howden

Professional Indemnity Division

Cyber Liability

PREPARE • PREVENT • PROTECT

OUR KNOWLEDGE: YOUR ADVANTAGE

“If you are the leader of a business, you should know how strong your company’s defences are, you should know if there are response plans in place in case a significant security breach occurs, and you should be getting regular reports on cyber security threats and what your company is doing to respond to those threats.”

Jacob Lew
U.S. Secretary of the Treasury

The Risk

Businesses of every size are increasingly reliant on information technology and data. If IT systems are interrupted or data is mislaid, stolen or rendered inaccessible, the business and its clients are exposed to a range of negative impacts from financial loss to reputational damage.

Some firms may be large enough to have an IT department, whilst others may outsource their IT support. Regardless of your situation, threats to your operating systems, data or website cannot be ignored.

It is vital to ensure that your organisation, and any third party provider, have resilient procedures in place to reduce the likelihood of a system or data breach. However, you also need to ensure that, should the worst happen, your organisation has access to the resources to get back up and running as quickly as possible, and to minimise damage to your reputation.

Prevention is, of course, the best way to protect against cyber-attacks – but sometimes that is not possible. If the first line of your defence is breached, cyber liability insurance and mitigation products will provide risk management tools and insurance protection designed specifically to help you manage and control the impact on your business.

Hackers obtained username and password d
third party. They then used the data to hack

JP Morgan issued a statement to shareholders following the data breach that the firm would double its cyber-security spending from USD 250 million annually in 2014 to USD 500 million in 4 years' time

JP M
security

One sensitive file was hacked containing a list of every application and program deployed on JP Morgan computers

The attack went unnoticed for two months which also coincided with a large turnover with JP Morgan's information security group

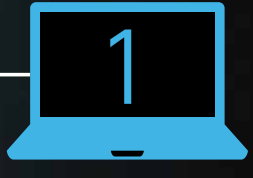
ata for a JP Morgan website maintained by a
into the bank's employee benefits website.

organ
breach

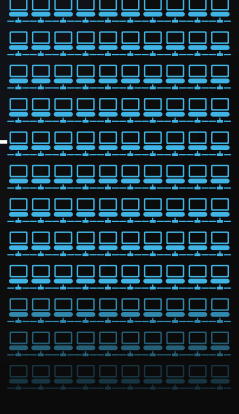
83 million
online accounts breached

76m household

6m small businesses



One computer was compromised to access the bank's network



90+
servers were compromised with administrative privileges within JP Morgan's network rummaging through customer databases

