Barbican PROTECT

Cyber Liability Insurance

Data Security, Privacy and Multimedia Protection

Barbican PROTECT

Cyber Liability Insurance
Data Security, Privacy and Multimedia Protection

What is a Cyber Risk?

Technology is advancing at such an alarming rate and business is more and more reliant on IT systems. Therefore any organisation or business is at risk of a cyber attack through their use of online networks and systems.

Just under half (46%) of all UK businesses identified at least one cyber security breach or attack in the last 12 months. This rises to two-thirds among medium firms (66%) and large firms (68%).

Source: Cyber security breaches survey 2017 – Department of Culture Media & Sport.

The following will provide evidence of how we can all be affected and what impact this can have on daily life;

Any Business or Organisation

- The financial controller receives an email purporting to be from the company Chief Executive requesting that an urgent payment be sent to one the company's regular suppliers, the email adds that the supplier has a new bank account and provides details of it.
- The financial controller suspects nothing is wrong and inadvertently, in the rush to comply with the urgency of the matter, fails to carry out the usual out-of-band authentication check to verify the existence of new bank account with the supplier. £50,000 was paid over.
- Needless to say the email came from criminals not the Chief Exec and the money did not reach the bank account of the genuine supplier.
- Our Cyber Deception Extension would pay out half the amount lost, after deduction of the £25,000 Excess.

Local Haulage Company

- The company's IT manager discovered that files had been uploaded onto the company's servers by an unidentified third party from a 'phishing' e-mail which ultimately corrupted their data
- As a result a breach of services/forensic consultants was required to restore the data contained in the damaged files costing £30,000 and an additional £5,000 for employee overtime both these costs were covered by the Data Recovery section of the Policy.

High Street Accountant

- The accountant discovered that an unauthorised third party had gained access to their servers which contained financial records including those of high profile celebrities
- A message was then sent to the accountant stating the information had been encrypted and a threat that this would be published in the public domain unless a ransom of £25,000 was paid
- The Data Extortion section of the Policy would indemnify the insured for the ransom payment, less the Excess, and additionally would pay for the costs of restoring any data that remained corrupted or encrypted after the attack.

Hotel Chain Owners

- Theft of a senior director's lap top containing sensitive personal data of the hotel's clients and employees whilst their car was parked
- Access to the lap top was protected by a password and the personal data it contained was encrypted
- Although not compelled to under the law as it stood at the time of the incident, the company voluntarily notified The Information Commissioner who investigated the incident and fined the company £10,000 for breaches of the then current data protection legislation.
- The Privacy regulation, defence and penalties section of the policy would pay for the costs of specialist legal assistance in compiling the company's defence to put before the ICO in a hope it would reduce the ultimate fine imposed. Cover would not extend to pay the fine itself, as legally imposed fines are uninsurable at law in the UK.

Estate Agents

- A high street estate agent were advised by their website development and hosting company that a Dedicated Denial of Service (DDoS) attack had occurred via the uploading of spam to their website server, the extent of which meant that it had to be shut down.
- The best resolution was to rebuild the website using a new platform which would be more secure. The insured's current website company had the expertise to carry out the work at a cost of £2,000.
- The Data Recovery section of the Policy paid both the costs of restoring the website, less the Excess, and the £1,500 investigation costs incurred by the appointed loss adjusters.

Marketing Consultants

- Whilst constructing and developing a client's website they used several logos and images similar to those which had been copyrighted by another entity.
- Legal proceedings commenced with the claimant demanding damages in excess of £1m.
- Cover for infringement of copyright is provided under the Multimedia liability section of the Policy.

Barbican PROTECT

Do you require a Data Security, Privacy and Multimedia Protection Policy?

WHAT COVER DO YOU NEED?		IS COVER IN PLACE?					
Potential Risk	**Potential Exposure**	Data security, privacy and multimedia	Data security, privacy and multimedia cover and costs expenses	Data breach costs cover	Information and communication asset rectification costs cover	Data recovery and loss of business income cover	Cyber extortion cover
Do you provide a website?	Breach of intellectual property rights	✓	✓	✓			
	Misleading advertising	✓	✓				
	Libel and slander	✓	✓				
	Unauthorised access	✓		✓			
Do you hold HR/payroll data on your network?	Breach of employees privacy rights	✓	✓				
	Failure to handle, manage, store or de-stroy data correctly	✓	✓				
Do you hold third party data?	Breach of intellectual property rights	✓	✓				
	Failure to handle, manage, store or destroy data correctly	✓	✓	✓			
Do you store sensitive data that is accessible via your web server?	Libel and slander	✓	✓				
	Breach of intellectual property rights or confidentially	✓	✓	✓			
	Potential for that data to be threatened by a hacker - extortion				✓		✓
	Breach of the Data Protection Act	✓	✓				
Do you allow third party access to your network?	Damage to your computer system due to virus or hacking attack.		✓		✓		
	Consequences to your business due to down time, business interruption exposure		✓	✓		✓	
	Potential for that access to be threatened by a hacker - extortion						✓
Do you allow staff to use the internet or e-mail?	Libel and slander	✓	✓				
	Damage to your systems due to virus or hacking	✓	✓		✓	✓	
	Damage to third party systems by forwarding a virus	✓	✓				
	Employees hacking your network	✓			✓	✓	
	Breach of the Data Protection Act	✓	✓				
Do you transact or communicate any business via a website or e-mail?	Damage to your systems due to a virus or hacking attack	✓	✓		✓	✓	
	Lost revenue or assets due to a virus or hacking attack		✓			✓	
Do you hold any customers card or personal details on your network?	Breach of the Data Protection Act	✓	✓				
	Potential for that data to be threatened by a hacker - extortion				✓		✓

