A Framework for the Implementation of a National CIIP Structure for Developing Nations

Ian Ellefsen & Sebastiaan von Solms
{iellefsen,basievs}@uj.ac.za
Academy of Computer Science and Software Engineering
University of Johannesburg, South Africa
Outline

• Introduction
  • ITU-UJ Cyber Security Centre of Excellence
  • CIIP and Developing Regions
  • Community-based CIIP
  • Top-down, Bottom-up, and Holistic Structures

• Framework
  • Stages of Development: Initial
  • Stages of Development: Intermediate
  • Stages of Development: Mature
  • Continuous Development
  • Cyber Security Awareness
  • Milestones

• Future and On-going Work

• Conclusion
Introduction

• The development of CIP and CIIP Structures in developing regions should be a priority.
• CIIP Structures are tightly woven into the environment that they are deployed.

• Developing regions are in a unique position to create all-encompassing CIIP Structures.
  • Addressing all levels of society.
  • No predefined requirements for CIIP.
  • There is no one solution that “fits all”.

• We aim to present a framework for the creation of a holistic CIIP Structure:
  • Generic in nature.
  • Able to be used to define a plan of action.
  • Able to define a set of deliverables for implementation.
ITU-UJ Cyber Security Centre of Excellence

• A joint-venture between the University of Johannesburg and the ITU.
• First such Centre in Africa.
• The Centre will serve South Africa, Southern Africa, and eventually Africa.
• Operational from 1 January 2012.
• The material and expertise of the ITU will be available to the Centre and by extension, to South Africa and Africa.
ITU-UJ Cyber Security Centre of Excellence

- Services planned by the Centre:
  - Provide Cyber Security Awareness products.
  - Offer Cyber Security Awareness courses.
  - Provide Capacity Development and Skills Development courses.
  - Provide help and support regarding Legislative and Policy aspects in Cyber Security.
  - Provide support on aspects related to National Computer Security Incident Response Teams (CSIRTs).
  - Do research in Cyber Security and Critical Information Infrastructure Protection (CIIP).
  - Do testing and provide advice on Cyber Security matters.
  - Be a central contact point in Africa where all aspects related to CIIP and Cyber Security are coordinated, where expertise and skills in these areas is available.
• The Internet and related facilities can be seen as a critical information infrastructure.
  • National Backbones (Tier-1 Providers)
  • Large Corporate Networks (Banks, Telecommunications)
  • SCADA Systems

• Relates to the physical infrastructure used to provide interconnectivity.

• Systems of critical importance utilise these networks:
  • Electricity Distribution and Control
  • Water Distribution and Control
  • Financial Systems
  • Telecommunications

• Internet users are not isolated - no matter how effective your firewall you are at risk.
Introduction – The Situation

Image released into the Public Domain by original author.
Introduction – Community-based CIIP and Developing Countries

• The developing world presents a number of unique challenges:
  • Technological growth
  • Limited understanding of cyber threats
  • Increasing reliance on Information Infrastructures
  • Lack of effective policy
  • Lack of effective legislation

• South Africa does not have a coordinated Cyber Security Policy.
  • February 2009 - Department of Communications - Draft Cybersecurity Policy.

• Most other African countries do not have a coordinated Cyber Security Policy.

• Community-based structures can be implemented in areas where there are no preexisting cyber security structures:
  • Operate independently
  • Operate through community interaction
  • Can be integrated into a national cyber security structure
  • They are cheaper to implement over a CSIRT-like structure
“Citizens and Small and Medium Enterprises (SMEs) constitute the largest group of Internet users in the EU. IT systems owned and operated by these users are popular targets for hackers...”

- EISAS – European Information Sharing and Alert System for citizens and SMEs

**Africa: The Future Home of the World’s Largest Botnet?**

“African IT experts estimate an 80% infection rate on all PCs continent-wide, including government computers ... with the arrival of broadband services... there will be a massive, target-rich environment of almost 100 million computers available for botnet herders.

