INTERCONNECT COMMUNICATIONS
Consulting in Communications Regulation and Strategy

ccTLDs and Cyber-Security

A DRAFT Guide for Policy-Makers

African Internet Summit / Afrinic 20

Djibouti, June 2014

Maria Farrell

Project Background I

Global
Cyber Security
Capacity Centre

UNIVERSITY OF
OXFORD

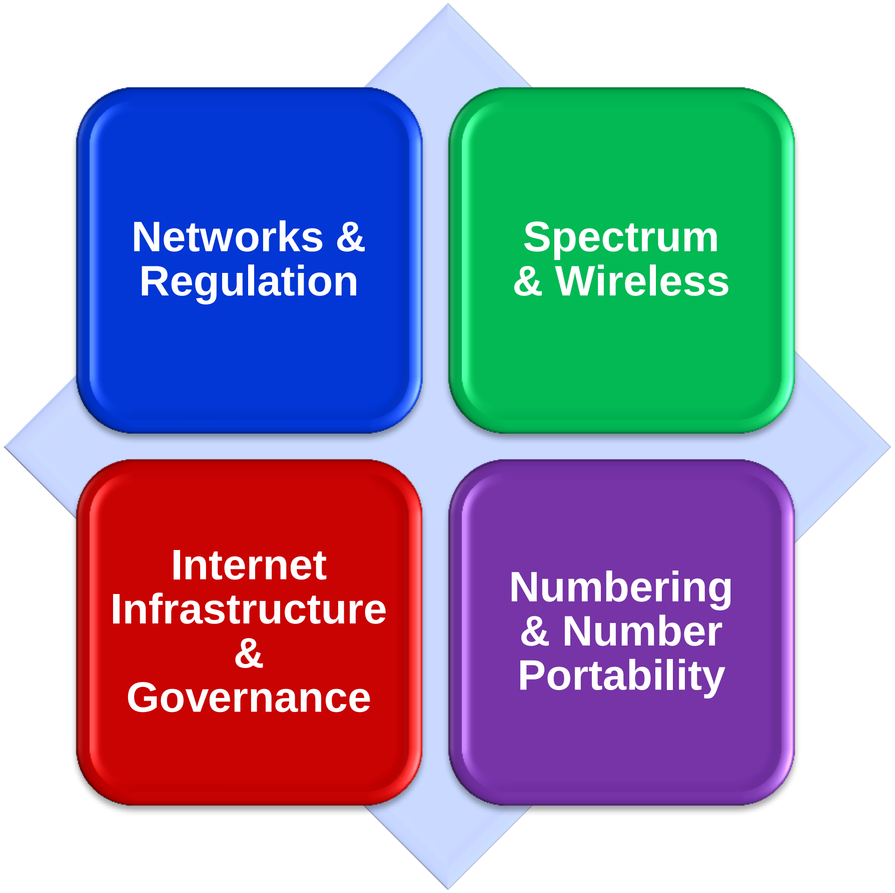
Project Background II

Global Cyber Security Capacity Building Centre aim:

“Our aim is to understand how to deliver effective cyber security both within the UK and internationally. We make this knowledge available to governments, communities and organisations to underpin the increase of their capacity in ways appropriate to ensuring a cyber space which can continue to grow and innovate in support of well-being, human rights and prosperity for all.”

InterConnect Communications

Established in 1984



Networks & Regulation

Spectrum & Wireless

Internet Infrastructure & Governance

Numbering & Number Portability

InterConnect Communications

Trusted supplier in developing area of Internet Infrastructure and Governance:

- Providing technical expertise and policy experience on technological, political, economic and social impacts of the Internet:
  - ➢ Internet Governance and Policy
  - ➢ Emerging Internet Architecture (DNS, IPv6, CGN)
  - ➢ Internationalisation of the Internet (IDN)
  - ➢ Cyber Security (DNSSEC, Resource PKI)
- Key partner to ICANN in expansion of gTLD domain space and Accountability and Transparency reviews

UPCOMING, July 2014:

- **Master Class in Internet Governance and Policy:** an interactive course equipping delegates with the history, technical, legal and geographic underpinnings of the Internet, its key international policy issues and venues, and the most up to date information needed to be an effective advocate for their organisation's strategic interests.

