AIG®

What's Inside CyberEdge®

Start →

For full pdf features, please view in Adobe Acrobat.

What's Inside
CyberEdge®

AIG

CyberEdge

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 you stay ahead of the curve by helping you manage your cyber risk and protecting you if the worst does occur.

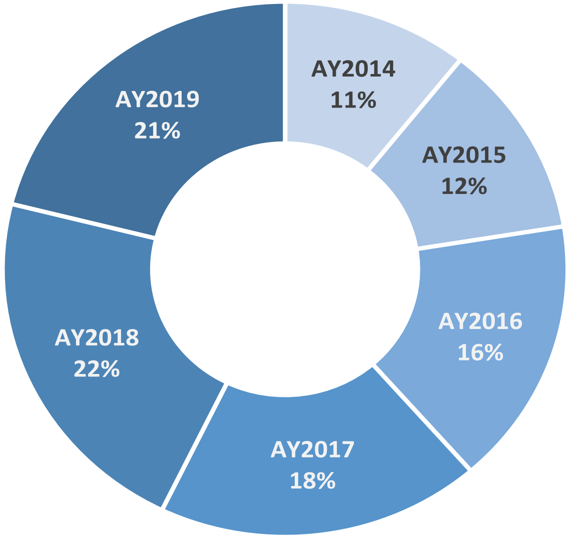
This booklet outlines some of the coverage options available under CyberEdge. Please refer to your insurance broker or the policy wording and schedule for further details of cover and terms and conditions.

Cyber Claims Expertise

CyberEdge is underpinned by the deep experience of our cyber claims teams. As more businesses purchase cyber cover, the volume of cyber claims we handle continues to increase (see chart).

The expertise of our cyber claims teams and our commitment to constantly stay abreast of the new cyber exposures ensures our clients are in safe hands whenever and wherever they face a cyber loss.

AIG APAC Cyber claims growth per year as a % of total



Cyber claims trends

Cyber Claims Expertise

Cyber Maturity Report

Complimentary Services

Coverage Sections

Cyber Maturity Report

Upon completion of the AIG application form, businesses can obtain insights into the cyber risks and threat likelihoods they face, via a complimentary summary report.

Once AIG cyber coverage has been purchased, businesses will receive a comprehensive report providing details of how their controls can be improved to help minimise risk, analysis of potential losses due to a privacy breach or denial of service attack and an assessment of their compliance with CIS Security Controls to help identify potential weaknesses in cyber defences.

Summary Report includes:

(FOR COMPLETING APPLICATION FORM)

- Quick scores of cyber readiness
- Top 5 risk scenarios
- Risk indices for key threat categories
- Summary of data breach and DoS impacts

View sample →

Executive Report includes:

(FOR PURCHASING A CYBEREDGE POLICY)

- Cyber readiness peer benchmarking
- Prioritised risk practices
- Data breach probabilities and impacts
- DoS probabilities and impacts
- Residual risk details and scenarios
- Threat likelihoods
- Cyber control effectiveness
- CIS alignment scores across controls
- Business impact details

View sample →

Maturity reports are only available in certain countries. Ask an AIG underwriter if it's available in your country.

Learn more from this video →

What's Inside
CyberEdge®

Cyber Claims Expertise

Cyber Maturity Report

Complimentary Services

Coverage Sections

Complimentary Services

The following complimentary tools and services are included with each CyberEdge policy for eligible clients

Services for eligible CyberEdge policyholders spending US $900 - $4,999 on their annual CyberEdge premium

Employee CyberSecurity Training

Timely and measurable managed training and compliance services for employees, tailored to employee roles to reinforce cybersecurity best practices.

Security Ratings

Using an easy A-F grading system, clients are scored from an "outside-looking-in" perspective on their overall cybersecurity in ten key risk categories.

