



CyberEdge®

Soluzioni *end-to-end* per la gestione dei rischi
informatici





CyberEdge® è una soluzione *end-to-end* per la gestione dei rischi, che consente ai clienti di stare al passo con la rapida evoluzione dei cyber-rischi.

CyberEdge offre le coperture assicurative, gli strumenti e l'accesso costante alle migliori prassi di cui i clienti hanno bisogno per valutare e attenuare la loro potenziale esposizione a svariati rischi: violazione di dati sensibili, pirateria informatica, errori commessi dal personale. Tutto ciò è possibile grazie all'esperienza da noi maturata nel corso degli anni con la copertura di questo tipo di rischi e grazie alla collaborazione con esperti informatici.

CyberEdge: una soluzione per la gestione dei rischi

CyberEdge offre agli assicurati un supporto orientativo in ogni fase, attraverso strumenti di prevenzione innovativi (finalizzati a informare i clienti e potenzialmente a prevenire gli incidenti informatici) e i servizi erogati dal nostro CyberEdge Breach Resolution Team in caso di sinistro.

Consulenza e prevenzione dei rischi	Copertura assicurativa	Breach Resolution Team
<p>Preparazione e informazione</p> 	<p>Danni a terzi derivanti da una violazione della sicurezza o dei dati</p> 	<p>Supporto 24/7</p> 
<p>Formazione e compliance</p> 	<p>Costi diretti sostenuti dall'assicurato in risposta a una violazione</p> 	<p>Servizi giuridici e consulenza forense</p> 
<p>Informazioni sulle minacce globali e valutazione</p> 	<p>Lucro cessante e costi di esercizio derivanti da una violazione dei dati o della sicurezza</p> 	<p>Call center per le notifiche, il <i>credit monitoring</i> e l'<i>ID monitoring</i></p> 
<p>Servizi di shunning</p> 	<p>Minacce di divulgazione di dati o di attacco a sistemi a fini di estorsione</p> 	<p>Esperti di <i>crisis communication</i></p> 
<p>Consulenza specializzata</p> 	<p>Diffamazione online e violazione di diritti d'autore e di marchi commerciali</p> 	<p>Oltre 15 anni di esperienza nella gestione di sinistri nel settore informatico</p> 

Consulenza in materia di rischi e prevenzione

La protezione offerta da CyberEdge rafforza efficacemente la prima linea di difesa di cui un'azienda dispone per contrastare le minacce informatiche al sistema IT aziendale. Monitoriamo costantemente il panorama informatico affinché i nostri assicurati siano sempre al passo con la tecnologia, in un mondo in cui i cyber-rischi sono in continua evoluzione. I nostri strumenti di prevenzione offrono ai clienti le conoscenze, la formazione, la sicurezza e la consulenza necessarie per adattarsi ai mutamenti in corso.

L'App Mobile CyberEdge per iPhone®, iPad® e Android™

Grazie alla App Mobile CyberEdge, gli utenti avranno a portata di mano le ultime novità in tema di incidenti informatici, oltre a notizie, opinioni e analisi dei rischi. Intuitiva e ricca di funzionalità, l' App rappresenta una novità assoluta in questo campo ed è disponibile per iPhone, Ipad e Android.



Caratteristiche:

- Data Breach Threat Map: una mappa delle violazioni di dati commesse nel mondo, oltre a informazioni sulla normativa in materia di notifiche vigente nel paese in cui è stata commessa la violazione.
- Esempi reali di sinistri relativi a violazioni informatiche per le quali CyberEdge offre copertura.
- Calcolatore: gli utenti potranno inserire i dati della propria azienda per calcolare i potenziali costi associati a una violazione di dati.
- Contenuti disponibili in inglese, francese e spagnolo.



K2 Intelligence: informazioni sulla “Dark Net”

La facilità con cui vengono commessi i reati informatici nonché i proventi che se ne ricavano sono sempre maggiori, soprattutto in un contesto in cui le società devono continuamente adeguarsi per operare in un mondo sempre più digitale e interconnesso.

K2 Intelligence può collaborare con i contraenti delle polizze CyberEdge a tariffe preferenziali fornendo informazioni aggiornate sulle informazioni che circolano tra gli hacker nella cosiddetta “Dark Net” (o rete oscura) a proposito delle aziende in questione. La “Dark Net” è la base operativa, il porto sicuro da cui i cyber-criminali più sofisticati sferrano i loro attacchi.

