

Incident Response Working Group Update

ICANN Seoul
ccNSO – October 28, 2009

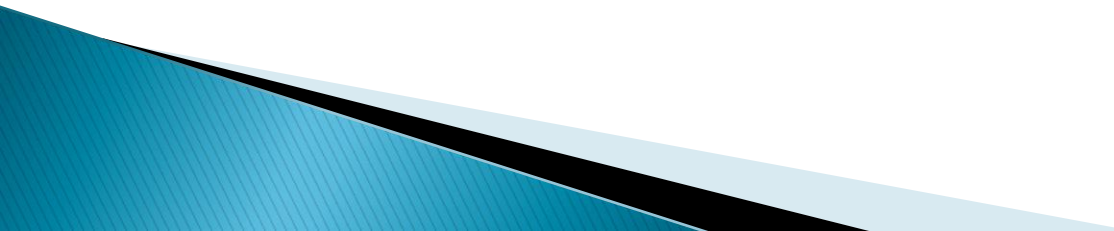
Norm Ritchie, CIRA



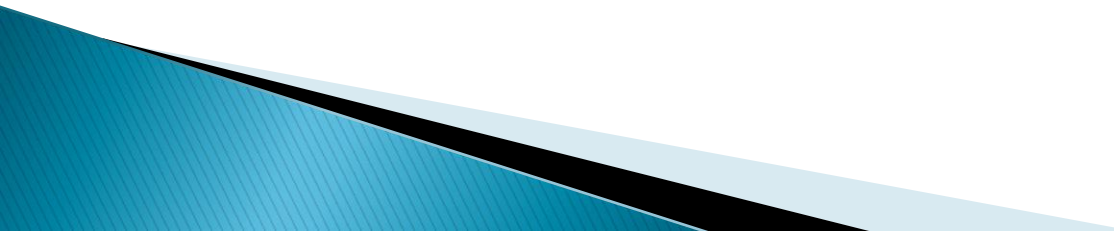
Background

- ▶ Heavy involvement of ccTLD Registries in pre-empting Conficker C in Spring'09
- ▶ Highlights of post-mortem at ICANN Sydney
 - It was not easy – we were not prepared
 - No established conduit for outreach
 - No mechanisms for blocking
 - Some domains already registered
 - No available resources
 - Lack of policies
 - Financial impact to some

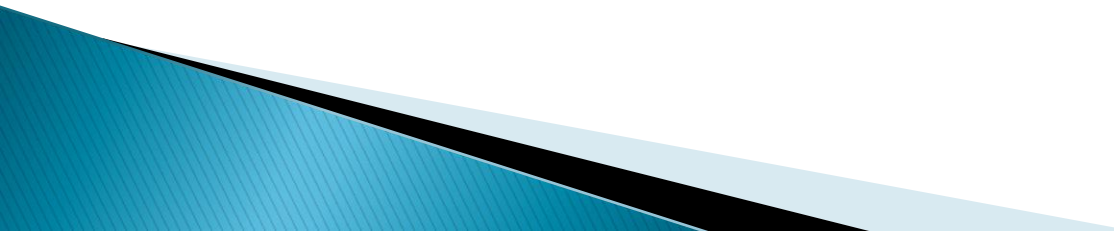
Moving Forward

- ▶ Conficker was just a wake-up call
 - This was not a singular event
 - ▶ The ccNSO Incident Response WG was formed
 - Adhoc WG
 - Develop repository, processes and procedures for ccTLD Emergency Response contacts
- 

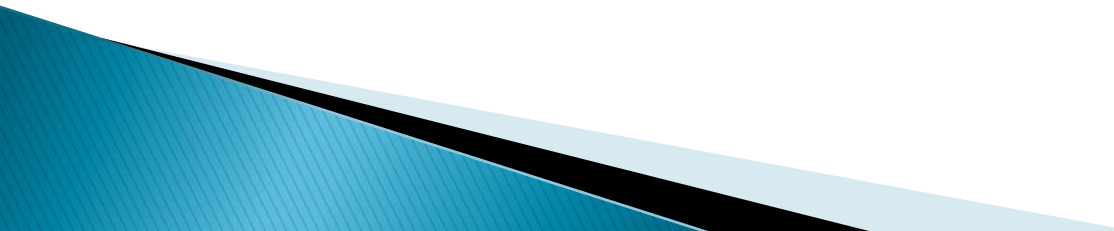
Guiding Principles of WG

- ▶ Preserve the security and stability of the DNS
 - ▶ Non-binding relationship of the ccTLD registries to any one particular entity except possibly with their own governments
 - ▶ Diversity of language, timezone, resources, expertise
 - ▶ Respect particular policies and practices by which ccTLDs may be guided
- 