Cyber Maturity Report

Upon completion of the AIG application form, businesses can receive a detailed analysis of their cyber maturity via a comprehensive report. The report provides clarity on how AIG views the business and our approach to underwriting the risk, including the quality of controls that reduces their risk.

AIG Cyber Services Orientation

One-hour remote session with an AIG Risk Consultant to address questions around the Cyber Maturity Report and discuss complimentary services available.

CyberEdge Claims Hotline

Once a call is made to the 24/7 hotline, the CyberEdge claims team will coordinate with the client to implement their response plan, engage any necessary vendors to identify immediate threats and start the restoration and recovery processes.

In addition, these services are available to CyberEdge policyholders spending US$5,000+ on their annual CyberEdge premium.

Phishing Simulator

Part of the eLearning tool, the phishing simulator delivers real-world scenarios to reinforce learning and remediate behaviors. Identify susceptible users and compare performance over time.

Blacklist IP Blocking

Enables organisations to control their exposure to criminal activity by leveraging vast threat intelligence repositories, precision geoblocking, and blacklist automation to reduce risk.

Infrastructure Vulnerability Scanning

Clients can select up to 250 of their IP addresses to be examined by experts to identify critical vulnerabilities that are open to potential exploits by cyber criminals, with a follow up scan 90 days later to verify their efforts at remediation.

Coverage Sections

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

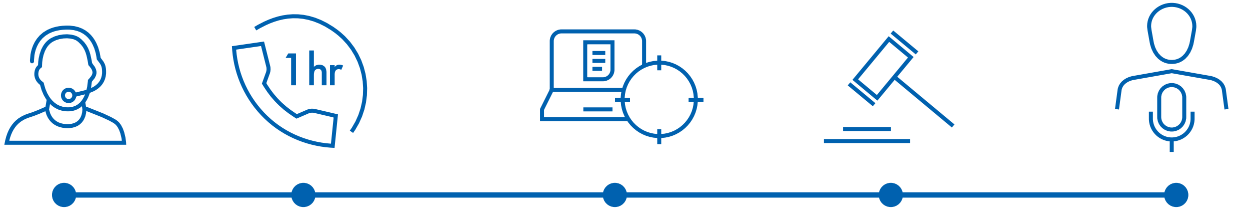
- First Response
- Cyber Extortion
- Event Management
- Network Interruption
- Security and Privacy Liability
- Criminal Reward Fund
- Digital Media Content
- Cyber Crime

Coverage
Sections

First Response

The first 24 hours are vital when responding to a cyber incident and AIG's First Response service (where provided) delivers best-in-class legal and IT forensics within 1 hour of ringing our hotline.

The coordinated response is provided for 48 or 72 hours depending on the policy. This tried and tested service is an outstanding market differentiator for CyberEdge and can be used whenever clients have (or suspect) a cyber incident, with no policy retention and without prejudicing policy coverage.



24/7 global hotline.

Legal Response Advisor will contact you within 1 hour to record 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, PR Advisor and Cyber Extortion Advisor appointed to mitigate reputational damage and advise on extortion or ransomware events

What's New:

