



MANCHESTER  
UNDERWRITING  
MANAGEMENT

## MUM CYBER INSURANCE

### WHY DO BUSINESSES NEED CYBER COVER?

Cyber-attacks are not just reserved for the corporate giants with the types of incident that we read about in the daily papers. Every business is exposed to some form of indiscriminate cyber risk. Over 875,000 SMEs have declared that they have been affected by a cyber-attack in the last year. With costs from £10,000 up to over £2.5m, enough to put a small to medium sized business in financial trouble. There are many potential consequences, including the cost of getting things rectified, business interruption and third party exposures.

### HOW WOULD YOU:

- Respond to a security or privacy breach? Do you have a plan in place with immediate access to individuals who are experienced at handling cyber events?
- Restore maliciously corrupted or encrypted systems and data?
- Respond to a system disruption? What is the likely impact on your business?
- Deal with any reputational issues arising from a breach?
- Manage communications with the Information Commissioner's Office?
- Manage any civil suits and regulatory actions seeking damages or imposing penalties?

# OUR SOLUTION AND OFFERING

## 1. WEBSITES AND SOCIAL MEDIA

**THREATS INCLUDE:**  
Distributed Denial of Service Attack (DDoS) – where the online service becomes overwhelmed by a volume of traffic from multiple sources and is unable to function.

**CONSEQUENCES INCLUDE:**  
Business interruption and loss of profit.

**INSURANCE PROVIDED BY MUM INCLUDES:**  
Business Interruption Loss – reimbursement of loss of net profit following a deterioration or failure in computer systems including where arising from a DDoS.

## 2. COMMUNICATIONS & MARKETING

**THREATS INCLUDE:**  
Breaches of Privacy and Electronic Communications Regulations – which provide individuals with specific privacy rights in relation to electronic communications such as automated marketing calls, emails and texts.

**CONSEQUENCES INCLUDE:**  
Regulatory investigations, fines and penalties.

**INSURANCE PROVIDED BY MUM INCLUDES:**  
Regulatory Proceedings – defence costs and civil fines and penalties (to the extent that such fines and penalties are insurable at law), in connection with an investigation or regulatory proceeding.

## 3. SALES / ADVISORY SERVICE

**THREATS INCLUDE:**  
Disruption of outsourced services – just as any company is vulnerable to a range of cyber threats, so each of its technology service providers (for example cloud services) is similarly vulnerable and, if affected, will be equally disruptive to the company's business.

**CONSEQUENCES INCLUDE:**  
Reputational harm and consequential loss of customers.

**INSURANCE PROVIDED BY MUM INCLUDES:**  
Reputational Harm – reimbursement of loss of net profit resulting from the termination of current or future customer contracts, where such termination arises from a system security failure including where arising from a ransomware incident or from the loss or theft of data.

## 7. PAYMENTS TO THIRD PARTIES

**THREATS INCLUDE:**  
CEO Fraud – will often occur where an email is sent from a fraudster (posing as the company's CEO or MD) to an employee in a company's finance department. The employee will be instructed to transfer funds to a certain bank account for a specific reason, which the employee will do, only to find that they have sent the funds to the fraudster's account.

**CONSEQUENCES INCLUDE:**  
Financial loss.

**INSURANCE PROVIDED BY MUM INCLUDES:**  
Social Engineering Fraud – provides indemnification arising from fraudulent instructions provided by a third party that misleads an employee and that results in the company's own money, security or other assets being lost.

## 4. PRODUCTION & DELIVERY

**THREATS INCLUDE:**  
Ransomware – an increasingly common form of malicious software that encrypts files and threatens to permanently block access to the victim's data unless a ransom is paid, usually in difficult to trace cryptocurrencies, such as Bitcoins.

**CONSEQUENCES INCLUDE:**  
Costs to reconstruct the data.

**INSURANCE PROVIDED BY MUM INCLUDES:**  
Data Recovery Costs – costs and expenses incurred to restore, replace, repair or regain access to data.

## 6. PAYROLL / HR / ADMINISTRATIVE FUNCTIONS

**THREATS INCLUDE:**  
Malicious insider threat – refers to permanent or temporary employees or contractors who have legitimate access to personal information or commercially sensitive information or the ability to sabotage the company's computer system and who maliciously exploit such access for their own personal gain or cause.

**CONSEQUENCES INCLUDE:**  
Investigation costs.

**INSURANCE PROVIDED BY MUM INCLUDES:**  
Breach Management Expenses – including expenses to investigate the cause and scope of a breach, preserve evidence of any criminal wrongdoing and to end or contain any breach.

## 5. BILLINGS / DEBIT / CREDIT CARDS

**THREATS INCLUDE:**  
PCI loss – where the Payment Card Industry levy assessments in order to recover fraudulent card charges and the costs to reissue compromised cards on behalf of the card issuing financial institution and/or fines and penalties for the responsible merchant's actual or alleged failure to comply with PCI Data Security Standards.

**CONSEQUENCES INCLUDE:**  
PCI assessments and penalties including payment card reissuance costs; administration charges; fraudulent card charges.

**INSURANCE PROVIDED BY MUM INCLUDES:**  
PCI Liability – indemnification against amounts that the company is contractually obliged to pay following receipt of a PCI demand from a payment card brand (Visa, Mastercard etc.), financial institution or payment processor.

Cliff White  
Head of Cyber Insurance

T 020 7933 9364

M 07432 567 035

cliff.white@manchesterunderwriting.com

www.manchesterunderwriting.com

