A broker guide to selling cyber insurance

THIS INFORMATION IS INTENDED FOR INSURANCE BROKERS AND OTHER INSURANCE PROFESSIONALS ONLY

CyberEdge® Playbook

AIG

Start >

Cyber Threats

Cyber is consistently one of the top three risks businesses face, with the average cost of a data breach globally at approximately $4 million. [1]

2016 Trends and Facts

£2.53m

Average cost of a UK data breach in 2016, up 78% since 2008. [1]

1.2m

Approximate number of new malware or variants on average each day.[2]

62%

of businesses attacked are small or medium in size.[3]

Ransomware is the #1 security issue

clients are dealing with.[2]

209 days

Average time from initial infection until discovery of breach.[4]

Other hot topics

Increasing awareness of the potential for reputational harm has led to more C-Suite involvement in strategic cyber initiatives.

I.T. departments cannot be the sole source for defending against cyber risk.

Cloud computing and mobile technology are growing areas of concern when it comes to potential sources of cyber risk.

Clients are increasingly aware of cyber network downtime as a potential loss from a cyber issue.

1 IBM (2016) Cost of a Data Breach Study retrieved from www.ibm.com/security/data-breach/
2 Symantec (2016) Internet Security Threat Report retrieved from www.symantec.com/security-center
3 Crowdstrike (2015) Global Threat Report retrieved from www.crowdstrike.com/global-threat-report-2015/
4 Verizon (2016) Verizon Data Breach Incident Report retrieved from www.verizonenterprise.com/resources/reports/rp_dbir_2016_report_en_xg.pdf

Incident Management

With cyber threats increasing and new regulations set to introduce higher potential fines, how a business responds to a data breach has never been more important. CyberEdge assists clients to quickly respond to an incident and manage the event from breach through to resolution.

Immediate Response

As soon as a cybersecurity incident is detected or suspected, clients can call the 24/7 CyberEdge hotline to be connected to response consultants. This immediate response is important as many cyber incidents occur during downtimes.

Access to Experts

Clients are advised by legal and I.T. consultants who are experts in cybersecurity incidents and data breaches. How a company responds to and manages an incident can influence the outcome of a regulatory investigation and therefore being guided by experienced specialists is critical.

Breach Coach

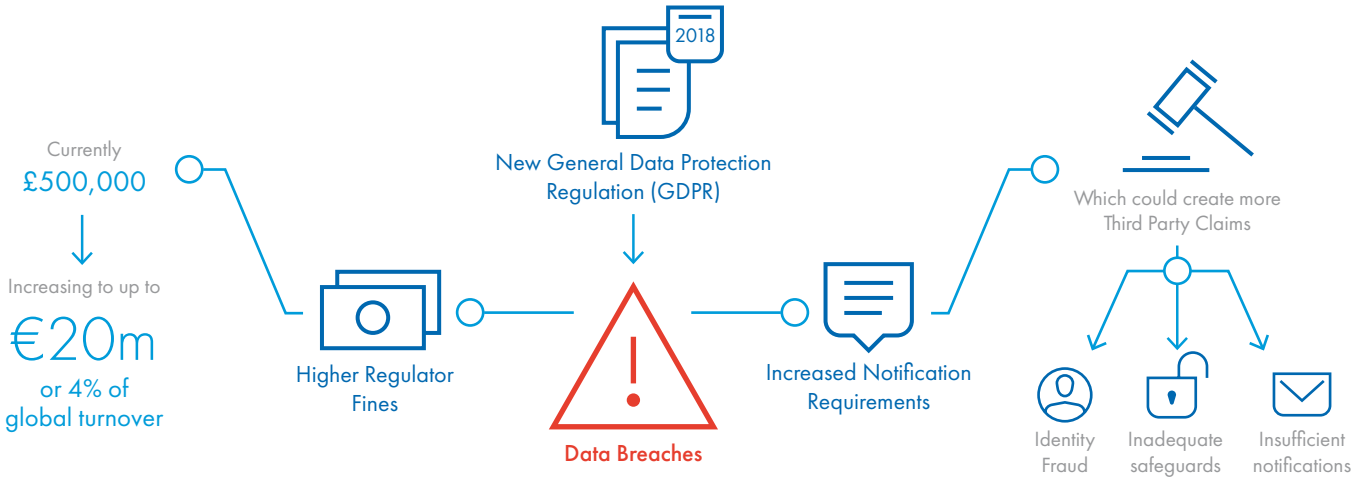
CyberEdge's response and event management is led by legal advisers at top UK law firms who also have global footprints. This legal guidance is crucial to ensure a coordinated response and to minimise potential liabilities faced by the business.

