INFORMATION SECURITY AWARENESS & TRAINING PROGRAM

By Serah Francis
MSc Student, Gjøvik University, Norway
ISES Member

IFIP TC3 – ISES Project

INTRODUCTION

- Africa has 167 million Internet Users and is estimated that by 2025, that figure will raise to 600 million Internet users and 360 million smartphones
- In 2013, Internet contribution $18 billion and is estimated to be $300 billion in 2025.
- Every second, 18 adults become a victim of cybercrime, resulting in more than 1.5 million cybercrime victims each day on a global level

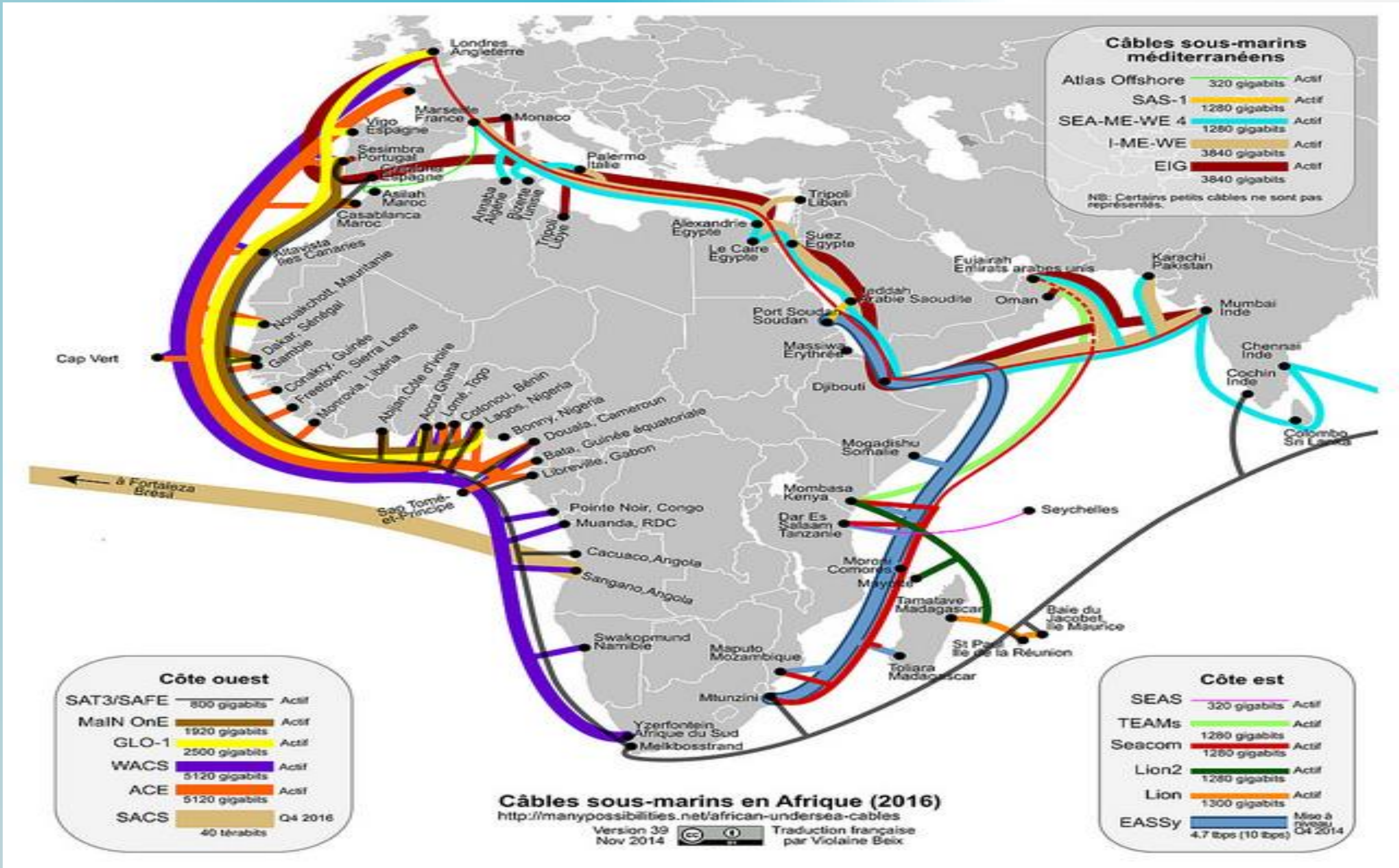
CRIME

- theft of personal data
- fraud
- inside threats
- abuse on children
- Inside threats
- terrorism.

