CYBER INSURANCE
EVERYTHING YOU NEED TO KNOW

A GUIDE FOR INSURANCE BROKERS

Pen underwriting

CYBER INSURANCE EXPLAINED

STARTER FOR 10: WHAT IS CYBER INSURANCE?

We understand that there's still a lot of confusion around cyber cover, and even some fear that it might be too complex to understand – which is why we've produced this guide.

Let's start with a different question: Ask yourself what part of your business **isn't** reliant on digital systems and, if a cyber attack meant that was the only part of your business still functioning, what could you do?

Not much? That's what cyber insurance is for. It's about keeping businesses trading in a world where digital systems dominate.

For example:

- If you came into work and you were told you that someone had got into your systems and accessed your data, would you know what to do next?
- Or if someone hacked your business – to put out messages on social media for example – would you know how to stop them and repair the reputational damage?
- Or you came in and switched on your computer and there was no response except for a ransom demand? Who would you call? Would you pay?

Cyber insurance is designed to tackle all of these threats and more. It not only protects businesses, but supports them to meet their commitments to customers and employees if their digital systems are compromised, paralyzed or attacked.

WHAT DOES CYBER INSURANCE ACTUALLY DO?

- It's cover against hackers stealing data and demanding a ransom not to release it
- It's cover against the fines and penalties that businesses will incur if they are assessed as non-compliant on data protection or privacy
- It's cover against viruses that paralyze systems – and cover for the income lost while they are being restored
- And cover against the accidental loss of data – followed by legal action by customers

WHAT ABOUT CYBER CRIME?

Financial cyber crime is covered on most cyber policies (including Pen's) via an optional extension.

Our extension, called e-Theft, provides cover to businesses whose bank accounts are targeted by criminals by hacking or phishing.

Phishing, otherwise known as social engineering, is where businesses are duped into transferring money to criminals, as a result of fraudulent emails purporting to come from employees, directors, customers or suppliers.

We would also cover the business if the e-Theft occurred as a result of a financial institution acting on their behalf.

Our e-Theft extension is one of the most competitively priced on the market.

It's our job to help businesses understand how reliant they are on digital systems; and therefore how great the risks are - financial, operational, reputational, legal and regulatory – if they don't have proper cyber cover.

WHY NOW?

Insurers have been talking about cyber cover for the last decade, why are businesses going to start taking cyber seriously now?

We believe we are at a tipping point. At present, businesses can only be fined up to €500K for losing data, but from May 2018 the EU General Data Protection Regulation (GDPR) will come into force, bringing with it fines of up to 4% of annual global turnover, or €20M (whichever is greater) for businesses that do not adequately protect customer data.*

Coupled to this is a requirement within the GDPR that if the potential harm to the data subject (the business's customer, employee, supplier etc) is not "remote" then new notification requirements come into force, along with any existing EU national law requirements.

(And, before you ask, the Government has confirmed that the UK's decision to leave the EU will not affect the commencement of the GDPR.)

In the USA, the introduction of stronger data protection legislation and requirements was the tipping point for the growth of cyber insurance and most market commentators believe the UK will follow the same path.

At present, 90% of the £2 billion global expenditure on cyber insurance is in the US marketplace, but, according to PwC, this is expected to treble by 2020, due to growth in the UK and Europe.**

