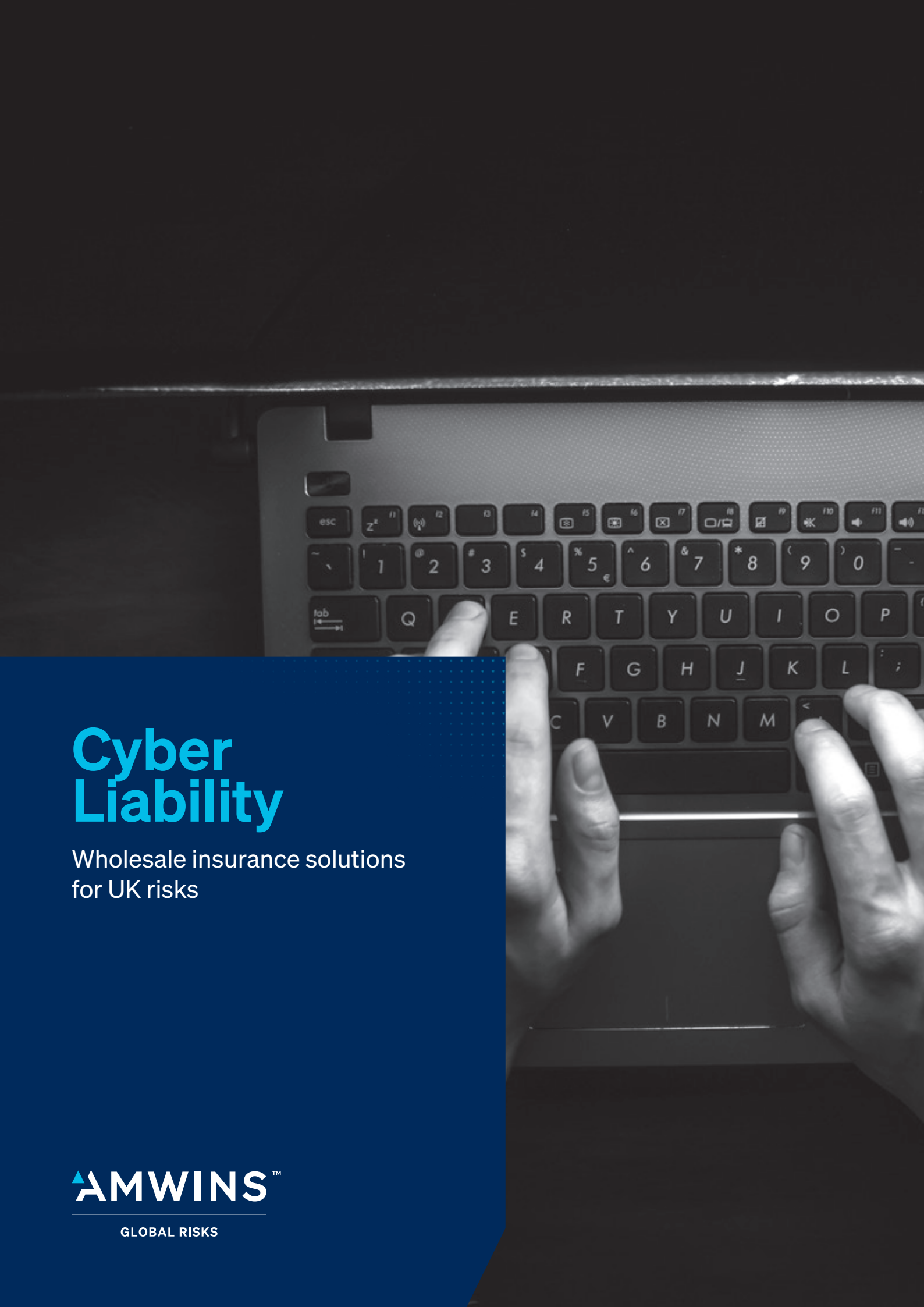


Cyber Liability

Wholesale insurance solutions for UK risks

AMWINS™

GLOBAL RISKS

THE IMPACT OF CYBER CRIME

COST OF CYBER CRIME

RISK MANAGEMENT

RECENT SME CYBER CRIME VICTIMS

OVERVIEW OF COVER

CLIENT CHECKLIST FOR BROKERS

TYPES OF ATTACKS AND COSTS

HOW CAN A DATA BREACH OCCUR?

