Cyber Risks

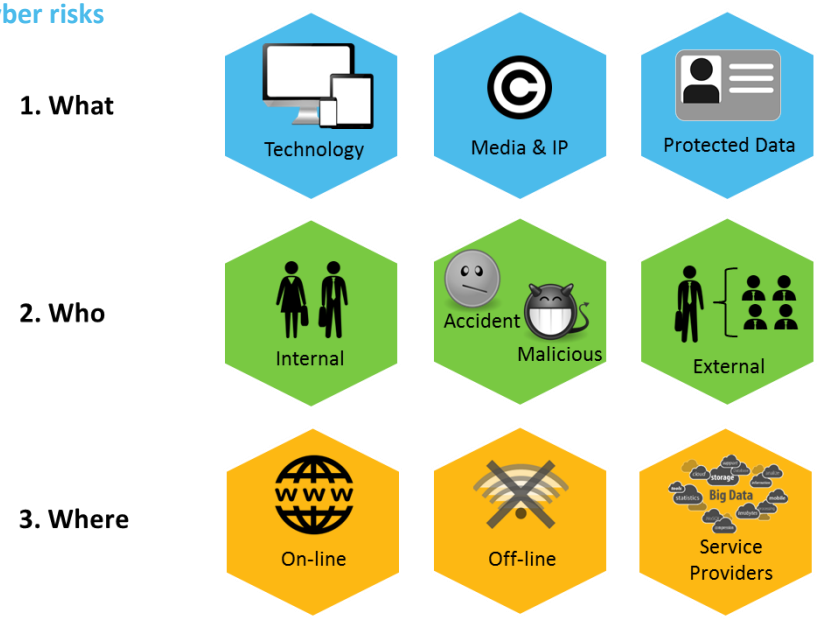
Intangible company assets such as computer systems and data have become increasingly under threat. In the past 12 months we have seen a steady increase in attacks using malicious code, hacking and social engineering tactics.

With companies so heavily reliant on computers systems and data to function it is critical to expand perception of risk from tangible to intangible assets and the consequences on reputation and finances if these intangible assets are attacked.

Cyber security is a continuingly evolving task that requires multiple strategies to manage a company's people, process and technology.

Staying ahead of well-funded and resourced criminals is proving difficult and therefore risk transfer mechanisms such as insurance provide part of the solution.

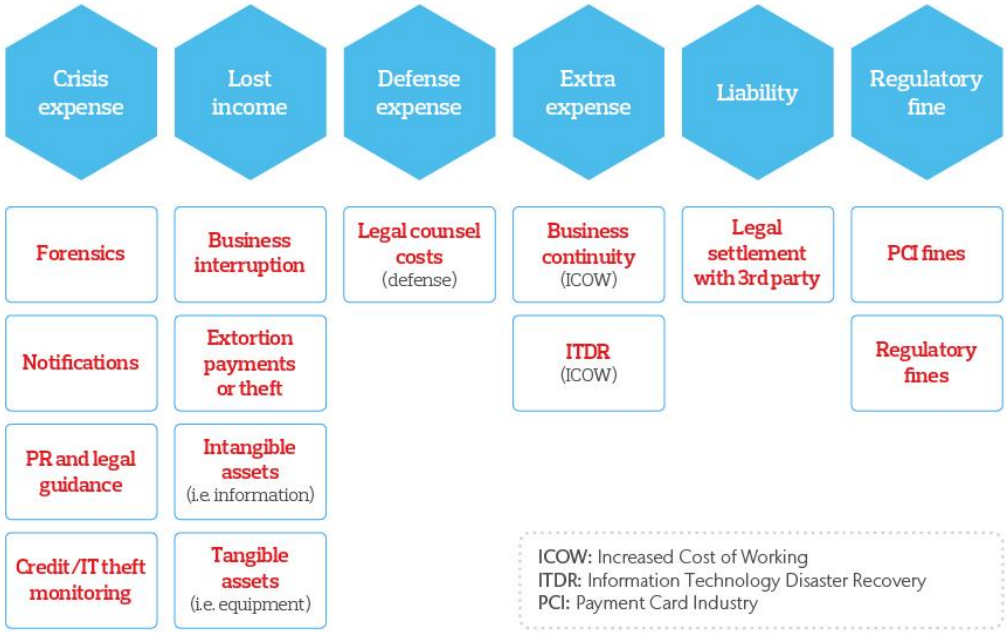
Cyber risks



What are the consequences of a cyber-attack?