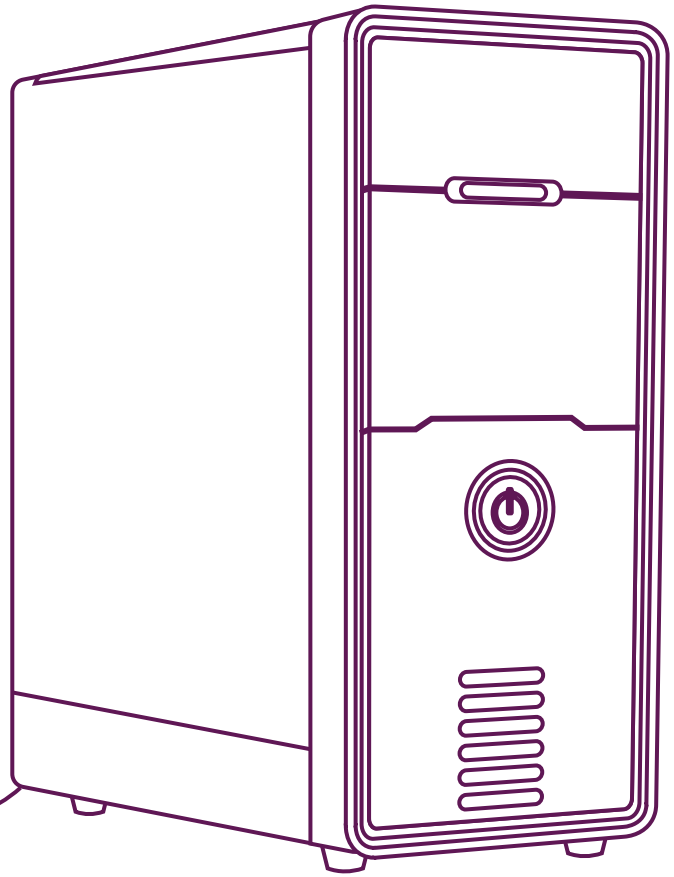
14% of small businesses rate their ability to mitigate cyber risks, vulnerabilities and attacks as highly effective.
(2016 Ponemon Institute "Cost of a Data Breach)"

*Information Commissioner's Office April 2017
**PwC "Insurance 2020 & beyond: Reaping the dividends of cyber resilience" September 2015

CYBER SECURITY: WHERE TO START?

ASK YOUR CLIENT THE FOLLOWING QUESTIONS:

- What would your client do if their business was attacked?
- What would they say to their customers and employees?
- Who would they call for help and advice?
- What is their public relations plan?
- Do they know what regulations they have to comply with?
- How would they get back up and running again – fast!



CYBER RISK HEALTHCHECK

Ask your client which areas of their business are digitally vulnerable	What might happen if they are not protected?	Ask your client about their business. Where is digital protection in place? Then ask how, despite the protection, someone could harm it. The answer is in the question, right? Digitally.	Look at the answers below and ask your client if they feel their business is adequately protected.	
ABILITY TO TRADE	Denial of service attacks on your systems – resulting in the business being unable to meet commit-ments to employees, suppliers or customers	Do you trade with customers electronically?	Yes	No
		Is delivery of goods/services to your customers dependent on digital systems?	Yes	No
		Do you operate a website that provides you with an income?	Yes	No
		Do you have a process in place if your website is successfully attacked/corrupted?	Yes	No
		Do you have a process in place if your website is attacked but the attack is not successful?	Yes	No
		Is your payroll dependent on digital systems?	Yes	No
		Is your supplier-invoicing process dependent on digital systems?	Yes	No
DATA	Loss or theft of customer or employee information	Do you keep customer or employee information electronically?	Yes	No
		Are customer credit card or bank details kept on your systems?	Yes	No
		Are these details encrypted?	Yes	No
		Do you have an IT policy in place regarding the handling of this type of data?	Yes	No
		Do you have a Privacy policy in place governing your collection of private data?	Yes	No
		Do you back your data up regularly?	Yes	No
		Do you permit your data to leave your system eg do you store it in a cloud?	Yes	No
		Do you have a contract with the third party that clearly defines what they can and cannot do with your data?	Yes	No
		What would you do if the third party's system went down?	Yes	No
MONEY	Phishing attacks ie the business themselves transferring money to a criminal, as a result of a fraudulent email	Do you use temps in your finance team?	Yes	No
		Do you update security software as soon as advised?	Yes	No
		Are there automated checks and audit trails built into your financial systems?	Yes	No
		Do new supplier bank details need the approval of your Financial Director?	Yes	No
		Are monthly checks made monthly on funds leaving the business's account?	Yes	No
REPUTATION	Spoof websites or attacks on social media accounts, but more importantly, loss of customer trust if the business fails to respond confidently to any of the above	Do you regularly check for spoof websites, e.g. using Google Alerts?	Yes	No
		Would you know what to do if your social media accounts were hacked?	Yes	No
		Do you have a contract in place with a PR agency who would support you if you were attacked?	Yes	No
		Do you have an incident response plan for cyber attacks?	Yes	No

WHY PARTNER WITH PEN

PEOPLE
Pen Underwriting's specialist cyber team is headed up by Adrian Scott, who played a key role in the development of the cyber insurance market in the US. His last role was as Executive Vice President and Chief Underwriting Officer at a leading cyber security firm founded and headed by a former US Head of Homeland Security.