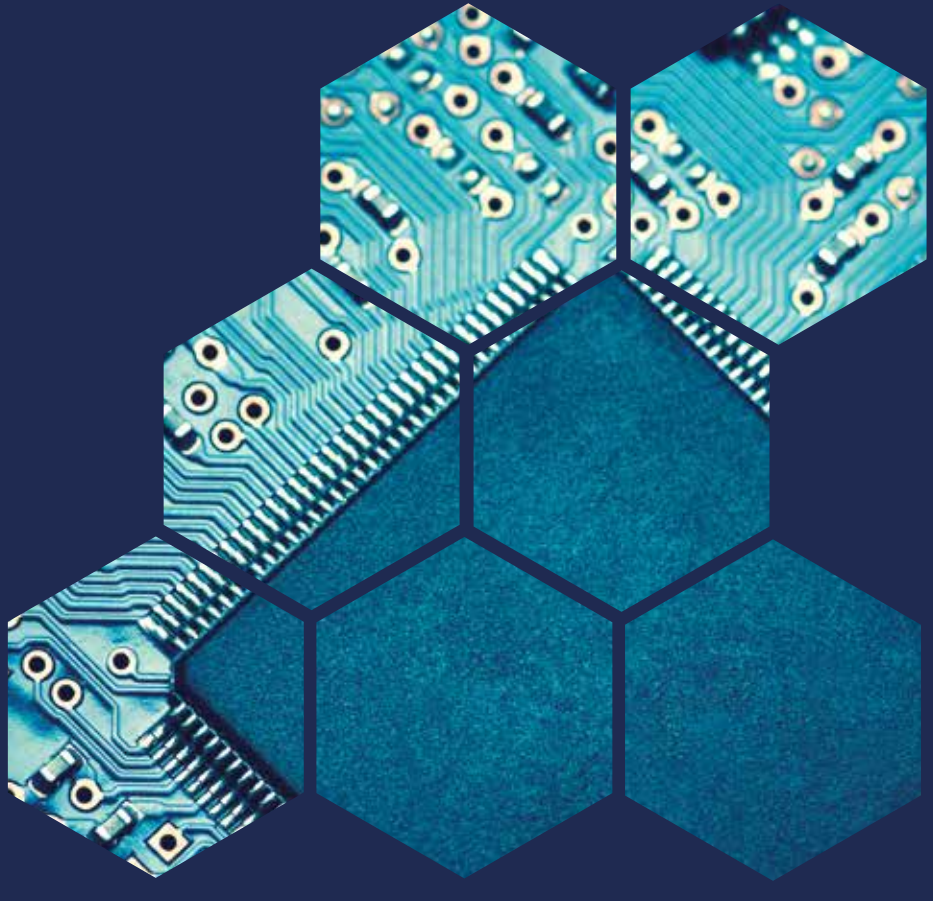
CASE STUDY

In 2014 a small U.S. law firm admitted to losing its entire library of legal documents to a virus called the Cryptolocker Trojan, a form of malicious software specifically written to generate ransom payments from relatively cash-rich but time-poor businesses.

The virus infected the company's main server, leaving every single document used by the firm in an encrypted state, after an email with a malicious attachment was mistaken for a message sent from the firm's phone answering service. The virus also warned that if the firm tried to tamper or decrypt anything, the main server would be permanently locked which would leave their IT department unable to do anything to rectify the situation. The firm then attempted to pay the ransom but discovered that the grace period – another nasty aspect of Cryptolocker – had expired.
It is estimated that there are over 130,000 victims of Cryptolocker in the UK with over 50,000 PCs infected between the summer of 2013 and June 2014. The software is thought to have been used to extort more than £18m of ransom payments globally but the total costs associated with reinstating affected systems is likely to significantly exceed this.

Why buy cyber liability cover?

With increasing publicity surrounding the vulnerability of technology, risk conscious firms are resorting to cyber liability mitigation and insurance products to form a key part of their risk management strategy. However, there appears to be a common misconception as to what cover is offered under a cyber policy and how this differs from the cover offered by a professional indemnity (PI) insurance policy.



WHY BUY CYBER LIABILITY COVER?

Access to an immediate response team

In the event of a cyber or data related incident, you need to be confident the situation can be rectified quickly. This will be critical to ensuring that your clients' data is protected and it may also be vital to ensuring that your business can continue operating. Do you have the technical skills or relationships with IT suppliers to do that? The costs charged by IT forensic firms may be very high, unless negotiated in advance.

First and foremost cyber insurance is a risk management product which, through the provision of practical support provided by specialists, reduces the impact of the event in both practical and financial terms. The policies are intended to support insureds if their systems are compromised and will assist in restoring an organisation to their original position prior to the incident by providing:

- IT forensic experts to investigate the occurrence and effect repairs
- Legal experts, with specialist experience in the privacy/regulatory arena
- Crisis communication consultants to minimise reputational damage.

Our policies provide you with access to a panel of industry experts, including, legal and IT forensics specialists, operating under pre-negotiated rates to help you respond as quickly as possible.

> Reputational damage was considered the most damaging impact of a cyber breach; the impact of losing your clients could see your business hit financial hardship.
>
> Survey published by PwC
> **Global Economic Crime Survey 2016**

A cyber liability policy will cover the cost of hiring specialist PR consultants to help limit reputational damage.

WHY BUY CYBER LIABILITY COVER?

Protecting operating costs

Professional indemnity policies are designed to respond to a "demand for damages or compensation" by a third party. In the event of a data breach, the affected third parties (i.e. your clients) probably won't know they have been affected. Therefore, a claim, under the definition of the professional indemnity policy, will not be made and the policy may not respond. This is important as your business is likely to start incurring costs as soon you become aware of the breach but a PI policy may not cover all of these costs.