One botnet of one million hosts could conservatively generate enough traffic to take most Fortune 500 companies collectively offline. A botnet of 10 million hosts (like Conficker) could paralyse the network infrastructure of a major Western nation.

As of today, there is no unified front to combat botnets of this size.”

Introduction – Top-down vs Bottom-up Structures

• Development of a Holistic CIIP Structure.

• Top-down Structure:
  • Coordinated protection for larger entities.
  • CSIRT (or equivalent).

• Bottom-up Structure:
  • Community-based protection for smaller stakeholders.
  • C-SAW Structure.

• Holistic development:
  • Creating an “all-encompassing” CIIP structure.
Framework Development

- The developmental requirements for any national CIIP structure is tied to the environment.
- A framework should be generic such that it can be customised for the environment.

- Developmental framework is divided into three periods:
  - Initial Stage
  - Intermediate Stage
  - Mature Stage

- Each developmental stage consists of a number of activities and milestones, with the aim of establishing an effective CIIP Structure.
Framework – Initial Stage

- Understanding the environment.
- A number of environmental assessments.
- Environmental Stakeholders (International and National)
- Technological
- Legislative

- Each assessment has various activities.

- Other activities that are present in this stage:
  - Small-scale CSIRT deployment.
  - Establishment of Community-based structures.
Framework – Intermediate Stage

- Test the waters.
- Continuing development of a small-scale CSIRT, and Community-based structures.
- Eventual transition into larger, fully functioning, CSIRT Structure.
- Once the CSIRT Structure is partly operational, Community-based structure then can be integrated.
Framework – Intermediate Stage

- Once the small-scale CSIRT deployment has concluded, a permanent CSIRT structure can be deployed.
- Community-based teams can then be integrated into the CSIRT structure and integrated into the national CIIP structure.
Framework – Mature Stage

• “All systems go”.

• Reached when the CIIP structures is self-sustaining:
  • Able to respond to cyber incidents.
  • Built effective relationships between peers.
  • Information and knowledge sharing between components.

• However, the development cycle does not end:
  • Continuous Assessment and Evaluation.
  • Continuous Cyber Security Awareness Programmes.
Framework – Continuous Development & Assessment

• Assessment and Evaluation must take place to allow a CIIP Structure to address future threats.

• Assessment of the following components:
  • Environment
  • International & Local Partners
  • Technological
  • Legislation
Framework – Continuous Cyber Security Awareness

- Providing Continuous Cyber Security Awareness programmes reinforces the national cyber security structure.

- Millions of users gaining access to Internet-aware devices.
- Understanding the implications for national critical systems.

- Awareness is not limited to developing regions, however the perceived level of awareness could be considered to be lower.

- Aspects of the Initial Assessments, and a component of the development of Community-based structures can contribute to national cyber security awareness programmes.
Framework – Milestones

- Milestones that mark significant points in the developmental period:

- **Milestone 1** – Marks the point where the initial assessments have been conducted, simplistic community-based structures have been deployed, and steps towards a national CSIRT have been taken.

- **Milestone 2** – Marks the beginning of the development of a national CSIRT structure, community-based structures continue to develop.

- **Milestone 3** – Marks the end of the initial construction of a CSIRT structure, where relevant constituencies have been identified, and basic services are being deployed.

- **Milestone 4** – Marks the culmination of the development cycle, however not the end.
Future and On-going Work

• Investigations into the deployment of Community-based CIIP Structures (C-SAW Structures).

• Development of toolkits to aid in the operation of C-SAW Structures:
  • On-going

• Conduct further research into CIIP in developing regions with respect to the deployment of a CIIP structure.
Conclusions

• Improved technological factors in developing regions could impact on internal and international systems.
• Many developing countries do not have an effective cyber security strategy in place.
• There are millions of inexperienced users gaining access to “Internet-enabled” devices.
• The development of cyber security structure is unique to the environment to which it is to be deployed.
• All countries must take steps to address cyber security across all levels of society and create a holistic cyber security strategy.
• A framework of this nature allows a clear set of deliverables to be defined that is independent of a particular deployment environment.

Questions?