APPETITE
We have a broad appetite, with very few exclusions. We can consider companies with up to £600M in turnover.

WORDING
We have a broad, comprehensive wording with extensions for e-Theft and outsource/cloud provider failure

PROCESS
Our bespoke cyber trading portal has been designed to make the process as slick as possible, because we believe cyber cover can, and should be, simplified.

PRICE
We are price competitive – check out Pen Central and see for yourself

CLAIMS
Our claims service is provided by a specialist service, experienced in handling cyber claims.

BREACH SUPPORT
Businesses insured with Pen will have access to a dedicated 24/7 helpline and other support services needed in the event of a breach.

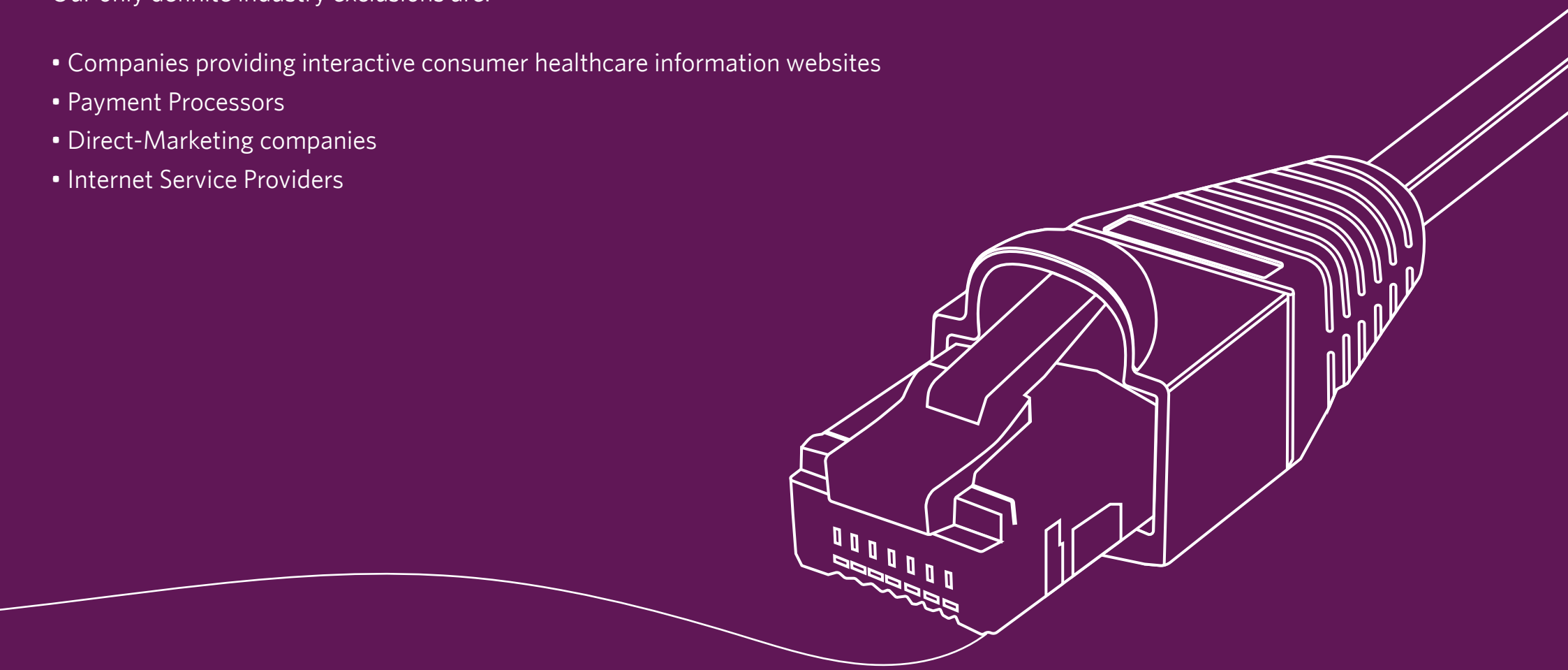
SALES SUPPORT
We don't expect you to be cyber specialists — that's our job. Pen can offer in-depth product training for you and your team, and support throughout the sales process.

