What are cyber risks?

Liberty Specialty Markets

We Insure. You Prosper.

What are cyber risks?

Cyber risks include a range of first and third party exposures relating to the use of information technology (IT). In addition, liability arising out of loss of data (whether electronic or otherwise) has also been specifically incorporated into some policies.

Examples of the type of cover that Liberty can offer (subject in each case to underwriting and to the agreed terms of each policy) are:

First party exposures

- **Loss or damage to digital assets**
  If you suffer loss or damage to data or software programmes, we pay costs incurred by you in restoring, updating, recreating or replacing these to the same condition they were in prior to the loss or damage. Uniquely, we will also consider insuring digital assets for a pre-agreed value if their recreation does not re-establish your financial position pre-loss.

- **Non-physical business interruption and extra expense**
  If you suffer any interruption, degradation in service or failure of your network, we pay for your income lost as a result of this, as well as interruption expenses incurred in mitigating and investigating the loss.

- **Cyber extortion**
  If someone tries to extort money out of you by threatening to damage or restrict your network, to release data that they have obtained from your network to cause damage to you, or to communicate with your customer base under false pretenses to obtain personal information, we handle the extortion demand and pay necessary extortion monies rather than allowing them to follow through with their threats and cause you further loss.

- **Reputational harm**
  If, as a result of a data protection breach being reported (whether factually correct or not), you suffer damage to your reputation that results in a loss of income, through, for example, loss of customers, we cover this loss of income as well as any increased costs of working and PR expenses. Although there are standalone products in the market for reputation, the fact that this cover may be incorporated within the cyber suite is a key differentiator for Liberty's product.

  Cover for first party policies depends on the loss being caused by an insured cause of loss. These can include not only computer crime and computer attacks by third parties, but also accidental damage or destruction and administrative or operational mistakes by employees and third party providers.

Third party exposures

- **Security and privacy liability**
  If you suffer a security breach on your network, transmit any malicious code, or if you breach any third party or employee privacy rights or confidentiality (not necessarily through the use of IT), we pay for your investigation and defense costs, as well as any civil damages. In some countries class actions are becoming more frequent and expensive.

  Please note our cover is not limited to liability to customers or clients only, but may include other third parties, such as the payment card industry for card reissuance, fraud and PCI assessment charges.

- **Privacy regulation defence**
  If you are also investigated by any regulator as a result of the above, we pay for your investigation and defence costs, as well as any awards and fines where insurable. In a majority of countries, responsibility is on the data owner, rather than any data processor you may outsource to.

- **Customer care and reputational expenses**
  Notification expenses – if there is a legal or regulatory requirement for you to notify any individuals of a security or privacy breach, we pay for the legal, postage and advertising expenses involved in this. The number of individuals affected can often run into the millions and under the Cyber Suite policy there is, for the vast majority of cases, no cap on the number of notifications that will be paid for under the policy, subject to the aggregate monetary limit of insurance purchased.

  Privacy assistance expenses – we assist those individuals whose privacy has been breached: for example by providing credit monitoring services and/or identity theft assistance.

  Crisis management expenses – we pay costs incurred by you to protect or re-establish your reputation or public image (for example by paying for PR) to the extent that it is likely to be damaged, or has been damaged, by a privacy and/or security breach.

- **Multi-media liability**
  If you infringe a third party's intellectual property rights (other than patents – cover can be arranged for this separately through our Intellectual Property policy), defame them, breach their privacy or commit any negligence in the publication of any content in electronic or print media, we pay for your investigation and defence costs, as well as any civil damages.

- **Available extensions to cover**
  - PCI fines and penalties
  - Up to 2 years prior acts
  - Dependent business income loss
  - Computer crime
  - Network integrity reputational harm
  - Incidental tech and miscellaneous E&O
  - Intellectual property value indemnification following a cyber attack
  - Property damage/BI as a result of a cyber event

The total direct loss from a data breach per record in the UK in 2014 therefore totaled $158

These are the costs for just one record. When hundreds, thousands or millions of records have been breached, the cost accumulates substantially and can threaten the continued existence of a company, often running into the millions.

What are some of the technical differentiators on the cyber suite?

