MANCHESTER UNDERWRITING MANAGEMENT

CYBER BROKER DEMANDS AND NEEDS

WHY MUM

The MUM Cyber product is designed for all types of businesses, from trade through to professional services	Coverage triggers when an Executive Officer discovers or reasonably suspects a cyber-incident	Business Interruption coverage applies to total or partial interruptions of the insured's or an outsourcer's computer system
A personal service with a specialist Cyber underwriter as your point of contact	Underwritten specifically as primary to any other applicable insurance	Extended Indemnity period for Business Interruption losses
An integrated breach management solution to manage, investigate, resolve and recover data from a security breach	Cover for computer system 'betterment' where the loss doesn't exceed that which would have been incurred	Loss mitigation expenses cover includes reimbursement of employee overheads or customer goodwill incentives, which serve to reduce the overall loss
Capacity provided by Munich Re Lloyd's Syndicate 457	No retroactive limitation	Worldwide territorial and jurisdictional limits

Questions to ask your client to educate them on cyber and ascertain what cover might suit them.

IT DEPENDENCY

1. What IT systems do you have within the business? (e.g. website, sales, production, payroll, HR)	
2. For how long can your business operate without access to its IT systems?	
3. What will be the impact on your revenue and reputation if you're unable to operate due to a system outage?	

CASE STUDY

Sector:
Estate Agency

Type of event:
Ransomware

Circumstances:
Company servers and computers encrypted by ransomware and a ransom demand received. Unfortunately, the Company's back-up device was connected to its network and became encrypted, so it was not possible to restore the system.

Outcome:
The insurer paid the ransom and IT consultants were engaged to ensure that the ransomware had been completely removed from the company's systems.

Examples of how MUM Cyber insurance will benefit the policyholder:

a. Provide emergency access to and pay for IT security experts to investigate the cause and scope or end or contain a system security failure or extortion threat.
b. Pay for your loss of net profit arising from computer system interruptions as a consequence of a system security failure.
c. Pay for crisis management expenses incurred to minimise harm to your brand or reputation which is reasonably likely to arise from unfavourable media reports.

DATA HANDLING

1. What sensitive or personal data do you hold on your systems? (employee, customer, credit/debit cards etc.)	
2. What security measures do you have in place to prevent the loss or corruption of this data? (anti-virus, firewalls, intrusion detection software, 24/7 security, CCTV etc.)	
3. What will be the impact on your revenue and reputation if this data is lost, notwithstanding the security measures that you have in place?	

CASE STUDY

Sector:
Accountants

Type of event:
Lost paper files

Circumstances:
The firm lost paper files containing sensitive personal data pertaining to an employment claim.

Outcome:
Over the course of the next 5 days, the firm incurred legal costs in respect of regulatory and notification issues and was fined by the ICO for the privacy breach.

Examples of how MUM Cyber insurance will benefit the policyholder:

a. Indemnify you for defence costs and legal liability arising from a system security failure or privacy breach.
b. Reimburse you for your reduction in net profit which results from the termination of current or future customer contracts.

EMPLOYEES AND INFORMATION SECURITY STANDARDS

1. What access do employees have to the IT systems and sensitive or personal data?	
2. Have your employees been trained in the handling of sensitive or personal data and would they know what to do if they suspected a security or data breach?	
3. Does the business follow any form of information security standard? (e.g. cyber essentials, ISO27001)	

CASE STUDY

Sector:
Utility Company

Type of event:
Employee negligence

Circumstances:
An email was incorrectly addressed and sent to the wrong customer, revealing the original customer's name, address and account details.

Outcome:
The ICO found that a privacy breach had occurred and fined the company, publishing details of the breach on the ICO's enforcement action website. The company undertook retraining of staff regarding privacy and security matters.

Examples of how MUM Cyber insurance will benefit the policyholder:

a. MUM cyber policyholders benefit from 12 months free access to Berea's Cyber AMI product and receipt of a Berea Cyber Safety at Work advice pack:

Cyber AMI
A unique online cyber security self-assessment and education service, designed to help you understand, implement and maintain better working practices to improve your cyber security, without the expense of a consultant. Also work towards, obtain and surpass the UK Government-backed Cyber Essentials scheme, which is considered the benchmark for cyber security in a business of any size.

Cyber Safety At Work
The Cyber Safety At Work advice pack will provide you with resources to inform and educate staff about better cyber practices within the workplace.

SUPPLIERS

1. Do you use any third party suppliers that directly relate to your IT? (e.g. cloud service providers, web-hosting, credit/debit card payment processor systems etc.)	
2. Do you have any rights of recourse against suppliers in the event that their service is interrupted or your data is lost or corrupted whilst in their care?	

CASE STUDY

Sector:
Solicitors

Type of event:
Malware

Circumstances:
The malware infection resulted in the compromise of the firm's practice management system login details.

Outcome:
The security breach was contained and eradicated by engaging external IT consultants and forensics. External legal advice was also required in order to obtain access to the firms third party data centre and regarding regulatory notification issues.

Examples of how MUM Cyber insurance will benefit the policyholder:

a. Reimburse your loss of net profit arising from computer system interruptions as a consequence of a system security failure, including where your computer system is owned, operated or controlled by an outsourcer.
b. Pay for legal advisors to pursue your rights to an indemnity under a written agreement with a third party.

GENERAL DATA PROTECTION REGULATIONS

1. What steps have you taken to prepare for GDPR?	
2. How will you manage notification to the ICO within 72 hours of becoming aware of a data breach? (legally required when there is a likely risk of harm to individuals' rights and freedoms)	
3. How will you manage notification to the affected individuals in the event of a data breach? (legally required when there is a high risk of adversely affecting individuals' rights and freedoms)	

CASE STUDY

Sector:
Video Game Rental

Type of event:
SQL injection attack

Circumstances:
The firm's website was subject to a SQL injection attack in which over 26,000 customer details were accessed.

Outcome:
The ICO fined the firm £60,000 for failure to take appropriate technical measures against the unauthorised or unlawful processing of personal data.
The ICO enforcement manager said:

> "Regardless of your size, if you are a business that handles personal information then data protection laws apply to you."
>
> "If a company is subject to a cyber-attack and we find they haven't taken steps to protect people's personal information in line with the law, they could face a fine from the ICO. And under the new General Data Protection Legislation (GDPR) coming into force next year, those fines could be a lot higher."

Examples of how MUM Cyber insurance will benefit the policyholder:

a. Provide emergency access to and pay for legal advisors to identify and comply with any legal or regulatory obligations.
b. Reimburse you for the costs of notifying regulators and affected individuals regarding any privacy breach, whether such notification is legally required or performed voluntarily.
c. Pay defence costs pertaining to a regulatory investigation as well as fines and penalties issued by the regulator, to the extent that such fines and penalties are legally insurable.

Given what we have discussed, how confident are you that your business can continue uninterrupted and unaffected by a security failure or data breach?

Cliff White
Head of Cyber Insurance
T 020 7933 9364
M 07432 567 035
E cliff.white@manchesterunderwriting.com

Richard Webb
Director
T 01494 781 113
M 07584 685 065
E richard.webb@manchesterunderwriting.com