WHO CAN WE COVER?

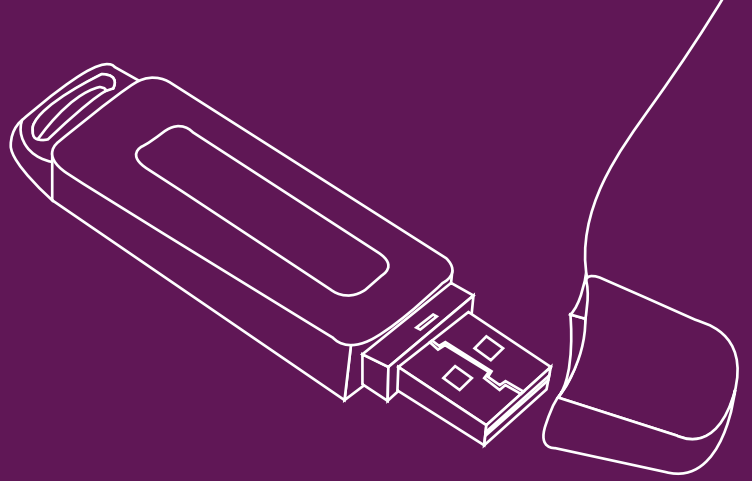
We have a very broad appetite. Any company with up to £600M in revenue can be considered for cover.

Our only definite industry exclusions are:

- Companies providing interactive consumer healthcare information websites
- Payment Processors
- Direct-Marketing companies
- Internet Service Providers



WHAT MAKES UP PEN'S CYBER COVER?



THE CORE COMPONENTS

BREACH COSTS
This is the first line of defence. In the event of a breach (the loss, theft or compromise of systems or data) this part of the policy covers the costs of notifying affected customers, offering credit monitoring, setting up call centres for concerned customers, and bringing in forensic teams to ascertain the reason for the data breach and – above all - removing the hacker or virus/malware from the business's systems.

COSTS FOR DAMAGE TO DATA OR PROGRAMS
If data or security is lost or compromised during a breach, this part of the policy covers the costs of restoring the affected data or security programmes.

INSURED'S NETWORK FAILURE - INCOME LOSS AND EXTRA EXPENSE
This covers business interruption losses arising as a result of a breach, or computer network failure.

CYBER EXTORTION AND RANSOMWARE
If a hacker steals data or locks down systems, then demands a ransom to avoid leaking the information or to make the systems available again, (a "ransomware" attack) this part of the policy will cover the costs of any cyber extortion or ransomware payments/expenses associated with the attack.

WHAT TYPES OF "DATA LOSS" ARE COVERED?

1. Accidental deletion: For example, when an employee accidently deletes information from a business's system. We will cover any reasonable costs associated with restoring the data

2. Loss of hardware: For example, when an employee loses a laptop or memory stick containing customer data. Pen covers the costs of informing affected customers and other action the businesses might need to take, such as a PR response

3. Virus or attack: For example when a malware attack wipes the data on your systems. We will cover any reasonable costs associated with restoring the data

60% of companies that have been a victim of cyber-attacks are out of business within six months.
(2016 Ponemon Institute "Cost of a Data Breach")

CORE COMPONENTS CONTINUED....

NETWORK SECURITY, PRIVACY AND CONFIDENTIALITY LIABILITY
This covers a business's liability in the event that they suffer a data breach and are sued by affected customers, vendors or employees.

NETWORK SECURITY, PRIVACY LIABILITY (REGULATORY)
This covers legal costs incurred as a result of complying with any regulatory action taken as a result of a breach.

MULTIMEDIA LIABILITY
This covers a business's liability in the event that they are sued as a result of information provided within their multimedia channels – for example on their website, Twitter feed or Facebook page. Typical examples would be breach of copyright, libel or slander, plagiarism or defamation.

CYBER TERRORISM
This covers losses due to actions by individuals, groups or governments acting for political, religious or ideological purposes, which causes destruction, disruption or subversion of the business's computer systems.

