



**Trusted Information
Sharing Network**
for Critical Infrastructure Protection

CIP NEWSLETTER

For owners and operators of critical infrastructure

Vol. 6 No. 1 June 2009

Contents

GovCERT.au leads Australian contingent to Idaho National Laboratory	1
Cyber Storm III - all systems are go!	2
Cyber Storm - an industry player's perspective	3
Australian Hotels Association holds anti-terrorism forum	4
Business-Government Advisory Group meets in Canberra	4
Critical Infrastructure Protection Branch has moved	4

ISSN: 1833-5861 (Print)
1833-5888 (Online)

Published on behalf of the Trusted Information Sharing Network for Critical Infrastructure Protection by the Australian Government Attorney-General's Department Critical Infrastructure Protection Branch

Contact:

p. +61 2 6141 2945
f. +61 2 6141 3046
e. cip@ag.gov.au
www.tisn.gov.au

GovCERT.au leads Australian contingent to Idaho National Laboratory

On 28 March 2009 two members of the Australian Government Computer Emergency Readiness Team (GovCERT.au) left Australia to lead a group of critical infrastructure Supervisory Control and Data Acquisition (SCADA) / Control Systems engineers to participate in a US Government sponsored SCADA security training workshop. The workshop took place at the Idaho National Laboratory (INL) in Idaho Falls, Idaho, USA.

This is the third year that GovCERT.au has attended the training workshop along with participants from Britain, Canada, New Zealand, and the US.

This year, for the first time, international participation was extended to the 15 member nations of the International Watch and Warning Network (IWWN), of which Australia is a member.


As part of a Government initiative to increase the cyber and SCADA security skills of Australian critical infrastructure organisations, the Attorney-General's Department subsidised four participants from Australian industry to attend.

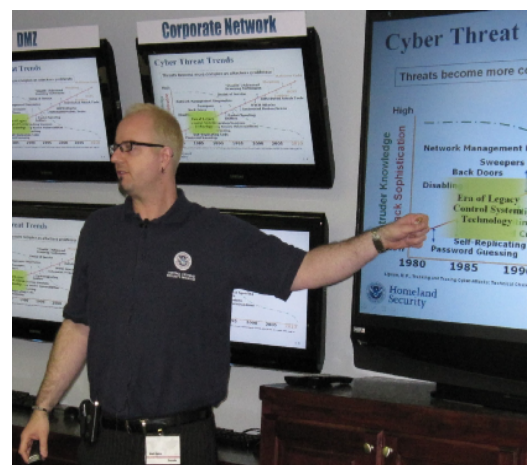
Participants received instruction in how to better secure Control and SCADA systems to withstand ever-increasing cyber threats from both inside and outside their networks. They were also involved in a red / blue team scenario designed to show how best to defend a chemical plant against

cyber attacks in a simulated environment.

Guest lecturers included Mark Fabro, V.P. of Professional Services at Lofty Perch Inc., an organisation specialising in cyber security and critical infrastructure. Mark also lectures at the Idaho National Laboratory.

INL is operated for the US Department of Homeland Security, and is recognised as one of the best training facilities in the world for Control and SCADA systems. It is at the forefront of a variety of areas including Nuclear Fusion and Power Generation, Robotics, Genetics, Biology, Chemistry, Metallurgy, Computational Science and Hydropower.

To cater for increasing demand from Australian critical infrastructure owners and operators for cyber security training, AGD has negotiated a separate 'Australia only' course, to be held in October this year. An Expression of Interest to attend this course will be coordinated by AGD in June/July with participation by the Department of Broadband, Communications and the Digital Economy. 



Mark Fabro takes delegates through a cyber security training session.

Cyber Storm III - all systems are go!

Preparations are ramping up for the international cyber exercise and there is still time for organisations to opt in.

Australia will again take part in Cyber Storm, the major international cyber exercise hosted by the US Department of Homeland Security.

Cyber Storm III is planned for late September/October 2010 and preparations are already well under way.

Cyber Storm II, held in March 2008, brought together the United States, Australia, New Zealand, the United Kingdom and Canada to test their cyber security. Japan and nine European nations have also been invited to participate in Cyber Storm III.

Cyber Storm is a unique opportunity for stakeholders across the spectrum of e-security and critical infrastructure protection in Australia to participate in an exercise aimed at testing the communications and decision-making which underpins any technical response. It is structured and executed as a large scale national exercise within an international framework.

Cyber Storm II participants included Australian Government agencies, the Western Australia and South Australia State Governments, industry groups and private

companies drawn from the IT industry, and four critical infrastructure sectors - Water, Banking and Finance, Energy and Communications.

In all, 56 Australian organisations participated in Cyber Storm II and the report on the exercise can be found on the Attorney-General's Department website. The view of the majority of participants was that the Cyber Storm framework is a cost effective way of conducting a business continuity or disaster recovery exercise.