Covering the cost of notifying affected parties

At present there is no legal requirement in the UK to notify individuals who are potentially affected by a breach. However, it is anticipated this will become a mandatory requirement following the introduction of the European General Data Protection Regulation (GDPR) which is anticipated to take effect some time during the first half of 2018.

At that point, a company that has been impacted by a breach will be required to notify all those likely to have been affected. In addition to the administrative costs of handling this requirement, companies could also be impacted by a range of other costs including the cost of providing credit monitoring services to those affected, advice on crisis management and specialist legal advice. Subject to application of the policy excess, a comprehensive cyber liability policy would cover these costs.

CASE STUDY

In late 2013 £7m was stolen from a financial adviser's client by cyber criminals who had gained access to their email account by tricking them into giving up access to their private email. They then set up a filter so client correspondence skipped the adviser's inbox, corresponded with the client and/or a clearing bank and tricked them into transferring their money. It is believed that at least six wealth managers fell prey to this scam in late 2013 costing clients a total of £45m.

“The GDPR is the key legal change that European cyber risk insurers have been waiting for. Cyber insurance provides indemnities for a variety of first party losses and third party liabilities arising out of cyber incidents. In particular, these policies indemnify the costs and expenses incurred by policy holders in the aftermath of data breaches. Such costs are a familiar feature in the US, sometimes running into millions of dollars. This is because it is typical for US companies suffering data breaches to be legally obliged to notify regulators and affected data subjects. For most companies that suffer data breaches or cyber-attacks in the EU, there is no such requirement to notify either regulators or data subjects. Therefore, data breaches often go unreported with companies facing limited financial and reputation exposure as long as the breach is not made public.”

Hans Allnutt, Partner
Global, DAC Beachcroft

WHY BUY CYBER LIABILITY COVER?

Preserve your business critical data

Corruption of your customer and prospect databases will have a significant impact on your ability to operate. Cyber policies will cover restoration costs which, as they typically constitute a first party loss, may not be covered under a professional indemnity policy.

Limited cover under professional indemnity policies

Some professional indemnity policies contain sub-limits for "loss of documents", or indeed "loss of electronic records". These sub-limits will often be set at around £25,000 in the aggregate. You should question whether this sum of money is sufficient to resolve a situation where an employee inadvertently deletes key files, with no recourse to back-ups.

What about the loss of actual money?

A query that we, as brokers, are often confronted with. Cyber insurance policies were not initially designed to provide cover for the loss of client funds in the event of a cyber-attack. Depending upon the situation, this exposure may be covered under your professional indemnity (PI) cover but you should seek the opinion of your insurance broker before assuming they are. If cover is afforded under the PI policy, the threat to client funds of a data breach should not be the catalyst for purchasing cyber insurance.

Although client funds lost due to a breach are not covered, some cyber products provide a level of reimbursement for the loss of the law firm's own funds due to a 'social engineering attack'. It is important to note that these losses are becoming increasingly prevalent. Fundamentally, they involve a criminal misleading an employee, or sending communications purporting to be a member of the firm, requesting the transfer of funds to a third party account.

Howden is actively working with insurers to extend the cyber liability cover we offer to professional services firms to include cover for first party losses, arising from social engineering.

Cyber extortion

You receive a communication from a third party stating that they have obtained confidential information held on your system. They are threatening to disclose this information unless you pay them a sum of money, such as £50,000. This payment would not be covered by a conventional professional indemnity policy.

CASE STUDY

One common tactic that cyber attackers have adopted is social engineering. How it works is that your Finance Director receives an email purporting to be from the Managing Director, which convinces the Finance Director to transfer money from the company's bank account to a third party bank account. It is possible that the Managing Director's email account was hacked, or that the email was sent from an alternative account with a very similar email address. This loss would not be covered under a typical professional indemnity policy because it's a 'first party loss' amounting to the theft of your company's funds.

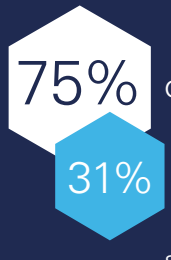
Howden is working with insurers to extend the cyber liability cover we offer to professional services firms to include cover for first losses arising from social engineering. We already offer this cover to conveyancers and solicitors.