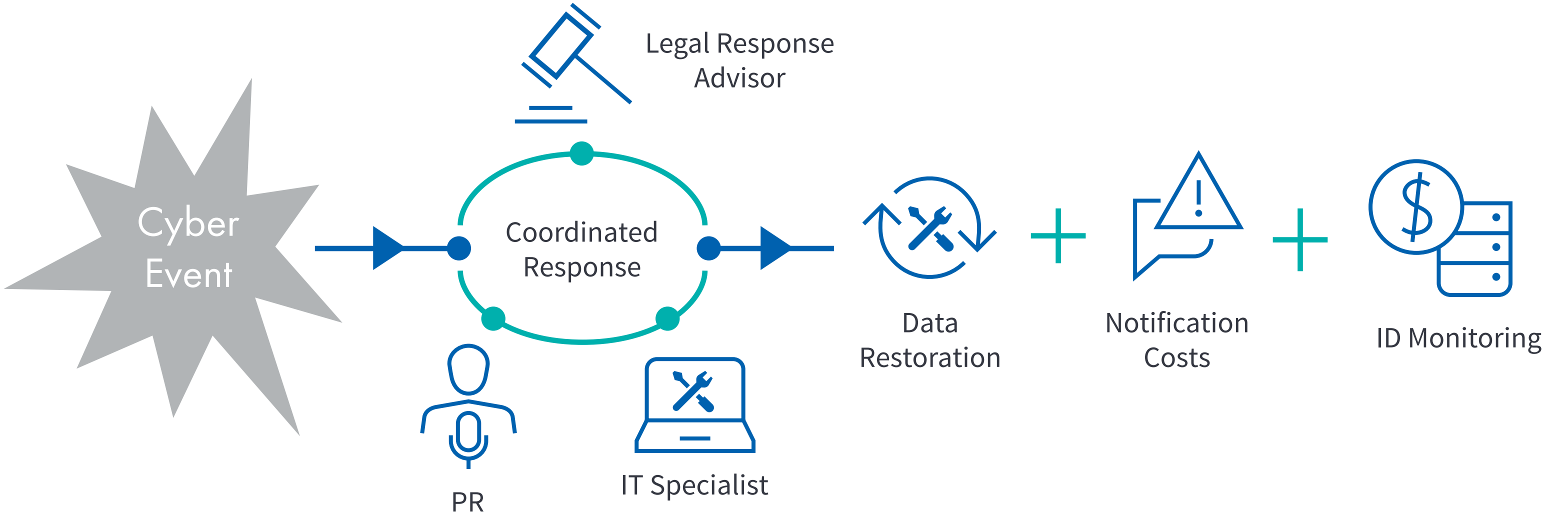
- Clarifies access to AIG's incident response vendors.
- First Response is the process of how a cyber incident is managed.

Additional Information

Event Management

After a cyber-attack, organisations will require a range of services to get their business back on track.

CyberEdge's Event Management pays for Legal, IT, PR services, Credit and ID Monitoring in addition to Data Restoration and Breach Notification costs. When an event occurs, having the correct expertise on hand can result in dramatically improved outcomes - especially when underpinned by First Response.



What's New:

- Includes cover for computer systems and industrial control systems
- Coverage for replacement of obsolete/unavailable system components with upgraded ones.
- Coverage for devices owned by employees used under a "Bring Your Own Device"

