UNIVERSITY OF ESWATINI

ACADEMIA/UNESWA: Capacity building initiatives to strengthen Eswatini's Cybersecurity space

Presented by Dr Zenzo P Ncube

31 October 2019,Sibane Hotel ,Ezulwini,Eswatini

UNIVERSITY OF ESWATINI

Outline

- Global Cybersecurity Index (GCI)
- Cyber attacks vs National security
- Importance of cyber security awareness
- Topics to be covered in cyber defense training
- Benefits of cyber security awareness training
- Attributes of an effective cyber security awareness programme
- Role of academia in cyber security
- Cybersecurity research themes
- National Cybersecurity R&D Laboratory
- Cyber Security and Forensics (CSF) Research Group
- Research Partnerships
- Conclusions
- References

Global Cybersecurity Index (GCI)

- The Global Cybersecurity Index (GCI) is a composite index combining 25 indicators into one benchmark to monitor and compare the level of the cybersecurity commitment of countries with regard to the five pillars of the Global Cybersecurity Agenda (GCA).
- These pillars form the five sub-indices of GCI.
- The main objectives of GCI are to measure:
- • the type, level and evolution over time of cybersecurity commitment in countries and relative to other countries;
- • progress in cybersecurity commitment of all countries from a global perspective;
- • progress in cybersecurity commitment from a regional perspective;

Global Cybersecurity Index (GCI)(…)

- • the cybersecurity commitment divide (i.e. the difference between countries in terms of their level of engagement in cybersecurity initiatives).
- The goal of the GCI is to help countries identify areas for improvement in the field of cybersecurity, as well as motivate them to take action to improve their ranking, thus helping raise the overall level of cybersecurity worldwide.
- Through the collected information, GCI aims to illustrate the practices of others so that countries can implement selected aspects suitable to their national environment, with the added benefit of helping to harmonize practices, and foster a global culture of cybersecurity.
- The Global Cybersecurity Agenda (GCA) is an ITU framework for international cooperation aimed at proposing strategies for solutions to enhance confidence and security in the information society.

The ITU framework for international multi-stakeholder cooperation in cybersecurity

- The ITU framework for international multi-stakeholder cooperation in cybersecurity aims to build synergies between current and future initiatives, and focuses on the following five pillars:
- 1. Legal: Measures based on the existence of legal institutions and frameworks dealing with cybersecurity and cybercrime.
- 2. Technical: Measures based on the existence of technical institutions and framework dealing with cybersecurity.
- 3. Organizational: Measures based on the existence of policy coordination institutions and strategies for cybersecurity development at the national level.

The ITU framework for international multi-stakeholder cooperation in cybersecurity

- 4.Capacity building: Measures based on the existence of research and development, education and training programmes, certified professionals and public sector agencies fostering capacity building.
- 5.Cooperation: Measures based on the existence of partnerships, cooperative frameworks and information sharing networks.
- These five designated areas form the basis of the indicators for GCI because they shape the inherent building blocks of a national cybersecurity culture.
- The Global Cybersecurity Agenda (GCA) is an ITU framework for international cooperation aimed at proposing strategies for solutions to enhance confidence and security in the information society.

GCI 2018 indicators per pillar

Legal

Cybercrime legislation
Cybersecurity regulation
Containment/curbing of spam legislation

Technical Measures

CERT/CIRT/CSIRT
Standards Implementation Framework
Standardization Body
Technical mechanisms and capabilities deployed to address Spam
Use of cloud for cybersecurity purpose
Child Online Protection mechanisms

Organizational Measures

National Cybersecurity Strategy
Responsible Agency
Cybersecurity Metrics

Capacity Building Measures

Public awareness campaigns
Framework for the certification and accreditation of cybersecurity professionals
Professional training courses in cybersecurity
Educational programs or academic curricular in cybersecurity
Cybersecurity R&D programs
Incentive mechanisms

Cooperation Measures

Bilateral agreements
Multilateral agreements
Participation in international fora/associations
Public-Private Partnerships
Inter-agency/intra-agency partnerships
Best Practices

GCI groups

Countries are classified according to their level of commitment: high, medium, and low.