After calling the CyberEdge hotline, clients can expect:

Breach component	CyberEdge response
BREACH	Immediate response within 1 hour from claims and breach counsel
FORENSICS	Expert forensics: what's been affected, how can it be contained, repaired or restored
LEGAL/PR	Expert legal advice and PR consultancy to contain reputational damage
NOTIFICATION	Costs of notifying data subjects who may be affected by the breach – and credit monitoring to prevent further losses
FINES & INVESTIGATION	Professional preparation for any investigation, insurable fines, and penalties by a data protection regulator
LIABILITIES	Defence costs and damages for: • Any breach of personal or corporate data • Contaminating someone else's data with a virus • Theft of system access code • A negligent act or error by an employee

The General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR) comes into force in May 2018 and will replace the Data Protection Act 1998 in the UK. Amongst other features, the GDPR makes the rights of data subjects clearer and places more requirements on organisations that process personal data.



One significant element of the GDPR is the size of potential fines for non-compliance. Organisations will face the prospect of significantly increased fines, up from their current maximum of £500,000 to €20m or 4% of annual global turnover. In addition, mandatory notification requirements will require organisations to inform the Information Commissioner's Office (ICO) of data breaches within 72 hours. This notification requirement in turn has potential to create an increase in third party liability claims.

If it's not already, the GDPR will make data protection a boardroom level issue and will force organisations to closely examine how they intend to respond data breaches.

CyberEdge can play a critical role in a business's planning for GDPR. The Data Protection and Cyber Liability module can provide cover for investigation costs and insurable regulator fines in addition to damages and defence costs arising from third party liability claims.

First Response and Event Management cover can assist organisations initiate a coordinated response to a data breach, managing the regulator notification and ensuring all practical steps have been taken to reduce the likelihood or size of a fine should the businesses be found in breach of the GDPR.

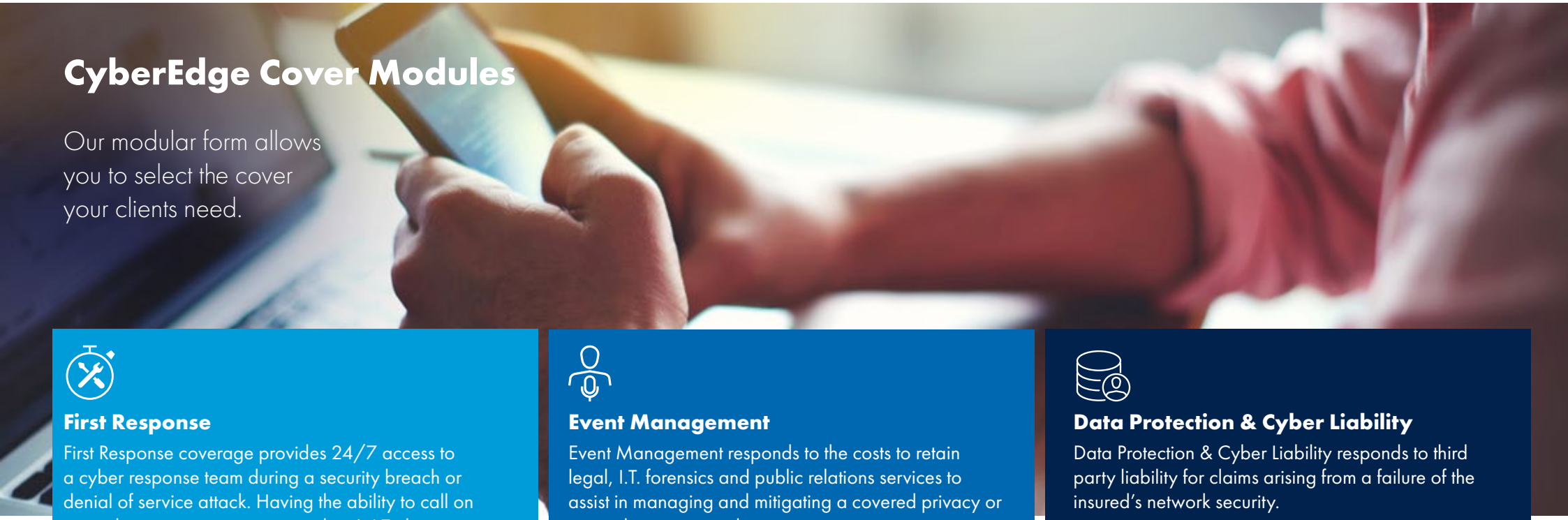
Change is coming.

