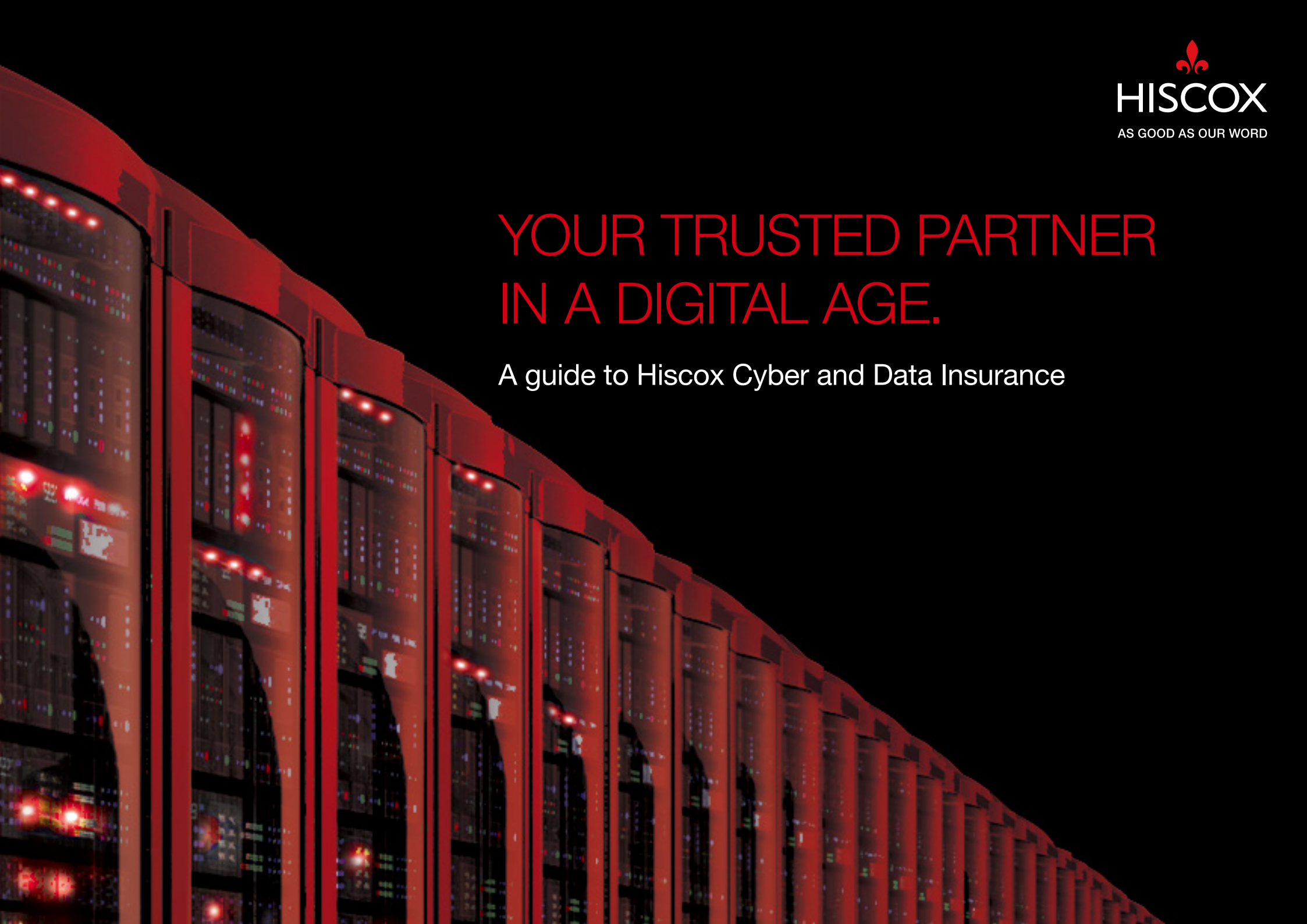


HISCOX

AS GOOD AS OUR WORD

YOUR TRUSTED PARTNER IN A DIGITAL AGE.

A guide to Hiscox Cyber and Data Insurance

THE CYBER AND DATA RISK TO YOUR BUSINESS

This interactive guide will help you find out more about the potential cyber and data risks to your business, the insurance protection available, as well as some real examples of insurance claims and answers to your most frequently asked questions.

Is your business at risk?

Your business could be vulnerable to a data breach or loss of vital business services if you:

- hold sensitive customer details such as names and addresses or banking information;
- are reliant on computer systems to conduct their business;
- have a website;
- are subject to a payment card industry (PCI) merchant services agreement.

Who is this product for?

Our appetite for Hiscox Cyber and Data insurance extends beyond our core industry specialisms and we will actively consider businesses operating in the following sectors:

- accountancy
- advertising and marketing
- construction
- consultancy
- education
- hospitality
- hotels
- law
- manufacturing
- media
- publishing
- recruitment
- retail
- technology
- telecoms
- transport
- restaurants.

Why choose Hiscox?

A trusted partner in the event of a claim
Insurance alone is not enough to deal with these new and evolving risks. So Hiscox will not just pay out when you suffer a loss but will also provide you with access to a team of experts who will actively work with you to minimise your loss and the possible damage to your business.