Significant cost can be incurred for post breach mitigation services to find and repair quickly the areas affected by the cyber incident, develop and execute public and regulatory disclosure strategies to minimise reputational damage, and position legal services to minimise the impact of lawsuits. A company is also exposed to loss of productivity, loss of profit and possibly a decline in a company's value.

Breakdown of costs



Theft of money / fraudulent funds transfer

Cyber insurance focuses on intangible data and systems, whilst a Crime policy has traditionally covered theft of money by employees and third parties.

The distinction between the two has become blurred due to theft of money being carried out via electronic means.

Scamming has become more sophisticated through the use of social engineering and the stealing of information from computers or emails.

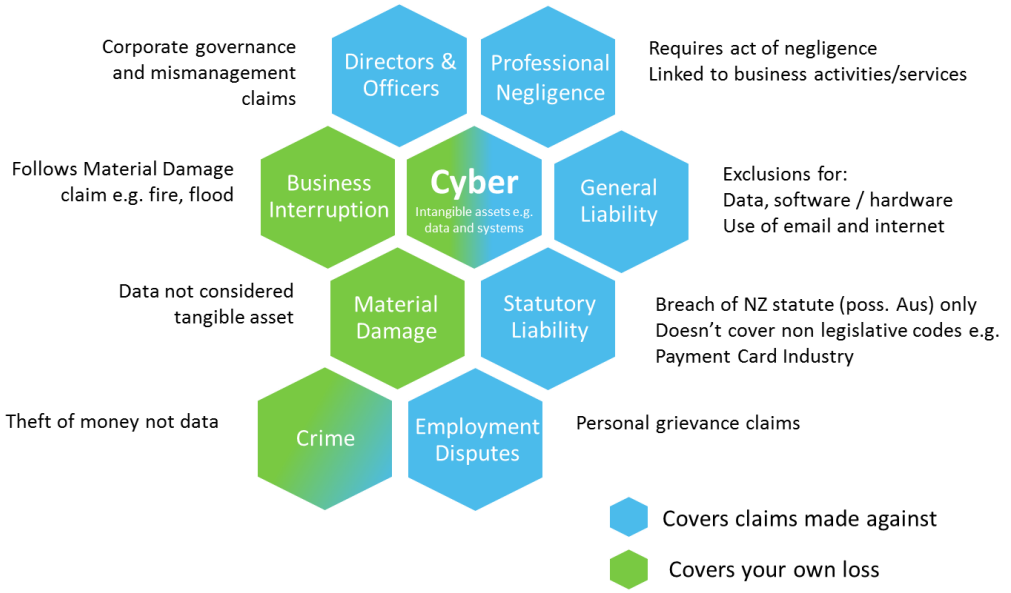
All companies should consider their vulnerability to fake invoices, orders, payments and other instructions that could result in the loss of own or third party money.

Consideration should be given as to how the risk is managed via Cyber or Crime insurance or a blend of both.