‘ccTLDs and Cyber-Security, a Guide for Policy-Makers’ is:

- A work in progress
- Aimed at policy-makers with little background in cyber-security
- Needs input and expertise from the community
- Will be freely available for all

Project Goal

- To make policy-makers more informed about the challenges ccTLD operators face so they can understand and assist in improving national and global cyber-security

- Goal is NOT to encourage re-delegations or governance changes – this guide respects the many different governance and operational models ccTLDs employ

ccTLDs and Cyber-Security – Specific Challenges

- Most ccTLDs are ‘SMEs’ with the risk profile of a major brand and critical national asset, but;
- Fewer resources – financial, even technical - than organisations with similar risks
- On the plus side: ccTLDs enjoy a global network of peers to tap into

Structure

1. ccTLDs as SMEs – general information security
2. Specific cyber-security challenges for ccTLDs
3. ccTLDs’ role in improving cyber-security around them

ccTLDs as Small to Medium Enterprises (SMEs):

- Big disparity between cc’s
  - The ten biggest cc’s = >65% of all 120 million ccTLD registrations
  - Biggest ones: EPP, automation, resilience
  - The smallest ones can be run using a paper notebook or a spreadsheet and domestic PC

1.1 General Cyber Security Issues

- What are the most common vulnerabilities?
- What are their potential impacts on the organisation?
- How to prepare and respond?

1.2 Most Common Vulnerabilities

- Unauthorised access to and/or dissemination of information
- Theft or unauthorised access to computers or mobile devices
- Unauthorised changes to systems
- Exploitation of unpatched systems or applications
- Damage to or defacement of the organisation’s resources, such as websites
- Attacks on information and assets held by third parties, e.g. cloud services, vendors or banks

1.3 Potential Impacts

- Financial loss
- Disruption and costs of repair
- Damage to reputation
- Prosecution under relevant legislation, e.g. for failure to protect data including personal data

1.4 Preparation and Response

- Inventory physical IT and information assets, systems and applications, and who has access
- Do a risk assessment
- Create a security governance, policy and practice plan, including legal & policy obligations
- Implement plan: training, resourcing & controls
- Test the incident/crisis response plan, involving third parties and practicing recovery procedures

1.5 Detailed topics

- Training
- Access control: physical and systems
- Remote devices
- Software protection (patches, malware)
- Network security
- Incident response

2 Specific cyber-security issues for ccTLDs

ccTLD cyber security fundamental aims are to ensure:

- Availability of name resolution: domain names resolve
- Integrity of data: the domain names link to the correct websites

2.1 ccTLD Security Challenges

Increased exposure to risk, compared to other similarly sized organisations:

- Hacktivism
- Extortion
- New domain for spammers and phishers
- Source of personal and business data

Resource limitations:

- Technical, time, financial, peer-networking

Consequences for the ccTLD:

- Financial, political

2.2 ccTLD Cyber Security Challenges

Consequences for the country:

- Loss of access to e-government services and information leading to significant political and economic impacts
- Loss of access to business and other websites using the ccTLD leading to significant economic impacts
- Loss of national credibility as a centre of ICT competence or excellence, leading to a marked decline in national competitive advantage

2.3 Three Key Areas for ccTLDs

A ccTLD’s cyber security roles are best understood in three key areas:

- Governance and Policy
- Operational and Network Security
- External Impact and Engagement

2.4 Governance and Policy

- The key anchor to ccTLD security is a stable, transparent and responsive set of governance arrangements

2.5 Governance – Essential

An effective governance arrangement is publicly documented and should include an articulation of its guiding principles, for example:

- Operation to promote the public good
- Cooperation with relevant authorities
- Respect for national and international law, fostering Internet security and stability