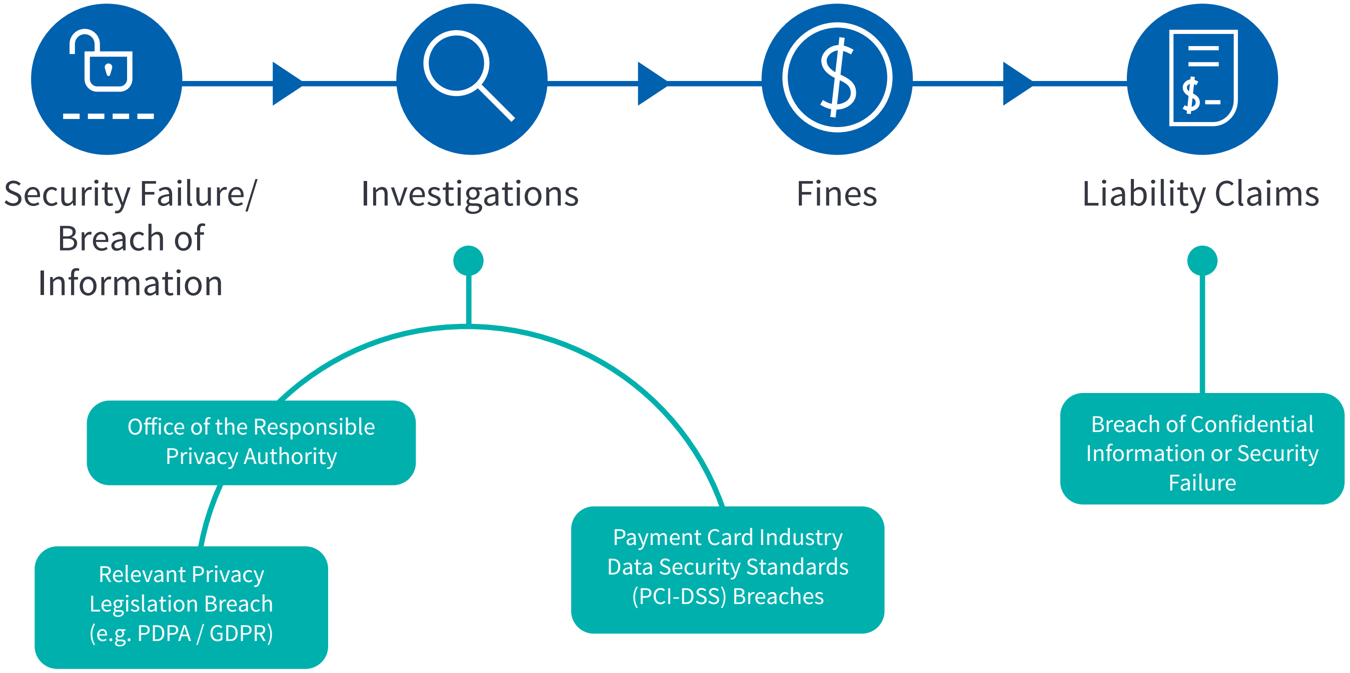
Optional extras

Coverage
Sections

Security & Privacy Liability

Our Security and Privacy Liability module responds to third-party liabilities resulting from breaches of confidential information, security failure, failure to notify the regulator and breaches of PCI compliance.

Cover is more important than ever in the wake of more onerous privacy legislation like GDPR, and includes defence costs and insurable fines in relation to any regulator of Data Protection legislation – from the Information Commissioner's Office (ICO) to its equivalent across worldwide jurisdictions.



Security Failure/ Breach of Information

Investigations

Fines

Liability Claims

Office of the Responsible Privacy Authority

Relevant Privacy Legislation Breach (e.g. PDPA / GDPR)

Payment Card Industry Data Security Standards (PCI-DSS) Breaches

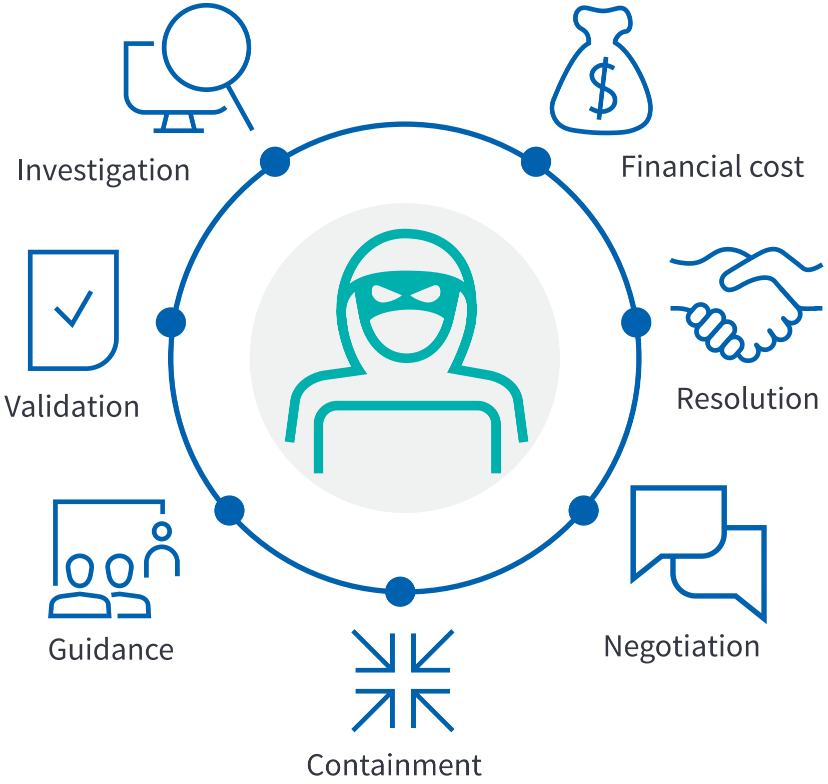
Breach of Confidential Information or Security Failure

