



# Cyber security exercise report

## Supply chain software

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: IT management software

	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"/>
Our suppliers meet a minimum cyber security standard.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

### Observations from Inject 2: Cyber incident

We have points of contact in place with our software providers who we can contact in the event of urgent queries.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
We have identified sensitive data or critical systems that could be exposed to third-party software providers.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
We have an up-to-date and tested incident management plan.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

### Observations from Inject 3: Compromise confirmed

We track all software deployed in our organisation, including versions and patch levels.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Our organisation has mechanisms in place to securely coordinate our response.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Our organisation has robust business continuity plans in place.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

## Observations from Inject 4: Dealing with the incident

	Not at all confident	Slightly confident	Somewhat confident	Fairly confident	Completely confident
Our organisation has effective systems for log collection, monitoring and analysis.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
We have developed and tested a communications plan to respond to the media in the event of a cyber attack.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Our organisation is aware of our obligations for reporting data breaches under the Australian Privacy Act 1988.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>