2.6 Governance - Ideal

- Identification of sponsoring organisation and operator
- Clear delineation of respective responsibilities
- Public reporting of accountability information, e.g. financial, membership of oversight bodies, process for participation
- Periodic technical and operational reviews
- Clear articulation of trigger and process for re-delegation
- Reference to relevant national legislation and bilateral or international agreements(e.g. bilateral trade treaties with measures for dispute resolution for intellectual property in contested names)

2.7 Policies

- E.G. Accountability and participation mechanisms
- Registration and anti-abuse policies (name transfers, deletions, anti-cybersquatting and phishing)
- Registry-registrar (if that model is used)

Should be:

- Publicly available

2.8 Network and Operational Security

- System Resiliency, Diversity and Redundancy
- Monitoring
- Pros and Cons of outsourcing the back-end
- Pros and Cons of UDRP
- Topics in development: Whois, DNSSEC, Crisis Response

2.9 System Resiliency, Diversity and Redundancy

- Service availability
- Resiliency:
  - Geographical diversity (mirroring partnerships, back-ups stored with third parties, crisis recovery, including natural or other physical disasters)
  - Software diversity – Operating systems, BIND,
- Redundancy
  - Capacity
  - Multiple DNS secondary servers

2.10 Monitoring

- Implement monitoring software and practices
- Monitor the logs even / especially if you use a back-end provider

2.11 Pros and Cons of Outsourced Back-End

Pros	Cons
Access to world class resources and technical expertise	Loss of control over information and other assets, may be an issue for information or data protection laws and vulnerability of information assets to access requests by government in hosting country
Lower overhead and staff costs	Possible cost unpredictability, e.g. certain cyber-attacks can greatly increase the access requests
Potential greater availability, reliability, scope and resilience for registration and traffic growth	Loss of national ccTLD operator as local and regional developer of ICT talent

3 External Impact and Engagement

ccTLDs’ role in improving cyber-security around them:

- Cooperation with law enforcement, subject to national laws
- Participation in national Internet ecosystem
- Participation in regional / global Internet ecosystem

Your input is needed!

- How relevant and useful is the draft?
- What topics should / shouldn’t be covered?
- How are we handling sensitive issues?
- Do you have any case studies that could be shared to help others?
- What metrics can be used to help understand ccTLD cyber-security performance in a constructive way?

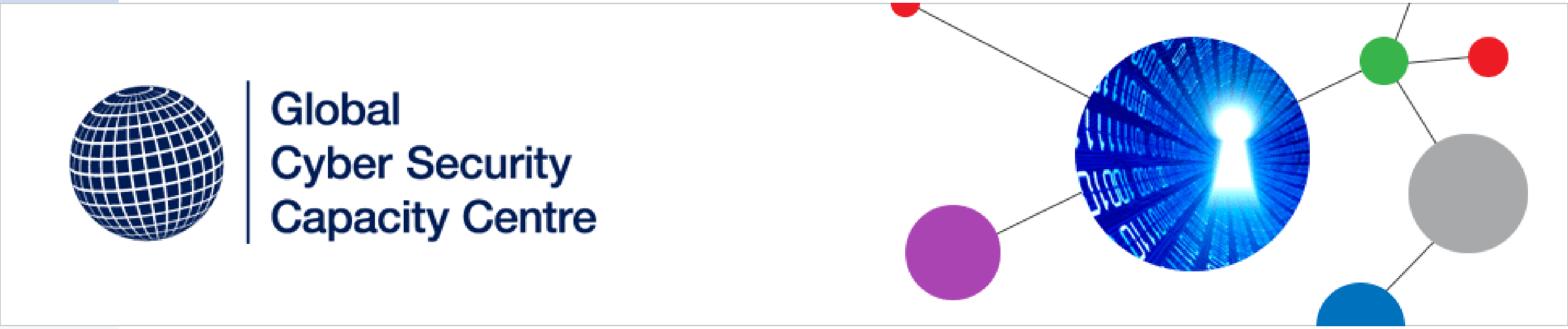
QUESTIONS?

To receive a draft copy:

mariafarrell@

icc-uk.com

Future updates:



www.oxfordmartin.ox.ac.uk/cybersecurity