Australian Government
Department of Defence
Intelligence and Security

CYBER SECURITY OPERATIONS CENTRE

PROTECT

SEPTEMBER 2012

Preparing for and responding to cyber security incidents

Introduction

1. Cyber security incidents can include denying, disrupting or stealing of information on ICT systems. In addition to the damage done to Australia's economic wellbeing and thereby to all Australian citizens, such compromises damage the reputation of affected organisations, undermine public confidence in the Australian government and unnecessarily consume scarce money and staff resources to continually clean up compromises. Agencies should assess the value of information stored on their networks and apply security measures commensurate to the risk.

2. Cyber security incidents affecting government networks can be costly to agencies, consuming money and staff resources. In particular, agencies can be impacted through:

   a. Service unavailability and lost productivity

   b. Damage to agency reputation and trust

   c. Lost or stolen information that could harm Australia's economic wellbeing, national security or the privacy of Australian people

   d. Staff time and costs associated with restoring systems to a trusted state.

3. It is imperative that cyber security incidents are reported and resolved in an efficient and timely manner. The severity, scope, amount of damage and therefore cost of a cyber security incident increases with every hour it remains unresolved. The following advice will enable quicker response to a cyber security incident.

4. While responding to cyber security incidents quickly is important, agencies can implement strong mitigations to prevent incidents occurring in the first place and enable rapid detection. DSD's *Strategies to Mitigate Targeted Cyber Intrusions* document provides guidance in this area. DSD's Cyber Security Operations Centre (CSOC) provides government with a better understanding of sophisticated cyber threats and coordinates operational responses to cyber events of national importance across government systems.

5. This document assists senior managers assess their preparedness of their agencies to respond to cyber security incidents.

Questions for senior management to ask their IT security team

6. Senior managers should ask the following questions to determine how well their agency is positioned to respond to a cyber security incident.

Reporting

a. What are our legislative requirements and obligations for incident reporting?

b. Who has primary responsibility for incident response in our agency?

c. Are procedures in place to provide information and reporting to relevant parties during an incident? Is the ITSA familiar with the Cyber Security Incident Reporting process to the CSOC?

Planning and Preparation

d. Do we have a business continuity plan and disaster recovery plan and have these plans been regularly tested?

e. Do we have an up-to-date and regularly tested incident response plan?

f. Do we have up-to-date documentation such as System Security Plans and Standard Operating Procedures?

g. Do our agreements with contracted IT service providers have arrangements in place for incident response?

h. Have we identified our critical systems?

i. Do we have monitoring in place to assess our environment for cyber security threats?

j. Do we have processes in place to detect when an incident may have occurred?

Responding

k. How easily and quickly can we access resources key to mitigating an incident? (For example, system managers, technical experts, Internet Service Provider, system logs and physical system infrastructure.)

l. Do we have an up-to-date after hours contact list for key personnel and external stakeholders?

m. Do we have the ability to identify and isolate an affected workstation or system?

Preparing for and responding to cyber security incidents

7. An agency should asses their readiness to respond to a cyber security incident and their ability to provide adequate data to the CSOC if required. This document will help an agency assess their response capabilities and enable quicker response.

8. An agency should maintain awareness of the cyber threat environment to assist in implementing appropriate mitigation strategies. Engaging with DSD for information on cyber security and the current threat environment can help agencies plan for cyber security incident response. Maintaining a current security risk management plan for information security systems is imperative. The aim of the security risk management plan is to reduce the overall risk to agency information systems. The plan should include:

   a. Evaluating key assets and information

   b. Identifying assessed risks to those assets

   c. Performing a cost-benefit analysis for implementing potential risk mitigation strategies

   d. The risk treatments implemented.

9. Ensuring agency ITSAs have well documented incident response procedures can save time, money and staff resources. This will ensure incidents can be contained and mitigated quickly.

10. Early reporting of cyber security incidents to CSOC via a Cyber Security Incident Report form (available from DSD's website) will enable faster CSOC triage, mitigation and containment of the threat if required.

Further Information

11. The *Australian Government Information Security Manual* (including an Executive Companion) is available at www.dsd.gov.au/infosec/ism.

12. The *Strategies to Mitigate Targeted Cyber Intrusions* document is available at www.dsd.gov.au/infosec/top35mitigationstrategies.htm.

13. The Cyber Security Incident Report form is available at www.dsd.gov.au/infosec/incidentreport.htm and on DSD's OnSecure Portal at https://members.onsecure.gov.au.

Contact Details

Australian government customers with questions regarding this advice should contact the DSD Advice and Assistance Line on 1300 CYBER1 (1300 292 371) or dsd.assist@defence.gov.au.

Australian businesses or other private sector organisations seeking further information should contact CERT Australia at info@cert.gov.au or by calling 1300 172 499.