



# Cyber security exercise report

## Third-party software compromise

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: Third-party hacked

	Not at all confident	Slightly confident	Somewhat confident	Fairly confident	Completely confident
We have considered the risk from third-party service suppliers and have a defined procedure in place to deal with the compromise of one of these suppliers.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

### Observations from Inject 2: Stolen credentials

We only have necessary services accessible from the internet.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
A strong password policy is implemented in our systems in which users must choose unique passwords.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
All the systems in our organisation are securely configured with Multi-Factor Authentication (MFA).	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

## Observations from Inject 3: Sensitive data

	Not at all confident	Slightly confident	Somewhat confident	Fairly confident	Completely confident
We know what our most sensitive data is and where it is stored.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
We appropriately protect our sensitive data considering the implications of this data being attacked.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Our monitoring system collects events with sufficient detail to determine an attacker's movements.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Our organisation has an incident response procedure to prevent an attacker further compromising our network.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

## Observations from Inject 4: Temporary disruptions

We have a plan to manage temporary disruptions to business due to technical faults or cyber incidents.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
We have a business continuity plan in place to allow the organisation to continue to function should we be severely impacted.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
We have a good understanding of our Service Level Agreements (SLAs) and contingency plans with our third-party suppliers.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>