



JAKEMAN BUSINESS SOLUTIONS PTY LTD

ABN: 72 101 963 240

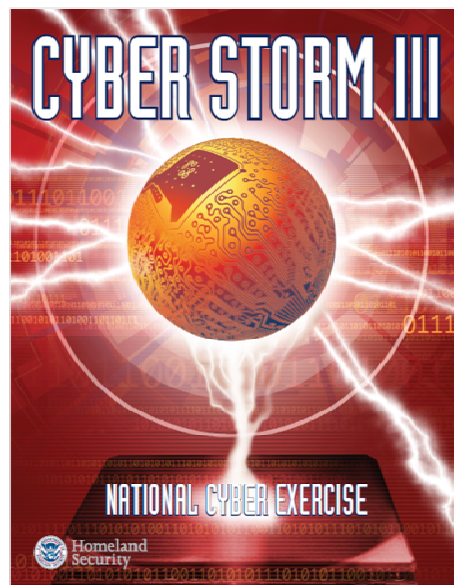
ACN: 101 963 240

RTO: 88134

Specialising in business
strategy, training, and
management consulting
services to
meet the specific needs
of our clients

Cyber Storm III Cyber Security Exercise 27-30 September 2010

Findings



1/10 Kennedy Street
Kingston ACT 2604

jakeman.com.au

T + 61 2 6162 1149 F +61 2 6162 1153



A MEMBER OF THE

citadel group
PROVEN. PREFERRED.



Contents

| | |
|-------------------------|---|
| Background | 3 |
| Conduct | 3 |
| Findings | 4 |



Background

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*.

Cyber Storm III was the third exercise of this type and involved the United States, Australia, New Zealand, Canada, and the United Kingdom. Japan and nine European nations were also invited to participate as members of the International Watch and Warning Network.

In Australia, approximately 50 participants were involved including Australian Government and state and territory agencies, and over 30 organisations from the banking and finance, energy, food, transport, water, IT and communications sectors.

Cyber Storm III was planned and developed over two years and culminated in the conduct of a four day exercise between 27-30 September 2010. It was conducted as a 'no-fault' exercise, with the strategic national-level objective being to test and evaluate Australia's new crisis management arrangements in order to most effectively address an international cyber security event of national significance. Complementary to this, *Cyber Storm III* participants' objectives included:

- Evaluating organisations' capability to prepare for, protect from, and respond to cyber attacks' potential effects;
- Evaluating strategic decision making and inter-agency coordination of incident response(s) in accordance with national level policy and procedures;
- Validating information sharing relationships and communications paths for collecting and disseminating cyber incident situational awareness, response and recovery information; and
- Evaluating the means and processes through which sensitive information is shared across boundaries and sectors without compromising proprietary or national security interests.

Whilst each *Cyber Storm* builds on lessons learned from previous exercises and real world incidents, enhancements in the nation's cyber security capabilities, an ever-evolving cyber threat landscape, and the increased emphasis and extent of public-private cooperation, made *Cyber Storm III* unique.

Conduct

The exercise was run, as much as possible, with participants playing from their normal operating environments using everyday communications. It was coordinated from a central control cell in Canberra, where events from a consolidated master list were passed on to the players for their responses. These events included, for example, emails reporting problems and phone calls asking questions. The problems or incidents in the exercise were all simulated – no live systems were involved.

Telstra, ASX, Woolworths, ANZ, and domain name registrar AuDA were among the private sector organisations involved. Agencies involved include the Defence Signals Directorate, CERT Australia within the Attorney-General's Department, Australian Federal Police and other agencies represented in the Cyber Security Operations Centre (CSOC).

The Attorney-General, Robert McClelland, launched the exercise and noted that "The Government's National Security Statement identified cyber security as a top national security priority". He also described cyber security as a "rapidly evolving and increasingly important" threat and one in which "A serious assault against the networks that control key systems in our economy could have devastating consequences, as would major disruptions to the flow of information across the internet itself."

Executive director of Telstra's network and IT operations, Craig Hancock, commented that "Exercises like *Cyber Storm III* were a great opportunity to test the veracity of these network protection measures, in addition to communications and decision-making processes which underpin any



technical response to a cyber event. By actively testing our response processes we can evaluate and improve our effectiveness in managing and responding to cyber security incidents."

Findings

The key findings from the exercise were:

- Key Finding 1: The exercise provided insight into key decision making processes within government, business and industry. These insights could not have been achieved without processes being tested in an exercise:
 - *Within government*, the exercise provided a good test of new processes including the interim cyber security crisis management plan, with players able to identify gaps and revise processes accordingly;
 - *Within industry*, a number of participating organisations advised that their internal processes were effectively tested, and they were still able to identify some gaps, in particular in relation to escalation procedures, which have led to processes being refined and improved;
 - *Within individual businesses*, many participants noted that the exercise had provided an invaluable opportunity to engage with their CEO's and, as a result, had highlighted the importance of cyber security to senior management; and,
 - *Cross-sectorally*, the exercise revealed many areas where internal and cross-sector partnerships worked effectively to communicate and resolve issues, but also highlighted areas where communications and planning could be further developed.
- Key Finding 2: Cyber Storm III proved very successful in enabling people to practice, learn and review their performance in relation to others working within and across the broader cyber-related crisis management frameworks. Indeed, substantial 'good will' was generated between government and industry as part of the entire Cyber Storm III activity, and this should continue to be built upon.
- Key Finding 3: The exercise planning and management process allowed for the development of trusted external organisational relationships that would assist in a real cyber event with training, tools and processes provided by AGD serving as a good foundation for future use.
- Key Finding 4: Australia should continue to plan and undertake regular cyber exercises as part of a broader national and international engagement program that practices and evaluates performances across tactical, operational and strategic levels.

In addition to these key findings, participants noted that the following benefits flowed directly from the exercise:

- It was a cost-effective way of conducting a business continuity or disaster recovery exercise;
- It provided an opportunity to network with people in their organisation and sector that they may need to engage with in a crisis situation;
- It provided an opportunity to exercise and test relationships with key vendors and stakeholders across sectors, to explore inter-dependency issues and build new relationships;
- It helped build stronger resilience into business and supply chains; and,
- It allowed for the identification of opportunities for improvement.