K2 Intelligence perlustra la “Dark Net” alla ricerca di dati utilizzando crawler di ricerca e sofisticate tecniche di raccolta di informazioni da fonte umana (*human intelligence*). Questo tipo di informazioni personalizzate è estremamente prezioso per le aziende che

- adottano un approccio proattivo nel predisporre i loro programmi di gestione dei rischi in materia di sicurezza informatica, assicurando l'introduzione di adeguati standard e protocolli di *corporate governance*;
- effettuano fusioni e acquisizioni. La consulenza fornita dagli esperti di K2 Intelligence e le informazioni raccolte possono tornare utili alle aziende in fase di fusione o acquisizione per l'attività di *due diligence* in relazione alla sicurezza informatica.

IBM: verifica delle vulnerabilità delle infrastrutture

A clienti selezionati IBM offre un servizio di rilevamento delle vulnerabilità delle infrastrutture. IBM effettua una verifica a distanza delle infrastrutture esterne di tipo web-facing (visibili dal web) dei clienti, contribuendo così a individuare potenziali vulnerabilità che un hacker remoto potrebbe sfruttare via Internet. Inoltre il servizio di verifica delle vulnerabilità infrastrutturali:

- rileva e classifica secondo priorità i rischi insiti nell'infrastruttura di rete visibile al pubblico;
- offre un quadro dettagliato delle vulnerabilità dell'azienda affinché i clienti possano monitorare e capire meglio il proprio profilo di sicurezza e produrre relazioni a riguardo;
- classifica secondo priorità le vulnerabilità rilevate, consentendo ai clienti di ridurre la loro esposizione complessiva alle minacce;
- comprende efficaci funzioni di reporting che contribuiscono ad accelerare l'individuazione delle vulnerabilità e l'attuazione di soluzioni.

BitSight: rating sulla sicurezza

BitSight genera rating sulla sicurezza per conto delle aziende al fine di monitorare e misurare le prestazioni della rete aziendale e di quella dei fornitori. I rating sono generati senza intrusioni attraverso la misurazione continua di dati osservabili dall'esterno. I rating sulla sicurezza si basano sui seguenti elementi concreti:

- eventi che interessano la sicurezza, ovvero attacchi informatici sferrati con successo (tra cui botnet, spam, malware);
- dati sull'attività di *due diligence*, o indicatori in base ai quali si possa stabilire se l'azienda abbia adottato provvedimenti per prevenire un attacco (compresa un'analisi adeguata della configurazione di sicurezza).

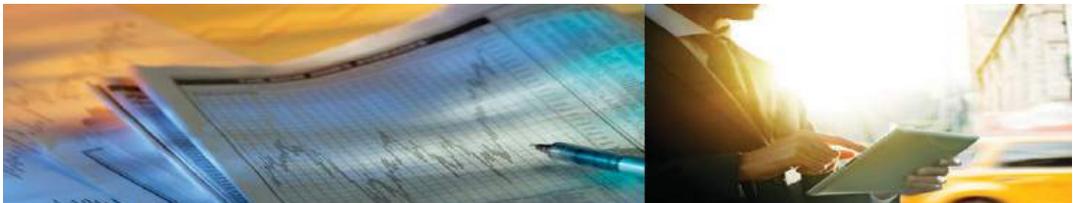
Assicurati CyberEdge selezionati potranno richiedere a BitSight un rapporto complementare relativo al rating sulla sicurezza per misurare le prestazioni dell'azienda sotto il profilo della sicurezza. I contraenti delle polizze CyberEdge beneficiano inoltre di tariffe scontate sui prodotti e servizi di BitSight.

Gli assicurati possono scegliere di utilizzare rating giornalieri nell'ambito del proprio programma di gestione *end-to-end* dei cyber-rischi. Questi rating offrono un quadro chiaro dei cyber-rischi all'interno dell'intero ecosistema aziendale.

RSA: valutazione del grado di maturità in tema di cyber-sicurezza

Gli assicurati hanno diritto a usufruire una sola volta, per un periodo di sei mesi, della soluzione complementare GRC (Governance, Risk and Compliance) di RSA, per valutare i rischi relativi alla cyber-sicurezza dell'azienda. La valutazione si basa sulla soluzione GRC di RSA Archer, che rappresenta un riferimento nel settore.