GDPR puts data protection in the spotlight and creates a significant opportunity for Cyber insurance.

CyberEdge at a glance

Through our modular wording, clients can choose the level of cover and support they require – ensuring they receive tailored insurance for the risks they face.

	Module	Prevention	Breach/Forensics	Business Impact/ PR / Notification	Legal	Liabilities
			Breach Component			
Cover	First Response		✓ 24/7 I.T. support to identify and correct the immediate network issues			
Cover	Event Management		✓ I.T. services and data restoration	✓ Notification costs, credit/ID monitoring and reputation protection services	✓ Legal services	
Cover	Data Protection & Cyber Liability				✓ Defence costs and regulatory data protection fines	✓ Actual or alleged breaches of confidential information
Cover	Network Interruption			✓ Loss of net profit from a cyber- security breach		
Cover	OSP Network Interruption			✓ Losses from an interruption to an outsourced service provider		
Cover	System Failure			✓ Network interruption losses from a system failure not related to a cybersecurity breach		
Cover	Electronic Data Incident			✓ Accidental damage or destruction of computer system		
Cover	Digital Media					✓ Breach of intellectual property or negligence with electronic content
Cover	Cyber Extortion		✓ Assistance and financial cover to end a threat			
Cover	Telephone Hacking			✓ Charges that result from the unauthorised access and use phone systems		
Cover	Computer Crime			✓ Direct financial loss from fraudulent electronic fund transfers arising from a cybersecurity breach		
Cover	Goodwill Coupon			✓ Retain customers by offering a discount or rebate on future services		
Cover	Criminal Reward Fund			✓ Reward for info on individuals involved in a cybersecurity breach		
Endorsement	Loss Prevention Services	✓ Mobile App/Infrastructure Scan/Proactive Shunning/ Information Portal				



CyberEdge Cover Modules

Our modular form allows you to select the cover your clients need.

First Response

First Response coverage provides 24/7 access to a cyber response team during a security breach or denial of service attack. Having the ability to call on specialist support to augment a client's I.T. department can be crucial as data may still be leaving the system or a hacker may still be inside network.

- The cyber response team contains technical experts, experienced incident managers and forensic specialists.
- Often involves coordinating across suppliers quickly to establish the facts and apply defence controls.
- No policy retention applies for the first 48 or 72 hours of cover.*

*Refer to policy schedule and wording for details of retention free period.

Event Management

Event Management responds to the costs to retain legal, I.T. forensics and public relations services to assist in managing and mitigating a covered privacy or network security incident.

- Includes costs to notify consumers of a release of private information.
- Includes cost of credit-monitoring or other remediation services to help minimise damages to those victimised by a covered privacy or network security incident.
- Includes costs associated with losses to information assets such as customer databases resulting from a failure of network security.
- Covers costs to restore data that is corrupted or not machine readable.

Data Protection & Cyber Liability

Data Protection & Cyber Liability responds to third party liability for claims arising from a failure of the insured's network security.

- A broader definition of "computer system" includes leased computers and cloud computing services.

Claims can be against:

- A failure to protect personally identifiable information from misappropriation, including disclosures as a result of social engineering attacks (e.g., phishing).
- A failure to protect or wrongful disclosure of private or confidential information.
- Violation of privacy regulations in connection with failure to protect private information.
- PCI-DSS non-compliance.

MORE >

CyberEdge Cover Modules Continued

Network Interruption

Network Interruption responds to an insured's loss of income and operating expenses when business operations are interrupted or suspended due to a failure of network security.

