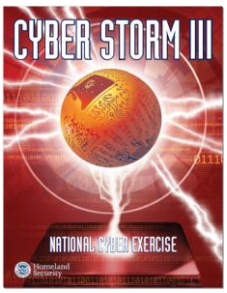

Cyber Storm III – Fact Sheet

What is Cyber Storm?

The National Cyber Security Division of the United States Department of Homeland Security sponsors a series of large scale cyber security exercises collectively called Cyber Storm. In March 2008, Australia conducted a national exercise in conjunction with the second of these exercises. Canada, New Zealand and the United Kingdom also participated.

These exercises centre on cyber security scenarios that will escalate to a level requiring a coordinated national response.

Exercises such as Cyber Storm are critical to maintaining and strengthening relationships between businesses, business sectors, government agencies and nations. They enhance processes and communications linkages, and ensure continued improvement in responses to significant cyber security events.

CERT Australia is responsible for planning and running Cyber Storm III.

Who is involved in Cyber Storm III?

Cyber Storm III involves the United States, Australia, New Zealand, Canada, and the United Kingdom. The US has also invited the members of the International Watch and Warning Network to participate. In Australia, many of the organisations involved in Cyber Storm II will again participate as it was widely acknowledged that the Cyber Storm framework is an extremely cost-effective way of testing responses to major cyber security events.

When is Cyber Storm III?

Cyber Storm III is scheduled to be held in the third quarter of 2010.

How will Cyber Storm III run?

The exercise will be run, as much as possible, with participants playing from their normal operating environments using everyday communications. It will be coordinated from a central control cell, taking events from a Master Scenario Event List and passing them to the players.

This might, for example, be in the form of an email reporting a problem or a phone call asking a question. The problems or incidents in the exercise are all simulated – no live systems are attacked.

Cyber Storm III will be conducted as a 'no-fault' exercise. Its purpose is not to obtain a stock-take of each participant's internal crisis management arrangements. Nor is the exercise a test of the resilience of participants' networks to cyber attack. The starting point for the exercise is that the adversary has sufficient time, money and motivation to penetrate any network.

What are the benefits to organisations who are participating?

- A cost-effective way of conducting a business continuity or disaster recovery exercise.
- An opportunity to test international arrangements within a trans-national organisation.
- An opportunity to exercise and test relationships with key vendors across sectors.
- An opportunity to network with people in their organisation and sector that they may need to engage with in a crisis situation.
- An opportunity to explore interdependency issues.
- An opportunity to test and explore regulatory issues with government regulators, without impact.
- The development of a new set of relationships and engagements.
- Building stronger resilience in their business and supply chains.
- Building a stronger relationship and partnership with government and other industry that they may need to engage with in a crisis situation.
- The identification of opportunities for improvement.