No complicated modules
Our simple to understand policy provides comprehensive cover so clients know what they are buying and can be confident they will be covered in the event of a loss.

Specialist underwriting expertise
We have been providing cyber and data insurance for 14 years, so we understand the changing risks that clients face and have evolved our product to protect them.

Worldwide network of privacy lawyers and technical specialists
Who will offer expert support and guidance in the event of a claim.

Free access to Hiscox eRiskHub
We give clients access to tools and resources to help them stay up to date with evolving risks, understand their exposure and establish a response plan.

PROTECT YOUR BUSINESS

We offer comprehensive protection for your computer systems and data (electronic or non-electronic), all available in a single insurance policy.

Costs your business may incur as a result of an incident

Breach costs
We offer practical support in the event of a data breach (electronic or otherwise) including forensic investigations, legal advice, notifying customers or regulators, and offering support such as credit monitoring to affected customers

Crisis containment
In the event of a data breach, prompt, confident communication is critical to help minimise the damage to a company's reputation. We include crisis containment cover with a leading public relations firm who can provide expert support, from developing communication strategies to running a 24/7 crisis press office.

Cyber business interruption
We will provide compensation for loss of income, including where caused by damage to your reputation, if a hacker targets your systems and prevents your business from earning revenue.

Cyber extortion
We will protect you if a hacker tries to hold your business to ransom with any final ransom paid, as well as the services of a leading risk consultancy firm to help manage the situation.

Hacker damage
We will reimburse you for the costs of repair, restoration or replacement if a hacker causes damage to your websites, programs or electronic data.

Amounts you may be liable to pay to other parties

Privacy protection
We will pay to defend and settle claims made against you for failing to keep customers' personal data secure. We will also pay the costs associated with regulatory investigations and settle civil penalties levied by regulators where allowed.

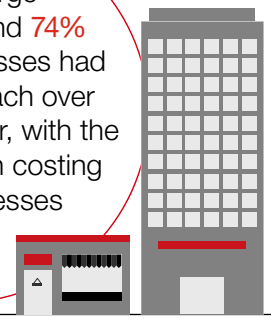
Multimedia liability
The policy includes protection if you mistakenly infringe someone's copyright by using a picture online for example, or inadvertently libel a third-party in an email or other electronic communication.

Additional cover options for your Hiscox policy

Cyber crime
We will cover direct financial loss following an external hack into your company's computer network. This could be theft of money, property, or your digital assets.

Telephone hacking
We will pay the costs of unauthorised telephone calls made by an external hacker following a breach of your computer network; includes traditional fixed-line telephony systems, as well as online systems (VoiP, Skype, etc).

90% of large businesses and 74% of small businesses had a security breach over the previous year, with the average breach costing small businesses £75k.*



*According to the 2015 Information Security Breaches Survey,

WHAT HAPPENS IN THE EVENT OF A BREACH

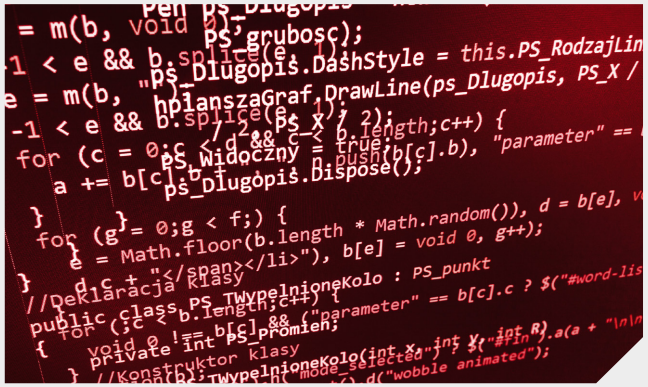
Data breaches are becoming increasingly common, so it's important to consider how you would react rapidly to enable business continuity and protect your business against reputational damage.

OUR INSURANCE IN ACTION

We have dealt successfully with many cyber and data related claims. From a client held to ransom by a Russian hacker, to a customer being tipped off by 'white hat hackers' that their information was for sale on the dark web, here are some recent examples.

The technology business and malware

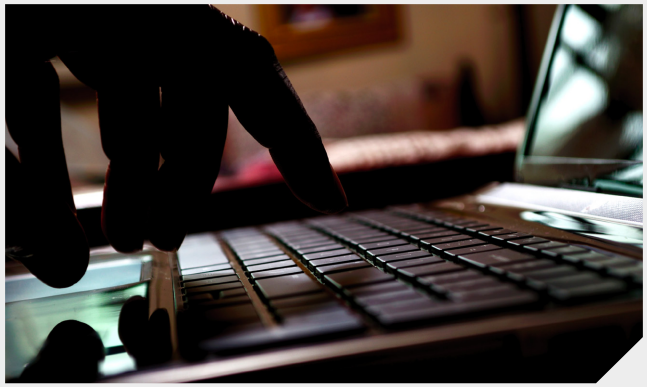
Cost covered by Hiscox: £250k



Our client was contacted by a government agency and advised that government security services had detected an intrusion on its systems. Our IT forensic experts were deployed to investigate and assess the extent to which the network had been compromised. A significant amount of malware was discovered on our client's servers so a containment plan was executed to remove all malware. Our client was also able to take legal and PR advice under their insurance cover to help them decide how and when to communicate this incident to their clients.