Sectors applicable

Tier 1

Manufacturing, Credit Unions, Construction, Restaurants, Utility, Government, Technology Professional, Healthcare/Medical, Property, Professional Services, Legal Services, Education, Sports Clubs/Gyms, Senior Living, Transport

	Limit of Indemnity in the aggregate defence costs inclusive					
Revenue	**£50,000**	**£100,000**	**£250,000**	**£500,000**	**£1,000,000**	**Deductible**
Up to £100,000	£100	£110	£132	£176	£220	£500*/24hr**
£100,101 – £250,000	£140	£150	£180Ā .	£240	£300	£500/24hr
£250,001 – £500,000	£200	£215	£258	£344	£430	£500/24hr
£500,001 – £1,000,000	£300	£325	£390	£520	£650	£1K/24hr
£1,000,001 – £1,500,000	£390	£425	£510	£680	£850	£1K/24hr
£1,500,001 – £2,000,000	£510	£550	£660	£880	£1,100	£1K/24hr
£2,000,001 – £2,500,000	£600	£650	£780	£1,040	£1,300	£2.5K/24hr
£2,500,001 – £3,000,000	£690	£750	£900	£1,200	£1,500	£2.5K/24hr
£3,000,001 – £4,000,000	£900	£975	£1,170	£1,560	£1,950	£2.5K/24hr
£4,000,001 – £5,000,000	£1,070	£1,175	£1,410	£1,880	£2,350	£2.5K/24hr
£5,000,001 – £7,500,000	£1,500	£1,600	£1,920	£2,560	£3,200	£5K/24hr
£7,500,001 – £10,000,000	£1,900	£2,050	£2,460	£3,280	£4,100	£5K/24hr
£10,000,001 – £12,500,000	£2,300	£2,500	£3,000	£4,000	£5,000	£7.5K/24hr
£12,500,001 – £15,000,000	£2,600	£2,800	£3,360	£4,480	£5,600	£7.5K/24hr

Tier 2

Retail, Telecoms Professional, Media Professional, Financial Institution, E-Commerce, Insurance Broker/Company, Hotels, Staffing/Recruitment

	Limit of Indemnity in the aggregate defence costs inclusive					
Revenue	**£50,000**	**£100,000**	**£250,000**	**£500,000**	**£1,000,000**	**Deductible**
Up to £100,000	£175	£193	£231	£308	£385	£1K*/24hr**
£100,101 – £250,000	£245	£263	£315	£420	£525	£1K/24hr
£250,001 – £500,000	£350	£376	£452	£602	£752	£1K/24hr
£500,001 – £1,000,000	£525	£569	£683	£910	£1,137	£2K/24hr
£1,000,001 – £1,500,000	£683	£744	£893	£1,190	£1,487	£2K/24hr
£1,500,001 – £2,000,000	£893	£963	£1,155	£1,540	£1,925	£2K/24hr
£2,000,001 – £2,500,000	£1,050	£1,138	£1,365	£1,820	£2,275	£5K/24hr
£2,500,001 – £3,000,000	£1,208	£1,313	£1,575	£2,100	£2,625	£5K/24hr
£3,000,001 – £4,000,000	£1,575	£1,706	£2,048	£2,730	£3,412	£5K/24hr
£4,000,001 – £5,000,000	£1,873	£2,056	£2,468	£3,290	£4,112	£5K/24hr
£5,000,001 – £7,500,000	£2,625	£2,800	£3,360	£4,480	£5,600	£10K/24hr
£7,500,001 – £10,000,000	£3,325	£3,588	£4,305	£5,740	£7,175	£10K/24hr
£10,000,001 – £12,500,000	£4,025	£4,375	£5,250	£7,000	£8,750	£15K/24hr
£12,500,001 – £15,000,000	£4,550	£4,900	£5,880	£7,840	£9,800	£15K/24hr

Insurance Premium Tax, where applicable, to be added to the premiums shown above.

*Excess each and every claim
** The number of hours that must elapse before the recovery of loss of income can be considered.

