



International Financial Lines | United Kingdom



Why choose AIG for Cyber?

This marketing material is intended for insurance brokers and other insurance professionals for their information.
For full terms, conditions and benefits related to AIG products, please refer to the policy and associated documents.

For full pdf features, please view in Adobe Acrobat.

For over two decades, AIG has been a pioneer and trusted partner in navigating the complexities of cyber risks. Today, we continue to evolve with the threat landscape, delivering forward-looking solutions that proactively help clients identify vulnerabilities, strengthen defences, and respond swiftly to incidents.

Rapid Incident Response

Included with our primary Cyber policies*

First Response: Support Without Barriers

- Access to cybersecurity experts with global reach and capability, including legal counsel, forensic analysts, and crisis communicators for up to 48 or 72 hours depending on the policy.
- Clients can use First Response whenever they have (or even just suspect) a cyber incident, with no policy retention.
- The service helps to minimise financial losses from operational disruption, legal liabilities, and regulatory fines.

Why Retention-Free and Without Prejudice Matters

- First Response does not erode policy limits, and does not require a retention – it's about helping clients resolve an incident.
- Engaging First Response will never compromise a client's claim. Whether the incident is covered or not, First Response begins immediately.
- No retention ensures no delays. Clients can focus on resolving the crisis, not worrying about upfront expenses.

The Value It Brings to Your Clients

- There are no additional costs or need to carve out premium to other providers, providing a cost-effective solution for clients.
- Our experts act in the best interest of your clients, without unnecessary limitations or red tape.
- Even large clients with inhouse legal and IT security support can benefit from additional expert capabilities during a cybersecurity incident.



24/7 hotline.



Legal Response Advisor will contact within 1 hour: take details, advise on next steps and assist with response coordination.



IT Specialist appointed to help determine what has been affected and how it can be contained, repaired or restored.



Initial legal advice on requirements to notify regulators and individuals.



If required, Crisis Communicator appointed to mitigate reputational damage and Cyber Extortion Advisor for extortion or ransomware.

How it Benefits Brokers

Brokers can confidently promote First Response as a critical value-add, helping clients recover swiftly and with minimal disruption. AIG stands out from competitors by providing immediate assistance without upfront costs or coverage concerns.

* First Response may NOT be available on all policies, including potentially in LATAM, Excess policies, quota share, or specific accounts. Please contact your local AIG underwriter for specifics.



Proactive Cyber Resiliency

AIG doesn't just insure against cyber risks; we help businesses prevent them. We combine our technical expertise and decades of claims insights with targeted cybersecurity services from industry-leading cybersecurity firms to help clients act before threats become realities.

From notifying clients of unpatched vulnerabilities to employee cybersecurity training services, our comprehensive, data-backed Cyber Resiliency Programme approach helps clients proactively mitigate a cyber incident and its far-reaching effects.

400+

Clients alerted mid-policy of unpatched vulnerabilities, misconfigurations, and malware findings.

10,000+

Cyber claims reviewed for control failures and threat actor tactics to help advise clients on key claim factors.

5,000,000

Connections blocked monthly for clients using Blacklist IP Blocking service.



Proactive Cyber Resiliency

RISK ADVISORY
TEAM

AIG's Cyber Risk Advisory Team

Our in-house AIG Cyber Risk Advisory team is comprised of experienced cyber risk experts with vast knowledge of the latest threats. They work with clients throughout the policy period to analyse their current cybersecurity posture and use claims insights, root cause analysis investigations, and best practices to identify steps to help clients improve their cyber risk posture.

Technical Underwriting Input

Cyber Risk Advisors provide support during the underwriting process for complex placements and nuanced risks and remain available throughout the policy lifecycle. This technical input strengthens client confidence and enhances the broker's credibility by including expert insight during account placement.

AIG Cyber Loss Control Onboarding

A one-to-one call to present each of the complimentary services listed in the Cyber Resiliency Programme.

Real-Time Threat Intelligence and Alerting

AIG's alerting process makes clients aware if key vulnerabilities, misconfigurations, or malware are identified in their public infrastructures so they can be addressed before leading to a cyber incident.

AIG Claims Process Orientation

Clients can also benefit from a one-on-one review of critical response and reporting steps they should take in the event of a cyber incident.

MEET AIG'S CYBER RISK ADVISORY TEAM

How it Benefits Brokers

By introducing your clients to AIG's Cyber Risk Advisory Team, you strengthen their cyber posture while demonstrating your commitment to their long-term success.

Proactive Cyber Resiliency

LOSS CONTROL
SERVICES

Loss Control Services

AIG has partnered with industry-leading cybersecurity firms to provide eligible CyberEdge policyholders targeted services that can help proactively prevent a cyber incident and its far-reaching effects.