- La soluzione utilizza il NIST Cybersecurity Framework per valutare il grado di maturità di un'azienda in tema di cyber-sicurezza e per facilitare l'individuazione dei miglioramenti da apportare nelle funzioni chiave.
- Al termine della valutazione, l'azienda avrà un quadro complessivo delle lacune da colmare per raggiungere il grado ottimale di esposizione al rischio.
- Gli assicurati avranno accesso ai servizi Advanced Cyber Defense (ACD) di RSA, che forniscono consulenza operativa con l'obiettivo di colmare le lacune e proteggere le risorse vitali di un'azienda.



RiskAnalytics: servizio di shunning proattivo

I clienti selezionati possono accedere a informazioni aggiornate sulle minacce globali e a una tecnologia all'avanguardia che isola, con la tecnica dello *shunning*, gli indirizzi IP attualmente utilizzati dai criminali. Prima di iniziare un attacco a una rete, i criminali effettuano innanzitutto una "ricognizione" per confermare che determinati indirizzi IP siano obiettivi adeguati. Lo *shunning* impedisce a queste comunicazioni di raggiungere una determinata rete e di confermare che gli indirizzi IP sono obiettivi validi. Quando, in un tentativo di attacco, la fase di ricognizione fallisce, il rischio di un'intrusione successiva è ampiamente ridotto.

Lo *shunning* può inoltre proteggere contro gli attacchi sferrati dall'interno. Se un computer di una rete è già compromesso dalla presenza di malware, lo *shunning* può evitare la comunicazione di ritorno ai server di comando e di controllo dei criminali, disarmando efficacemente il malware. Lo *shunning* avviene in tempo reale alla velocità di linea ed è scalabile per proteggere una sola sede o tutte le sedi di un'azienda a livello globale.

Axio Global: analisi del portafoglio

I contraenti delle polizze CyberEdge possono ricorrere ai servizi di Axio Global (Axio) per tracciare un quadro generale della propria esposizione ai cyber-rischi e armonizzare efficacemente i controlli tecnologici e operativi dell'azienda dotandoli di una copertura assicurativa. La metodologia utilizzata da Axio esamina l'intera gamma dei potenziali danni in materia di cyber-sicurezza: furto di dati, responsabilità civile, danni a cose e danni ambientali, lesioni personali e interruzione dell'attività. I contraenti delle polizze CyberEdge possono usufruire, a prezzi scontati, dei seguenti servizi di Axio:

- seminario di un giorno su possibili scenari di sinistro, per valutare l'impatto finanziario dei potenziali sinistri sui sistemi informatici e di controllo; gli scenari sono personalizzati in base alle specifiche esigenze del cliente e sono organizzati in una tassonomia che può essere utilizzata per sottoporre a prove di stress la copertura assicurativa;
- analisi dell'intero portafoglio delle coperture ramo Danni del cliente, al fine di individuarne la capacità di rispondere a un incidente informatico complesso. Abbinata al seminario sugli scenari di sinistro, questa analisi sottopone a "prove di stress" il portafoglio assicurativo sulla base di scenari realistici;
- autovalutazione del programma di cyber-sicurezza del cliente sulla base del Cybersecurity Capability Maturity Model (C2M2), una metodica raccomandata per la diffusione del NIST Cybersecurity Framework. I risultati della valutazione sono presentati in un report. Uno dei fondatori di Axio è l'ideatore del modello e mette le sue competenze al servizio delle aziende, aiutandole a interpretare il contenuto di questo strumento per effettuare un esame efficace ed efficiente dei rispettivi programmi di cyber-sicurezza.

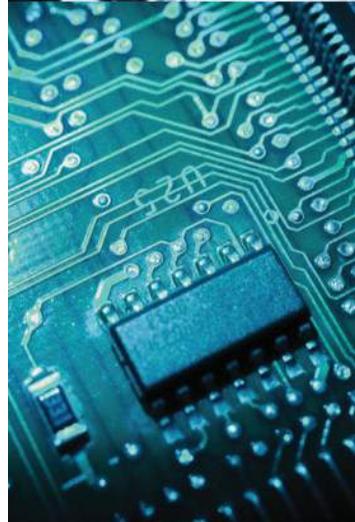
Copertura assicurativa

CyberEdge offre alle aziende una protezione contro i seguenti rischi:

