New cyber guidelines: 'Ignore at your peril'
By JOE KELLY

The Australian
Wednesday 28th February 2024
593 words
Page 5 | Section: THE NATION
300cm on the page

New cyber guidelines: 'Ignore at your peril'

CHIEFS TOLD TO PLAN FOR ATTACKS

JOE KELLY

EXCLUSIVE

NATIONAL AFFAIRS EDITOR

Home Affairs Minister Clare O'Neil has endorsed world-first governance guidelines to hold Australian company directors to higher standards and help them better prepare for cyber incidents by responding swiftly, accurately and transparently during attacks.

Ms O'Neil said the new governance principles should be embedded by all Australian organisations "into how they do businesses".

The 62-page handbook containing the principles urges directors to prepare for potential attacks by developing detailed readiness plans, regularly simulating attacks to improve resilience and maintaining strict data management policies to make companies harder for cyber criminals to target.

It also provides key advice for company directors on how to respond to attacks and ransom demands.

For listed companies, the principles – prepared by the Australian Institute of Company Directors, the Cyber Security Co-operative Research Centre and leading corporate law firm Ashurst – include guidance on how to comply with continuous disclosure obligations during cyber incidents and make difficult judgment calls such as whether to initiate a trading halt.

Research centre chief executive Rachael Falk told The Australian "cyber is the thing that keeps CEOs up at night".

She warned that business leaders who did not take cyber security seriously were "simply planning to fail", while institute chief executive Mark Rigotti said directors who ignored the new guidelines were "playing roulette with their companies".

Ms Falk said the new governance principles could be used by a court to determine whether a company had taken sufficient steps to counter the risk of a cyber attack and "at least incorporate whatever they could depending on their size and budget".

The new handbook is touted as the "first of its type", with Ms Falk saying it elevated Australia as a leader among Five-Eye nations "in helping directors understand their obligations".

The new principles come after major data breaches at Optus in September 2022, where a hacker gained access to the details of 10 million customers, and Medibank Private, which refused to pay a ransom that November after the personal information of 9.7 million current and former customers was stolen.

Mr Rigotti said the new governance principles made clear that the government, while recommending against paying cyber criminals, had opted to leave this choice to company boards.

"It's a really hard issue," he said. "You are paying money to an extortionist, but on the other hand you might need to pay money to preserve life."

Ms Falk said her advice to company directors was mostly "to not pay the ransom".

"When you pay the ransom you are just feeding the food chain of cyber criminals. The best way to break the food chain is not to pay the ransom," she said.

The governance principles state that any decision about paying a ransom "should be the responsibility of the board" based on the consideration of several factors: reputational impact, legal consequences, who was making the threat and the potential impact on customers and stakeholders of a ransom not being paid. Larger firms are also encouraged to plan for the engagement of specialised ransom negotiators.

The governance principles said it was critical for boards to implement clear policies for data collection, sharing and use.

Ms Falk said this should include periodic destruction. "Not enough companies have data governance plans and they don't destroy data often enough," she said. "If you have 30 candidates for a job, destroy the details of candidates that didn't get the job.

"It goes further; destroy hardware. Get it securely destroyed."