What's New:

- Includes PCI as standard.
- Covers actual or alleged failure by a Company to notify a Data Subject or any Regulator.
- Covers Company's legal liability caused by third party information holders or cloud/other hosted computer providers.

Cyber Extortion

Cyber extortion is an increasingly prevalent cyber threat faced by businesses. CyberEdge covers an extensive range of specialist services to combat the use of ransomware in these instances, including conducting investigations to validate a threat, containment and negotiations to end an extortion and ransom payments.



What's New:

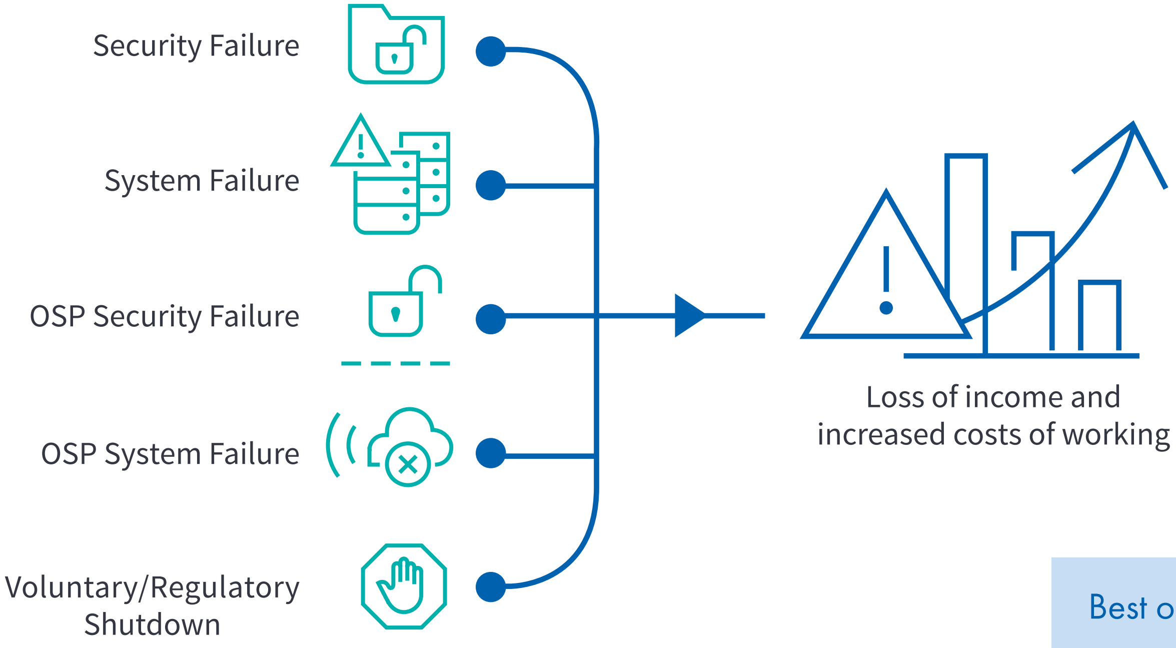
- Covers a full range of cyber extortion services to identify, validate, and resolve an event
- Covers use of Cryptocurrency and the cost to obtain a cryptocurrency in order to pay a ransom.