- richieste di risarcimento di terzi derivanti da una falla nella sicurezza della rete dell'assicurato o dalla mancata protezione dei dati. La polizza offre inoltre una copertura contro i provvedimenti delle autorità di regolamentazione connessi a un incidente di sicurezza, a una violazione della privacy o alla mancata segnalazione di un incidente di sicurezza o di una violazione della privacy;
- costi diretti sostenuti dall'assicurato per rimediare a un incidente di sicurezza o a una violazione della privacy; sono coperti i costi connessi a notifiche, pubbliche relazioni e altri servizi necessari per la gestione e il contenimento di un incidente informatico. Sono altresì coperti tutti i costi connessi a indagini forensi, consulenze legali e monitoraggio dell'identità (*identity monitoring*) sostenuti per tutelare le vittime della violazione;
- In caso di interruzione dell'attività causata da una falla nella sicurezza della rete è previsto un indennizzo a copertura della perdita di fatturato e delle spese di esercizio. L'assicurazione copre inoltre la perdita di clientela e il danno reputazionale; la copertura assicurativa può essere estesa al malfunzionamento dei sistemi dei fornitori di servizi esternalizzati o del cloud;
- minacce aventi a oggetto la rete informatica e le informazioni confidenziali di un'azienda, poste in essere da un soggetto esterno al fine di estorcere denaro o altri beni. La copertura indennizza le somme di denaro estorte pagate per fare cessare la minaccia e i costi delle indagini condotte al fine di accertare la causa della minaccia stessa;
- responsabilità delle aziende per i contenuti pubblicati sul proprio sito Internet. Sono inclusi in copertura numerosi rischi connessi alla responsabilità editoriale, tra cui violazione di diritti d'autore o marchi commerciali, diffamazione e invasione della privacy.

Breach Resolution Team

Il CyberEdge Breach Resolution Team è pronto ad assistere gli assicurati al primo sospetto di una potenziale violazione della loro rete. Il nostro Team ha una presenza locale ma può contare su risorse a livello globale: in questo modo i nostri esperti sono in grado di gestire un sinistro seguendone l'evoluzione e di rispondere rapidamente alle richieste degli assicurati.



Laddove vi sia il sospetto che sia stata commessa una violazione, gli assicurati potranno avvalersi del nostro CyberEdge Breach Resolution Team, che vanta più di 15 anni di esperienza nella gestione di sinistri specificamente attinenti al settore informatico.

- Gli esperti di gestione sinistri dispongono dei livelli di autorizzazione necessari per prendere decisioni e fornire una rapida assistenza ai clienti in caso di sospetta violazione della sicurezza.
- Da quando, nel 1999, abbiamo introdotto l'assicurazione della responsabilità per gli incidenti informatici, abbiamo aiutato migliaia di aziende e oltre venti milioni di privati a contrastare gli attacchi informatici;
- la vastità del nostro "inventario sinistri" dimostra che siamo nella posizione migliore per individuare e prevedere l'andamento delle richieste di risarcimento e i valori di liquidazione;
- in media i nostri esperti liquidatori vantano più di sette anni di esperienza nella gestione di richieste di risarcimento complesse avanzate da assicurati e soggetti terzi in relazione a sinistri informatici.

Potendo contare sulla forza della nostra vasta rete di fornitori di servizi, il CyberEdge Breach Resolution Team offre al servizio informatico delle aziende il supporto aggiuntivo necessario per fronteggiare un attacco informatico.

- Il *cyber response team* di KPMG è composto da tecnici, esperti di gestione degli incidenti ed esperti forensi.
- Viene fornita un'assistenza legale specializzata attraverso il nostro partenariato con due importanti studi legali, Norton Rose Fulbright e CMS Cameron McKenna.
- Quando si verifica un incidente informatico, il tempo è un fattore cruciale. Disponendo di un piano di intervento e dell'accesso a risorse esterne, le aziende potranno reagire in maniera efficiente ed efficace sul piano dei costi e porre rimedio ai danni derivanti da una violazione informatica.

- Accesso 24/7 al nostro call center, per **denunciare** il sinistro e ricevere istruzioni.
- Un unico punto di accesso per la segnalazione, l'accertamento e la gestione tempestivi dei sinistri.
- Contatto con i nostri esperti liquidatori locali, che operano sul campo in tutto il mondo.
- Un gruppo di consulenti legali internazionali con competenze locali nella gestione dei sinistri informatici.