The exercise is run with participants operating as much as possible from their normal work spaces using normal communications. In the lead-up to the exercise, organisations, or 'players' as they are known, fine tune scenarios which will best test their particular organisation. They can also devise the scenarios to test interdependencies with other organisations, which many participants of Cyber Storm II noted was a crucial element of the exercise.

The exercise is coordinated from a central control cell which directs the 'play'. Each player has a

representative present in the control cell. Scenarios may then be triggered, for example, by way of an email reporting a problem or a phone call asking a question. The problems or incidents in the exercise are all notional – no live systems are attacked.

Benefits of participation include:

- a new set of relationships and engagements with customers
- the building of stronger resilience in business and supply chains
- the building of a stronger relationship and partnership with government and other industry that can be used during a crisis, and
- a cost effective way of testing incident, crisis management and business continuity plans.

Any organisation interested in learning more about the exercise can download a detailed fact sheet from www.tisn.gov.au 

Cyber Storm - an industry player's perspective

Dave Walcott, Information Security Manager for Country Energy, tells us why his organisation is looking forward to even greater involvement next time around.

“Country Energy participated in exercise Cyber Storm II as a designer, player and observer.

We deliberately took a conservative approach using the KISS principle as we did not want to fully commit the business without knowing what the ramifications of participation would be.

Country Energy had eight people participate part time in the exercise play itself. There was one person involved in the planning and design of the exercise and

this involved attending approximately 7 meetings. We also had one member participate at EXCONTROL near Melbourne for the five days of the exercise.

We could not have tested dependencies with Government, partners and supply chains to the same level as this exercise provided. It allowed us to simulate the pressure of a real incident response in a controlled manner.


There were many key points learnt from our participation in the exercise.

We learnt that it is too late to exercise your incident response plans during an incident or crisis.

You need to know who and what escalation paths are available and you need to have formal relationships and identification in place with Government and partners for use during a crisis it is too late to meet during the incident itself.

We also learnt that our incident response was inward focused and did not fully cover the affects that others outside our business may have on us or we may have on them.

If we had our time over we would be much more aggressive in our approach, we would include much more of our business in the exercise.

We would also commit to participating in other scenarios to test impact with our partners and suppliers such as Telecommunications, Water, and Banking Finance.” 

If you would like to discuss any aspects of Cyber Storm III, please contact either:

Australian Exercise Coordinator

Quentin Pinner
E-Security Policy and Coordination Branch
Attorney-General's Department

+612 6141 2979

quentin.pinner@ag.gov.au

Australian Deputy Exercise Director

Annie Weir
E-Security Policy and Coordination Branch
Attorney-General's Department

+612 6141 2984

annie.weir@ag.gov.au

Australian Hotels Association holds anti-terrorism forum

The Australian Hotels Association (AHA) held its annual Hotel Security and Anti-Terrorism Forum in Melbourne on 27 February 2009.

The Forum was officially opened by Attorney-General, Robert McClelland, and featured presentations by officials from the Attorney-General's Department and ASIO.


More than 50 representatives from Australia's major hotels

attended the event which is highly regarded by the industry.

The Chief Executive Officer of the Australian Hotels Association, Mr Bill Healy said 'The aim of the Hotel Security and Anti-Terrorism Forum is about keeping members informed of the security environment so that safe hotels in Australia become even safer.'

The Forum ensures that hotels have the latest information to

further assist them in recognising threats and minimising security risks.

Michael Jerks, Assistant Secretary, Critical Infrastructure Protection in the Attorney-General's Department, presented on the Trusted Information Sharing Network for Critical Infrastructure Protection and other initiatives such as organisational resilience. 

Business-Government Advisory Group meets in Canberra

Business leaders from Qantas, Telstra, Westfield, Rio Tinto, Santos, Accor, the Australian Chamber of Commerce and Industry and the Business Council of Australia joined Attorney-General, Robert McClelland, the former Minister for Home Affairs, Bob Debus, and senior Australian Government officials for the sixth meeting of the Business-Government Advisory Group on National Security in Canberra on 27 March.

The group, chaired by the Attorney-General, met to discuss national security issues that affect business, with a focus on the national security reform agenda.

The meeting received an update on the current domestic security environment; a briefing on the threats posed by serious, organised crime and Government proposals for dealing with it; and a briefing on the outcomes of the E-Security Review and new

arrangements to exchange computer security information with business.

The meeting also received briefings from the AFP and ASIO and an update on disaster risks and the role for business in disaster resilience strategies. There was consensus that the strengthening of the business-government partnership is crucial in ensuring a safe and secure environment for the Australian community. 

The BGAG communiqué is available at www.attorneygeneral.gov.au

Critical Infrastructure Protection Branch has moved

The Critical Infrastructure Protection Branch of the Attorney-General's Department is now located at 3-5 National Circuit, Barton.

**Email addresses remain the same but phone numbers have changed.
If you need to contact a CIP officer by phone, please call the switchboard on
+ 61 2 6141 6666**