CyberEdge®
End-to-End Cyber Risk Management Solutions
In a rapidly changing landscape, CyberEdge® provides clients with an end-to-end risk management solution to stay ahead of the curve of cyber risk.

CyberEdge provides the insurance coverage, tools, and continued access to emerging best practices — learned from our years covering this risk and from the cyber experts we work with — necessary for clients to assess and mitigate potential vulnerabilities to sensitive data breaches, computer hacking, employee error, and more.
CyberEdge Risk Management Solution

From our innovative loss prevention tools to educate and potentially prevent a breach, to the services of our CyberEdge Breach Resolution Team if a breach does occur, insureds receive responsive guidance every step of the way.

<table>
<thead>
<tr>
<th>Risk Consultation and Prevention</th>
<th>Insurance Coverage</th>
<th>Breach Resolution Team</th>
</tr>
</thead>
<tbody>
<tr>
<td>Education and Knowledge</td>
<td>Third-Party Loss Resulting From a Security or Data Breach</td>
<td>24/7 Guidance: 1-800-CYBR-345</td>
</tr>
<tr>
<td>Training and Compliance</td>
<td>Direct First-Party Costs of Responding to a Breach</td>
<td>Legal and Forensics Services</td>
</tr>
<tr>
<td>Global Threat Intelligence and Assessment</td>
<td>Lost Income and Operating Expense Resulting From a Security or Data Breach</td>
<td>Notification, Credit, and ID Monitoring Call Center</td>
</tr>
<tr>
<td>Shunning Services</td>
<td>Threats to Disclose Data or Attack a System to Extort Money</td>
<td>Crisis Communication Experts</td>
</tr>
<tr>
<td>Expert Advice and Consultation</td>
<td>Online Defamation and Copyright and Trademark Infringement</td>
<td>Over 15 Years’ Experience Handling Cyber-Related Claims</td>
</tr>
</tbody>
</table>
Risk Consultation and Prevention

The protection that CyberEdge provides is a valuable additional layer to the most powerful first line of defense against cyber threats, a company’s own IT system. Constantly monitoring the cyber landscape, we keep insureds at the forefront of the industry as cyber risks continue to evolve. Our preventative tools provide our clients with the knowledge, training, security, and consultative solutions to help them stay ahead of the curve.

CyberEdge Mobile App for iPhone®, iPad®, and Android™

The CyberEdge Mobile App combines the latest cyber breach information, news, opinion, and risk analysis users want at their fingertips. With a sleek look and many features globalized, the app is the first-of-its-kind and available for iPhone, iPad, and Android.

Features include:

- Data Breach Threat Map that displays breaches occurring around the world, including information about breach notification laws in the U.S. state where the breach occurred.
- Claims narratives providing examples of real-world cyber breaches covered by CyberEdge.
- Breach calculator, allowing users to input their company’s details to calculate the potential costs associated with a data breach.
- Majority of the content available in English, French, and Spanish.

RiskTool™ Powered by RiskAnalytics

The easy-to-use comprehensive web-based platform helps clients streamline the cybersecurity risk management process and address the human element of this risk.

Organizations can use RiskTool to:

- Build a culture of security through strong company policy and employee awareness.
- Educate employees with user-friendly training.
- Manage vendor security compliance with a streamlined process.
- Demonstrate appropriate diligence and compliance via fast, easy reporting and documentation.
**Dark Net Intelligence** *Powered by K2 Intelligence*

The ease and profitability of carrying out cyber crimes continues to increase for bad actors, especially with the continued shift organizations are making to operating in more of a digital, interconnected world.

K2 Intelligence can work with CyberEdge policyholders at preferred rates to stay apprised of what the latest chatter is inside the black hacker markets and forums known as the ‘dark net’ about their entity. The dark net is the staging ground, the safe haven, from which the most sophisticated cyber criminals launch their attacks.

K2 Intelligence mines the dark net for data using web crawlers and sophisticated human intelligence gathering. This type of customized intelligence is extremely valuable as organizations:

- Take a proactive approach in developing and refining their cybersecurity risk management program, ensuring the appropriate corporate governance standards and protocols are in place.
- Engage in M&A transactions. K2 Intelligence’s experts and intelligence can be used to provide cybersecurity due diligence when organizations engage in a merger or acquisition.

**Infrastructure Vulnerability Scanning** *Powered by IBM*

Our qualified clients receive infrastructure vulnerability scanning powered by IBM. IBM conducts remote scanning for clients’ web-facing external infrastructures, which helps to identify potential vulnerabilities that could be exploited by a remote hacker via the Internet. In addition, the infrastructure vulnerability scanning service:

- Detects and prioritizes hidden risks on public-facing network infrastructure.
- Provides a detailed view of a company’s vulnerability status so clients can better track, understand, and report on their security posture.
- Prioritizes vulnerabilities so clients reduce their overall threat exposure.
- Includes unique reporting capabilities to help speed vulnerability identification and remediation.
**BitSight Security Ratings**

BitSight generates security ratings for organizations 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. Security ratings are based on evidence of the following:

- Observed security events, or evidence of successful cyber attacks. This includes communication with botnets, spam, malware, and more.
- Diligence data points, or indicators of whether a company has taken steps to prevent an attack. This includes proper security configuration analysis.

