Management Protection Package
Cyber Risk

Cyber risks are a real and serious threat to all types and sizes of business, but they're also risks that traditional policies don't address.

Our policy covers:

1. Data Liability
2. Network Security
3. Remediation Costs
4. Cyber Business Interruption

What is covered:

- Claims handling
- 24/7 incident management
- IT Forensics
- Public Relations advice
- Legal advice
- Defence costs, fines & penalties (where legal)
- Loss of data: notification costs, identity & credit monitoring costs, civil liability, data restoration costs
- Cyber extortion
- Cyber business interruption

Statistics:

- Around 52% of businesses think they have cyber cover
  In reality less than 10% actually do
- 60% of small business suffered a cyber-security breach in 2014

Source: HM Government & Marsh UK Cyber Security Report March 2015

News:

- Cyber Security Breaches Survey 2016

Cyber Risk – how different trades can be affected by cyber events

- Almost all businesses use computers and store data, making them vulnerable to cyber risks
- The extent of this vulnerability is different depending on the nature of the business
- Understanding the most common risks to a particular industry can help to quantify the hazard and the potential fall-out of a cyber-event

SCENARIO	CONSEQUENCE	KEY COVERAGES
MANUFACTURING A virus introduced by opening a phishing email or a malicious hacking attack can cause an automated system to fail or corrupt process data, disrupting production.	Down-time and lost revenue with a potential knock on effect on contracts.	IT forensics and data restoration costs to investigate the cause of the disruption and recover the data. Cyber business interruption to pay for lost income.
OFFICE A data liability event triggered by a hacking attack, a lost data device or a malicious employee can lead to customer data being lost, stolen or published.	Breach of privacy legislation, and unhappy customers have a knock on effect on reputation and revenue.	Notification costs, monitoring costs and public relations advice to reassure customers and minimise ongoing costs, legal advice to address privacy legislation and cyber business interruption to recover lost revenue.
RETAIL Customer and financial data can be compromised at the point of sale or a website can be taken offline by a denial of service attack.	Unhappy customers, Reputational damage and lost revenue, as well as breach of privacy legislation.	Notification costs, monitoring costs and public relations advice to reassure customers and minimise ongoing costs, legal advice to address privacy legislation, cyber business interruption to recover lost revenue and IT forensics to resolve the website issues.
HOSPITALITY A virus introduced by opening a phishing email or a malicious hacking attack can compromise customer data or shut down a booking system.	Unhappy customers, reputational damage and privacy breach, plus lost revenue.	Notification costs, monitoring costs and public relations advice to provide redress to customers and reduce consequent costs, legal advice to address privacy legislation, cyber business interruption to counteract lost revenue and IT forensics to resolve the booking system issues.