We offer a range of complimentary loss control tools and expert services.

[SELECT ITEM TO LEARN MORE](#)

Tools and services eligibility varies by premium size.*

Tier 3

Premiums of £5,000 or greater.

Tier 2

Premiums of £900-£4,999.

Tier 1

Premiums of £899 or less.

* Premium eligibility is the same for pounds, euros or dollars

Proactive Cyber Resiliency

ADDITIONAL TOOLS
AND SERVICES

Additional Benefits, Tools and Services

In addition to the services included with eligible policies, all AIG cyber clients have access to the following services at a preferred rate, some of which are available for a free demo. These services have been specifically selected based on our decades of experience and how well they can help strengthen the cybersecurity maturity of an organisation.

BITSIGHT

BitSight Security Ratings
powered by BitSight Technologies

SpyCloud

Enterprise Protection
powered by SpyCloud

CROWDSTRIKE

Endpoint Detection and Response (EDR)
powered by CrowdStrike's Falcon Insight

SafeBreach

Breach & Attack Simulation
powered by SafeBreach

CYBERARK

CyberArk DNA
powered by CyberArk

SILVERFORT

Unified Identity Protection Platform
powered by Silverfort

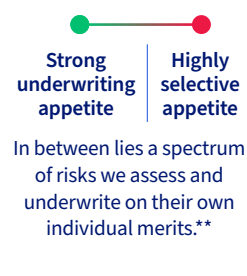
Outstanding Coverage and Multinational Capabilities



We have a broad risk appetite for businesses and organisations of all sizes, across a host of business sectors:

Industries

Most industry sectors	●
Businesses and organisations of all sizes:	
SME	●
Mid-Market	●
Corporate	●
Multinational	●
Businesses and organisations in most geographies*	●
Credit rating agencies	
Social media platforms	●
Crypto currencies/brokers	●
DNA testing	●



COVERAGE SECTIONS

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



- First Response
- Event Management
- Security and Privacy Liability
- Network Interruption:
 - Security Failure Cover
 - System Failure Cover
 - OSP Security Failure Cover
 - OSP System Failure Cover
- Voluntary Shutdown
- Cyber Extortion
- Telephone Hacking
- Computer Crime
- Criminal Reward Fund
- Digital Media

Why is this Important to Brokers

Many organisations operate across multiple territories, and the evolution of cyber cover has increased the need for local policies. Subsidiaries may use different IT infrastructure, rely on separate third-party providers, or act as independent data controllers – all of which can create exposure requiring local policy issuance or claims payments. AIG's dedicated multinational team can design, implement and execute custom-made solutions across multiple jurisdictions and oversee placements throughout the life-cycle of the programme.

* Subject to sanctions and territorial exclusions

** Guide only - every case written on its merits. Risk quality is the driver for risk selection.

Outstanding Coverage and Multinational Capabilities



We have a broad risk appetite for businesses and organisations of all sizes, across a host of business sectors:

Industries

Most industry sectors	●
Businesses and organisations of all sizes:	
SME	●
Mid-Market	●
Corporate	●
Multinational	●
Businesses and organisations in most geographies*	●
Credit rating agencies	
Social media platforms	●
Crypto currencies/brokers	●
DNA testing	●

● — ●
Strong underwriting appetite | Highly selective appetite

In between lies a spectrum of risks we assess and underwrite on their own individual merits.**

GLOBAL CLIENTS

For clients with overseas operations, we have outstanding multinational capabilities.

Cyber Multinational Excellence

AIG can create multinational solutions in over 200 countries and jurisdictions.* This means we can build and service robust and compliant global cyber programmes, ensuring no gaps in cover, wherever in the world clients are located.

Global Fronting Solutions

AIG has an award-winning captive fronting team and decades of experience and expertise in Financial Lines Multinational captive fronting and risk transfer solutions.

*Through AIG-owned operations, AIG licenses and authorisations, and network partner insurers.

Why is this Important to Brokers

Many organisations operate across multiple territories, and the evolution of cyber cover has increased the need for local policies. Subsidiaries may use different IT infrastructure, rely on separate third-party providers, or act as independent data controllers – all of which can create exposure requiring local policy issuance or claims payments. AIG's dedicated multinational team can design, implement and execute custom-made solutions across multiple jurisdictions and oversee placements throughout the life-cycle of the programme.

* Subject to sanctions and territorial exclusions

** Guide only - every case written on its merits. Risk quality is the driver for risk selection.

Unmatched Claims Expertise

CASE STUDY 1

AIG's specialist Cyber Claims Team is one of the most experienced in the market. Our adjusters have expertise in insurance, law, and industry-specific challenges. Our team have also handled all types of cyber incidents including ransomware, business email compromise or breaches of personal information.

