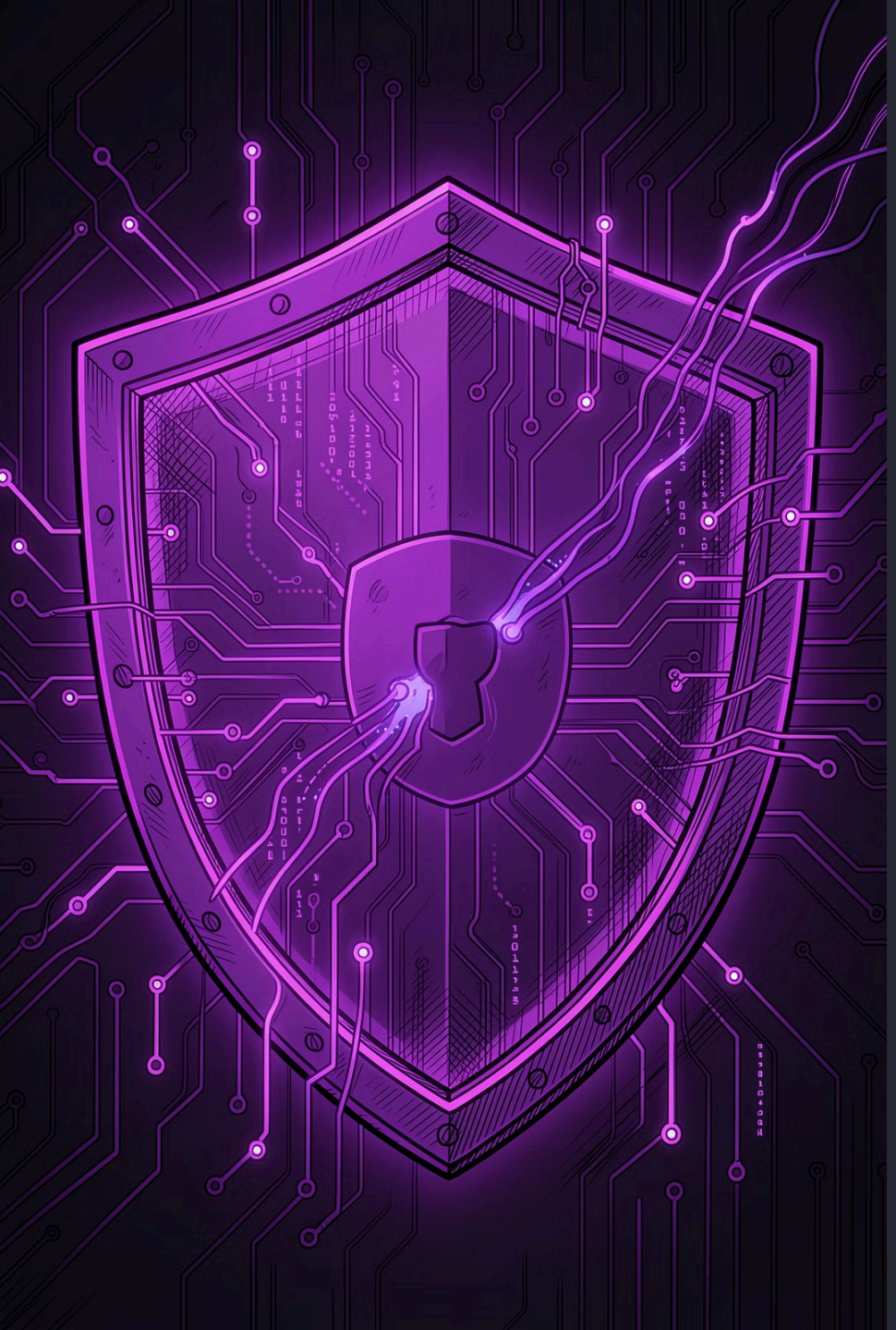


BOARD INSIGHT MICRO LEARNING III · MAY 2026

Cyber Security Risk Essentials for Boards

Helping you understand the digital risks facing your organisation — and the critical questions every board member must be prepared to ask.