Wider insured causes of loss for damage to digital assets and non-physical business interruption and extra expense modules

Whilst many cyber policies offer cover for damage to digital assets and non-physical business interruption and extra expense, the vast majority will only trigger this cover if caused by computer crime and computer attacks e.g. if the damage or network interruption is caused by a hacker or malicious employee. Whilst we also include this as an insured cause of loss, we also cover damage to digital assets and network interruption losses caused by 'accidental damage or destruction' and 'administrative or operational mistakes'. Many instances of network interruption and system damage are caused by these latter two scenarios, as opposed to hack/crime.

Voluntary notification

Liberty Specialty Markets' definition of "notification expense" includes a provision to allow cover for the notification of customers even when the insured is not legally obligated to do so, but where this may mitigate or avoid a claim. This is particularly important where there is uncertainty surrounding the insured's legal obligations or where the insured holds the data of individuals who are resident outside such jurisdictions where notification is mandatory.

Liberty cyber assessment – Liberty uses contracted specialists in cyber risk assessment to appraise the information security and data privacy posture of our insureds, using key performance indicators to evaluate the appropriateness of measures in place and against best practice benchmarks, and ultimately providing an invaluable roadmap for improved information security and network availability for our insureds.

Reputational cover

As evidenced in studies by the Ponemon Institute, it is often the indirect costs of a data breach that harm a business the most; costs such as customer churn, loss of confidence and reputational damage affecting supplier relations. The vast majority of policies have little or nothing to offer when it comes to covering these and whilst they might cover the PR costs as Liberty's also does, they will not cover the loss of business income arising out of loss of customers who have lost faith in the insured due to their damaged reputation following the breach. Liberty's Cyber Suite policy offers a reputational harm section that operates in a similar manner to business interruption cover. It covers loss of income attributable to adverse perception of the company. This calculation will be made by comparing provisional projections for the insured net profit versus actual profit during the reputational indemnity period, taking into account any other temporary factors not related to the data breach that could have affected the insured's bottom line. The length of the reputational indemnity period is scheduled in.

Cyber terrorism

The majority of cyber policies utilise broad exclusions for war and terrorism inherited from property policies. Most market terrorism exclusions would by definition encompass hacktivist groups on the basis that their acts are committed for 'political or ideological' reasons, as well as more recognised terrorist organisations who carry out hacking attacks. Liberty's Cyber Suite policy has a write back for terrorism activities when conducted electronically or otherwise that are directed towards the destruction, disruption, or subversion of communication and information systems, infrastructure, computers, the internet, telecommunications or electronic networks and/or its content thereof or sabotage and/or threat there from.

Design/architecture exclusion

Most cyber policies exclude claims or losses arising out of errors in the design, architecture or configuration of the insured's systems in order to avoid covering errors that were inherent in those systems. Liberty's policy also has this exclusion but it will only apply to the 'damage to digital assets' and 'non-physical business interruption and extra expense' modules and furthermore will only be applied to these modules when the loss arises out of undelivered programmes (programmes, applications or software including updates where the development stage has not been finalised or they are not ready for operational use because they have not yet passed all test runs or where they have not been proven successful in a live environment for a continuous period of 12 months).

Insured's network definition

When an ever increasing proportion of businesses are outsourcing parts of their IT network to third parties, cyber policies are seeking to adapt to cover these networks when hosted by cloud providers and other IT services companies. Liberty Cyber Suite policy's definition of insured's network automatically includes networks operated by third party providers for the insured. Whereas a few other insurers may offer this type of cover (by no means all), they often sublimit heavily; this is not Liberty's standard practice.

Definition of multimedia activities

Multimedia coverage is becoming increasingly common amongst cyber policies; however often this is limited to electronic publications, such as websites and blogs. Liberty's Cyber Suite policy goes further by also offering coverage for print publications. This makes it a useful addition of cover to those businesses that can't justify spend on a standalone media policy.

Cover for emotional distress or mental anguish

Many cyber policies will have an absolute bodily injury exclusion. It is however important to cover the emotional distress and mental anguish element of a claim given the framing of many lawsuits and class actions where plaintiff lawyers will look to try and include this within the damages sought. This is why Liberty has a write-back within their bodily injury exclusion for emotional distress or mental anguish.

Innocent insured provision

Liberty's Cyber Suite policy includes a broad innocent insured provision. Cover will not be avoidable or otherwise prejudiced because of breach of the notification condition or the dishonesty of the C-suite exclusion in respect of innocent insureds who were not responsible for the breached condition or who did not personally commit or have knowledge of the dishonest act.

