



Cyber security exercise report

Insider threat resulting in a data breach

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: Data breach

	Not at all confident	Slightly confident	Somewhat confident	Fairly confident	Completely confident
We have a clear method for reporting security incidents or data breaches.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

We have an effective way to track and monitor data being removed from our network.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
------------------------------------------------------------------------------------	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------

Observations from Inject 2: Investigation

We can effectively identify the unauthorised or accidental misuse of systems or data.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
---------------------------------------------------------------------------------------	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------

We can tie users to such activity and determine where data has been sent via audit trails/logs with a high level of accuracy.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
-------------------------------------------------------------------------------------------------------------------------------	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------

We have a clear user security policy and users are made aware of the impacts of misuse of business systems.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
-------------------------------------------------------------------------------------------------------------	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------

Observations from Inject 3: Removable media

We have a clear corporate policy controlling the use of removable media.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
--------------------------------------------------------------------------	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------

We have a clear corporate policy managing the use and sharing of sensitive information, and activity is monitored.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
--------------------------------------------------------------------------------------------------------------------	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------

Observations from Inject 4: Regulatory response

	Not at all confident	Slightly confident	Somewhat confident	Fairly confident	Completely confident
We have an agreed approach to reporting data breaches, which includes an understanding of our regulatory obligations.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
We have an effective communication plan that covers cyber incidents, to communicate with the media and public when needed.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>