- Broadened definition of loss includes lost business income, normal operation expenses (including payroll) and those costs that would not have been incurred but for the interruption.
- Full limits of insurance apply to any incident; hourly sublimit restrictions do not apply.

10001101
00110100
10001101
00110101

Electronic Data Incident

Cyber-crime isn't the only reason data can be lost or corrupted. Power surges, electrostatic build-up, fire/floods, natural disasters, overheating and physical vandalism can also result in data being unaccessible.

- Expands the data restoration coverage under the Event Management section to include a wide number of electronic data incidents.

Network Interruption: Outsourced Service Providers

Outsourced Service Providers (OSPs) - including cloud services - provide a range of valuable services to organisations such as web hosting, payment processing, data collection and data storage.

If/when there is a disruption to these services it can have a significant impact on a client's network and generate network losses.

- Cloud computing considered an OSP.
- Network interruption losses resulting from an OSP.
- Costs associated with mitigating the OSP interruption.
- Includes security failures.
- Can be extended to include system failures.

Network Interruption: System Failure

As organisations become more reliant on their own computer systems to operate efficiently, the need to cover financial losses arising from service disruptions across their networks is becoming more critical.

- Network interruption losses resulting from an internal system failure not necessarily arising from a cyber security breach.
- Costs associated with mitigating the system failure such as staff overtime.

Digital Media

In a dynamic and fast moving digital environment, it is now easier than ever for companies to inadvertently infringe on trademarks or misappropriate creative material.

- Damages and defence costs incurred in connection with a breach of third party intellectual property, or negligence in connection with electronic content.

MORE >

CyberEdge Cover Modules Continued

Cyber Extortion

Cyber extortion is a growing threat and cyber criminals are becoming increasingly ambitious, demanding larger sums to avert or prevent an attack. Like any extortion event, organisations need the support of experienced advisors to investigate and negotiate on their behalf to attain the best outcome possible.

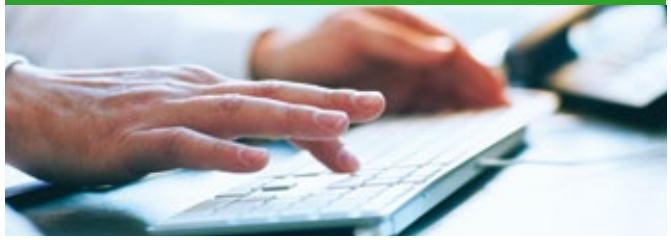
- Cyber Extortion pays to negotiate and settle network security related extortion demands made against the insured.
- Triggers when there is a threat to the insured's computer system.
- Includes the costs of investigations to determine the cause of the extortion threat and to settle the extortion demand.

Computer Crime

Fund transfer fraud is a form of computer crime where criminals use details obtained from a cybersecurity breach to fraudulently transfer funds from an account maintained at a financial institution.

- Covers direct financial loss from fraudulent electronic fund transfers arising from a cybersecurity breach.

CyberEdge's computer crime extension relates to a specific crime event, an independent Crime policy would offer wider coverage and include other types of third party crimes.



Goodwill Coupon

When confidential client data is breached it can have a hugely negative impact on a company's relationship with their customers. Goodwill coupons can go a long way to reverse that ill feeling and help to retain a client's customer base.

- Flexibility to choose either Credit and ID Monitoring or a Goodwill Coupon.
- Provides a discount or rebate for a future purchase.
- Activates from breach of confidential information or a material interruption.
- Sublimit applies.

Telephone Hacking

Telephone system (PBX) hacking (a.k.a. phreaking or toll fraud) is a global criminal business. Criminals who hack into a phone system can run up large charges against an innocent organisation's line account.

- Covers call charges resulting from unauthorised access to a telephone system.

Criminal Reward Fund

Cybercriminals and hackers may be a loose collection of people who are well known to a wider online community. Rewards for information to identify individuals can lead to their arrest but can also act as a deterrent for future attacks.

- A reward fund for information that leads to the arrest and conviction of individual committing or trying to commit a cyber attack or extortion against the insured.
- No policy retention applies.

CyberEdge includes a wide range of complimentary tools and services to help businesses reduce the likelihood of a cyber-attack.

Complimentary loss prevention

Available to all CyberEdge policyholders.