ABOUT AMWINS GLOBAL RISKS

THE STATISTICS

WHAT HAPPENS AFTER A DATA BREACH?

The power of Amwins Global Risks: $26 billion in annual premium working for our UK clients just as much as for our global clients.

The impact on SMEs of cyber crime

Big brands make big news when they suffer cyber attacks:

MARRIOTT
500 MILLION
accounts hacked in 2018

EBAY
145 MILLION
accounts hacked in 2014

UNDER ARMOUR
150 MILLION
accounts hacked in 2018

EQUIFAX
143 MILLION
accounts hacked in 2017

TALK TALK
77 MILLION
accounts hacked in 2015

SONY PLAYSTATION
77 MILLION
accounts hacked in 2011

SMEs are often unaware they face a triple threat!

Rarely newsworthy, cyber crime is unfortunately NOT a rare occurrence for SMEs. Attacks are frequent, the cost is high, and yet SMEs are currently under-insured.

Financial professionals, and professions such as Design & Construct, are among the vulnerable industries.

Attacks are frequent, the cost is high, and yet SMEs are currently under-insured.

Recent SME cyber crime victims

SME RETAILER

A third party payment provider suffered a breach affecting 5,000 of the insurer customer's records. The cost of the claim was over £50,000 including over £12,000 in PR and communication costs.

SME ACCOUNTANCY FIRM

Two employees opened an infected Word document, which downloaded malware to the client's network, preventing users accessing data. The network was down for over 30 hours and the claim amounted to nearly £50,000 including £8,000 in legal costs.

SME MEMBERSHIP ORGANISATION

The insured suffered a persistent Denial of Service attack which affected all of its websites. When the websites worked again one of the insured's customers was able to view another customer's details including financial information. ID monitoring costs of nearly £6,000 and legal costs of £12,000 were elements of this £62,000 claim.

SME MARKETING AGENCY

A back-up tape, holding the details of 3.2 million members, was collected by the wrong courier. In a claim amounting to over £100,000 the notification costs alone were over £20,000 and the ID monitoring costs over £35,000.

SMART HOME PROTECTION LTD - JUNE 2019

The Information Commissioner's Office (ICO) fined Smart Home Protection Ltd £90,000 for making nuisance calls to people registered with the Telephone Preference Service (TPS).

MALWARE - JANUARY 2021

A malware botnet called Emotet, that was used by cybercriminals to infiltrate thousands of companies and millions of computers worldwide, was taken down by the National Crime Agency in an international operation. Nigel Leary, Deputy Director of the National Cyber Crime Unit, said: "Emotet was instrumental in some of the worst cyber-attacks in recent times and enabled up to seventy percent of the world's malwares including the likes of Trickbot and RYUK, which have had significant economic impact on UK businesses".

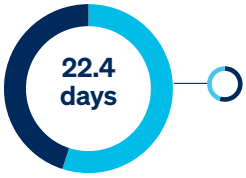
ONLINE CRIMINAL MARKETPLACE - DECEMBER 2020

The National Crime Agency and teams across the Team Cyber UK network shut down an online criminal marketplace that advertised 12 billion stolen credentials from over 10,000 data breaches.