I rischi informatici hanno una dimensione mondiale

Attraverso la nostra piattaforma di servizi globale Passport, offriamo ai clienti una soluzione efficiente e completa per stare al passo con l'evoluzione dei cyber-rischi. Mettiamo inoltre a loro disposizione la competenza dei nostri team locali, dotati del know-how necessario per intervenire nelle sedi di attività dei clienti, e del CyberEdge Breach Resolution Team, pronto a offrire assistenza e un supporto orientativo in qualunque parte del mondo. La nostra soluzione per la gestione dei rischi *end-to-end* non conosce confini.

Una protezione globale migliore, più rapida e più efficiente

Passport è uno strumento semplice ed efficace per usufruire di una vasta gamma di vantaggi globali:

- una copertura conforme alla normativa locale e ai requisiti di legge, erogata nel rispetto delle consuetudini locali e nella lingua del paese;
- l'accesso a risorse locali con esperienza in campo assicurativo e nella gestione dei sinistri;
- una copertura intuitiva e coordinata in tutto il mondo.

Un modo più semplice per affrontare i rischi globali nel campo della cyber-sicurezza

Con Passport è molto più semplice dotarsi della necessaria protezione contro i cyber-rischi in tutto il mondo.

- Il cliente riceve un'unica proposta assicurativa contenente i termini del suo programma globale contro i cyber-rischi, comprendente la polizza mondiale e le polizze locali eventualmente richieste.
- La copertura è accettata e resa operante.
- Attraverso i nostri uffici locali disseminati nel mondo vengono emesse opportune polizze locali. Le polizze locali sono predisposte in conformità della normativa locale, delle prassi del settore e dei rischi.¹

¹ I massimali dipendono dalla gestione delle capacità; è possibile che in taluni paesi esistano limitazioni per quanto riguarda la disponibilità di un unico massimale aggregato piuttosto che separato per il Mondo Intero.