CyberEdge Mobile App

iPhone®, iPad® and Android™

The CyberEdge Mobile App for phones and tablets delivers the latest cyber breach information, news, opinion and risk analysis. It includes a data breach threat map displaying breaches around the world, claims examples of cyber breaches covered by CyberEdge and a breach calculator for businesses to calculate their potential costs of a data breach.

Loss Prevention Services Endorsement

Complimentary for CyberEdge clients with premiums over £5,000.

Infrastructure Vulnerability Scan

An external scan for up to 49 of an insured's public facing IP addresses that detects vulnerabilities across network devices, servers, web applications, and databases to help reduce risk and better manage compliance requirements.

Proactive Shunning Service & Training Services

Shunning hardware that stops an attack by bi-directionally blocking communication to known "bad" IP addresses. The attack information is sent to the accompanying account. The dashboard will update in real-time and outline the known "bad" IP addresses that have been shunned.

Cybersecurity Information Portal

A centralised hub of educational and technical cybersecurity information that can help assist in the prevention of a breach. Resources include training tips, cyber news and articles, cyber risk assessments and a variety of valuable tools and calculators.

AIG Risk Consulting Services

AIG's team of cyber risk consultants brings over 50 years combined experience in IT security to help our clients stay ahead of their cyber risk. Our team works directly with CyberEdge insureds to provide detailed, technical expertise and consulting services.

Cyber Defence Review

AIG's Cyber Defence Review service takes a look at the client's people, processes, and tools that make up their cybersecurity program and identify areas of strength and weakness.

- Consultants conduct passive reconnaissance and active vulnerability testing of the client's systems to identify intelligence that attackers can see.
- Client receives a final report that includes all findings and recommendations, with an industry comparison.

Internet Facing Systems

This service is designed to help clients identify risks and exposures in their public facing infrastructure from the external attacker's perspective.

- Consultants conduct passive reconnaissance and active vulnerability testing of the client's systems to identify intelligence that attackers can see.
- Client receives a final report that includes all findings and recommendations, with an industry comparison.

Incident Simulation Workshop

Our Incident Simulation Workshop is designed to help clients ensure their incident response plan will help their organisation respond efficiently when a security incident occurs and to help clients better maximise their CyberEdge benefits.

- Client and AIG consultant identify and perform 2-3 incident simulation exercises tailored to the client's organisation.
- Client receives a final report that includes an executive summary, incident response plan recommendations, workshop feedback, and any other recommendations.

Executive Threat Brief

This workshop is designed to help our clients better understand their current security threat landscape, specific to their industry as well as current methods attackers are using so that clients can better defend their business.

- Client's c-level executives and other staff benefit from this 2-3 hour interactive workshop, which covers:
  - Current cyber risks or threats related to the client's industry,
  - How cyber criminals are exploiting those threats, and
  - How the client can to better protect their organisation.

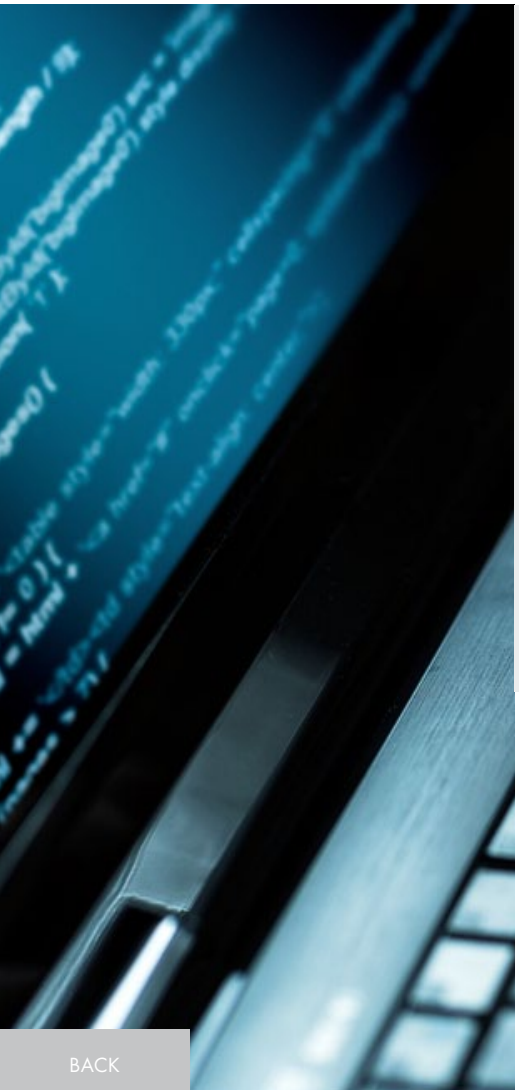
Cyber Engineering Study

Our Cyber Engineering Study takes a look at the client's people, processes, and tools that protect critical systems and industrial controls within their environment.

