



Gateway
Network
Governance
Body

Honey Bee III: From Exercise to Action

Cyber resilience is built well before an incident occurs. Through the relationships, processes and decisions organisations put in place, as well as through opportunities to test whether those arrangements work in practice.

This was the focus of Operation Honey Bee III, GNGB's latest industry-wide cyber exercise, which brought together 68 participants and observers from 33 organisations across Australia's superannuation ecosystem. Over five hours, participants worked through seven escalating scenarios designed to test how the sector might collectively respond to a significant cyber incident.

While the exercise demonstrated the progress that has been made across the sector, its real value lies in what happens next. Exercises provide an opportunity to challenge existing assumptions, consider an incident from different perspectives and identify practical improvements that can be made before organisations are faced with the real thing.

For organisations that participated in Honey Bee III, the focus now turns to translating those lessons into action. But the takeaways extend beyond those who were in the room. We've pulled together some practical actions that organisations across the superannuation ecosystem can take now to strengthen their cyber response.

1. Expect different experiences of the same incident

One of the important themes reinforced through Honey Bee III was that a sector-wide cyber incident is unlikely to affect every organisation in the same way, or at the same time.

Different organisations may be exposed to different threat vectors, receive different information and experience different operational impacts, even where those impacts relate to the same broader event. During an incident, it can be easy for an organisation's

own experience to shape its understanding of what is happening across the sector. In reality, that view may only represent one part of a much larger picture.

Being able to compare information across the ecosystem can help organisations understand whether an issue is isolated or more widespread, identify emerging patterns and build a more complete picture as an incident develops.

During a sector-wide incident, what your organisation is experiencing may only be one part of the picture.

2. Bring intelligence together

Threat intelligence can come from many places, and not all of it will arrive through traditional cyber security channels. During an incident, relevant information may come from government agencies, regulators, third-party providers, industry peers, operational teams, relationship managers or member-facing functions. Organisations need to consider whether their internal structures allow those different pieces of information to come together quickly enough to inform decision-making.

Clear processes for escalating, triaging and sharing intelligence internally can help organisations develop a fuller picture of what is happening and respond accordingly.

Organisations should consider whether these arrangements are clearly understood across the relevant teams and, importantly, whether they have been tested.

3. Use exercises to revisit the fundamentals

Exercises naturally focus attention on incident response, communication and decision-making, but they should also provide a reason to revisit the technical and operational foundations of an organisation's cyber resilience. Following Honey Bee III, 60% of respondents said they would review their patching and vulnerability management processes.

The same approach can be applied more broadly. Honey Bee III highlighted the following areas that will be well embedded in existing plans, but should be reviewed to ensure they are up to date with the evolving threat landscape:

- Review critical systems and dependencies – do these remain the same as last time you tested? Operations are evolving and so should your plan
- Escalation pathways – who has decision making ability within the business to ensure an agile response?
- Business continuity arrangements – who makes the call and when, to switch to back up processes and how long are those processes manageable for? Critical Infrastructure advice is to now consider a period of 3 months in your contingency planning.
- Manual workarounds should also be considered in practical terms: not simply whether they exist in a plan, but whether they would remain workable during a prolonged disruption affecting multiple organisations.
- And of course, how do your established vulnerability management timeframes match up to the evolving ability of threat actors to exploit vulnerabilities at speed and scale?

60% of participants said they would review their patching and vulnerability management processes following Operation Honey Bee III.

4. Understand what sits beyond your organisation

Australia's superannuation ecosystem is highly interconnected. Funds, administrators, gateways, technology providers, government agencies, regulators and other service providers all play different roles

in supporting the movement of data, payments and services across the system.

For individual organisations, this makes understanding external dependencies an important part of cyber preparedness. It is not enough to consider only the systems and services an organisation directly controls. Organisations also need visibility of the providers and shared services they rely on, and an understanding of what disruption elsewhere could mean for their own operations.

Map your data and payments value chains to understand your service providers and other services you are dependent on.

Recovery also needs to be considered in this broader context. In an interconnected environment, decisions about disconnecting, reconnecting or restoring services can affect other ecosystem participants. Understanding those dependencies, and continuing to test them collectively, will be an important part of strengthening resilience across the ecosystem.

5. Prepare for disruption that lasts longer than expected

A significant cyber incident may not be resolved within the timeframes contemplated by traditional business continuity plans. The response may continue for days or weeks, while investigation, containment, recovery, stakeholder communications and operational backlogs create different pressures at different stages.

Organisations need to consider whether their existing arrangements remain practical over a longer period. This includes the sustainability of manual workarounds, availability of key personnel, fatigue management, member communications and the ability of contact centres and operational teams to manage increased demand.

These considerations take on additional importance in the Payday Super environment. Higher transaction volumes and shorter processing windows mean disruption can have a greater impact and there may be less scope to rely on manual processes for extended periods.

Business continuity and incident response arrangements need to reflect this changing operating environment and the possibility that disruption may extend beyond an individual organisation.

6. Keep building the relationships behind the response

One of the most important benefits of an exercise such as Honey Bee III is the opportunity to build relationships across the ecosystem.

During a real incident, organisations need to know who to contact, where information can be shared and how government, regulators, industry bodies and other organisations fit into the response. Document roles and responsibilities within your plans, beyond your organisation, so expectations are well understood.

As one Honey Bee III participant put it:

7. “Practice, practice, practice. Preparation is key.” From lessons to action

Operation Honey Bee III provided an opportunity to test the sector’s collective response in a controlled environment. The challenge now is to make sure the experience leads to practical improvements.

This means taking the findings back into the business, considering them in the context of their own arrangements and identifying the actions that should be prioritised. Senior leaders and Boards also have an important role in ensuring those actions receive appropriate attention and resourcing.

At an ecosystem level, continued collaboration will be just as important. Cyber incidents do not respect organisational boundaries, and the effectiveness of the sector’s response will depend not only on the preparedness of individual organisations, but on how effectively they can work together when it matters.

There has been considerable progress in cyber preparedness across the superannuation ecosystem in recent years. Maintaining that progress will require organisations to keep testing their arrangements, challenging assumptions and strengthening the relationships that underpin a collective response.

The value of an exercise is not only in what it identifies, but in what organisations do next.

GNGB will continue to bring organisations across the superannuation ecosystem together to practise collective response, strengthen collaboration and build resilience as the threat landscape and operating environment continue to evolve.