- High: Countries that demonstrate high commitment in all five pillars of the index.
- Medium: Countries that have developed complex commitments and engage in cybersecurity programmes and initiatives.
- Low: Countries that have started to initiate commitments in cybersecurity.

UNIVERSITY OF ESWATINI

Cyber attacks vs National security

- Cyber security attacks can:
- Paralyse the Govt's decision making systems
- Cripple a nation's critical infrastructure
- Cause massive panic and trigger inadvent wars

UNIVERSITY OF ESWATINI

Importance of cyber security awareness

- According to the ITU Connect 2030, there will be 70 per cent Internet penetration by 2023, increasing the need for a more cyber-secure space.
- Equipping citizens/employees with the knowledge and skills they need to protect themselves from criminal elements.
- Cyber-crime shows no signs of slowing down, and a cyber-attack has the potential to incapacitate an organisation.
- The 2019 Annual Cybercrime Report says global cybercrime will cost $6 trillion US by 2021 through damaged data, lost productivity, intellectual property theft and more.
- 95% of cybersecurity breaches are due to human error
- only 38% of global organizations state that they're prepared to handle a sophisticated cyber attack.
- 54% of companies say they have experienced one or more attacks

Topics to be covered in cyber defense training

- Current threats
- Attack red flags
- Defensive procedures
- Threat reaction plans
- Mock phishing and malware messages to see how they react, and then provided targeted training to those who fail to respond in a secure manner.

UNIVERSITY OF ESWATINI

Benefits of cyber security awareness training

- Less exposure to cyber security related risks;
- Lower costs due to both the lower frequency of cyber-related loss-incidents and the severity of those incidents;
- Lower costs associated with cyber security Insurance premiums;
- Saving time, as a lot of time, is wasted post Cybersecurity incidents in both finding out what happened, as well as possibly having to redo do the affected work;
- Market edge over your business competition, as public knowledge of Cyber Incidents, will negatively affect your business reputation; and
- Positive staff culture regarding the Cyber and Information security.

UNIVERSITY OF ESWATINI

Attributes of an effective cyber security awareness programme

- Should be focussed on real-life examples, both with the most common causes and the effects these examples might have;
- The training programme should be based on your own organisation's culture, policies, procedures and perceived threats;
- Each individual needs to understand their role in securing the business information, the importance of their roles and the consequences of their actions;
- The training should cover the Prevention and the responses to Cyber incidents;
- The programme should be easy to understand, not too technical, and should be measurable; and
- The training needs to be updated as new threats emerge and as the business culture and operations change.

UNIVERSITY OF ESWATINI

Role of academia in cyber security

- Universities should pursue initiatives to
- Train students and workers
- Support industry
- Safeguard our country's critical infrastructure
- Research
- Increase the country's cybersecurity capacity.
- Establish partnerships with public and private sector, and international partners to enable Eswatini individuals and organisations to take part in national and international cybersecurity capacity building and R&D activities

UNIVERSITY OF ESWATINI

Cybersecurity research themes

- Scalable Trustworthy Systems
- Resilient Systems
- Effective Situation Awareness and Attack Attribution
- Combatting Insider Threats
- Threats Detection, Analysis and Defence
- Efficient and Effective Digital Forensics
- Cyberspace governance and policy research

UNIVERSITY OF ESWATINI

National Cybersecurity R&D Laboratory

- Provide users with a wide range of ready-to-use tools for cybersecurity testing in repeatable and predictable experimentation environments.
- Also provide useful datasets that researchers can utilise to conduct and validate their ideas and cybersecurity solutions.
- Hosted at the UNESWA School of Computing
- Facility serves as a synergistic platform for cybersecurity researchers, both locally and internationally, to collaborate on research projects and share data, resources and knowledge.
- The facilities will also be used for education purposes, such as providing hands-on training for students and industry experts on system vulnerabilities.