 Qualified CyberEdge insureds will be eligible to receive a complimentary BitSight Security Rating report to measure the organization’s security performance. CyberEdge policyholders are also eligible for reduced rates on BitSight’s products and services. Insureds can choose to arm themselves with daily ratings as part of their end-to-end cyber risk management program, allowing them to have insight into cybersecurity risk throughout their ecosystem.

**Cybersecurity Maturity Assessment** *Powered by RSA*

Insureds are eligible to receive a one-time six month complimentary pass to RSA’s Governance, Risk, and Compliance (GRC) solution to assess their organization’s cybersecurity risk. The assessment is built on the industry leading RSA Archer GRC solution.

- Leverages the NIST Cybersecurity Framework to assess an organization’s cybersecurity maturity level and help identify areas of improvements in key functions.
- Upon completion of the assessment, an organization will have a view of gaps between their current and ideal risk posture.
- Insureds will have access to RSA’s Advanced Cyber Defense (ACD) practice to provide operational expertise in closing the gaps and protecting the critical business assets.
Proactive Shunning Service Powered by RiskAnalytics

Qualified clients receive access to leading edge global threat intelligence and technology that isolates and shuns IP addresses currently being used by criminals. Before initiating an attack on a network, criminals first conduct reconnaissance to confirm that certain IP addresses are viable targets. Shunning prevents these criminal communications from reaching a network and confirming the IP addresses as viable targets. When the recon phase of the attack fails, the risk of follow-on intrusions is greatly reduced.

Shunning can also guard against attacks from within. If a computer on a network is already compromised by malware, shunning can prevent communication back to the criminal’s command and control servers, effectively disarming the malware. Shunning occurs in real time at line speed, and it is scalable to protect a single location or a global enterprise.

Portfolio Analysis Powered by Axio Global

As a CyberEdge policyholder, clients can retain Axio Global (Axio) to assist in obtaining a holistic picture of their cyber exposure and more effectively harmonize their technological and operational controls with insurance coverage. Axio’s method addresses the full range of potential cyber losses, including data theft, liability, property and environmental damage, bodily injuries, and operational disruption. Clients have access to the following services from Axio at reduced rates as a CyberEdge policyholder:

• One-day loss scenario workshop to estimate the financial impact of information technology and control systems loss scenarios customized for a client’s particular needs and organized into a taxonomy that can be used to stress test insurance coverage.

• Analysis of a client’s entire Property and Casualty insurance portfolio to identify how it would respond to a complex cyber event. Combined with the loss scenario workshop, this analysis stress tests a portfolio with realistic scenarios.

• Self-evaluation of a client’s cybersecurity program based on the Cybersecurity Capability Maturity Model (C2M2), a recommended approach for deploying the NIST Cybersecurity Framework. A scoring report is generated and presented with the results of the evaluation. One of Axio’s founders was the architect of the model and is well versed in helping organizations interpret the model content to achieve an effective and efficient cybersecurity program review.
Consultation

Clients have access to cybersecurity expert vendors and partners to help plan and prepare for a cyber breach. Consultation options include:

- Two complimentary hours from a specialized law firm to provide guidance on building and executing an incident response plan, as well as ensuring an organization is compliant with regulatory standards.

- One complimentary hour from a forensic firm on what an organization’s technical response plan should include.

- One complimentary hour from a vetted public relations firm to discuss an effective crisis communication plan to handle and mitigate the potential reputational and brand risk an organization would face in the event of a breach.

Insurance Coverage

CyberEdge can provide companies with protection against the following:

- Third-party claims arising from a failure of the insured’s network security or a failure to protect data. Insurance also responds to regulatory actions in connection with a security failure, privacy breach, or the failure to disclose a security failure or privacy breach.

- Direct first-party costs of responding to a security failure or privacy breach by paying costs of notifications, public relations, and other services to assist in managing and mitigating a cyber incident. Forensic investigations, legal consultations, and identity monitoring costs for victims of a breach are all covered.

- Business interruption caused by a network security failure by reimbursing for resulting lost income and operating expenses.

- Threats made against a company’s computer network and confidential information by an outsider attempting to extort money, securities, or other valuables. Coverage includes monies paid to end the threat and the cost of an investigation to determine the cause of the threat.

