pounds to cybersecurity and is working in collaboration with the industry to promote cybersecurity skills and awareness for all users in the UK. What UK is doing can be seen as far reaching by many in the developing world and they would argue that there are other more pressing issues to spend the

money on. Some aspects like working with the private sector, is something developing countries can improve on. Rwanda is also a good example in the African region for capacity building.

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.

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 marginalized people.

A visit to Kenya, Tanzania and Rwanda by authors of this paper gave them first experience some of the issues discussed in this paper. A sabbatical in Rwanda and Uganda plus working in a private university and visits to rural areas in Kenya and Tanzania this summer gave the authors a clear picture of the current situation in term of ICT awareness. For example, the government of Kenya has already rolled out e-government services (e.g. ID Cards, Passports and Tax Return) but many in the rural areas lack digital literacy. To give the government a credit, they are working very hard to roll out broadband in all corners of the country but this should go hand in hand with ICT and ICT-security training. An experience from Tanzania showed that cultural differences can also hinder development. Most people in Tanzania only speak Swahili, so it can be very difficult to train in English or any other language. The good news is: the kids and youth are eager to learn and are catching up quickly. Most areas are lacking internet infrastructure and the bandwidth is very low. This is a problem for users when updating their devices or installing antivirus software. Government offices and academic institutions lack professionals with relevant IT security skills in those areas. Most security awareness initiatives are concentrated in urban areas leaving rural areas behind. 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. In addition, a wealth of knowledge is required from all users.

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 and entrepreneurship.

5 RECOMMENDATIONS

We all live in a connected world. Rich countries and experts in cyber security or information security should show their solidarity in securing the cyberspace by assisting developing and least developed countries. This could be by establishing platforms for information and experience exchange between first world and least developed countries on state-of-the-art research; development and implementation of security management models; Governments, Businesses, NGOs and Academic institution to facilitate Student and experts' exchange; businesses and developers to deliver more secure software and internet services that are adaptable to minority and marginalized people in our communities. The model used by CSIRTs or FIRST can be studied and be used to achieve this.

IT-security education and awareness should be included in all education curricula and teachers training institutions. We need models to educate the cyber security work force in all nations. ICDL training program is a good example of a program which can be applied to all levels of education in any country to train the basic fundamentals of IT Security. The course includes ICT courses from basic to

advance knowledge. Raising awareness initiatives need to be tailored to social and culture backgrounds where community and church elders can be involved in rural areas. As well as the traditional mass media, social media has become a powerful tool especially with the youth. Educational institutions should have free access to internet at adequate speed. The model "train the trainer" should be applied. For example, students in higher institution doing IT courses could be trained to help in creating awareness in schools or community centres. Children learn very first and therefore, IT Security training should start from an early age. There are already initiatives in some developing countries helping with training the kids in ICT at a young age e.g. Rwanda's "One Laptop per Child" initiative. These initiatives could be used to include basic IT Security training for children.

Governments and policy makers should facilitate these processes by having legislative and policy measures that also ensure that human rights are protected.

REFERENCES

[1] UN, "UN Comprehensive Study on Cybercrime," United Nations Office on Drugs and Crime, 2012.

[2] Fisher, E.A. (2005). Creating a National Framework for Cybersecurity: An Analysis of Issues and Options.

[3] Luiijf E. and Besseling K. (2013). Nineteennational cyber security strategies. Int. Journal of Critical Infrastructure, vol. 9, no. 1/2

[4] Orji, U. (2012). Cybersecurity Law and Regulation. Wolf Legal Publishers, pp. 398-400.

[5] Goodwin, C.N.J. (2013). Developing a National Strategy for Cybersecurity. Microsoft Press.

[6] ABI Research (2015). Global Cybersecurity Index & Cyberwellness Profiles. ITU Report.

[7] Australian Government. (2009). Cyber Security Strategy. Common Wealth of Australia.

[8] Ministry of Economic Affairs and Communication of Estonia. (2014). Cyber Security Strategy 2014-2017.

[9] Information Security Policy Council of Japan. (2013). Cybersecurity Strategy: towards a world-leading, resilient and vigorous cyberspace. Information Security Policy of Japan.

[10] National Audit Office. (2013). The UK Cyber Security Strategy Landscape Review. The Stationery Office (TSO).

[11] Kigen P. et al. (2014). Rethinking Cyber Security: An Intergrated Approach. Kenya Cyber Security Report. Serianu Ltd.

[12] Government of Kenya. (2014). Cybersecurity Strategy. The Ministry for information, Communications and Technology.

APPENDIX: Comparison of Cyber Wellness Profiles

Countries:	**Australia**	**Canada**	**Estonia**	**Japan**	**Kenya**	**Nepal**	**Rwanda**	**UK**
Global Rank	**3**	**2**	**5**	**5**	**15**	**25**	**11**	**5**
Legal Measures								
Criminal legislation	√	√	√	√	√	√	√	√
Regulation and Compliance	√	√	√	√	√	√	√	√

Technical Measures								
CIRT (Computer Incident Response Teams)	√	√	√	√	√	X	√	√
Standards	√	√	√	√	x	X	√	√
Certification	√	√	x	√	x	X	x	√
Organisation Measures								
Policy	√	√	√	√	√	X	√	√
Roadmap for Governance	√	√	√	√	√	X	x	√
Responsible Agency	√	√	x	√	√	√	√	√
National Benchmarking	√	x	√	x	√	X	√	√
Capacity Building								
Standard Development	X	√	√	√	x	X	x	X
Manpower Development	√	√	√	√	√	X	√	√
Professional Certification	X	x	√	x	x	X	√	√
Agency Certification	X	x	x	x	x	X	√	√
Cooperation								
Intra-state Cooperation	√	√	√	√	√	X	√	√
Intra-Agency Cooperation	√	√	√	√	√	X	√	√
Public Sector Partnership	√	√	√	√	√	X	√	√
International Cooperation	√	√	√	√	√	√	√	√
Child Online Protection								
National Legislation and Strategy	√	√	√	√	√	√	√	√
UN Conventional and Protocol	√	√	√	√	√	√	√	√
Institution Support	√	√	√	√	x	X	x	√
Reporting Mechanism	√	√	√	√	x	X	x	√

Source: Global Cybersecurity Index & Cyberwellness Profiles. ITU Report by ABI Research (2015).