



Cyber security exercise report

Supply chain ransomware attack

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: Major supplier

	Not at all confident	Slightly confident	Somewhat confident	Fairly confident	Completely confident
We understand how a ransomware infection to one of our suppliers can impact our organisation.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Our risk management plan encompasses the discussion points and will help to minimise the impact to business operations.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
We have a comprehensive and up-to-date list of emergency points of contact for each of our major suppliers.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Observations from Inject 2: Ransomware propagation

We are confident our Incident Management plan will be effective in this scenario.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Our organisation has effective defence-in-depth to be able to mitigate a ransomware attack.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
We are confident our ransomware focused Incident Response playbook is up-to-date and would be effective.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Observations from Inject 3: Ransom demands

	Not at all confident	Slightly confident	Somewhat confident	Fairly confident	Completely confident
We understand the implications of paying a ransom.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
We can identify all our sensitive data.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
We understand the impact of the sensitive data being made available online.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Observations from Inject 4: Ransomware removal

We know which government agencies we need to contact in the event of a ransomware attack and what other groups we can contact for assistance.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
We have the right tools available to detect and remove malware on our IT systems.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Observations from Inject 5: System recovery

Our organisation structure has clear roles and responsibilities of the staff who would recover and harden our IT systems after a cyber incident.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
We have processes in place to ensure network diagrams, procedures and response plans are updated if our system changes after remediation activities (e.g. changes to hardware/software).	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Observations from Inject 6: Cyber insurance

We understand what may and may not be covered by cyber insurance.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
We have considered the benefits and drawbacks of cyber insurance to manage our cyber risk.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Observations from Inject 7: Sensitive information disclosed

	Not at all confident	Slightly confident	Somewhat confident	Fairly confident	Completely confident
We are confident that our communications plan will be effective in this scenario.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Our organisation has mechanisms in place to support employees during the incident.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Our communications plan will be effective in reassuring suppliers and customers.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>