- In 2012, banks in Kenya, Rwanda, Uganda, Tanzania and Zambia alone lost US$245 M to fraud
- Same year, a South African Bank lost $6.7 million when two of their employees’ account were hacked
- In 2013 South Africa was identified as one of the countries hosting more than average rate of phishing sites, and 70% of its citizens were victim of cybercrme compared to 50% globally
- Last year, 5,000 Kenyan Facebook users lost million of shillings through a hacking scam

CRIME FACILITATORS

- Fast Internet Connection
- Increase of mobile devices
- High rate of unemployment,
- Lack of national databases to track criminals,
- Growth of e-government initiatives and e-commerce,
- Use of unsecure or outdated hardware and software



Câbles sous-marins en Afrique (2016)

http://manypossibilities.net/african-undersea-cables

Version 39
Nov 2014

Traduction française
par Violaine Beix

IMPORTANCE OF INFORMATION SECURITY AWARENESS & TRAINING PROGRAM

- Makes individual aware of their responsibilities in relation to information security
- Allows them to recognize IT security concerns and respond accordingly
- Provide a focal point and a driving force for a range of awareness, training and educational activities related to information security.
- Security is everyone’s responsibility.

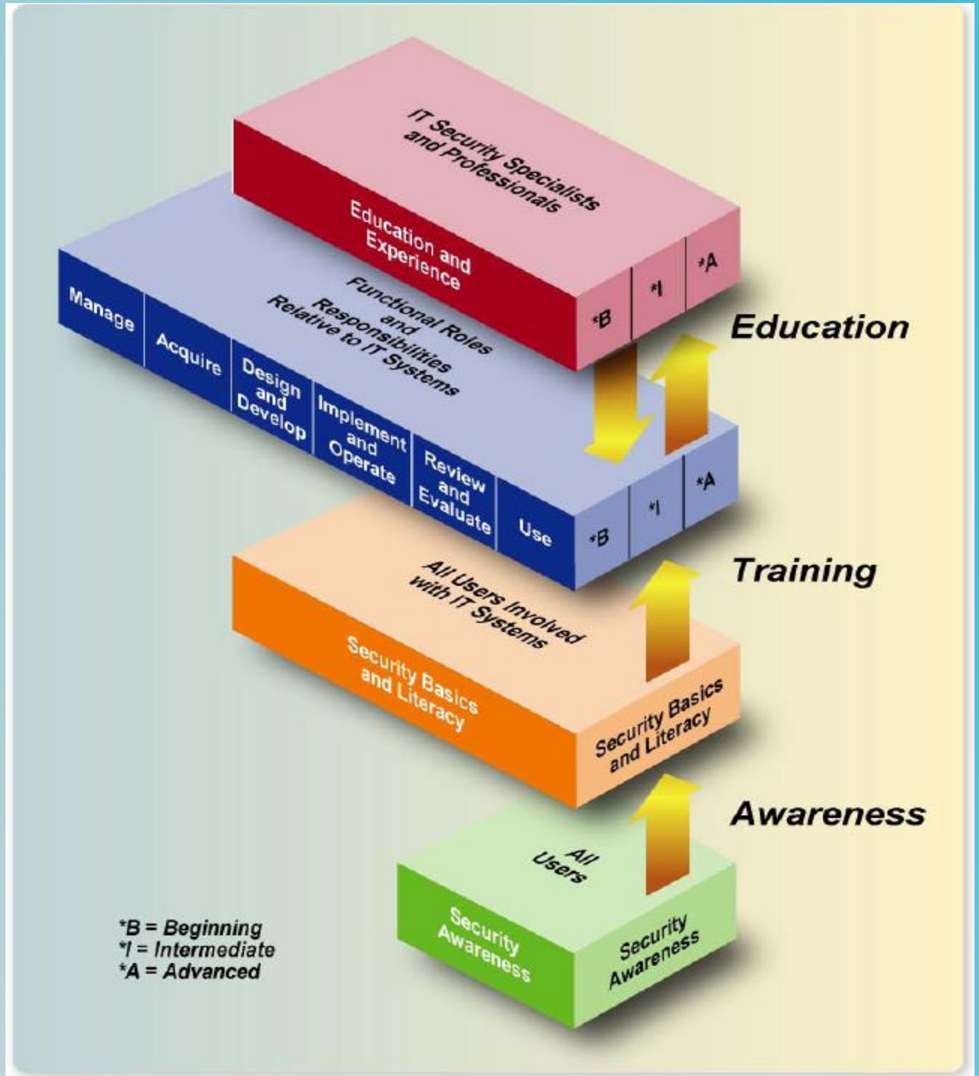
WHY SECURITY AWARENESS IMPORTANT FOR AFRICA

- For developing nations, ICT is a key component in improving the quality of life and participation in global economic activities.
- It provides opportunities for people with basic services such as e-banking, e-health, e-commerce and e-learning etc.
- **Important** that all users understand the risks of being online and the impacts of not using best practices.
- Failure to recognize the above could limit their use of internet services due to lack of trust and confidence

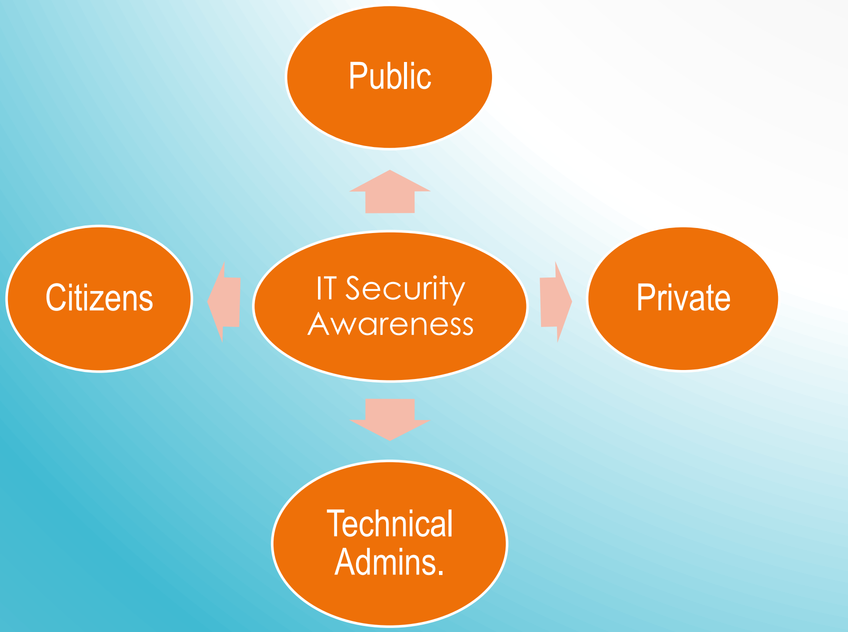
KEY CHALLENGES

- Shortage of information security professionals and skills
- Lack of basic awareness among users.
- Lack of knowledge/knowhow of importance of ICT Security.
- Lack of secure software and ICT-based applications.
- Lack of effective legislations and regulations
- Lack of collaboration between public, private, experts, academia and international organisations.

IT SECURITY LEARNING MODEL (1)



Target Group



Public

IT Security Awareness

Citizens

Private

Technical Admins.

