# Successfully managing cyber security risks

## What can you do?

- **Risk assessment –** Identify the security risks to information held by the organisation and the consequences of a breach of security.
- **Policy development –** Develop a policy or range of policies that implement measures, practices and procedures to reduce the identified risks to information security.
- **Staff training –** Train staff and managers in security and fraud awareness, practices and procedures, and codes of conduct.
- **Technology –** Implement technologies to secure information held by the firm, including through such measures as access control, copy protection, intrusion detection, and robust encryption.
- **Monitoring and review –** Monitor compliance with the security policy, periodic assessments of new security risks and the adequacy of existing security measures, and ensuring that effective complaint handling procedures are in place.
- **Appropriate contract management –** Conduct appropriate due diligence where services (especially data storage services) are contracted, particularly in terms of the IT security policies and practices that the service provider has in place, and then monitoring compliance with these policies through periodic audits.

## Our team at Gadens

**Antoine Pace**
**Partner**
+61 3 9612 8411
+61 405 151 604
antoine.pace@gadens.com

**David Smith**
**Partner**
+61 3 9252 2563
+61 419 890 225
david.smith@gadens.com

**Dudley Kneller**
**Partner**
+61 3 9252 7748
+61 438 363 443
dudley.kneller@gadens.com

**Hazel McDwyer**
**Partner**
+61 2 9163 3052
+61 402 264 958
hazel.mcdwyer@gadens.com

## Top tips and takeaways

1. Cyber breach events are increasing and pose substantial risk to both public and private sectors.
2. Given the stance regulators and government are taking on cyber risk, organisations which ignore cyber risk do so at their own peril.
3. Understand the new data breach notification laws
4. Policy review and updates.
5. Build awareness to reinforce compliance over time.
6. Allocate responsibility for privacy and data security at a Board Level.
7. Review insurance policies and assess coverage for data breaches; consider whether cyber insurance is required.
8. Train staff.