CYBER INSURANCE

Understanding an increasingly complex risk

Getting to grips with insuring your business is a daunting task for any business leader; understanding your exposure to cyberattacks can be even more intimidating. Industry surveys show a major lack of understanding when it comes to determining the adequacy of cybercover, while a large share of firms still do not have any sort of cyberinsurance at all.

---

Top reasons for taking out cyberinsurance
Average share of firms from Germany, the UK and United States that have cybercover

- The cost of a potential breach is high and I would like peace of mind: 41%
- I am concerned about the security of my data: 39%
- I am concerned that customers could make a claim against me: 33%
- New data regulations require that I have protection: 30%
- Cyberpolicies offer additional expertise that I do not have: 28%
- Previous experience of a breach: 25%
- Cyberinsurance is a legal requirement: 25%

---

Percentage of firms with cyberinsurance
An astonishing two thirds of companies still do not have any cover

- Not sure what cyberinsurance is: 4%
- Yes, we have it: 33%
- No plans to take it out: 36%
- Plan to take it out in next 12 months: 25%

---

Top reasons why some firms don’t purchase cyberinsurance

1. Premiums are too expensive
2. Coverage is inadequate based on our exposure
3. Property/casualty policies are sufficient
4. Too many exclusions, restrictions and uninsurable risks
5. Executive management does not see the value

---

Percentage of potential loss to assets covered by insurance
Companies still underinsured for cyber-risks

- Information assets: 15%
- Property, plant and equipment assets: 59%
Types of incidents covered by cyberinsurance
Percentage of companies with the following coverage

86%  External attacks by cybercriminals
84%  Malicious or criminal insiders
43%  System or business process failures
42%  Incidents affecting business partners, vendors of third parties that have access to internal information assets
34%  Human error, mistakes and negligence
33%  Other

Source of most common cyberinsurance claims
Based on claims received by AIG in Europe, Middle East and Africa between 2013 and 2016

Encryption ransomware extortion 16%
Data breach by hackers 14%
Data breach due to employee negligence 8%
Impersonation fraud 7%
Denial-of-service attacks 6%
Physical loss or theft of information assets 6%
Legal/regulatory proceedings based on violation of data privacy regulations 4%
System failure/outage 4%
Business interruption 10%
Other security failures/unauthorised access 10%
Other cyber-extortions 4%
Other virus/malware infections 10%
Other 9%

Cyber coverage provided by insurers
Percentage of companies receiving the following services

Forensics and investigative costs 60%
Notification costs to data breach victims 57%
Replacement of lost or damaged equipment 57%
Employee productivity losses 54%
Communication costs to regulators 52%
Regulatory penalties and fines 48%
Legal defence costs 47%
Third-party liability 45%
Revenue losses 30%
Brand damages 21%
Unsure 28%
Other 21%