Can you afford not to meet your cybersecurity compliance obligations?

Consider this:

76%

of Australians whose data was involved in a breach said they experienced harm as a result

70%

of Australians say privacy is extremely or very important when choosing a product or service

Data privacy is the 3rd most important factor to Australians when choosing a product or service

47%

of Australians said they would stop buying from an organisation that experienced a breach

12%

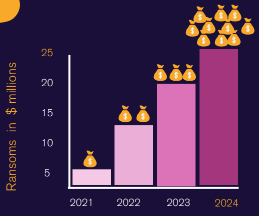
of Australians said there was nothing an organisation could do to appease them

Ongoing Australian Privacy Act reforms and regulatory framework updates continue to complicate compliance requirements

Geopolitical unrest is exponentially increasing risk to critical infrastructure

Ransomware attacks now include double-extortion (by leaking data online) and triple-extortion (using stolen data to attack customers or partners)

Ransom demands are increasing from millions to tens of millions of dollars



Multiple agencies are authorised to impose fines for failing to:

- Report incidents on time
- Protect personal information
- Implement proper security measures

Post cyber incident consequences for businesses :

- Class actions and court scandals
- Fines up to $50 million
- Negative publicity and damage to brand

Post cyber incident consequences for directors:

- REVOKED Revocation of directors' rights
- Fines up to $2.5 million
- Jail time

Compliance with the Australian Privacy Act and Essential Eight is complex.

But is non-compliance, obsolete defences and persistent breaches worth the risk?

As cyber security laws, regulations and frameworks continue to evolve, maintaining a fit-for-purpose cyber security programme is critical.

Read NCC Group's thought leadership to understand your cyber security compliance obligations, the challenges around meeting them and solutions that can help.

However while implementing baseline compliance measures may seem sufficient, is it really enough?

Read an alternative perspective on the value of proactive compliance.

Download NCC Group's 'Sustainable cyber security strategy' to understand how to:

- Defend from compromise and prevent theft of personal information
- Boost overall cyber security maturity
- Deliver quantifiable strategic value to your business.

Source - Australian Community Attitudes to Privacy Survey (ACAPS) 2023