



Cyber security exercise report

Internet of Things (IoT)

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: Visibility of IoT devices

	Not at all confident	Slightly confident	Somewhat confident	Fairly confident	Completely confident
We have a process for enrolling new IoT devices within our organisations.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
We have real-time monitoring capabilities for our IoT devices.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
We have an up-to-date asset register that is actively maintained.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Observations from Inject 2: Preventing an adversary from compromising IoT devices

We have implemented security controls to aid in mitigating threats to our IoT devices.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
We are aware if our IoT devices are end of life.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
We have managed the risk of legacy and end of life IoT devices on the organisation's network.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
We have an incident response plan that accounts for our IoT devices.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Observations from Inject 3: Protecting the internal network

	Not at all confident	Slightly confident	Somewhat confident	Fairly confident	Completely confident
We have implemented security controls that protects data at rest and in transit.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
We have implemented sufficient security controls to segregate IoT devices from our organisation's IT network.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Observations from Inject 4: Procuring secure IoT devices

We buy IoT devices from well-known, reputable companies/vendors.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
If data is shared from the IoT devices to third-parties such as the vendor, the data shared is minimised and its sharing is justified (e.g. it is required for operational or security reasons)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>