No sub-limits!

Liberty is able to offer each module of coverage up to the full policy aggregate limit. Other insurers typically look to sub-limit network interruption, regulatory fines and penalties and customer care and reputational expenses.

PCI assessment costs

PCI assessment costs - card reissuance costs, operations reimbursement costs, fraud reimbursement - are covered explicitly under the definition of liability expenses in Cyber Suite policy rather than by endorsement on request.

This is a summary of coverage advantages only and full language used is contained in the Cyber Suite policy. The cover offered to any particular insured depends on underwriting, and the availability of coverage in the event of a claim will depend on the particular terms and conditions contained in the insured's actual policy.

Cyber risks highlighted

During the integration of its systems with those of a newly acquired company, a rail operator suffered more than a year of train delays, lost freight and disruptions to crew schedules after one of its dispatchers accidentally input incorrect data into the customer logistics software system. This cost the company over £70m in lost business income and £50m in expenses on paying overtime to workers and fixing the system.

A healthcare reimbursement claims processing company mailed brochures to 260,000 patients with their social security numbers printed on the address labels. As a result of this error it agreed to pay $250k, and to make improvements to its systems so that patient ID numbers could be processed instead of social security numbers, to carry out a full audit of its mailing activities and to provide privacy training to its employees.

A computer server that contained personal information and healthcare details for almost a million of its customers was stolen from an insurance company. A man has been accused of the theft and of trying to extort $208k from the company by threatening to release the data on the internet.

A luxury hotel chain had its systems broken into by hackers who, over a three-month period, stole the credit card details of more than 700 of its guests. Losses through credit card fraud were estimated by the local police to be in the hundreds of thousands of dollars, with each loss averaging around $2k – $3k.

A UK travel advisory website has been threatened by a group defamation action from more than 400 establishments for publishing reviews that it claims are 'unbiased'. These reviews, written by members of the public, include comments on hotels, as well as other destinations and venues. Reviews have included statements such as 'I would not let my dog eat from this disgusting place' and 'A burger with salad and fries turned out to be cardboard, straw and some dry green stuff'.

A leading drug store chain, whose staff were dumping pharmaceutical bottles and prescription information into publicly accessible waste receptacles near its stores, has been fined $1m for violating the US Health Insurance Portability and Accountability Act.

Employees of a US school district left webcams activated on laptops that it issued to 2,300 of its high school students. The cameras captured around 56,000 images over a period of 2 years, with one student in particular being photographed 400 times in a two-week period. Settlements to students, totaling $610k, ranged from $10k to $175k.

A firm of accountants lost the personal records of 77,000 former and current public employees of one of its clients. As a result it agreed to pay for identity theft protection and either credit monitoring or a credit freeze, and to reimburse the victims for any losses incurred by them as a result of ID theft. It also incurred around $100k in notifying affected individuals.

Who should be buying this coverage?

All companies have some exposure to cyber risks to one degree or another. Anyone who has data on third parties or employees should consider their exposure and, the more voluminous and sensitive the PII (Personally Identifiable Information), the greater the potential liability to third parties or employees.

Depending on the local regulatory and legal regime, the civil damages, fines (not insurable by law in every case), customer notification and credit monitoring costs can be considerable. More jurisdictions are starting to impose a mandatory legal obligation to notify each individual whose data has been breached and, even where this is not the case, there can be a requirement either under contract or in relation to certain industry sectors. Insurance coverage can often be adjusted to respond to voluntary notification where it is not required by law. An insured with customers in a number of European countries or various states in the US may have a complex legal landscape to deal with following a breach.

In terms of the first party losses, such as loss of income through business interruption arising out of network failure, any company with online sales has a clear exposure, although even companies without this can be left unable to trade effectively when they have a failure of the critical applications within their network. If staff are unable to access sales/marketing lists, customer relationship management systems and supply chain related procurement systems, work can very quickly grind to a halt, resulting in a sharp drop in profits. Networks often control buildings, factories and warehouses and failure can disrupt manufacturing.

Do I already have some cover for loss of data under my other insurance policies?