Types of attacks and costs

On average the cost for the UK and the number of days it takes to resolve a cyber attack per type are as follows:

Malware - £1.57m



Web-based attacks - £1.52m

Denial-of-service (DoS) attacks - £1.31m

Malicious Insiders - £960,000

Stolen devices - £700,000

Malicious code - £960,000

Ransomware - £520,000

Phishing and Social Engineering - £960,000

Botnets - £260,000

Most vulnerable industries

- **MILITARY**
- **DESIGN & CONSTRUCT**
- **DATA CENTRES**
- **LOGISTICS**
- **HEALTHCARE**
- **GOVERNMENT**
- **EDUCATION**
- **FINANCIAL PROFESSIONS**

The statistics for SMEs

43%
of cyber attacks target small business.

58%
of SMEs are not allocating budget to mitigate cyber breaches.

43%
of data security breaches are caused by acts of malicious intent. Human error or system failure account for the rest.

38%
of SMEs regularly update software.

60%
of small businesses go out of business within 6 months of a cyber attack. The most common cause of an attack on SMEs is social engineering. SMEs spend an average of £710,425 because of damage or theft of IT Assets. In addition, disruption to normal operations cost an average of £771,68.

22%
of SMEs that encrypt data.

22%
of UK businesses buy cyber insurance.


f8
f9
f10
f11
f12
pause break
prt sc sysrq
delete insert
home
pgup
pgdn
end
backspace
num lk scr lk
enter
shift
enter
insert
delete

Cost of Cyber Crime

- Average annual cost of a data breach in the UK is £2.7billion
- UK cyber security market is worth £4M
- Industry has grown almost 40 times over the past 15 years
- Ransomware attacks alone have grown more than 350% annually
- Predicted cyber crime costs to hit £10.5 trillion annually by 2025
- Average cost per stolen record £113.88

Breached Networks

LinkedIn 167m 2016 /60m 2019

Instagram 14m 2019

Facebook 50m 2018/49m 2019/540m 2019

Sources:
Itgovernance.co.uk Wikipedia varionis.com Cisco www.export.gov
Infosecurity-magazine.com smallbiztrends.com globalnewswire.com

Overview of cover

Generally cyber risks fall into first party, (your own business assets) and third party risks, (the assets of others).

1st Party

- Data/Electronic Information Loss
- Business Interruption or Network Failure Expenses
- Cyber-extortion
- Reputational Harm
- Privacy Event Expense Reimbursement
- Expense Legal Guidance
- Reimbursement for third-party forensics costs
- Notification costs
- Call centre
- Public relations costs
- Credit monitoring

3rd Party

- Network Security Liability
- Privacy Liability
- Privacy Regulatory Proceedings and Fines
- Media Liability
- PCI-DSS Fines

How can a data breach occur?

- Malware/virus attacks/ransomware (unsecured networks)
- Loss or theft of device
- Inside job (employee misappropriation or improper access to information
- Stray emails, letters, even faxes
- Social engineering/phishing scams
- Failure to manage/purge/dispose of PII (personally identifying information)
- IP infringement

Cyber Essential accreditation involves a self-assessment questionnaire which is followed-up by a test of your client's system security.

What happens after a data breach?

INVESTIGATION

- Engagement of Privacy Counsel
- Determine what information is impacted (forensic vendor engagement)
- Determine legal and regulatory obligations/notification deadlines
- Assess involvement of law enforcement

RESPONSE

- Notify impacted individuals (notification vendors) and offer identity theft assistance
- Notify relevant regulators/government bodies
- Assess public relations requirements

REGULATORY INVESTIGATIONS & LAWSUITS

- Class action lawsuits
- Regulatory Investigations
- PCI (payment card industry)/card brand claims

REPUTATIONAL DAMAGE

- Loss of trust/customers
- Stock price/value impact
- Senior management scrutiny

VENDORS

Agent of Insurers

- Coverage/monitoring counsel

Agent of the Insured

- Breach coach
- IT forensics
- Notification/call centres/credit monitoring
- Forensic accounts (B.I.)
- Public relations

Risk Management

Questions that Brokers can ask their clients to help secure the sale

- Does the client have adequate security of the personal data they control?
- Does your client accept credit cards as a format of payment?
- Is the client a business-to-consumer business model?
- If a breach/misappropriation of data occurs, is the client ready to respond to regulators/affected individuals (clean data ready for notifications)?
- How would revenue be impacted if client's network slowed down/ went dark?
- Is the client reliant upon third-party technology providers for general operations?