The optician held to ransom

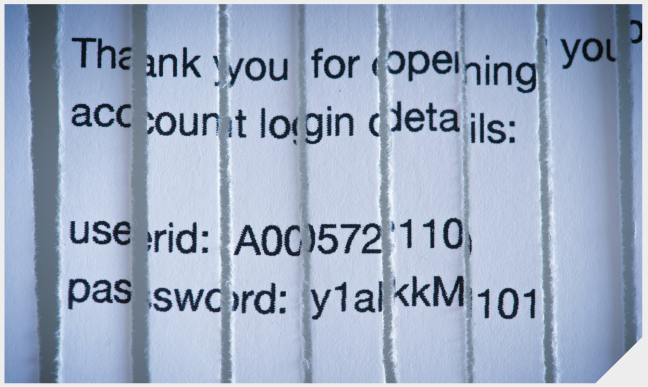
Cost covered by Hiscox: £60k



An employee from a chain of opticians – received an email to say that she had been caught speeding and clicked the button which offered to show a photograph of her being caught in the act. Shortly afterwards our client received an email from someone in Russia to say that they had infected their systems with the Cryptolocker virus and that all files on its servers were encrypted. The encrypted files included patient records and software used to run the business. The Russians were asking for £400 in Bitcoins for the decryption key. We approved the client's payment of the ransom. Unfortunately this only recovered 90% of the files and they needed an IT contractor to help them recover the remainder. Their insurance policy covered this business interruption as well as the costs of being unable to trade for a couple of days and not being fully up-to-speed for a couple of weeks.

The publisher's lost passwords

Cost covered by Hiscox: £10k



Contacted by a 'white hat hacker', our client was told that user names and passwords for two of its websites had been stolen. We called in IT forensic experts to investigate, who confirmed there had been a hack and set about plugging the security breach. Legal advice was also taken to confirm whether or not our client was required to notify the individuals whose user names had been compromised.

ASK A **HISCOX EXPERT**

YOUR QUESTIONS ANSWERED

What is your exposure?
As businesses become ever more reliant on technology and hold more and more data, the risks from suffering a loss related to problems with their computer systems or from holding sensitive customer data like bank account information or other personal /sensitive details, continue to grow. This can lead to costs from handling a data breach, lost revenue, a damaged reputation, and legal and regulatory costs, not to mention the associated business disruption.

What's the definition of a 'record'?
For the purpose of cyber and data, we define a 'record' as the details of an individual that a company processes, regardless of how many times that information is handled. For example, if you buy goods from an online retailer five times in one year, it would count as one record. Our experience shows that there is a direct relationship between the number of data subjects affected by a data breach and the costs of the breach. The volume of records therefore provides the best guide to the likely cost of a cyber and data claim.

I'm a small company, why do I need to buy insurance?
There's a black market where records are sold and bought, and hackers are only getting savvier. The Department for Business, Innovation and Skills reported that 74% of small businesses & 90% of large organisations suffered a data breach in 2014 and it is becoming increasingly common.

My IT department is confident we are secure, do I need a policy?
Carphone Warehouse, TalkTalk and many other large corporations like them have entire departments devoted to IT security, and they still suffered a data breach. A simple oversight like not updating software, not setting appropriate user authentication procedures for third party vendors, losing an unencrypted laptop, or a rogue employee with malicious intent, can all lead to a breach.

I outsource my payment and card processing. I don't have payment card exposures do I?
According to the PCI Compliance Guide, PCI compliance applies to ALL organisations or merchants that accept, transmit, or store any cardholder data, regardless of their size, or number of transactions. Merely using a third-party company does not exclude a company from PCI compliance. It may cut down on the risk exposure and consequently reduce the effort to validate compliance but it doesn't mean a merchant can ignore PCI compliance.

My data is stored in the cloud, so liability rests with them?
Not exactly. It would be in your best interest to carefully review your cloud contracts with legal counsel. Even if the risk is reduced, the liability may still fall on the shoulders of the insured. You can outsource the service but not the responsibility.

Does the Hiscox policy cover offline and online exposures?
Yes. The policy is triggered by the breach of electronic and non-electronic data which includes theft and loss. So you have insurance for a sophisticated hack but also for leaving a paper file on a train or sending information by email to the wrong person.

What is encryption?
It's the process of encoding information so that only authorised parties can read it. Encryption is important in evaluating a company's risk and exposure, since a breach of encrypted data is significantly less costly than a breach of unencrypted data. Encryption is a risk control measure viewed favourably by regulators including the Information Commissioner's Office (the office responsible for the enforcement of various data regulations in the UK). Many of the fines they have levied have involved the loss of unencrypted data by organisations.

I have a password, is that the same as encryption?
No. Encryption is the process of scrambling the data on a hard disk so it is unusable unless accessed with a decryption key. Only using password protection means that a hacker could bypass the password to access intact data that hasn't been encrypted.