PAYMENT CARD INDUSTRY DATA SECURITY STANDARD – FINES PENALTIES AND ASSESSMENTS
This covers fines incurred by a business due to failures to properly follow PCI security standards

OPTIONAL EXTENSIONS

OUTSOURCE SERVICE PROVIDER OR CLOUD SERVICE PROVIDER FAILURE - INCOME LOSS AND EXTRA EXPENSE
If a business is disrupted by the failure or interruption of a cloud or outsourced service provider, this part of the policy will cover lost income and any extra expenses.

E-THEFT EXTENSION
The e-Theft extension covers the theft of money etc through digital means. That could be as a result of the business themselves - or a financial institution acting on their behalf – transferring money to a criminal, sending access credentials ,or just simply being hacked and having monies stolen.

Cyber Terminology:
e-Theft is also known as phishing or – depending on the size of the fraud – whaling.


You can do everything possible to prevent a cyber breach*, but if the worst happens you need to know your client can call on specialist assistance.
*(the loss, theft, or compromise of data or systems)
BREACH COUNSELLING
NOTIFICATION ASSISTANCE
CRISIS MANAGEMENT


CALL CENTRE SUPPORT
REMEDIATION PLANNING
EVIDENTIAL SUPPORT
PUBLIC RELATIONS ASSISTANCE

CYBER MYTH 1

"I'M AN SME, IT WOULDN'T BE WORTH ANYONE'S WHILE TO ATTACK MY BUSINESS"

They probably already have. **SME cyber crime is increasing**

Plus, because SMEs have fewer processes, they are particularly vulnerable to human error, like the loss of data by an employee. And if that data loss involves sensitive customer data, such as names, addresses, banking information or other confidential records, the impact could be severe.

CASE STUDY
Sector: Construction
Type: Data breach and ID theft using a fake email
Scenario: An employee in a construction firm responded to an apparently genuine email request from a trusted source for confidential employee tax records and other information.
Sting: 'Spear phishing' involves sending a fraudulent email that looks genuine – but isn't. Hackers spoof the 'From:' line of the email so the sender feels real – say from the CEO or a trusted third party. The victim recipient then responds, clicking a malicious link in apparent good faith but that response – including any attachments – is re-routed to the hacker's email account
Investigation: That single email reply harvested the full names, addresses, employment status and tax records for every employee working for the company during 2015.
Conclusion: Never put blind faith in what arrives in the inbox. The sender may be fake and click-through links may be malicious. Human processes are key: always double-check all sensitive requests for information directly with the requester to establish bona fides.
Which part of Pen's cyber policy would cover this breach?
- Breach Costs
- Network Failure – Income Loss and Extra Expense
- Cost for damage to data or programs

- In 2016 66% of small firms surveyed were victims of cyber crime
- SMEs fell victim to seven million cyber crimes over 2014 and 2015.
- The total annual cost of cyber crime to SMEs over 2014 and 2015 was £5.26 billion.
- On average, SMEs will fall victim to four cyber crimes every two-year cycle.*

The annual losses to UK businesses from all types of fraud are estimated at around £98 billion**. **Yes, you read that figure correctly.**

* Federation of Small Businesses (FSB): Cyber Resilience Report 2016
**The Centre for Counter Fraud Studies: The Financial Cost of Fraud Report 2015

CYBER MYTH 2

"BUT MY BUSINESS DOESN'T HOLD CUSTOMER DATA, SUCH AS NAMES, ADDRESSES OR BANKING INFORMATION"

Ask your client:

- Are you reliant on computer systems and/or email and the internet to conduct business?
- Do you have a website that's a shop front, sales or support desk for your customers?
- Do you operate a payment card industry (PCI) merchant services agreement?
- Do you use social media?

If your client answers yes to any of the above, a cyber attack could stop them dead in their tracks.

For example: A denial of service (DoS) attack could paralyse a business's website while a 'ransomware' attack could lock commercial systems or information until a release fee is paid.

Plus, good cyber cover doesn't stop when the incident is resolved, it will also pay for income lost while the business can't operate

CASE STUDY

Sector: Transport

Scenario: In early 2015, an employee clicked on the link in an apparently innocent email – and nearly destroyed a small fleet hire firm in Blackburn, Lancashire.

Sting: Clicking on an embedded link in what appeared to be a genuine email released a virus that encrypted over 12,000 company files held on the network.

