PERSPECTIVES ON CYBER RISK 2017

In the past 12 months concerns about cyber-risk have intensified – with good reason.

$6 trillion
estimated global cost of cyber-crime by 2021

300 percent
increase in daily ransomware attacks in 2015 - 2016

$4 million
cost of each data breach

FIVE KEY THEMES

Awareness of cyber risk has increased as the problem grows – but concrete actions have not changed

Organisations are complacent about reviewing and testing their own cyber resilience and that of their suppliers

Cyber security is still (wrongly) seen as being primarily an IT issue

The privacy landscape is changing – both in Australia and overseas

The increasing uptake of cyber insurance indicates some willingness to act on managing cyber risk

BOARD PERSPECTIVE

CIO PERSPECTIVE

40%
are dissatisfied with their organisation's ability to prevent cyber incidents

42%
do not have a data breach response plan

52%
say their organisations have increased expenditure on IT security

90%
plan to deliver one or more IT functions via the cloud

56%
agree mandatory data breach notification requirements should be introduced

EMBEDDING CYBER RESILIENCE

1. Identify extent of exposure to cyber risk
2. Develop and implement procedures to protect the organisation
3. Deploy resources to identify a cyber breach in a timely manner
4. Implement procedures to respond and recover from a cyber breach

MinterEllison