



Cyber security exercise report

Managing a vulnerability disclosure

Prepared by: _____

Date: ____ / ____ / ____

Executive summary

Our team ran a discussion-based cyber security exercise session on the reported date using the Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC) Exercise in a Box. This report summarises the results of this exercise and includes recommendations for our organisation to consider.

Discussion outcomes

What we learned from running the exercise:

How our understanding of preventing this type of cyber security threat changed:

What will we look to change or implement:

Team statements

We rated our confidence against the following statements:

Observations from Inject 1: Vulnerability reported

	Not at all confident	Slightly confident	Somewhat confident	Fairly confident	Completely confident
Your organisation has a documented action plan for vulnerability disclosure and the relevant people know what this is and understand it as an important part of being prepared.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Your organisation actively monitors your social media channels to identify any issues that are raised that need attention.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Your organisation provides a simple vulnerability disclosure policy or guidelines, to ensure expectations around providing vulnerability reports are easily understood by reporters.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Your organisation has effective protective monitoring that should quickly alert you to potential security issues with your online services.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Observations from Inject 2: Vulnerability exploited

Your organisation has a procedure in place to quickly respond to malicious attacks on your website or external infrastructure.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Your organisation can engage with the relevant people and/or service providers and authorities to recover the website.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Observations from Inject 3: Communications

	Not at all confident	Slightly confident	Somewhat confident	Fairly confident	Completely confident
Your organisation has procedures in place to handle communications with your users in the event of a security incident that may affect them.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Your organisation has an appropriate media plan with a designated representative to respond to media enquiries.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Observations from Inject 4: Process and procedures

Your organisation has an effective vulnerability disclosure process in place or plans to implement this soon following further discussions and approvals.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Your organisation aims to acknowledge any reported vulnerabilities in a timely manner and will open a communications channel with reporters without threatening any legal action. Mitigation work can be communicated, including potentially taking back control of any resources that have been claimed by a security researcher.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>