



Cyber security exercise report

A ransomware attack delivered by a phishing email

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: Phishing email

	Not at all confident	Slightly confident	Somewhat confident	Fairly confident	Completely confident
We make it difficult for attackers to reach our users with phishing emails.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

We provide clear training to allow our users to identify, and report suspected phishing attacks.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
--	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------

Observations from Inject 2: Malware installed

We effectively detect and prevent malware running on our organisations IT.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
--	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------

We have a clear policy for keeping our organisation's software current and always apply the latest security updates.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
--	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------

Observations from Inject 3: Computer infection

We place appropriate limits on the software that can be installed or run on our organisations IT.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
---	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------

Observations from Inject 4: Files encrypted, ransom demanded

	Not at all confident	Slightly confident	Somewhat confident	Fairly confident	Completely confident
We have identified our critical systems and data and understand the potential impact of an infection.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
We have a tested incident response plan that covers key stakeholders, contact details, steps and procedures for dealing with a ransomware attack, and our legal and regulatory requirements.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
We have access to the resources required to execute the incident response plan if our systems are unavailable.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
If we lost access to our business-critical data, we could recover from our backups without significant disruption.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Observations from Inject 5: Media coverage

We have a clear and consistent approach for communication with staff, media and stakeholders during an incident.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
--	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------