Coverage
Sections

Network Interruption

Network Interruption covers loss of income, mitigation expenses and forensic accounting costs to quantify the loss when business operations are interrupted by a selected peril, including cybersecurity breach, system failure and voluntary shutdown to contain a cyber incident.

The module can also be extended to cover losses from security breaches or system failures at Outsourced Service Providers (OSP), such as cloud providers or payment processors. For a qualifying event after the waiting period has elapsed, cover is provided from 'hour zero' immediately after the event, subject to any retention.


Security Failure
System Failure
OSP Security Failure
OSP System Failure
Voluntary/Regulatory Shutdown
Loss of income and increased costs of working

What's New:

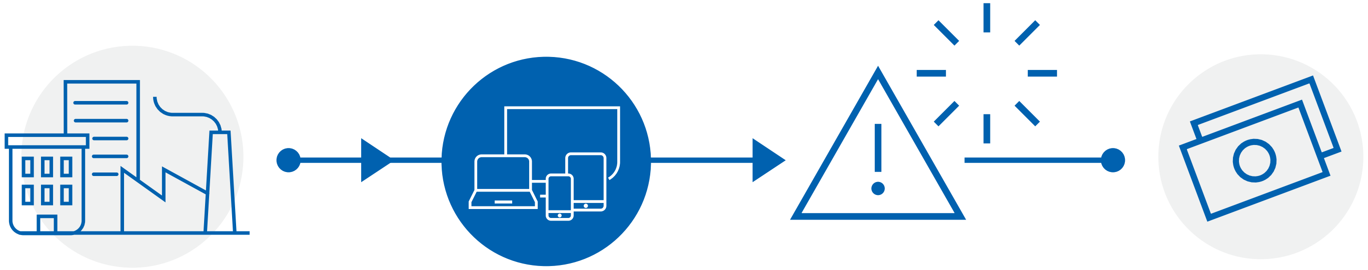
- 'Hour Zero' Network Interruption loss for events after the wait period but covering loss from 'hour zero' immediately after the event, subject to the monetary retention
- 'Best of both worlds' Network Interruption loss calculation (see callout)
- Mitigation costs covered from beginning of the cyber event, subject to retention
- Network Interruption cover after voluntarily shutting down systems to contain an incident

Best of both worlds

Digital Media Content

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

The Digital Media Content coverage section covers damages and defence costs for a breach of third party intellectual property, or negligence in connection with electronic content.



Company

Online Advertising
Website Content
Blogs
Social Media

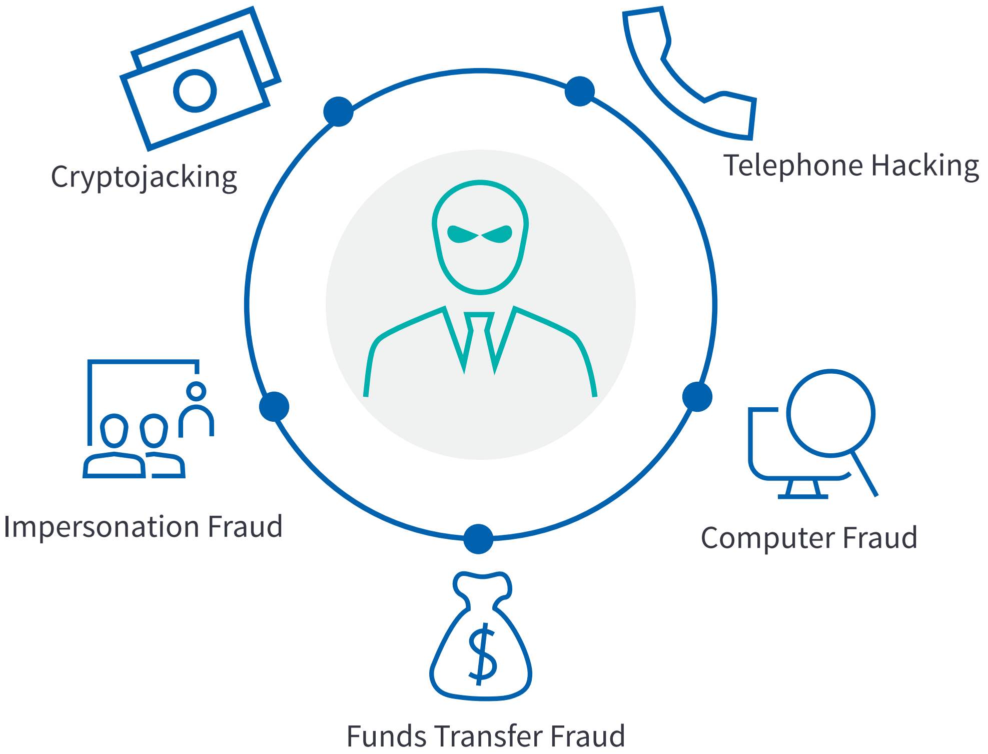
Defamation,
infringement etc.