Investigation: It was a 'ransomware' attack. Inevitably a blackmail demand followed from criminal hackers: 'give us £3,000 in exchange for decryption'. The ransomware virus was impossible to remove and the firm paid the criminals to unlock their critical files.

Conclusion: The business survived the attack, but at a price - not only did they have to pay a ransom but during the breach they couldn't trade or fulfil their obligations to their customers.

Which part of Pen's cyber policy would cover this breach?

- Breach Costs
- Costs for Damage to Data or Programs
- Network Failure – Income Loss and Extra Expense
- Cyber Extortion and Ransomware

CYBER MYTH 3

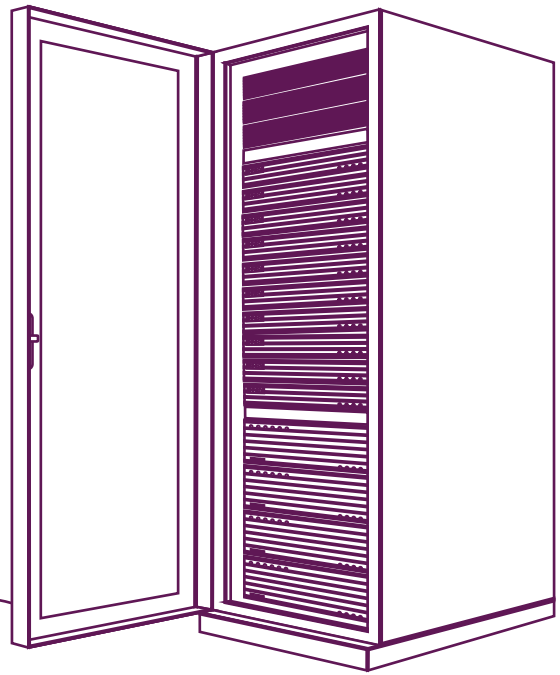
"BUT WE BACK-UP ON THE CLOUD, SO OUR SYSTEMS AND DATA ARE SECURE"

When it comes to data, there's no such thing as completely secure. While a loss of data by a cloud provider wouldn't be a bussines's fault, it could still have a huge impact on their reputation and earnings

CASE STUDY

Sector: Various
Scenario: Data was wiped from one of Google's data centres in Belgium* after the local power grid was struck by lightning four times. The data centre powers the Google Compute Engine, a service for business customers who rely on Google's massive servers to perform high-powered computing tasks.
Event: Some customers permanently lost access to their files.
Investigation: Google said it was "wholly responsible" for the outage, and it urged customers to consider duplicating their data through other services in future (ie back-up their back-ups).
Conclusion: While four successive strikes might sound unlikely, it happened and could happen again.
Which part of Pen's cyber policy would cover this breach?

- Breach Costs
- Network Failure – Income Loss and Extra Expense
- Outsource Service Provider or Cloud Service Provider Failure– Income Loss and Extra Expense



*BBC News 19 August 2015

CYBER MYTH 4

"BUT IM COVERED UNDER MY EXISTING INSURANCE"

Most existing insurance policies do not cover the full range of cyber threats.

What would your client say was their most important asset? Data? Reputation? Yet neither would be covered by most standard property or casualty insurance policies.

Without cyber insurance your client is vulnerable to a spectrum of electronic threats, from viruses and disruptive malicious software associated with highly motivated hackers to petty criminals and organised crime. Not forgetting the acts of careless employees – and even random cyber-saboteurs with no agenda other than scoring cheap and illegal thrills at a business's expense, simply because they can.

CASE STUDY
SECTOR: Retail
Scenario: An employee noticed that the corporate Twitter feed was broadcasting pro-ISIS propaganda.
Sting: The corporate website, email system and Twitter feed had been hacked by an ISIS-affiliate or web supporter.
Investigation: The client immediately called our hotline and, based on our advice, were able to identify how the hacker had got in and close the weak point in their cyber security. However, two weeks later, the hackers got in again. This time we sent in our team of cyber forensic experts who restored the security of the client's website, email system and Twitter feed.
Conclusion: Over £180K of forensic costs were incurred by insurers, a cost that without cyber insurance would have been carried by our client.
Which part of Pen's cyber policy would cover this breach?
- Breach Costs
- Costs for Damage to Data or Programs
- Multimedia Liability

CYBER MYTH 5

"BUT CYBER COVER IS EXPENSIVE"

Not taking out cyber cover could also be expensive.