Digital Risk AWARE LIMITED

The Cyber Criminal Motivations

Bad actors, whether criminally motivated or state sponsored are constantly looking at ways to either instantly bring organisations to their knees or through theft of intellectual property, reduce the strategic position of a business. To a bad actor, the motivations are driven by financial or strategic advantage, with four types of scenarios in their toolkit.

Key Digital Assets

Disable critical applications or AI solutions to halt operations.

Critical Infrastructure

Overload IT environments with Denial of Service attacks.

Data Environment

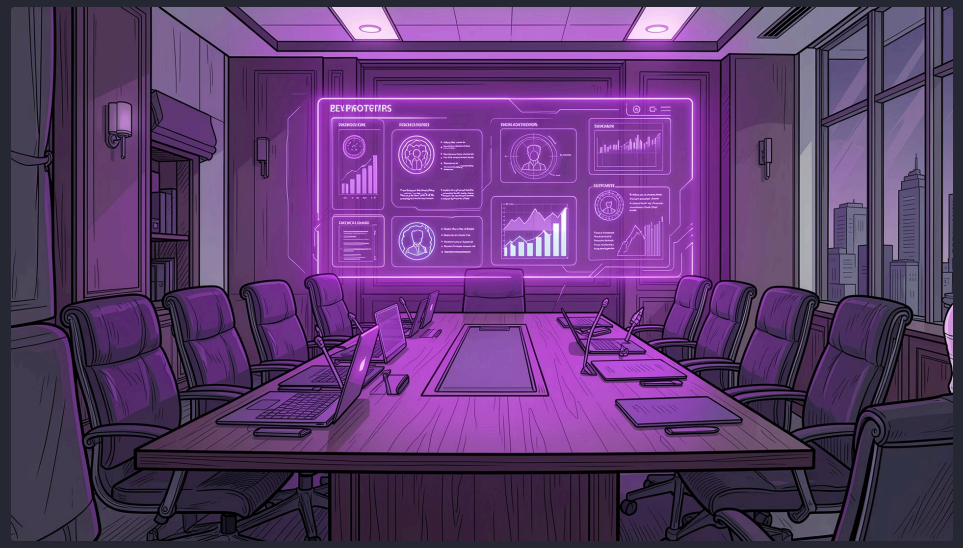
Steal or encrypt key datasets for ransom or competitive gain.

Third-Party Partners

Target your key third party partners to cut off a key dependency

Cyber Security: Demystifying the Complexities

There are so many perspectives, frameworks and industry guidance notes covering the Cyber Security agenda. Fundamentally, all breaches point back to four common themes that Boards really need to have confidence over



1 Know Your Crown Jewels

Do you understand where the crown jewels are in your business that are attractive for a Cyber Criminal (whether data or IT infrastructure)?

2 Understand Your Landscape

Do you understand your IT and Data Landscape to understand whether the crown jewels are vulnerable?

3 Countermeasures in Place

Are the countermeasures in place robust to minimis the inherent vulnerabilities identified?

4 People Can be Your Weakest Link

Is the weak underbelly of each organisation (your people) trained, based on a risk-based approach, to prevent opening doors to the criminals?

If you or the Board cannot answer these questions with confidence, then it will be critical to your business to develop a framework to ensure you have the insight and knowledge needed to specifically answers these questions for your business

BOARD ACCOUNTABILITY FRAMEWORK

Killer Questions: The Cyber Security Themes for Boards

If you cannot answer these with confidence, building a governance framework is urgent.

🔍 Crown Jewels

- Think like the Cyber Criminal – What are the doomsday scenarios?
- How could each materialise?
- What will the consequences be for each breach (reputation, operational, financial & reputation)?

🗺️ Vulnerabilities

- Using the scenarios & how each could materialise, assess the vulnerabilities for each to occur (inherent risk)?
- Assess each to determine whether inherent risk (impact/probability) above risk appetite?
- Evaluate whether the Cyber insurance covers the inherent risk and whether acceptable?

🛡️ Counter Measures

- Are the counter-measures for each inherent vulnerability appropriate & residual risk acceptable?
- How is the Board obtaining independent comfort that the counter-measures are designed appropriately and operating effectively

👥 Trained People

- Is there an effective risk assessment over the human roles interacting with the IT environment?
- Is the training aligned to the human risk profile?
- Using the risk profile, does an effective framework exist to validate the effectiveness of the training in place?