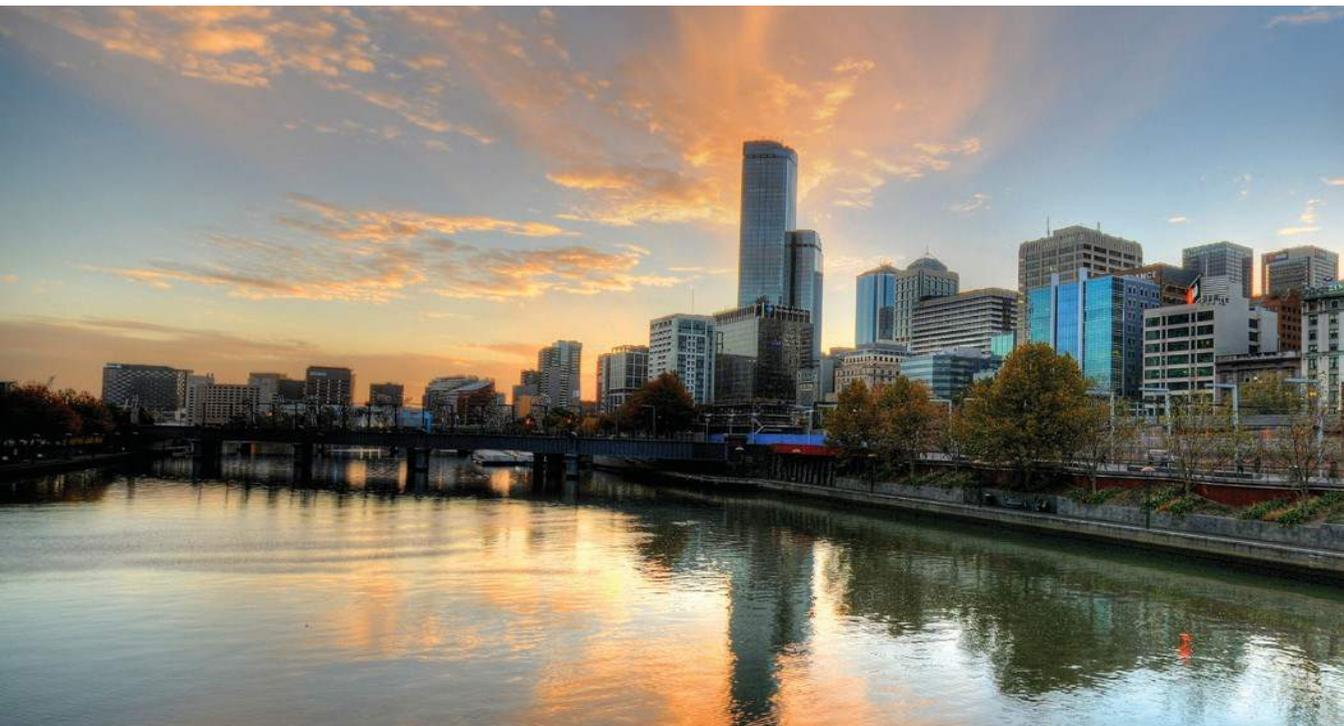


Il tuo "Passport" per le destinazioni CyberEdge

- Australia
- Austria
- Bahrein
- Belgio
- Brasile*
- Bulgaria
- Canada
- Cile
- Colombia
- Cipro
- Repubblica ceca
- Danimarca
- Ecuador
- Finlandia
- Francia
- Germania
- Grecia
- Hong Kong
- Ungheria
- Irlanda
- Israele
- Italia
- Giappone
- Kuwait
- Libano
- Lussemburgo
- Malesia
- Messico
- Paesi Bassi
- Nuova Zelanda
- Norvegia
- Oman
- Panama
- Filippine
- Polonia
- Portogallo
- Portorico
- Qatar
- Romania
- Russia*
- Singapore
- Slovacchia
- Spagna
- Sud Africa
- Corea del Sud
- Svezia
- Svizzera
- Taiwan
- Turchia
- Emirati arabi uniti
- Uganda
- Regno Unito
- Stati Uniti
- Uruguay

Il suddetto elenco di destinazioni è soggetto a modifiche. Per maggiori informazioni, contattate il vostro rappresentante Passport di riferimento.

*Per il Brasile e la Russia è previsto un premio aggiuntivo.



Per maggiori informazioni su CyberEdge:
scriveteci all'indirizzo: CyberEdge@aig.com • Visitate il nostro sito www.aig.com/CyberEdge
Contatti per l'Italia: Walter Villa • Email: walter.villa@aig.com T: +39 02 3690 419
Michele Lavaggi • Email: michele.lavaggi@aig.com T: +39 345 0468095

Download the CyberEdge Mobile App



Follow CyberEdge



Follow@AIGinsurance



Bring on tomorrow

American International Group, Inc. (AIG) è una compagnia di assicurazione leader a livello mondiale con clienti in oltre 100 paesi e giurisdizioni. Le compagnie del gruppo AIG sono al servizio di clienti aziendali, istituzionali e privati attraverso uno dei più estesi *network* mondiali nel settore assicurativo *Property-Casualty*. Negli Stati Uniti le compagnie del gruppo sono inoltre leader nei servizi assicurativi dei rami Vita e Previdenza. Le azioni ordinarie di AIG sono quotate sulle Borse valori di New York e di Tokyo.

Per maggiori informazioni su AIG: www.aig.com | YouTube: www.youtube.com/aig | Twitter: [@AIGemea](https://twitter.com/AIGemea) | LinkedIn: <http://www.linkedin.com/company/aig>

AIG è il nome commerciale delle imprese che fanno capo ad American International Group, Inc. e che operano in tutto il mondo nei rami Danni, Vita e Previdenza e Assicurazione generale. Per maggiori informazioni, visitate il nostro sito all'indirizzo www.aig.com. Tutti i prodotti e i servizi sono emessi o prestati da società controllate o collegate di American International Group, Inc. In alcuni paesi determinati prodotti e servizi potrebbero non essere disponibili; la copertura assicurativa è soggetta alle condizioni della polizza. Taluni prodotti e servizi non assicurativi potranno essere forniti da soggetti terzi indipendenti. I prodotti assicurativi potranno essere distribuiti attraverso società collegate o non collegate.

In Europa la principale impresa che eroga le coperture assicurative è AIG Europe Limited.

AIG Europe Limited è registrata in Inghilterra con il numero 1486260. Sede legale: The AIG Building, 58 Fenchurch Street, London EC3M 4AB.

AIG Europe Limited è autorizzata dalla Prudential Regulation Authority e regolata dalla Financial Conduct Authority and Prudential Regulation Authority (numero FRN 202628). Queste informazioni possono essere verificate sul sito del registro FS (www.fsa.gov.uk/register/home.do).

UC10000795 CyberEdge Services Br 2015