

## Country view: Australia

Australian C-suite respondents are far more wary of being hacked than their contemporaries. Seventy-three per cent of those surveyed think they are likely to be the target of a cyber attack, as do 77% of ITDMs, compared to 57% of those globally. Australian executives, aware of a series of high profile hacks, may feel a serious attack on their organisation is only a matter of time.

Being so aware of the consequences of a hack, both financial and reputational, may be the reason that Australia is the only market where C-suites estimate the cost of a serious, successful cyber attack to be higher than ITDMs – at US \$27.2 million. Both the C-suite (83%) and ITDMs (47%) also rate professionals as far greater a threat than any other type of hacker, which may also contribute to their fear of a successful attack.

Cyber security is a priority for the Australian government, which released its Cyber Security Policy in April last year. This was followed by some key appointments including Australia's first Minister Assisting the Prime Minister on Cyber Security, and a special adviser to the Prime Minister on cyber security.

Half of C-suite respondents and ITDMs (50%) say they will increase the time and resources spent on cyber security and defence in the coming year. However, almost a quarter (23%) of C-suite respondents think they have all the necessary skills to deal with a cyber attack, while only 7% of ITDMs agree. Businesses are also being warned not to have a set and forget mindset when it comes to their cyber security strategy.



50% of C-suite respondents say they will increase resources spent on cyber defence



77% of ITDMs feel they are likely to be targeted by a cyber attack

