



CyberEdge®

Cyber insurance to protect businesses from one of today's most volatile risks.

As the fourth industrial revolution becomes a reality, business success is increasingly reliant on the use of data. With evolving regulation around the handling of sensitive data and an increased reliance on computer systems to run a competitive business, cyber insurance is more vital than ever. CyberEdge's end-to-end risk solution helps your clients stay ahead of the curve.

Coverage Sections

CyberEdge is flexible modular policy which allows businesses to select cover that matches their specific risk profile.



First Response

Expert legal and IT forensics within 1 hour of ringing our hotline whenever clients have (or suspect) a cyber incident. No policy retention for 48 or 72 hours depending on the policy. [Learn more](#)



Cyber Extortion

Covers the costs specialist services to combat cyber extortion including investigations, containment, negotiations and ransom payments. [Learn more](#)



Event Management

Legal, IT, PR services, Credit and ID Monitoring, Data Restoration and Breach Notification costs after a cyber-attack. [Learn more](#)



Network Interruption

Loss of income, mitigation expenses and costs to quantify the loss when interrupted by a selected peril including cyber-security breach, system failure and voluntary shutdown. [Learn more](#)



Security and Private Liability

Defence costs and insurable fines for alleged breaches of confidential information, security failure, failure to notify the regulator and breaches of PCI compliance. [Learn more](#)



Criminal Reward Fund

A reward paid for information that leads to the conviction of anyone attempting to commit an illegal act relating to cover provided by CyberEdge. [Learn more](#)



Digital Media

Damages and defence costs for breaching third-party intellectual property, or negligence in connection with electronic content. [Learn more](#)



Telephone Hacking

Covers charges from unauthorised access and use of a business's telephone system, whether initiated on or off their premises. [Learn more](#)



Computer Crime

Financial loss from fraudulent electronic fund transfers arising from a cybersecurity breach, and impersonation fraud where clients are tricked by fraudulent emails. [Learn more](#)

Cyber Claims Expertise

CyberEdge is underpinned by the deep experience of our cyber claims team. At AIG, our adjusters have handled all types of cyber incidents including ransomware, business email compromise or breaches of personal information.

Cyber Loss Control Services

Complimentary tools and services are included with each CyberEdge policy for eligible clients* to provide knowledge, training, security, and advisory solutions.

- **Employee Cybersecurity eLearning**
- **Incident Response Plan**
- **Cyber Maturity Report Review**
- **Cyber Claims Hotline**
- **Network Security Rating**
- **Cybersecurity Information Portal**
- **CyberMatics****

* Clients purchasing CyberEdge and spending more than £900 in premium qualify for these complimentary services.

**Subject to availability. For details regarding availability, please contact AIG.

AIG may modify (by adding, removing or replacing a tool or service) or discontinue the Services at any time. AIG may partner with third party vendors to provide any or all Services. In some instances, AIG may have a referral fee structure in place, or an ownership interest, with certain third party vendors.

Cyber Claims Examples

Bogus Courier

A small marketing agency used a regular courier to transport their data cartridges. On one occasion a bogus courier arrived, and the data cartridges were handed over to them. It was only a few hours later, only when the real courier turned up that the agency realised the error. Whilst they initially assumed that this would be a crime claim, in fact as it was the data that was the target of the theft, and not money, it was the cyber policy that responded.

First response, data retrieval and notification costs in this instance exceeded £100,000.

Distributed Denial of Service Attack

A service agency that received and fulfilled online orders via its website suffered a Distributed Denial of Service Attack in which a “bad actor” attempts to disrupt the normal traffic of a target, service or network by overwhelming the target with a flood of Internet traffic.

This affected the availability of the agency’s website and its ability to accept online orders for two days (during the second busiest period of the year). The agency received three separate ransom emails but chose not to pay the ransom to stop the attack. Instead they instructed AIG’s appointed IT forensics team who assisted them in identifying malicious traffic in order to implement effective traffic filters in response.

In addition to the cost of the IT Forensics services the Policy also covered the insureds loss of income under the Network Interruption cover. (Which we know from our experience of handling cyber claims can add considerably to the cost of claims depending on the length of disruption.)