Liability Claims

Coverage Sections

Cyber Crime

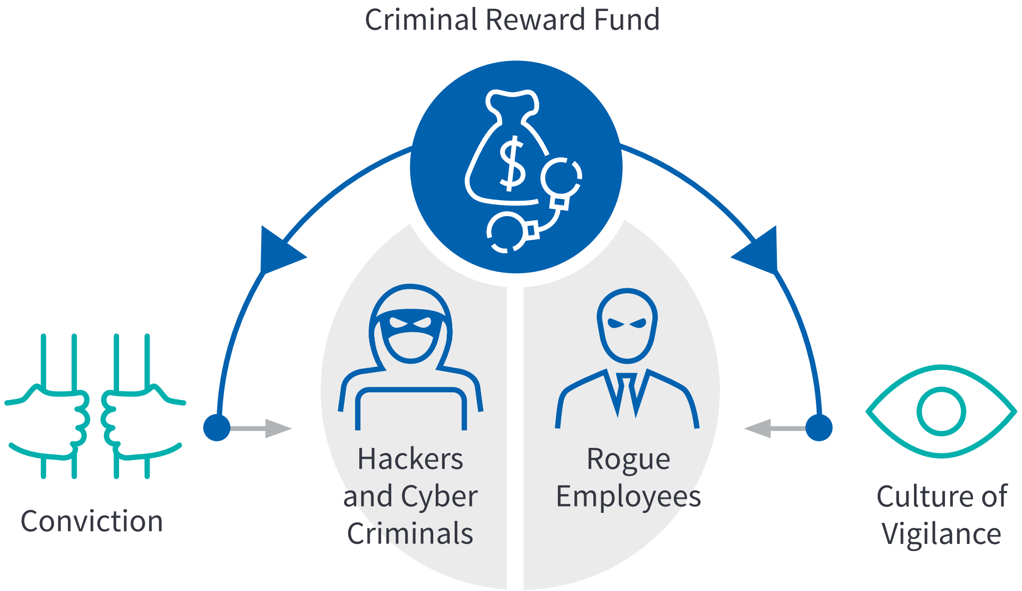
There are many types of fraud related to computer crime and Social Engineering. CyberEdge's Cyber Crime module can cover a variety of exposures, including:



Criminal Reward Fund

A Criminal Reward Fund may be paid for information that leads to the arrest and conviction of individuals who have or are attempting to commit an illegal act relating to cover provided under a CyberEdge policy.

This relates not only to hackers and cyber criminals but also to rogue employees, rewarding staff who notice and report suspicious behaviour.



www.aig.sg

American International Group, Inc. (AIG) is a leading global insurance organization. Building on 100 years of experience, 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.

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 SG CyberEdge What's Inside Guide 05-2020