Client checklist for brokers

1.
Estimate the number of individual personally identifiable (e.g., national insurance number, driver's licence number, healthcare information, credit card information) records currently stored within your own or third party networks.

2.
Does the company's cloud hoster, back-up data at least once per week and store these back-ups in a location that is separate from the company's physical premises?

3.
Does the company have anti-virus software and firewalls in place that are updated on at least a quarterly basis, with critical patch updates applied in line with the manufacturer's recommended time frames?

4.
Does the company encrypt all sensitive data that is physically removed from the premises by laptop, mobile/portable devices, USB or other means?

5.
Is the company PCI (payment card industry) compliant?

6.
Does the company have a process in place that requires legal sign off prior to content being published on the company's website, social media pages or physical media?

7.
Do at least two members of staff review and authorise any transfers or funds, signing of cheques (above £10,000) or for the issuance of instructions for the disbursement of assets, funds or investments?

8.
5-Year History: knowledge of any fact, circumstance, situation, event, or transaction which may give rise to a claim or loss under the proposed insurance with a value over £10,000.

Why Amwins Global Risks for Cyber Liability Insurance?

There's no denying that cyber exposures are complex and can be difficult to explain to clients. Let our professional risks specialists simplify the process for you and your clients. And with our outstanding market access we can also offer a facility specifically to accommodate the cyber needs of your larger clients. To keep ourselves, and our clients' safe too, Amwins Global Risks are Cyber Essentials Certified.

About Amwins Global Risks

We may be global by name, but we still have dedicated teams serving only UK clients with UK risks. Your usual contacts are ready, willing and able to use their expertise to help you and your clients.

For over 50 years we've been wholesale broking as THB (originally Thompson Heath & Bond). Founded in the UK, grew to be the largest specialty motor fleet wholesaler in the London Market, and now our UK teams provide wholesale broking services across commercial property and liability, motor fleet and a range of professional and financial risks. And for your UK clients with marine cargo, energy, aviation or construction risks? We can help here too. We have specialist colleagues in other Amwins Global Risks divisions who place these risks day in, day out.

In terms of professional indemnity, our specialists focus on complex high hazard accounts where we can add real value for our brokers. Areas such as design and construct, cladding risks, brokers' PI and surveyors' professional indemnity.

Management Liability, Medical Malpractice and Cyber Liability risks can be difficult to place, and sometimes difficult to sell to clients too. Bring them to us at Amwins Global Risks. We use our market connections and the leverage that comes from being one of the world's largest specialist wholesale brokers, to find homes for hard-to-place business, and to develop schemes and delegated authority arrangements that are attractive both to our brokers and their clients.

That's the power of Amwins Global Risks: $26 billion in annual premium working for our UK clients just as much as for our global clients.

And yes, our UK teams are still 100% wholesale – we have no competing retail arm.

Our professional and financial risk solutions

- Professional Indemnity
- Financial Institutions
- Management Liability
- Cyber Liability
- Directors' & Officers'
- Medical Malpractice


We bring our market
power to help you succeed.

AMWINS™
GLOBAL RISKS

Before renaming as Amwins Global Risks you knew us as THB.

As Amwins, we have the scale, stability and resources of a global (re)insurance broker.

We're still the same broking experts, still here for you.



We are one team | We strive for excellence | We do the right thing

SARAH BRAILEY
DIVISIONAL DIRECTOR
T: 020 7469 0245
M: 07867 456 881
E: sbrailey@amwinsglobalrisks.com

amwinsglobalrisks.com/uk

11.22