Employee Error – Breach of confidentiality

An employee, in error, emailed confidential payroll documents containing sensitive employee details to the wrong recipient. The unintended recipient confirmed that upon receipt of the information it was viewed by one person and then deleted from their computer systems. However the insured was aware they still had obligations under the GDPR. They called our First Response helpline for advice and within the excess free period of the first 48 hours AIG’s appointed Lawyers advised them and helped them draft the relevant notifications to the data recipient and to the Information Commissioners Office the regulatory body.

Ransomware

A UK retailer suffered a ransomware attack which encrypted their entire internal computer network. Their external website was unaffected, but orders could not be fulfilled as customer emails could not be sent, stock items confirmed, deliveries organised etc and their online business came to a halt. A ransom payment of £120,000 in bitcoin to decrypt the Insured’s computer systems was demanded.

The Insured notified AIG’s Emergency Response number and within an hour our breach response team had instructed IT Forensics, Lawyers and PR consultants to help mitigate and resolve the issue. The first 48 hours of costs were paid by AIG with no excess, we then continued to provide ongoing support as part of our Event Management cover. After a few days it was determined that there was no alternative but to pay the ransom and negotiators were instructed to organise the payment. It took a further 9 days of specialist work for the Computer systems to be fully restored.

The Policy covered IT Forensics costs, PR, Legal advice and negotiators’ costs and also Network Interruption to reimburse the loss of profit whilst the retailer could not trade. In this instance the policy paid the full limit of £1,000,000 because of the inclusion of the Network Interruption cover and the length of time the insureds systems were down.

Phishing attack

An employee in a firm of Architects received an email which appeared to be from Microsoft. The individual clicked on the link which granted the bad actor access to the employee’s email account.

Unknown to the employee or the Company, the attacker exploited the access to implement a rule on the employee’s email account to automatically forward all emails to the bad actor. As a result, they had access to all email traffic in and out of the company including confidential client and supplier information, invoices and bank details.


The client called the AIG helpline and IT and Legal experts were instructed to assist. Our appointed IT Forensics team removed the rule and confirmed the data that had been viewed or downloaded. With this knowledge of the compromised data, the client (aided by our appointed Lawyers, who helped draft the communication) was able to notify the relevant data subjects, including employees, clients, suppliers and the regulatory body, the Information Commissioners Office.

















OPEN MARKET

To find out more about our comprehensive open market solution visit: www.aig.co.uk/cyberedge

E-TRADE

CyberEdge is available to trade online via **AIG eXtra** and **Acturis** under three easy to purchase cover bundles.

Click on the  icon below for summary movie

BREACH Bundle	IMPACT Bundle	COMPLETE Bundle
 Security and Privacy Liability	+ BREACH Bundle  Cyber Extortion	+ BREACH Bundle + IMPACT Bundle
 Event Management	 Telephone Hacking	 Network Interruption: System Failure
 First Response	 Network Interruption: Security Failure	 Network Interruption: OSP Security Failure
 Criminal Reward Fund	 Network Interruption: Loss Preparation	 Network Interruption: OSP System Failure
 Loss Prevention Services (subject to eligibility, please refer to your quote/policy schedule)	 Loss Prevention Services (subject to eligibility, please refer to your quote/policy schedule)	 Digital Media  Loss Prevention Services (subject to eligibility, please refer to your quote/policy schedule)
+ OPTIONAL For all Bundles		 Computer Crime

To find out more about our e-traded solution visit: www.aig.co.uk/etrade



This document does not contain the full terms and conditions of the Policy. The full terms and conditions are in the Policy itself and its schedule, both of which will be issued following the Policy being taken out or specimens of which can be supplied upon request prior to the Policy being taken out. Scope and terms are subject to the terms and conditions of the policy. American International Group, Inc. (AIG) is a leading global insurance organization. AIG member companies provide a wide range of property casualty insurance, life insurance, retirement solutions and other financial services to customers in approximately 70 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. Additional information about AIG can be found at www.aig.com | YouTube: www.youtube.com/aig | Twitter: @AIGinsurance www.twitter.com/AIGinsurance | LinkedIn: www.linkedin.com/company/aig. These references with additional information about AIG have been provided as a convenience, and the information contained on such websites is not incorporated by reference herein. 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 jurisdictions, and coverage is subject to underwriting requirements and 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. American International Group UK Limited is registered in England: company number 10737370. Registered address: The AIG Building, 58 Fenchurch Street, London EC3M 4AB. American International Group UK Limited is authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and Prudential Regulation Authority (FRN number 781109). This information can be checked by visiting the FS Register (www.fca.org.uk/register).