GNGB

Gateway
Network
Governance
Body

Resilience Checklist

Lessons from Operation Honey Bee

In today's world, ensuring resilience through robust response and recovery strategies is vital for all organisations within the Australian Superannuation ecosystem. Protecting members from the impacts of cyber threats and disruptions is critical. GNGB ran a simulation exercise Operation HoneyBee, in collaboration with key stakeholders in the Superannuation ecosystem, designed to test the resilience of our ecosystem in the face of a simulated cyber attack.

The following insights derived from the exercise are being shared to support all organisations in enhancing response and recovery processes.

Who are your third parties?

Ensure third parties are included as key stakeholders in your response plans. Two-way communications can assist in sharing threat intelligence for protection of the broader ecosystem, but also allows your third parties to contribute practically to the response efforts when needed.

Taking your system offline?

In a tightly integrated ecosystem like ours, the decisions you make in response to an incident will likely impact both upstream and downstream components of your solution. Ensure your plan explicitly specifies who will be affected and who needs to be notified if systems and processes need to be halted.

The bad guys can't be trusted!

Does your organisation have a threat verification strategy? As cybercriminal strategies continue to evolve, they may claim to have data or access that they do not. Make sure your response plan includes strategies for verifying threats, especially in the cases of data extortion and ransomware scenarios. Explore how long the verification process may take under different conditions and how this impacts your ability to respond.

The opposite of silos

Often security teams are focussed on the job at hand during the early stages of incident response, including hunting for indicators the environment has been compromised. Have you thought about how to capture business metrics that may provide additional clues that all is not well? Operation Honeybee illustrated the value of combining insights from different parts of the organisation.

Education

Implement ongoing education initiatives for your key decisions makers, including your Board, and involve them in your response tests. Incorporate evolving threat actor tactics. Prepare your decision makers for the real possibility that cyber criminals may exert direct pressure during an extortion attempt. It is unlikely that an incident will play out exactly how you have rehearsed, but frequent and varied testing is a sure way to build muscle memory!

Not my incident!

The interconnected nature of our ecosystem means increasingly we are seeing significant consequences arising from cyber incidents originating outside our own environments. Clearly define in your plan who in your organisation is responsible for reporting an incident, even if the incident did not originate internally but has an impact on your organisation. Consider what your response plan looks like for the types of scenarios that originate elsewhere and require a response from you.

Decision making

During an incident, prompt decision-making is crucial. Often the bigger the blast radius, the more people involved! Establish and document who your decision makers are ahead of time to avoid confusion. Do you need to include all of these decision makers when you practice your plan? YES!

Government assistance

In the protection of Australian superannuation members, the need for industry and government to work together has never been more important. Government capabilities continue to develop and evolve with a number of separate and distinct resources such as:

- the **Australian Cyber Security Centre** (ACSC) for when you require operational assistance;
- **Australian Federal Police** (AFP) for law enforcement and criminal investigation; and
- the emerging capability of **The National Office of Cyber Security** (NOCS). This agency can play a key role in managing the consequences of an incident and assist with coordination of communications to large groups of government and citizen stakeholders.
- Engage with them now to understand how they can integrate into your response plans.