IT SECURITY LEARNING MODEL (2)

Four Level approach:

Awareness

- Designed to be presented to all users to focus their attention on security
- Intended to allow individual to recognize IT security concerns and respond accordingly
- It is a foundation of a good Information Security Awareness & Training program

Training

- Strives to produce relevant and needed security skills and competencies
- Builds upon information gathered from awareness presentations

IT SECURITY LEARNING MODEL (3)

Education

- Education and Experience level focuses on developing the ability and vision to perform complex multi-discplinary activities and skills needed to further the IT security profession and to keep pace with threat and technicies
- Strives to produce IT security specialists and professionals capable of vision and proactive response

Professional Development

- Intended to ensure that users posses a required level of knowledge and competence necessary for their roles
- Validation of skills typically through certification

AWARENESS

- Ensure upper management support
- Establish a policy
- Assign responsibility (CIO)
- Needs assessment
- Develop Awareness and Training Materials
- Implementation of the program
- Update and monitor program

AWARENESS -EXAMPLES OF TOPICS COVERED

- Undersanding the key concepts relating to the importance of secure information
- Protect computer and mobile devices from malware and unauthorised access
- Adopt safe habits of using email securely, social networks, and surfing the Web
- Back Up and restore data approariately and safely
- Secure dispose of data and device

AWARENESS – DELIVERY MODEL & EXAMPLES

- Partnership with Private Organisations, Education Institutions and NGOs
- Delivery through Social Media, T.V, Radio, Cybercafe, Digital Centres, Mobile Cinema & Posters, government & private websites

Examples

- Get Safe Online - https://www.getsafeonline.org/ - UK
- Stop Think Connect - http://www.dhs.gov/stopthinkconnect - US
- Slettmeg.no (("deleteme.no) - https://norsis.no/ -Norway
- Cyberstreetwise - https://www.cyberstreetwise.com/ - Soho, UK
- ENISA Cyber Security Month – https://cybersecuritymonth.eu/
- Kids Online - http://www.kids-online.net/

GOALS OF TRAINING

- To produce relevant skills & competence
- **Important:** Needs assesement to identify those individual with significant IT security responsibilities
- Each user may need specific training for their job
- Specific training programs may be tailored to specific organisations or systems e.g. Healthcare, Legal System
- Training can be delivered by Online or Live Instructor

TRAINING - TARGET GROUPS

- Users – Citizens with varying age and technical knowledge who use ICTs for personal use anywhere outside their work environment.
- All organisations’ personnel, Mid-level managers, Executive management & System administrators
- Third party – Partners, suppliers, consultant contracted to perform work in an organisation.

PROPOSAL FOR AFRICA (1)

- Align education system to include Information Security courses
- Raise Security Awareness using ways and methods fit for Africa
- Specialized Skills Training in Information Security could be established through local ICT Hubs or Computer Science Departments in public universities. This could lead to Train the Trainer courses and can be facilitated through Public Partnership,African CERT and NGO's based in Africa.

PROPOSAL FOR AFRICA (2)

- ECDL:
- Many African countries have adopted ECDL (ICDL) to promote digital literacy and ICT skills
- ECDL program is designed as an entry-level computer certification to demonstrate competence in computer use
- The program offers a range of IT modules and IT Security for basic skills
- Accredited Test Centres – which currently numbers more than 500, and now spans 22 territories in Sub-Saharan Africa.

CONCLUSION

- Educating Internet users to be safer and more secure requires collaboration and effort from government agencies, private organisation, academia, civil society and users. No government agency can reach everyone or provide all the necessary requirements on it’s own.
- The infrastructure of the internet is complex and requires all stakeholders to work together towards a common goal.
- Educating Internet users to be safer and more secure also gives them the trust and confidence in the use of ICTs and especially the more vulnerable people in our communities.
- There is an urgent need for a more coordinated and effective action in promoting IT Security Awareness & Training program across Africa and the rest of the world

REFERENCES

- Books
  - Managing an Information Security and Privacy Awareness and Training Program ISBN 978-1439815458
- Standards and Guidance
  - NIST SP 800-50 Building an IT Security Awareness and Training Program

?

Thank you