Professional Indemnity (PI)

If you are a 'professional' and have a PI policy, there may be some third party coverage for loss of data, but usually only if it arises in the ordinary course of your professional services. It is debatable if this coverage would respond in many instances. For example, if data was taken by a hacker from your servers, which were held offsite on a server farm on a weekend outside business hours, is this in the 'ordinary course of professional services'? There are many cases of expensive litigation in this area in the US presently and it is far better to buy a specifically tailored policy, than to rely on contingent coverage that is not tailored and may leave you with an uninsured loss.

A PI policy will also not usually cover claims made against the insured by its employees and will also be unlikely to cover malicious or unauthorised use of the Insured's own network to damage, misuse or destroy its clients' data or to cause a denial of service attack. Computer virus transmission is usually excluded and cover can sometimes be restricted to claims made by a client of the insured, and would exclude regulatory investigations. Liberty's Cyber Suite policy also provides further customer care and reputational expenses that are not covered under a standard PI policy and which often form the bulk of any costs arising from a privacy breach. Finally, there is usually no cover given in PI policies for first party losses such as loss of business income, damage to digital assets, cyber extortion or reputational damage.

General Liability (GL)

A GL policy will only cover bodily injury and property damage losses and, as data is deemed by the courts to be an intangible form of property, no coverage would usually be provided for breaches of privacy. Although attempts have been made to claim that a 'hack' is 'trespass' under a GL policy, this argument has met with limited success.

Property

Property insurance will typically only cover damage to tangible property. As explained above, data is deemed by the courts to be an intangible form of property, so no coverage would usually be provided for damage to data. Also, whilst you may have coverage for business interruption arising out of material damage, you will not usually have cover for business interruption arising out of non-material damage to your network. Computer viruses and network exposures are typically excluded specifically.

Computer all risks

This insurance covers you for costs involved in repairing damaged hardware (tangible property) and would not respond to claims for lost data that are covered under the Cyber Suite policy.

Why choose Liberty?

- Market-leading specialist underwriting team with business written out of our global office network
- Experienced and specialist claims team who deliver on their promise to pay valid claims
- Underwriting underpinned by excellent financial security, providing client with added protection and reassurance
- Technical underwriting knowledge with experience in helping brokers, CEO's, CIO's, etc. to tailor and bespoke appropriate cover for a business

How much does it cost?

- Our minimum premiums on transactional business are £2,000, €2,500 or $3,000
- Lower premiums may be considered for scheme/binder opportunities

What limit can I buy from Liberty?

- We can quote up to £10m, €15m or $15m either 100% or as co-insurance
- We can write primary or excess layers

What do we need to get a quotation?

In the infancy of cyber insurance many Insurers insisted on a survey being carried out, often paid for by the insured up front. This is usually not required nowadays for the more straightforward risks and a quotation can be obtained simply by completing the Cyber Suite policy proposal form. Please contact a member of the cyber liability team for a copy of this.

About Liberty

Liberty Mutual Insurance Group (LMIG), founded in 1912, is a Boston based diversified insurer with operations in 30 countries and economies around the world. Liberty Specialty Markets, part of LMIG offers specialty and commercial insurance and reinsurance products across key UK, European, Middle East, US and other international locations.

We provide underwriting expertise in intellectual property in addition to our offering of cyber liability insurance. For a full range of products, please visit: libertyspecialtymarkets.com

Liberty Mutual Insurance Group

$121.7bn Consolidated assets

$37.6bn Annual consolidated revenue

over **50,000** employees

over **800** offices worldwide

5th largest property & casualty insurer in US

73rd on US Fortune 100 list

Standard & Poor's rating 'A' (Strong)

Contact us

For more information, please contact a member of our team:

Matthew Hogg ACII
Underwriting Manager
T: +44 (0)20 3758 0368
M: +44 (0)7825 953 918
E: matthew.hogg@libertyglobalgroup.com

Phillipa Kelly ACII
Underwriter
T: +44 (0)20 3758 0384
M: +44 (0)7890 627 078
E: phillipa.kelly@libertyglobalgroup.com

Helen Gemmell
Underwriter
T: +44 (0)20 3758 1441
E: helen.gemmell@libertyglobalgroup.com

Roland Heinesch
Underwriter
T: +44 (0)20 3758 0388
M: +44 (0)7890 627 079
E: roland.heinesch@libertyglobalgroup.com

Camilla Walker
Assistant Underwriter
T: +44 (0)20 3758 0389
E: camilla.walker@libertyglobalgroup.com

Liberty Specialty Markets

libertyspecialtymarkets.com

CR405-02-17