AON
Empower Results®

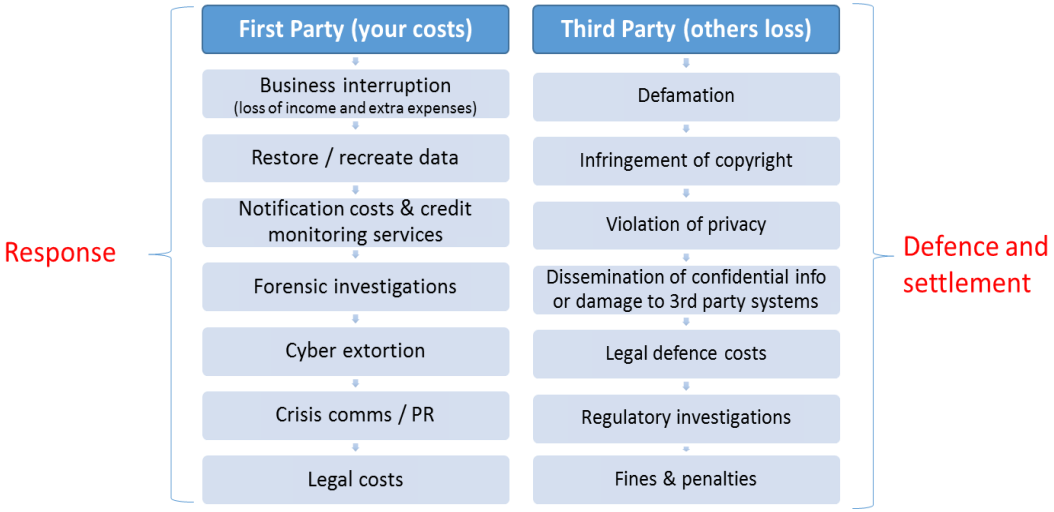
Traditional insurance

Traditional policies were never designed with cyber risks in mind. It is expected that providers of traditional insurance will add cyber exclusions now specific cyber policies are available.



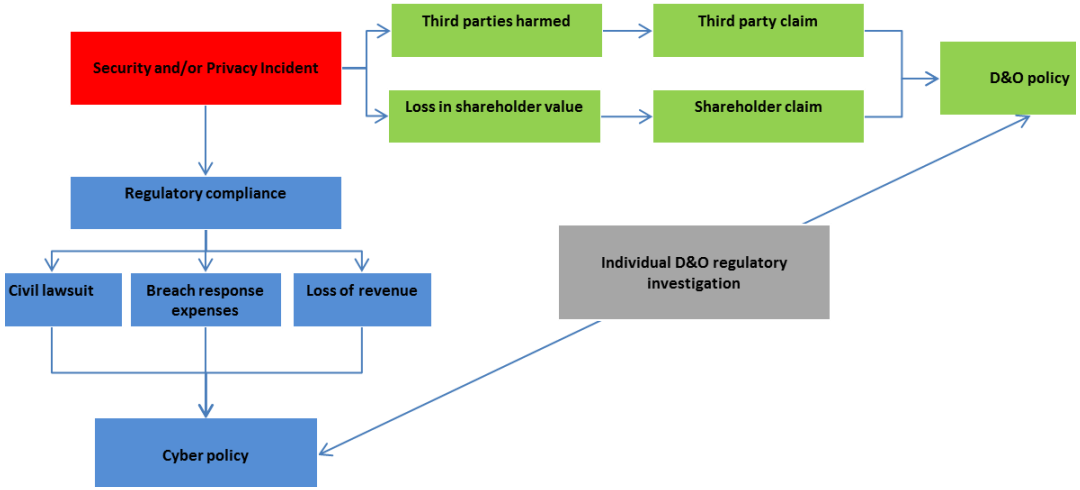
Cyber insurance at a glance

As highlighted above, Cyber insurance can provide cover for your own losses and claims made against you. The Cyber insurance market is still developing and no two offerings are identical, however most insurers look to cover the following:



What is driving the decision to buy cyber insurance?

1. **Complex and evolving risk landscape – People/Process/Technology**
2. **Realisation of value of intangible assets/consequential loss if disturbed**
3. **Director responsibilities**
   Satisfying directors and officers fiduciary obligations requires management oversight. Failure to meet obligations can create D&O claims. See diagram below.
4. **Access to insurers panel of experts 24/7 e.g. forensics, IT, Legal, PR etc.**
5. **Transfer unknown costs and close gaps in current insurance programme**
6. **Privacy laws**
   Laws around the world are evolving. The most onerous are mirroring the US where most states carry a mandatory requirement to notify customers and regulators and carry significant fines for failure to comply e.g. businesses in Australia can be fined up to $1.7m.



Next step - options available from Aon

1. Take free assessment www.aoncyberdiagnostic.com
2. Scope cyber insurance coverage and pricing
3. Gap analysis of current insurance programme
4. Develop risk map and in-depth quantification of cyber risks for greater confidence in financial exposures and compare against risk appetite and tolerance - supporting risk mitigation strategies.