- Consultants will review security architecture and processes related to industrial controls, interview staff to discuss what's working (and what's not), and review logs and other elements.
- Client receives a final report that includes all findings and recommendations, with an industry comparison.

Preferred Vendor Partner Services

We have partnered with experts in cyber risk to bring our clients additional options to add to their line of defence. These services have been specifically selected based on our nearly 20 years of experience and how well they can help strengthen the cybersecurity maturity of an organisation. All CyberEdge clients have access to the following services at a preferred rate.



Dark Net Intelligence

Powered by *K2 Intelligence*

K2 Intelligence works with clients to stay apprised of the latest chatter inside the black hacker markets and forums known as the 'dark net' about their business. K2 Intelligence mines the Dark Net using web crawlers and sophisticated human data gathering to help companies take a proactive approach around their cybersecurity risk management.

Security Awareness Training

Powered by *Wombat Security*

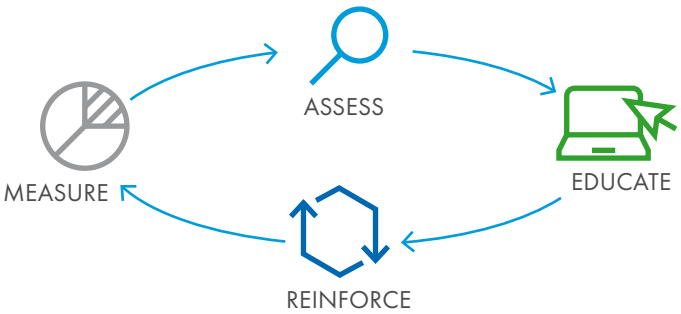
Security awareness training for employees including phishing training and simulations.

A unique Assess, Educate, Reinforce, Measure training methodology combines the four key components of successful cyber security awareness and training programmes.

Portfolio Analysis

Powered by *Axio Global*

Axio Global (Axio) can assist clients obtain a holistic picture of their cyber exposures and more effectively align their technological and operational controls with insurance converge. Instead of looking at cyber exposures in isolation, Axio's assessment methodology looks at the full range of potential losses, including data theft, liability, property and environment, damage, boldly injuries, and operational disruption.

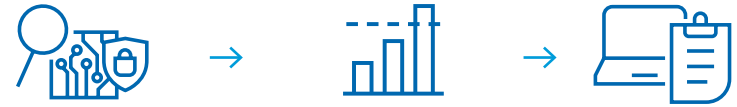


Preferred Vendor Partner Services Continued

Cybersecurity Maturity Assessment

Powered by *RSA*

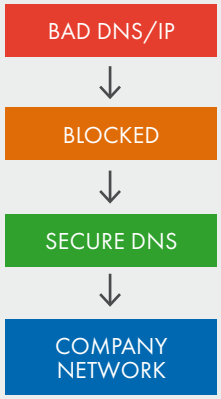
A one-time six month pass to RSA's Governance, Risk, and Compliance (GRC) solution to assess cybersecurity risk. This leverages the National Institute of Standards and Technology framework to assess the business's cybersecurity level, help identify areas of improvements in key functions. This is an ideal tool for large businesses or critical infrastructure companies (such as power generation, telecoms, public health).