Zero-Day Vulnerability and Data Breach



AIG's insured, a business-to-business human resource and payroll solutions company, utilised third-party software to transfer confidential information to their clients. A threat actor exploited a zero-day vulnerability in the software and exfiltrated sensitive information, including bank account numbers and payroll data, for approximately 500,000 data subjects.

The insured triggered AIG's First Response service and obtained immediate legal advice on the suspected breach of confidential information including their rights against the software supplier and their notification obligations to their clients and the data subjects. By accessing legal advice so quickly the insured was able to direct the response, protect their reputation and support their clients in fulfilling their own obligations as Data Controllers. AIG also worked with the insured to instruct a forensic expert, credit monitoring provider and crisis communications firm which reduced the insured's financial and reputational risk.

AIG continues to support the insured in defending multiple liability claims. AIG worked with the insured to settle contractual claims early; avoiding litigation and ensuring there was no damage to ongoing business relationships. And defence lawyers from AIG's expert panel continue to defend the insured against proceedings brought by data subjects in multiple European jurisdictions alleging a breach of the GDPR.

The scenarios described herein are offered only as examples. Coverage depends on the actual facts of each case and the terms, conditions and exclusions of each individual policy. Anyone interested in the above product(s) should request a copy of the standard form of policy for a description of the scope and limitations of coverage.

Unmatched Claims Expertise

CASE STUDY 2

AIG's specialist Cyber Claims Team is one of the most experienced in the market. Our adjusters have expertise in insurance, law, and industry-specific challenges. Our team have also handled all types of cyber incidents including ransomware, business email compromise or breaches of personal information.

Data Exfiltration and Dark Web Dissemination



An AIG insured in the entertainment service industry was notified by its cloud-based data warehouse provider that it had found evidence of a threat actor accessing the insured's account. The impacted dataset included the personal information of millions of the insured's customers.

The insured immediately contacted AIG's hotline for advice on how to proceed, including the approach for notifying customers and regulators, communications strategy and mitigating potential third-party exposure. An AIG cyber claims expert provided guidance to the insured and mobilised a specialist cyber and data privacy law firm along with a digital forensics expert to navigate immediate next steps, including containment and investigation. With AIG's assistance, a call centre was established to assist with customer queries and complaints.

When the threat actor advertised the insured's data for sale on the dark web, the AIG appointed law firm successfully obtained an injunction to prevent use or dissemination of the data. The law firm continued to assist the insured to successfully defend third-party demands and respond to regulatory queries.

AIG's First Response service enabled the insured to take urgent steps to contain the data breach and provided access to specialist vendors to manage the financial and reputational risk to the insured's business.

The scenarios described herein are offered only as examples. Coverage depends on the actual facts of each case and the terms, conditions and exclusions of each individual policy. Anyone interested in the above product(s) should request a copy of the standard form of policy for a description of the scope and limitations of coverage.

Unmatched Claims Expertise

AIG's specialist Cyber Claims Team is one of the most experienced in the market. Our adjusters have expertise in insurance, law, and industry-specific challenges. Our team have also handled all types of cyber incidents including ransomware, business email compromise or breaches of personal information.

The scenarios described herein are offered only as examples. Coverage depends on the actual facts of each case and the terms, conditions and exclusions of each individual policy. Anyone interested in the above product(s) should request a copy of the standard form of policy for a description of the scope and limitations of coverage.

Ransomware Attack



An AIG insured in the specialty industrial equipment and machinery industry was hit by a ransomware attack initiated through a phishing e-mail. The threat actor gained control of the insured's domain controller allowing lateral movement and system-wide encryption. Although personal and commercial data was accessed no data was exfiltrated.

With support from AIG, the insured engaged digital forensics experts and legal counsel to lead the response. Critical systems were restored quickly, minimising downtime and reducing operational disruption. Legal counsel ensured all regulatory reporting obligations were properly met.

Thanks to the swift response enabled by AIG, the insured was able to avoid paying a ransom and business interruption losses were contained. AIG covered the costs of forensics, legal support, and data recovery efforts. The insured resumed operations quickly and preserved its reputation with clients and partners.

CASE STUDY 3

www.aig.co.uk



American International Group, Inc. (NYSE: AIG) is a leading global insurance organization. AIG provides insurance solutions that help businesses and individuals in more than 200 countries and jurisdictions protect their assets and manage risks through AIG operations, licenses and authorizations as well as network partners. For additional information, visit www.aig.com. This website with additional information about AIG has been provided as a convenience, and the information contained on such website is not incorporated by reference herein.

AIG is the marketing name for the worldwide operations of American International Group, Inc. 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).