

COURSE OUTLINE

Anatomy of a Disaster

Introduces technical and non-technical impacts of disasters and cyber attacks, and the need for effective risk assessment and planning

Philosophy of Preparing for a Disaster or Attack

Presents an approach to preparing for a disaster or attack – based on sound risk assessment, business continuity planning, and threat awareness

Attack and Disaster Response Planning for the ccTLD

The process for assessing risk, developing mitigation strategy & plan, validating and maintaining the plan – presented in the context of ccTLD operations

- Determining Critical Assets and Operations
- Identifying Areas of Concern
- Threats and Threat Scenarios
- Risk Analysis
- Developing Mitigation and Business Continuity Plans

ccTLD Response Options for Today's Threats

Best practices in securing and responding to current and emerging threats

Evaluating & Maintaining Your Plans

Evaluation techniques: structured plan walk-through, table top exercises, functional / operational exercises

ACCOMMODATIONS

18 - 19 MAY 2008

RITZ CARLTON HOTEL -
KUALA LUMPUR

Website for Hotel Reservations:

<https://www.ritzcarlton.com/en/Properties/KualaLumpur/Reservations/Default.htm?gc=tldtlda>

Reservations Contact:

aileen_tee@ritzcarlton.com.my

Additional Accommodations:

Dorsett Regency Hotel Kuala Lumpur
(Across the Street from the Ritz Carlton)

Website:

<http://www.dorsettregency.com.my/>

Reservations Contact:

sm1@dorsettregency.com.my



PO Box 11-881, Wellington, New Zealand
tel: +64 4 495 2113 fax: +64 4 495 2115

<http://www.aptd.org>

Event Sponsored by:



4676 Admiralty Way, Ste. 330
Marina del Rey, CA 90292 USA
tel: +1 310 823 9358 fax: +1 310 823 8649

<http://icann.org>



APTLD

APTLD TRAINING WORKSHOP Attack & Disaster Response Planning

APTLD is delighted to announce a series of initiatives to better equip ccTLDs to handle both attacks and disasters.

Working with both ICANN and APNIC, APTLD is developing a series of training workshops in addition to APTLD's normal meeting schedule.

The Attack & Disaster Response Planning (ADRP) Workshop outlined in this brochure is being developed in conjunction with ICANN.

A Network Security Workshop that is being run by APNIC is integral to the support for both management and technical aspects of a ccTLD.

18-19 May 2008

Ritz Carlton Hotel - Kuala Lumpur
In conjunction with APTLD's Kuala Lumpur
Meeting Program (18-24 May 2008)

SOMETIMES THINGS GO

TERRIBLY WRONG - natural disasters, cyber attacks, human errors – all can have devastating effects on the daily operations of a ccTLD.

While many of these events can't be predicted or prevented, examining disasters after the dust settles highlights gaps in capability, knowledge, awareness, or preparedness which contribute to cascading failures.

Being able to respond effectively in today's competitive business environment involves planning and accurately assessing risks. Planning helps enable critical operations better survive and recover from a disaster or attack.

THIS WORKSHOP PRESENTS USEFUL METHODS, BEST PRACTICES, AND LESSONS LEARNED IN ASSESSING OPERATIONAL RISKS AND PREPARING A BASIC ATTACK AND DISASTER RESPONSES PLAN FOR ccTLD OPERATIONS. It

includes an introduction to current threats facing the Internet and TLD operations & infrastructures.

The knowledge and contacts gained from attending this course will assist ccTLD managers to understand today's Internet threats, what they can do about them, and where they can turn for help.

WHO SHOULD PARTICIPATE?

- ccTLD Managers
- ccTLD Operators

PARTICIPANTS WILL GAIN:

- An approach to preparing for a disaster or attack based on sound risk assessment, business continuity planning, and threat awareness
- Concepts of critical operations, assets, services, functions, and relationships in the context of a ccTLD -- things you need to protect for continuity of operations purposes
- An understanding of threats – natural, physical, input to services (power, communications), political, intentional vs. accidental (human error, criminal, malicious, personal), internal vs. external (authorised user/ authorised access vs. authorised user/ unauthorised access vs. unauthorised user)
- General considerations and process for planning, conducting, and assessing an exercise
- Contacts and resources for coordination and cooperation