Work Plan Objectives 1 / 2

- ▶ Provide a **reporting point** for receipt and remediation information of incident/threats reports relating to DNS
 - ▶ Provide mechanisms for the **coordination** of counter measures
 - ▶ Provide an effective communication channel for the ccTLDs to **inform and coordinate** with other ccTLDs, gTLDs, and the DNS root manager on security incidents
- 

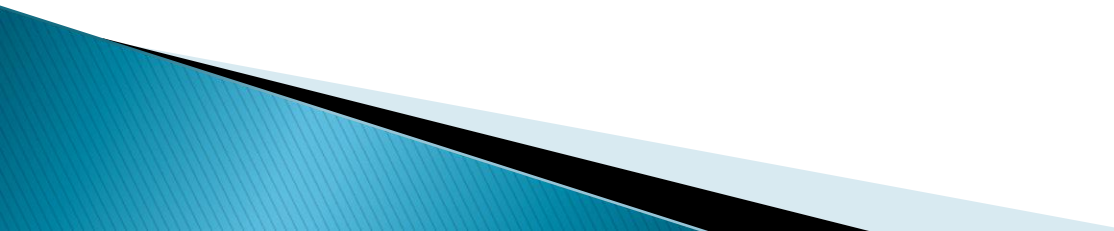
Work Plan Objectives 2/2

- ▶ Provide **technical support** in response to an incident
 - ▶ Ensure the security of the **DNS registration infrastructure**
 - ▶ Provide a **Common Incident Response Repository**
- 

Status

- ▶ High level of interest within and external to ccNSO
 - WG expanded from 4 to 30+
 - Vice-chair appointed: Hugo Salgado, nic.cl
- ▶ Draft plan created
 - Elements and mechanisms of the repository defined
 - Process defined for event handling
 - ICANN staff to create and operate repository

Tasks undone

- ▶ Finalize plan
 - ▶ Design & create repository database
 - Web interface for updating contact data
 - ▶ Populate repository
 - ▶ Test communication channels
 - ▶ Define process and mechanisms for incidents and threats originating from within ccTLDs
 - ▶ Identify threats (and remedies) to registration systems
- 

Thank you

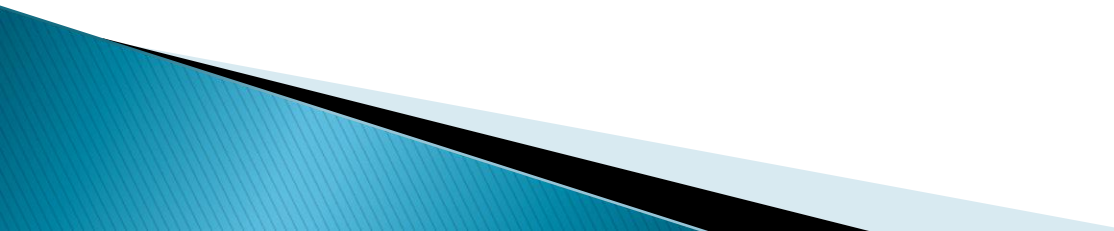
Questions?

norm.ritchie@cira.ca

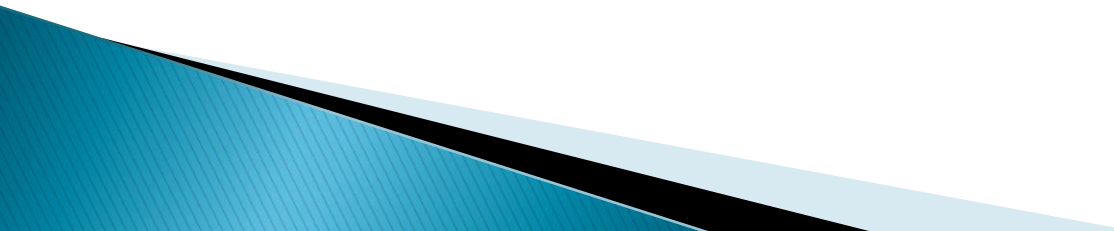


Additional Slides

Role of IR Contact

- ▶ Provide an effective emergency incident response to their ccTLD registry system for incidents that may impact the DNS or utilize the DNS to perform a malicious intent
 - May include multiple contacts
 - Includes regional organization contacts
 - 24/7 availability
- 

Contact Data

1. ccTLD name
 2. Name of person representing the team
 3. Host organization of ccTLD response contact point
 4. Country the contact is located
 5. Internet domain
 6. Regular telephone number (time-zone relative to UTC)
 7. Emergency telephone number (time-zone relative to UTC)
 8. Email address
 9. Messenger services (service, id)
 10. Facsimile number (country code, fax number)
 11. Other telecommunication facilities
 12. Language
 13. Availability of the defined of contact
- 

IR Process Flow – External Events