STEP 1: COMPLETE BINDING INFORMATION TABLE

Inception date	
Limit of Indemnity	
Premium	
Broker contact details	

STEP 2: PLEASE COMPLETE THE DETAILS BELOW REGARDING THE INSURED/PROPOSER

Name of Insured/Proposer	
Full address of Insured/ Proposer	
Company Number	
Business Description	
Annual turnover/income (for most recent 12 months, or as projected for new businesses)	£
Number of Personal Data records you hold (as defined by the Data Protection Act 1998 or subsequent legislation)	

Refer to:
https://ico.org.uk/media/for-organisations/documents/1549/determining_what_is_personal_data_quick_reference_guide.pdf

STEP 3: PLEASE CONFIRM THAT THE INSURED/PROPOSER AND ITS SUBSIDIARIES

1	Is all personally identifiable and confidential information that is removed from the Insured's premises in any electronic format encrypted? If not, then Unencrypted Portable Media Device Exclusion to apply.	Yes	No
2	Does the Insured regularly update (at least monthly) antivirus software and firewalls in place within their networks? If not, then the proposed insurance will be declined.	Yes	No
3	Does the Insured have a Business Continuity Plan in place that is tested annually, and can the Insured confirm that their systems can be backed up and running within 12 hours of a breach? If not, the BI section is deleted.	Yes	No

4	Is the Insured PCI (Payment Card Industry) compliant?	n/a	Yes	No
5	Has the Insured recently carried out an IT security audit and effected all recommendations and requirements from this? If the Insured has answered 'Yes', please provide a copy of the audit.		Yes	No

6 List the names of your two main third party vendors used for each of the following functions:

Managed security services (e.g. firewall, intrusion detection, anti virus)		
Cloud/Back up/Website hosting		
Internet service providers		
Business critical software providers		
Data processing (e.g. payment processing)		
Point of sale hardware providers		

7	In the past 5 years has the Insured ever had a security or privacy issue that is reasonably likely to have given rise to a loss or claim under this proposed insurance policy had it been in force? If 'Yes', please refer to Underwriters providing full details of the loss or claim.	Yes	No

Please read the following carefully before signing and dating the Declaration

It is essential that every Insured or Proposer when seeking a quotation to take out or renew any insurance makes a fair representation of the risk they are seeking to insure. The obligation to provide this information continues up until the time that there is a completed contract of insurance. Failure to do so may have serious consequences for coverage under the contract of insurance. If you have any doubt as to what constitutes a fair presentation please do not hesitate to ask for advice from your insurance advisor. If there is anything else the Insurers should know in order for this to be a fair presentation of the risk, please provide such information separately.

Your personal data may be processed and held by us in our capacity as data controllers in order for us to write and administer your policy and to assist in the claims handling process in accordance with applicable data protection laws. To read our data privacy policy in full and for more information about your data protection rights, please visit our website at: https://www.barbicanprotect.com/cookies-privacy-policy/.

STEP 4: COMPLETE THE DECLARATION

We hereby declare that to the best of our knowledge and belief the foregoing particulars and statements represent a fair presentation of the risk we are seeking to insure.

We hereby undertake to declare any material alterations or amendments to the foregoing particulars and statements which occur prior to the commencement of the contract of insurance.

STEP 5: PLEASE E-MAIL THE COMPLETED FORM TO: quotes@barbicanprotect.com

Underwriters reserve the right to review each application to determine whether a quotation will be provided. Completion of this proposal does not commit Underwriters to provide cover either at the premiums and terms illustrated in this proposal, or at all.

Signed on behalf of the Insured

Print name

Position held

Date

Cyber Deception Extension

We can now provide an optional extension to our cyber liability coverage to include a cyber deception component.

The extension applies in cases where the insured has been intentionally misled to transfer their own funds or goods to a third party under false pretences as part of a cyber-related deception. It also applies to instances where funds have been stolen following an unauthorised intrusion or breach of the insured's computer network

Cover is provided up to £100,000 in the aggregate which forms part of the overall aggregate policy limit of indemnity and will be subject to a deducible of £25,000 for each Cyber Deception Event. An additional premium of £450 + Insurance Premium Tax will be charged for this extension. Acceptance of cover is subject to prior satisfactory completion of the Cyber Deception Questionnaire.

Cyber Deception Questionnaire

Do you always implement **out-of-band authentication*** procedures with respect to:

- Customer/client/supplier instructions to direct funds, goods or services to a third party recipient; **AND**
- Transactions or instructions where customer/client/supplier account details vary from the account information held on record; **AND**
- Non-standard requests made by **senior management**** for the transfer of funds, goods or services

☐ N/A ☐ Yes ☐ No

If **'No'** to the above, do you implement **out-of-band authentication*** procedures when the transaction value of funds, goods or services is above £20,000?

☐ Yes ☐ No

*** out-of-band authentication** means verifying with the requestor of a transfer, payment or delivery of funds, goods or services, the authenticity/validity of the request, via a method other than the original means of that request.

For example if the insured get an email, they verify by calling their usual contact number. If they get a call, they check by letter or email; a different method from that by which they were contacted.

****senior management** means 1) past, present and future duly elected or appointed director, officer, trustee or governor of a corporation, management committee member of a joint venture and member of the management board of a limited liability company or equivalent position including a de facto director, officer, trustee, governor, management committee member or member of the management board of such entities; and 2) past, present and future General Counsel and Risk Manager (or equivalent position), of the insured.

Signed _____ **Dated** _____