SecureDNS

Powered by *RiskAnalytics*

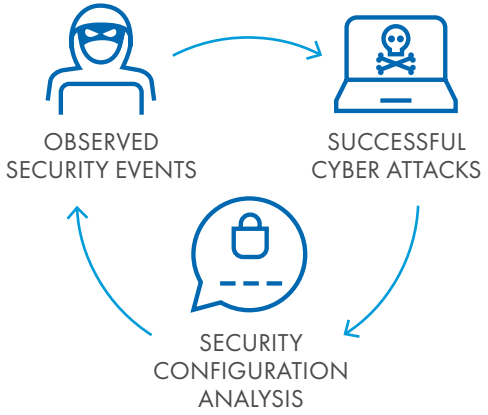
SecureDNS provides an always-on defence against domain-based threats by identifying communication with malicious domains and redirecting users to a safe landing page or sending bad traffic to a sinkhole. This removes a critical route used by hackers to phish and trick users, deliver ransomware, infect systems, remove stolen data and cause a cyber-breach.



Security Ratings

Powered by *Bitsight Technologies*

BitSight generates security ratings for organisations to measure and monitor their own network and those of their third-party vendors. The ratings are generated unobtrusively through BitSight's continuous measuring of externally observable data. Qualifying* CyberEdge clients will also be eligible to receive a complimentary BitSight Security Rating report to measure their business's security performance.



*Available on a complimentary basis to CyberEdge policyholders with premiums in excess of £5,000.

Vendor Security Ratings

Powered by *Security Scorecard*

Partner, supplier, and vendor security risk is a major area that many businesses tend to ignore. Vendor Security Ratings provides a scorecard that enables organisations to measure and monitor the security of own network and of those their third party vendors. This allows organisations to take control of their third party ecosystem, and prioritise their riskiest vendors. A demo or trial is available upon request.

Global Claims Expertise

At AIG, we process approximately four cyber claims every business day. Our underwriting and claims teams partner together to help create the best possible experience. The CyberEdge claims team is ready to assist clients as soon as they suspect a potential network breach.

Support When Clients Need it Most

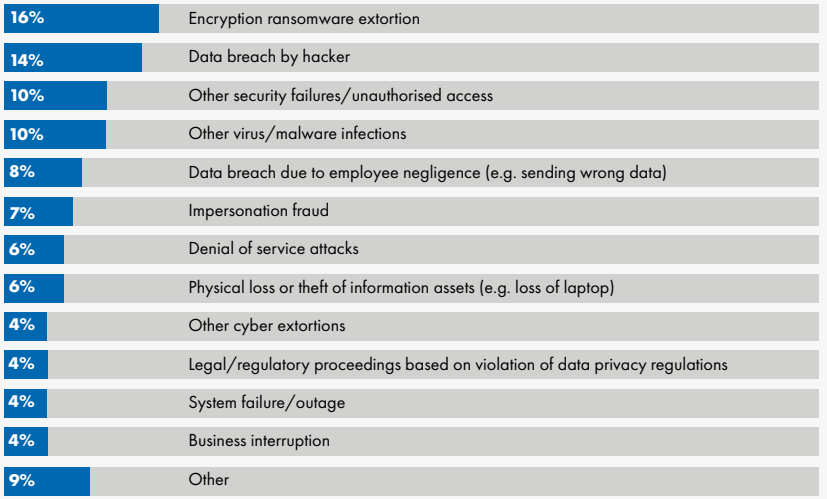
- Our claims specialists react quickly to guide our clients, from assessing their needs to processing their claim.
- Our network of legal firms, forensic investigators, and public relations firms offer immediate support for insureds managing the consequences of a breach.

Rapid Technical Support

- Our CyberEdge hotline is available 24/7/365 for those policyholders with First Response cover. Once a call is made to the hotline, the CyberEdge Claims Team will coordinate with clients and engage any necessary vendors including breach counsel and forensics firms to identify immediate threats (such as a hacker inside a network), and start the restoration and recovery processes.

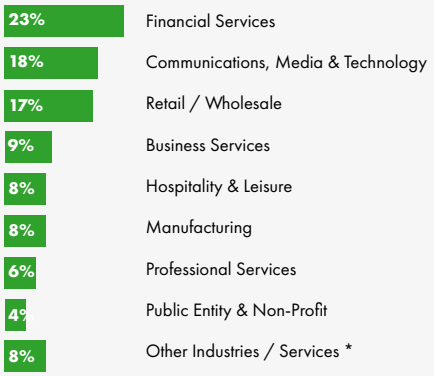
Since 1999, we have helped thousands of companies globally respond to cyber-attacks.

