Cyber Data Breach & Liability Quotation

Data **breach** insurance and **cyber liability** insurance helps **cover** the costs of a data security **breach** for things like identity protection solutions, public relations, legal fees, **liability** and more depending on the coverage you choose.

1st Party losses (your own loss)	
❖ Breach/forensic/investigation costs ❖ Cyber ransom losses ❖ Cyber-attack losses ❖ Data recovery costs ❖ Human Error ❖ Business interruption Losses (3months) ❖ Reputation protection ❖ Key person cover ❖ System failure	❖ As selected* any one claim and in the aggregate any one period
3rd Party losses (claims made against you)	
❖ Privacy liability ❖ Privacy investigations ❖ GDPR investigations ❖ PCI liability ❖ Online liability ❖ Network security	❖ As selected* any one claim and in the aggregate any one period
Financial Fraud & Crime	
❖ Electronic theft ❖ Social engineering ❖ Telephone fraud ❖ Client social engineering fraud ❖ Fraudulent use of your identity	❖ As selected* any one period
Optional Extensions- not covered	
❖ Dependent business interruption	Dependent business interruption **Not covered, for example** if Amazon website went down this could have an impact to your business and needs to be extended
❖ Property damage	Physical destruction of computer equipment due to a virus/hack
❖ Operational error **Business Interruption only**	Loss of income due to human error (unplugging a server)
❖ **ADDITIONAL INCREASED COST OF WORKING**	ADDITIONAL INCREASED COST OF WORKING allows you to extend the existing business interruption cover to go beyond the economical limit (spend a £1 to save a £1) – if an online retailer suffered a loss and they needed to spend more/provide vouchers to keep customers this is required.

*alternative limits are available

Extensions	
Wide definition of cyber trigger	Future proofed wording including unknown threats
Cyber exposure impact calculator	www.hiscoxgroup.com/cyberexposurecalculator
Directors personal cyber liability	10% of indemnity limit
Cyber clear academy for all staff	Free online training
Betterment of software	Up £25,000 or 10% of the loss
Key person replacement cover following a cyber event	Replacement senior member of staff
Extended event clause (retroactive date of cover)	None – on a discovered only basis
Control Risks	Cyber response team provides crisis management advisory support, technical forensics expertise and investigations capability to guide and support you.
Pinsent Masons	Specialist cyber team that will coordinate and project manage cyber events
Hill & Knowltons	With over 85 offices in more than 45 countries and nearly 90 years' experience, Hill and Knowlton's world-class teams of trusted advisors/

- Access to the best experts in the business
- Future proofed product
- Breadth of cover is the widest available
- Simple to understand policy
- Hiscox CyberClear Academy
- Online cyber-attack financial impact calculator
- Hiscox have been underwriting cyber insurance since 1999 – over £1m customers in that time and 5,000 claims

Market review

We have undertaken a market review and have provided you with our recommended programme. There are many cyber products available and many are not, in our opinion, fit for purpose. We have provided you below with 3 options:

Policy enhancements/warranties/limitations
Market leading cover – we provide market-leading cover that standard insurance policies do not include: ✓ **Future proofing +** - One of the four policy triggers is Cyber-attack which is defined as 'any digital attack designed to disrupt access to or the operation of a computer system ***How will it benefit?*** *You can have comfort knowing that your cyber policy is future proofed and will not only respond to attacks known in the current times, but an attack which could be developed in the future which is designed to disrupt their system.* ✓ **Nil excess** for all losses related to a breach+ Notifying Hiscox within 72 hours means the whole excess will be waived for losses related to the breach ***How will it benefit?*** *Hiscox will waive the excess if there is good practice and fostering good culture within the business. Other insurers typically only waive the excess for breach costs, we are doing it for all losses related to a breach* ✓ ***Full GDPR coverage+*** *Full GDPR coverage for data breaches, but also alleged breaches of the regulation.* ***How will it benefit?*** *Not all regulatory actions commence due to a data breach, there could be alleged breaches of GDPR which result in a regulatory investigation and it this is particularly pertinent for clients that hold significant amounts of personal data.* ✓ ***CyberClear Academy+*** *– a GCHQ certified computer based training platform for all companies under 10M in revenue. We can look at companies above this threshold on an adhoc basis. If 80% of staff complete the training, we'll reduce the excess by £2,500 in the event of a claim – most policies we have for clients under 10M revenue have an excess of £2,500 anyway, so basically nil excess* ✓ **Directors' personal cover** - Directors who incur personal loss are covered as standard for all cover taken up by the main insured. ***How will it benefit?*** *Directors own cyber losses, not just the company itself e.g. directors' transferring personal funds to a hacker or having their family photos held to ransom on their personal laptop* ✓ **Betterment / repeat event mitigation -** Express cover to upgrade existing kit or bring in consultants to improve IT security in the event of an incident. ***How will it benefit?*** *We can upgrade their existing kit or provide consultants to advise best practice in order to prevent reoccurrence of an incident* **Key person cover** - Costs to bring a third party in to the business to temporarily replace the person within the insured business if they are caught up dealing with the cyber incident or; manage the cyber incident internally. ***How will it benefit?*** *If there is an incident, there are likely to be very senior individuals spending a lot of time dealing with it, with this element of cover, they can go back to doing what they do best – running their business – and leave it up to someone else or bring someone in to cover their position for the time the incident lasts*

- ✓ **24/7/365 hotline – Insurers** provide a 24/7/365 response

  How will it benefit? *Would the MD / CEO know who to contact if something like this happens? Given the data held on individuals, they also need to be mindful of the 72-hour reporting requirements under GDPR. Would they know how to do this and investigate the breach within 72 hours* ***and*** *draft an appropriate response to the regulator without assistance?*

- ✓ **No retroactive date** – most policies provide cover from the date you purchase. But 80% of hacks/viruses are sit dormant in your system for 260 days on average

  How will it benefit? *No need to prove when the virus first entered your system.*

- ✓ **Financial crime/fraud** – no second line of defence/system control clause

  How will it benefit*? Most insurers have a stipulated process of check to invoke crime cover. Under our policy this is not required*

- ✓ **Online cyber-financial impact calculator** – calculate the true impact of a cyber incident to your business today

- ✓ **Specialist risk management** access to forensic teams, PR agencies and media lawyers

The above can exclude financial crime or have lower indemnity limits and premiums will reduce – we do not however recommend this as this is a vital cover. We have highlighted the major difference in the policy quotations and the full insurer schedule and wording should be read.

Conditions

Please refer to policy schedule and statement of fact for full policy terms and conditions