Managing the risk

Threats to systems and data are constantly evolving, making them hard to predict and prevent. Whilst those with criminal intent are using increasingly sophisticated methods, it must be remembered that a data breach is just as likely to happen due to simple human error, for example the loss of a memory stick.

The human factor

Staff-related breaches feature notably in PWC's most recent Security Breaches survey.[1] PWC found that three-quarters of large organisations suffered a staff-related breach and nearly one-third of small organisations had a similar occurrence (up from 22% the previous year).



75% of large organisations ▲ up from 58% a year ago.

31% of small businesses ▲ up from 22% a year ago.

suffered staff related security breaches in the last year.

When questioned about the single worst breach suffered, half of all organisations attributed the cause to inadvertent human error.

50% in a year were caused by inadvertent human error. ▲ up from 31% a year ago.

[1] PWC: 2015 Information Security Breaches Survey https://www.pwc.co.uk/assets/pdf/2015-isbs-technical-report-blue-03.pdf

Be prepared

Controls should be embedded in internal culture; ensuring employees at all levels take data security seriously.

This is not intended to be a comprehensive guide to managing cyber risk but, as a minimum, businesses should:

- Ensure that system and data security is discussed and owned at Board level
- Work with professional advisers to take an informed decision on the purchase of stand-alone cyber liability cover
- Make sure that all staff are aware of the threat of impersonation and that they understand and apply the security checks to verify the identity of an individual (at all times)
- Understand the evolving regulatory environment and keep abreast of the latest threats
- Be clear about who in the organisation is responsible for information security
- Develop and implement risk controls that take account of the nature of the personal data held, the way that data is held and the harm that may result from a breach
- Review risk management procedures on a regular basis to ensure they remain robust and compliant with changing regulation
- Encrypt email and consider using a client portal, the majority of which are encrypted by default
- Ensure that you are happy with the competency, resilience and insurance arrangements of any third party providers you are using
- Make sure the right physical and technical security is used, backed up by robust policies and procedures and reliable well-trained staff with the necessary understanding of the topic
- Keep browsers, operating systems and anti-virus systems fully updated and don't forget this applies to laptops being used off site

£75k – £311k is the average cost to a small business of its worst security breach of the year

Approximately 80% of organisations had a security breach in the last year

69% of large organisations were attacked by an unauthorised outsider in the last year

60% of respondents reported seeing a 'significant increase' in demand for Cyber insurance products.

Our expertise

Cyber risks are multi-dimensional and will impact upon different firms in different ways. To ensure that businesses are equipped to respond rapidly and effectively in the event of a data breach and are covered for any losses arising, we have developed a range of exclusive cyber liability products specifically for professional services firms. For those firms requiring a more tailored approach, our cyber liability experts will use their knowledge of the professional services industry and cyber exposures to develop bespoke solutions.

About us

We employ over 130 professional services insurance specialists, covering professional indemnity, directors and officers and cyber liability insurance. We recognise the importance of developing strong relationships with both your business and your insurers. We believe in building relationships based on trust and respect.

We work with businesses that take their insurance seriously and recognise the value that working with a specialist broker can add.

Our first priority is always to ensure that you and your business benefit from breadth of coverage and that the person you deal with understands the cover you require and can clearly articulate the product you are buying. Where coverage requires tailoring to meet a specific business need we have the knowledge to identify the requirement, the expertise to design the solution and the negotiating strength with insurers to deliver it.

Our experience and relationships with insurers combine to enable us to find and develop insurance solutions at a time when insurers don't or can't underwrite the business due to rising claims volumes. This is why we dominate some of the most challenging professional sectors – in excess of 250 medium to large legal firms, 40% of the UK's survey and valuation firms and six of the UK's top ten financial advisers and networks.

Established in 1994, Howden UK Group employs over 2,200 people around the world. Whilst our size gives us a significant advantage when it comes to negotiating coverage, premiums and claims with insurers, we remain absolutely committed to ensuring our customers continue benefitting from the personal relationships, quality of service and specialist knowledge they have received over the last 20 years.

Howden UK Group Limited
16 Eastcheap, London, EC3M 1BD, United Kingdom
020 7133 1300 pii@howdengroup.com

howden