UNIVERSITY OF ESWATINI

National Cybersecurity R&D Laboratory (Cont…)

- Offer integrated experimentations and services to support government agencies, academia and industry in their enterprise IT and operations technology cybersecurity research, technology evaluations and training.

UNIVERSITY OF ESWATINI

Cyber Security and Forensics (CSF) Research Group

To promote research, commercialization and training in cybersecurity.

- **Mission:** To promote research in cyber security and forensics so as to continually produce world class knowledge and foster the development of highly successful Cyber Security professionals in Eswatini.
- **Vision: To** be a leader in promoting cyber security and forensics research in Eswatini and beyond

UNIVERSITY OF ESWATINI

Cyber Security and Forensics (CSF) Research Group (Cont..)

As a result, the CSF Research Group will endeavour to:

- Conduct cyber security research and training to Build Eswatini's capacity and expertise in cyber security.
- Help in the development of educational curriculum and related materials for Eswatini.
- Help in developing Frameworks that support investigations and prosecution of cyber criminals.
- Conducting research to assess the levels of cyber security awareness across Eswatini.
- Promoting End-user education (Awareness) on cyber security good practices across Eswatini

UNIVERSITY OF ESWATINI

Cyber Security and Forensics (CSF) Research Group (Cont..)

As a way to promote collaboration and information sharing on cyber security both nationally and internationally, under the Eswatini National Cyber Security Strategy (NCS) 2022 (strategic Goal 5), the **CSF** Research Group will also focus on:

- Helping to Develop Frameworks that encourages information sharing and collaboration both nationally and internationally

UNIVERSITY OF ESWATINI

Courses

Proposed Training in Cyber Security and Forensics

1. Introduction to Computer Crime
2. Digital Forensics and Investigations
3. Cyber Security and Digital Forensics
4. BSc,MSc,PhD spacialising in Cyber Security
5. Certificates/Short courses

UNIVERSITY OF ESWATINI

Research Partnerships

- CSIR SA (Mr Erick Dube)
- UJ (Dr Barnabas Gatsheni)
- UP (Prof Venter)
- FH (Prof Khulumani Sibanda)

UNIVERSITY OF ESWATINI

Conclusions

- Global Cybersecurity Index (GCI)
- Cyber attacks vs National security
- Importance of cyber security awareness
- Topics to be covered in cyber defense training
- Benefits of cyber security awareness training
- Attributes of an effective cyber security awareness programme
- Role of academia in cyber security
- Cybersecurity research themes
- National Cybersecurity R&D Laboratory
- Cyber Security and Forensics (CSF) Research Group
- Research Partnerships

UNIVERSITY OF ESWATINI

References

- https:// www .itu .int/ en/ ITU -D/ Statistics/ Documents/ publications/ misr2018/ MISR -2018 -Vol -1 -E .pdf
- Cyber Security and Forensics (CSF) Research Group (For a Safer and Secure Eswatini Cyberspace) UNESWA document
- https://www.nrf.gov.sg/programmes/national-cybersecurity-r-d-programme
- https://www.nrf.gov.sg/programmes/strategic-research-programmes
- https://ncl.sg/

References

- https://fraudwatchinternational.com/security-awareness/what-is-cyber-security-awareness-training/
- https://www.itweb.co.za/content/XGxwQDM1dyL7lPVo
- http://www.verizonenterprise.com/
- https://www.pandasecurity.com
- https://www.darkreading.com

UNIVERSITY OF ESWATINI

References

- https://www.itjungle.com/
- https://www.universityaffairs.ca/news/news-article/academia-is-playing-a-growing-role-in-cybersecurity/
- https://www.herjavecgroup.com/the-2019-official-annual-cybercrime-report/

UNIVERSITY OF ESWATINI

THE END