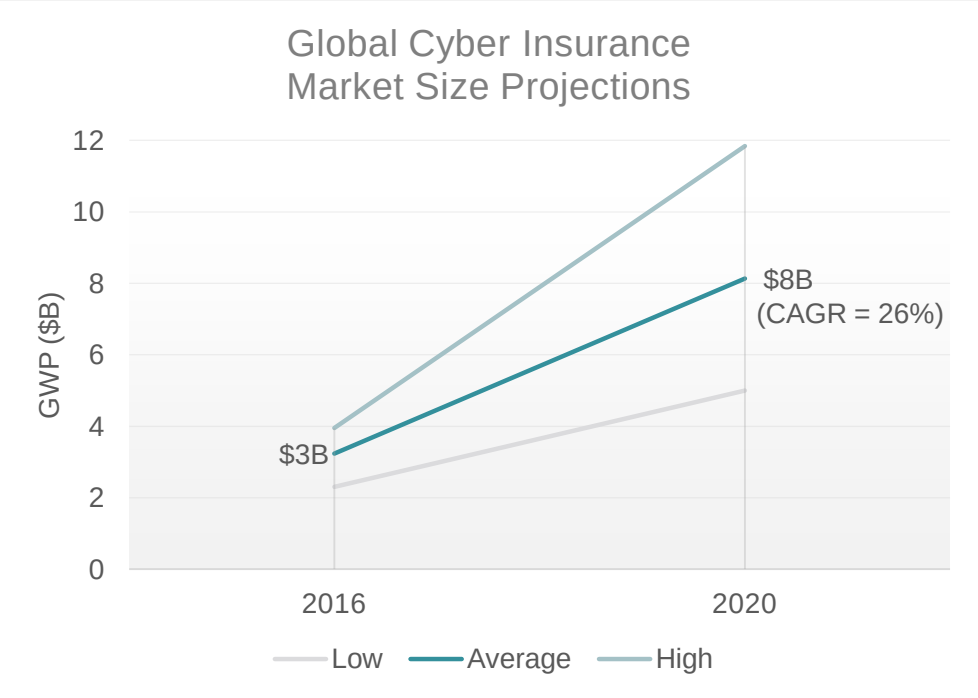
Cyber insurance

18 April 2017

Rory Egan, Cyber Consultant, Munich Re

Munich RE

Cyber insurance – market overview



Taken from multiple sources (March, PwC, Allianz, Fitch, Aon, Advisen, ABI, Allied Market Research, Betterley)

Overview

- ~$3B market increasing to ~$8B by 2020
- US business is 85-90% of global premium
- AIG, Chubb, XL Group have ~45% of US market (source: Fitch) but scores of new entrants in last few years
- Lloyds – 65 syndicates wrote £500m in 2016 (source: Beazley)
- Insurance towers of capacity are approaching $1B

Drivers of growth

- Increasing reliance on technology in business and every day life (e.g. IoT)
- New legislation in EU from 2018 (“GDPR”)
- Greater awareness of risk (and need for protection/insurance) among SMEs, Middle Market and Consumers
- Improved risk modelling allowing insurers to increase their underwriting risk appetite

What is covered?

No such thing as standard cyber policy, but in approximate order of likelihood of cover…

- ***Privacy breaches**:* covers claims relating to expenses incurred in the response to a data breach, including crisis management costs (e.g., IT forensic costs, notification costs and in some cases regulatory fines).
- ***Data and software loss:*** The cost of reconstituting data or software that have been deleted or corrupted.
- ***Cyber extortion**:* covers claims relating to the extra costs incurred in dealing with an infection coming from ransomware and – where legally allowed – the ransom if deemed necessary to pay it.
- ***Network, IT security failure**:* BI insurance, covering an insured's loss of income, operating expenses and often data restoration costs when business operations are interrupted or suspended due to a failure of IT security as a result of malicious attack, including DDoS events.
- ***Network, IT system failure:*** BI insurance, with similar coverage to security failure (above) but when business operations are interrupted or suspended due to failure of IT systems (non-malicious cyber events) and sometimes human error/mishap.
- ***Reputational damage:*** Loss of revenues arising from an increase in customer churn or reduced transaction volumes, which can be directly attributed to the publication of a defined security breach event.
- ***Media liability**:* covers claims such as infringement of intellectual property, copyright/trademark infringement and libel and slander.
- ***Network liability**:* covers damages at a third-party provider as a result of a disruptive event coming from or passing through the insured's system.
- ***Contingent business interruption (CBI)**:* covers the insured's loss of income and operating expenses in case of a disruption at a digital supplier (e.g., a cloud provider) and in some cases also at a conventional utility service (e.g. electricity) provider.
- ***Others occasionally found within standalone cyber policies, or commonly seen in 'mixed' policies:***

  Technology E&O, PI, financial theft and fraud, IP theft, physical asset damage, death and bodily injury, D&O, product liability, environmental damage

Sources: Swiss Re, Cambridge University/RMS