Cyber Liability

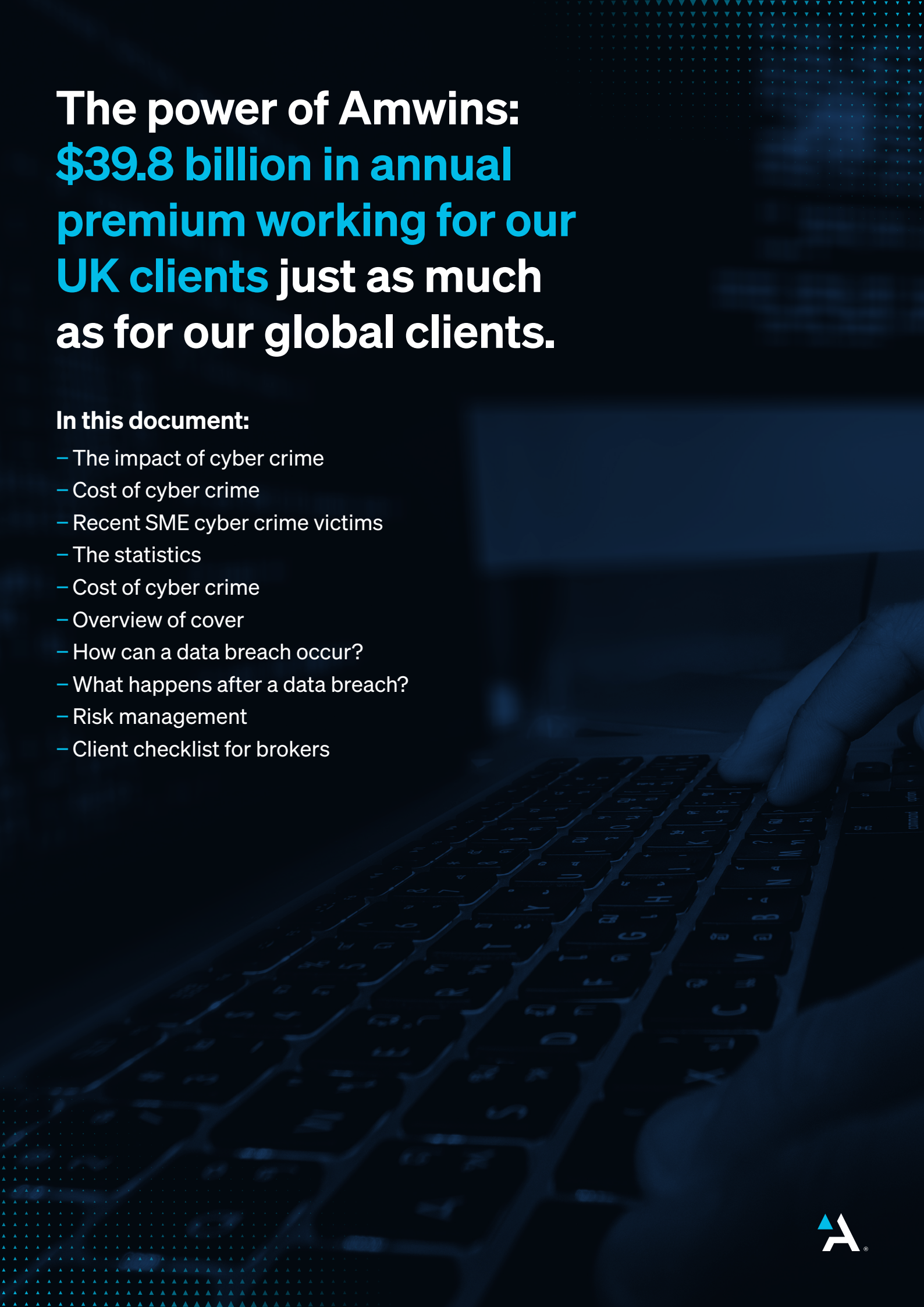
Wholesale insurance solutions for UK risks

AMWINS®

GLOBAL RISKS

The power of Amwins: $39.8 billion in annual premium working for our UK clients just as much as for our global clients.