Cyber claims received by AIG EMEA (2013-2016) - By type



Note: Figures may not add up to 100% due to rounding

Cyber claims received by AIG EMEA (2013-2016) - By industry



*Construction, Food & Beverage, Information Services, Other Services, Transportation, Agriculture & Fisheries, Energy and Real Estate
Note: Figures may not add up to 100% due to rounding

For more cyber claims insights, refer to our:
Claims Intelligence Series - Behind the numbers: Key drivers of cyber insurance claims report

VIEW REPORT >

VIEW SME CLAIMS EXAMPLES >

SME Claims Examples

The costs of a cybersecurity incident can rack-up quickly, even for small and medium sized businesses. Here are some examples that highlight the costs involved in a claim.

	Retailer	Accountants	Membership Organisation	Marketing Agency
Size of Business	£3,000,000	£1,500,000	£3,000,000	£5,000,000
Loss Description	A third party payment provider suffered a breach affecting 5,000 of the insured customer records	Two employees opened an infected word document which downloaded Crypto Locker Malware on to the client's network preventing users to accessing their data. Network was down for approx. 32 hours.	The insured suffered a persistent Denial of Service attack which affected all of their websites. Once the websites were back up and running, a customer logged on to their account and was able to view another customers details including financial information.	A back-up tape was collected by the wrong courier. The back-up tape held the details of 3.2M members
Response Costs	£9,633.94	£15,533.00	£12,338.00	£12,694.14
Legal Costs	£6,476.60	£8,854.00	£9,600.00	£21,761.38
Notification Costs	£3,238.30	-	£6,874.00	£20,725.12
PR/Communication Costs	£12,082.10	£6,875.00	£13,453.00	£13,673.40
ID Monitoring Costs	£3,750.00	£8,000.00	£5,648.00	£35,862.75
Network Interruption Costs	-	£8,943.00	£14,650.00	-
PCI Costs	£16,191.50	-	-	-
Total Cost	**£51,372.44**	**£48,305.00**	**£62,563.00**	**£104,716.79**

LONDON
58 Fenchurch Street
London EC3M 4AB
Tel: 020 7954 7000

BELFAST
Forsyth House, Cromac Sq
Belfast BT2 8LA
Tel: 02890 726002

BIRMINGHAM
Embassy House,
60 Church Street
Birmingham B3 2DJ
Tel: 0121 236 9471

CROYDON
2-8 Altyre Road, Croydon
Surrey CR9 2LG
Tel: 020 8681 2556

GLASGOW
Centenary House
69 Wellington St
Glasgow G2 6HJ
Tel: 0141 303 4400

LEEDS
5th Floor Gallery House
123-131 The Headrow
Leeds LS1 5RD
Tel: 0113 242 1177

MANCHESTER
4th Floor, 201 Deansgate
Manchester M3 3NW
Tel: 0161 832 8521

www.aig.com

American International Group, Inc. (AIG) is a leading global insurance organisation. Founded in 1919, today AIG member companies provide a wide range of property casualty insurance, life insurance, retirement products, and other financial services to customers in more than 80 countries and jurisdictions. These diverse offerings include products and services that help businesses and individuals protect their assets, manage risks and provide for retirement security. AIG common stock is listed on the New York Stock Exchange and the Tokyo Stock Exchange.

Additional information about AIG can be found at www.aig.com and www.aig.com/strategyupdate | YouTube: www.youtube.com/aig | Twitter: @AIGinsurance | LinkedIn: www.linkedin.com/company/aig.

AIG is the marketing name for the worldwide property-casualty, life and retirement, and general insurance operations of American International Group, Inc. For additional information, please visit our website at www.aig.com. All products and services are written or provided by subsidiaries or affiliates of American International Group, Inc. Products or services may not be available in all countries, and coverage is subject to actual policy language. Non-insurance products and services may be provided by independent third parties. Certain property-casualty coverages may be provided by a surplus lines insurer. Surplus lines insurers do not generally participate in state guaranty funds and insureds are therefore not protected by such funds.

AIG Europe Limited is registered in England: company number 1486260. Registered address: The AIG Building, 58 Fenchurch Street, London EC3M 4AB. AIG Europe Limited is authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and Prudential Regulation Authority (FRN number 202628). This information can be checked by visiting the FS Register (www.fca.org.uk/register).

GBL00001916 0517