AI cyber threats have changed

What boards must do now

Our Annual Threat Dynamics report highlighted the increase of AI threats over the past year, and how rapidly this is evolving. A recent example of that is the announcement of Anthropic's Claude Mythos Preview which again has shifted the dial on how organisations must prepare for an AI-enabled future.

The development is significant because it represents a step change, not an incremental one. Anthropic says Mythos has already identified thousands of zero day vulnerabilities, including flaws in foundational software that underpins commerce, finance and government.

At the same time, AI compresses the traditional gap between vulnerability discovery and exploitation, making Mean Time to Patch a critical board-level metric and increasing the importance of prioritised, automated patching.

Anthropic has also made clear that any defender advantage is likely temporary, as similar capabilities are expected to spread to hostile actors within months, making resilience and containment just as important as prevention.

What practical steps can organisations take?

1. Advise Executive and Board/relevant Board sub-committee of what has changed and the steps below which need to be taken in a heightened risk environment.
2. Prepare for new releases of software from the technology companies who have been provided access to Mythos through Project Glasswing and the additional 40+ organisations also provided access.
3. Budget for replacement of legacy software prior to Mythos (or a competitor alternate) becoming available to all.
4. Add in a clause on Mythos type testing to cloud/software provider contracts.
5. Assess and strengthen third party vulnerability management requirements and phase out suppliers that fail to meet new faster requirements.
6. Keep testing their production systems for misconfigurations.
7. Develop and test plans for zero day incidents/crisis response.
8. Establish AI defensive cyber security capabilities and approaches.

For those organisations who develop their own software and write their own code:

Prepare a prioritised list of their in-house developed code to run through an available LLM and repeat when Mythos (or a competitor alternate) becomes available, and set aside budget to implement any required fixes.

Re-engineer the SDLC for Mythos code review during build.

Bottom Line for the Board and Senior Management

Project Glasswing is not just a cyber security initiative – it is an early warning signal that:

AI has crossed a threshold where offensive cyber capabilities used by attackers scale faster than traditional defence.

The window for preventive action is shrinking.

Boards and senior management should expect cyber risk to become more frequent, faster moving, and more systemic.

In practical terms, this further elevates the importance of cyber resilience, architectural simplicity, and response readiness to core enterprise issues, not just CIO or CISO concerns.

Contact Us

Peter Malan

Cybersecurity & Privacy Practice Leader, PwC Australia

peter.malan@au.pwc.com

Robert Di Pietro

Partner, Cybersecurity & Privacy, PwC Australia

robert.di.pietro@au.pwc.com

Andrew Gordon

Partner, Cybersecurity & Privacy, PwC Australia

andrew.n.gordon@au.pwc.com

Brett Hayes

Partner, Cybersecurity & Privacy, PwC Australia

brett.hayes@au.pwc.com

PWC201217336