



Cyber security exercise report

Threatened leak of sensitive data

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: Extortion demand

	Not at all confident	Slightly confident	Somewhat confident	Fairly confident	Completely confident
Your organisation implements effective access control to ensure that sensitive documents can only be accessed by the appropriate employees at your organisation.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Your organisation can accurately monitor access to files to determine who has accessed a file.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Observations from Inject 2: Insider threat

Your organisation has a clear process for offboarding employees in a secure manner, ensuring that access to corporate data and services is revoked.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Your organisation has effective monitoring in place that could allow you to determine which other documents the employee may have had access to.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Your organisation has clear methods of monitoring sensitive data leaving the network. It would be possible for you to determine if any employee information had been exfiltrated.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Observations from Inject 3: Incident response

Your organisation has a clear process to deal with the legal and regulatory implications of an incident involving potential leaking of sensitive information.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Employees are aware of how to respond if they receive a sensitive data leak threat and are aware how to escalate such an incident if necessary.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>