There are almost always immediate costs, for example:
- Let's say your client's business has 100,000 customer records that are compromised.
- It will probably be required to write a letter to each of them to report this (a letter is needed because the worst thing a business can do after a data loss is to email their clients to report it)
- At 65p for a first class stamp, that's £65K gone before the business even starts to look at legal costs.
- When all the costs are tallied up, PwC puts the average cost per lost record at £110*

Could your client's business support this?

Then there are long term costs, for example, your client's business may be fined. From May 2018 businesses can be fined up to 4% of annual global turnover, or €20m, whichever is greater.

CASE STUDY
Sector: Charity
Scenario: A charity working with vulnerable children issued employees with unencrypted laptops
Event: A laptop containing information about the care of four young children was left outside the London home of their prospective adoptive parents one evening in December 2011.
Investigation: The charity were fined £70,000 in October 2012 by the Information Commissioners Office.
Conclusion: The charity appealed stating that the fine was "disproportionate" but the ICO stuck to its guns responding that the incident was "entirely avoidable" and using this as a warning to all charities to fulfil their obligations under the Data Protection Act.
Which part of Pen's cyber policy would cover this breach?
- Breach Costs
- Network Security, Privacy and Confidentiality Liability
- Network Security and Privacy Liability (Regulatory)

*http://www.pwc.co.uk/assets/pdf/2015-isbs-technical report-blue-digital.pdf

IT'S INCREDIBLY EASY TO GET A CYBER QUOTE FOR YOUR CLIENTS

Unlike most insurers who have an underwriting process with long applications, we have an online platform with just a few questions.

And the questions aren't difficult. If your client has a Head of IT, they will be able to answer them easily. If your client is a sole trader, they should be able to answer the questions themselves.

You should be able to complete the form with your client in 2-3 minutes – test it and see.

Once your client approves the quote, it takes just a few more minutes to complete the binding process.

WE SUGGEST

Before you go into a renewal meeting with your client, **get a quote for their business from our new e-trading platform, Pen Central.**

Don't worry if you need to make amendments after speaking to your client, because the answers are easy to change.

OUR CYBER COVER IS AVAILABLE ON PEN CENTRAL, OUR NEW E-TRADING PLATFORM

Interested? Your local Business Development Manager can arrange your Pen Central log-in and help you to get started on the system:

SCOTLAND & NORTHERN IRELAND
Michael Bolton 07827 984637 michael_bolton@penunderwriting.com

NORTH
Paul Broadbent 07970 672440 paul_broadbent@penunderwriting.com

MIDLANDS
Derek McCormick 07557 238725 derek_mccormick@penunderwriting.com

EAST
Mark Briggs 07785 426065 mark_briggs@penunderwriting.com

LONDON
Chris Dark 07825 439617 christopher_dark@penunderwriting.com

SOUTH
Carl Filo 07807 241 076 carl_filo@penunderwriting.com

WEST
Tegan McKernon 07976 313264 tegan_mckernon@penunderwriting.com

- There's no cost to sign-up
- If your brokerage already has a TOBA already in place with Pen you don't need to sign a new agreement
- Cyber is not the only product on Pen Central, you will also be able to access our new Mid-Net-Worth cover

Pen CENTRAL

HAVE YOU DOWNLOADED THE PEN APP YET?

EVERY PRODUCT, EVERY CONTACT, EVERYTHING YOU NEED TO KNOW ABOUT PEN IN ONE PLACE

The Pen App is the easiest way to access Pen's people and products.

- It's a risk placement tool that lets you search for solutions by product and industry
- You can call and email senior underwriters direct from the App
- The newsfeed will keep you up to date on the latest offers from Pen
- Unlike a brochure, the Pen App is always up to date!

Available on the App Store

GET IT ON Google Play

PEN UNDERWRITING
67 Lombard Street,
London,
EC3V 9LJ
United Kingdom

www.penunderwriting.co.uk
www.linkedin.com/company/pen-underwriting-uk

Pen
underwriting