- Liability faced by companies for content distributed on their website. Coverage is provided for numerous media perils including copyright infringement, trademark infringement, defamation, and invasion of privacy.
Breach Resolution Team

The CyberEdge Breach Resolution Team is ready to assist insureds as soon as they suspect a potential network breach. Our team has local presence supported by global resources, allowing our experts to manage unfolding events and quickly respond to inquiries.

If a breach is suspected to occur, insureds will be connected with our CyberEdge Breach Resolution Team with more than 15 years worth of experience in handling cyber-specific claims.

• Claims specialists have the authority to promptly make decisions and rapidly assist clients who may have just faced a breach.

• Since introducing cyber liability insurance in 1999, we have helped thousands of companies and more than twenty million individuals respond to a cyber attack.

• The breadth of our claims inventory means that we are uniquely positioned to identify and anticipate claim trends and settlement values.

• On average, our claims specialists have more than seven years of industry experience handling the most complex first-party and third-party cyber claims.

• 24/7 access to our call center for claim reporting and guidance supported by IBM.

• Single point of entry to report, acknowledge, and process claims in a timely fashion.

• Access to our local claims specialists on the ground around the world.

• Access to a panel of domestic and international attorneys with local expertise in handling cyber claims.

Backed by the strength of our extensive vendor network, the CyberEdge Breach Resolution Team provides the additional layer of support an IT department needs to face a cyber attack.

• Insureds have access to an IBM-supported hotline for IT professionals to consult on identifying key indicators of a breach.

• IBM and our expert network of legal firms, forensic investigators, public relations firms, and more offer immediate support for our insureds facing a cyber attack, anytime and anywhere.

• When a breach event occurs, time is of the essence. Having a response plan in place with access to third-party resources will help you efficiently and cost-effectively respond to and recover from a breach.
Cyber Risk Travels the World

Through our global service platform Passport, clients are provided an efficient and seamless way to stay ahead of the curve of cyber risk. Add the expertise of our local teams who have the know-how in the places where you do business. Count on the CyberEdge Breach Resolution Team for responsive guidance and assistance services that follow the sun. Our end-to-end risk management solution knows no borders.

Better, Faster, and More Efficient Global Protection

Passport is a simple, effective means to far-reaching global advantages, including:

• Coverage that is admitted locally and in sync with local laws, regulatory requirements, language, and customs.

• Access to local experts in underwriting, claims, and litigation management.

• Easy to understand coverage, coordinated worldwide.

A Less Complex Way to Address Global Cybersecurity Exposure

Passport makes securing the necessary protection against cyber risk around the world as simple as possible.

• A client receives one proposal detailing the terms of its global cyber program, including the worldwide policy and any requested locally admitted policies.

• The outlined coverage is accepted and it is done.

• Appropriate local policies are issued through our local offices around the world. Local policies are crafted in accordance with local regulations, industry practices, and exposures.¹

¹Limits are subject to capacity management; certain countries may limit the availability of either a single aggregate or a separate world limit.
Passport for CyberEdge Destinations

- Australia
- Austria
- Bahrain
- Belgium
- Brazil*
- Bulgaria
- Canada
- Chile
- Colombia
- Cyprus
- Czech Republic
- Denmark
- Ecuador
- Finland
- France
- Germany
- Greece
- Hong Kong
- Hungary
- Ireland
- Israel
- Italy
- Japan
- Kuwait
- Lebanon
- Luxemburg
- Malaysia
- Mexico
- Netherlands
- New Zealand
- Norway
- Oman
- Panama
- Philippines
- Poland
- Portugal
- Puerto Rico
- Qatar
- Romania
- Russia*
- Singapore
- Slovakia
- Spain
- South Africa
- South Korea
- Sweden
- Switzerland
- Taiwan
- Turkey
- UAE
- United Kingdom
- United States
- Uruguay

New destinations are added constantly, so please check with a Passport representative for more information.

*Special handling and additional premium required for Brazil and Russia.
American International Group, Inc. (AIG) is a leading global insurance organization serving customers in more than 100 countries and jurisdictions. AIG companies serve commercial, institutional, and individual customers through one of the most extensive worldwide property-casualty networks of any insurer. In addition, AIG companies are leading providers of life insurance and retirement services in the United States. 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 | YouTube: www.youtube.com/aig | Twitter: @AIGinsurance | LinkedIn: http://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.

Apple, the Apple logo, iPhone and iPad are trademarks of Apple Inc., registered in the U.S. and other countries. App Store is a service mark of Apple Inc. Android and Google Play are trademarks of Google Inc.

No warranty, guarantee or representation, either express or implied, is made as to the appropriateness or sufficiency of any product, service or provider described herein for any specific organization or purpose. Use of the service providers discussed herein in no way guarantees any particular result, including the avoidance of loss, the fulfillment of any obligations under any insurance policy or contract or compliance with any law, rule or regulation. The information provided herein should not be construed as business, risk management or legal advice or opinion.

© American International Group, Inc. All rights reserved.

04/15