



Welcome to our Evolving Cyber Risk Seminar  
November 2019

# Welcome James Carnie

November 2019

# Topics

1. Cyber security risks
2. Legal risks
3. Privacy Laws
4. Data breaches
5. Managing risks by contract
6. Other steps to reduce/manage risks

# Cyber security risks

1. Notable data breaches include Yahoo, Facebook, Equifax, Uber and Adobe.
2. Any business can be affected. Hosted service providers (e.g. NAAS) often now include specific (e.g. DDOS) rights to suspend services
3. Ransomware is now common.
4. Legal risks and reputational damage.

# Legal risks

Legal risks include:

1. Contractual risks (including confidentiality and privacy obligations)
2. Negligence/tort (various); and
3. Privacy laws

# Privacy Laws

- GDPR now in force (May 2018 onwards)
- May affect NZ businesses (depends on customer identities/locations)
- Data processing a central focus
- To engage subcontractors to process data, a data processing agreement is mandatory.
- NZ privacy laws under review

# Data breaches

Europe: GDPR requires mandatory disclosure of any data breach (within 72 hrs)

Australia has also adopted “notifiable data breaches” regime

US = mandatory disclosures

NZ – no mandatory disclosures yet, but only a matter of time

# Managing confidentiality and privacy risks by contract

- Ensure that all relevant privacy laws are complied with (including privacy and data policies, data processing agreements etc).
- Avoid 'absolute' assurances to customers regarding data security and confidentiality.
- Limit liability.
- Include appropriate disclaimers in terms of trade



# Other steps for reducing risks

- Comply with privacy laws and policies
- Store and backup customers' data (in encrypted form)
- Educate your employees and contractors (including implementing an AUP for devices, network)
- Get appropriate insurance

**Thank you**