In this document:



The impact on SMEs of cyber crime

Big brands and entities make big news when they suffer cyber attacks:

The Guardian – 2022
Ransomware attack causing employees to be locked out of office

NHS – 2022
Ransomware attack causing widespread outages

Marriott Hotels – 2022
Over 500 million accounts hacked

UK Government – 2024
40 million voters hacked by Chinese intelligence agencies

Amazon – 2022
100 million people's person information stolen

British Airways – 2022
380,000 customers hacked

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 underinsured.

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

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).

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.

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".

Most vulnerable industries

Military

Data Centres

Logistics

Design & Construct

Healthcare

Government

Education

Financial Professions

The statistics for SMEs

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.

58%

of SMEs are not allocating budget to mitigate cyber breaches.

43%

of cyber attacks target small business.

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.

22%

of SMEs that encrypt data.

22%

of UK businesses buy cyber insurance.

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

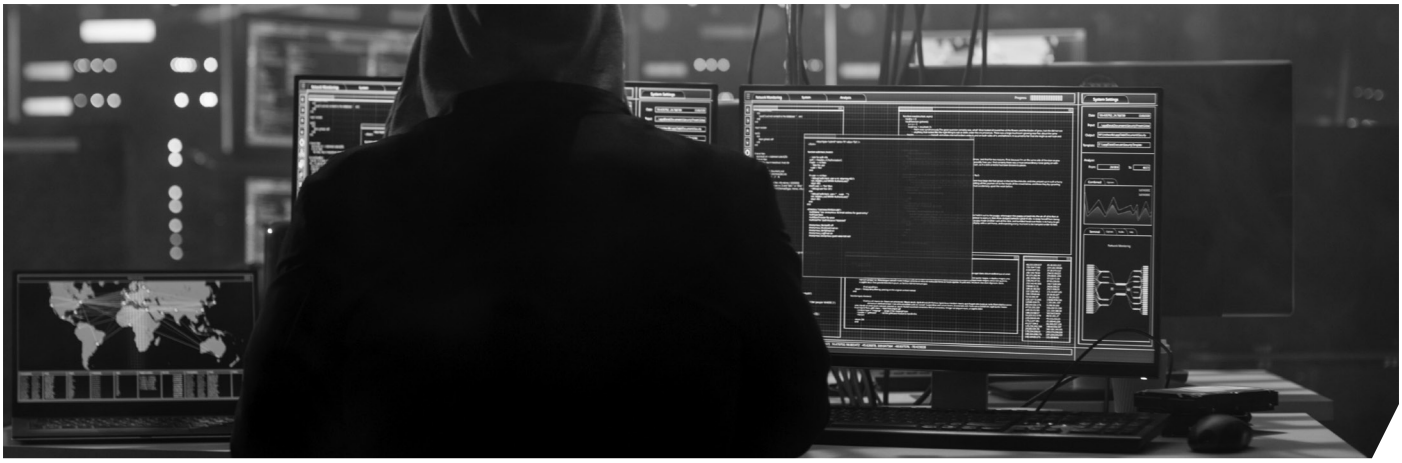
Generally cyber risks fall into first party, (your own business assets) and third party risks, (the assets of others).

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

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

- ☑ 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.
- ☑ 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?
- ☑ 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?
- ☑ Does the company encrypt all sensitive data that is physically removed from the premises by laptop, mobile/portable devices, USB or other means?
- ☑ Is the company PCI (payment card industry) compliant?
- ☑ 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?
- ☑ 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?
- ☑ 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. **We bring our market power to help you succeed.**

AMWINS
GLOBAL RISKS

Amwins Global Risks is the international division of Amwins, the largest specialty wholesale distributor in the world, placing more than $39.8bn in annual premium. We place over $2.8bn of that premium, bringing the market muscle and global reach required to find solutions for the most complex risks. With over 750 employees around the world, and a global footprint across more than 120 countries, we've cemented our place as a top 10 contributor to Lloyd's. We're the largest independent wholesale broker, and binding authority broker, in the London Market.

Visit **amwinsglobalrisks.com** for more information.

Professional & Financial Risks

+44 (0)20 7469 0100

Joe Williams
Divisional Director
+44 (0)2074 449 527
joe.williams@amwins.com

Ralf Emerton
Broker
+44 (0)7767 160 960
ralf.emerton@amwins.com

Patrick Keane
Broker
+44 (0)2074 449 549
patrick.keane@amwins.com

Alex Gilham
Junior Broker
+44 (0)7825 680 965
alex.gilham@amwins.com