



# What's Inside CyberEdge<sup>®</sup>



# 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 and 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.

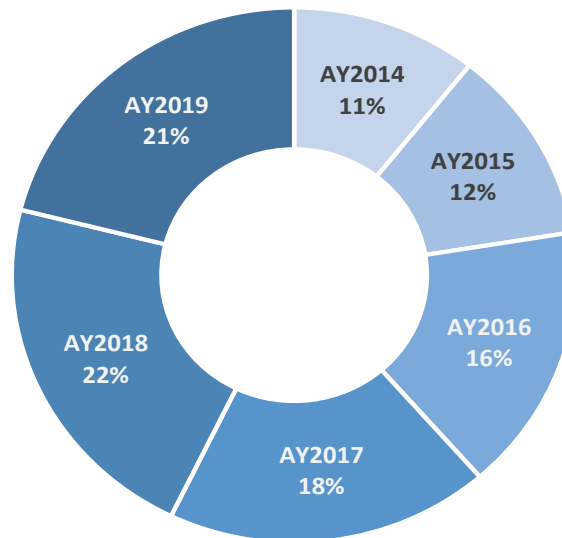
# Cyber Claims Expertise

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, constantly staying abreast of new cyber exposures, ensures that clients are in the safest hands whenever and wherever they face a cyber loss.



AIG APAC Cyber claims growth per year as % of total



# Cyber Maturity Report

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

Should they purchase AIG cyber coverage, they will receive a comprehensive report including risk reducing qualities of their controls, analysis of potential losses 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.



Cyber Maturity Report

## 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

## Executive Report includes:

(FOR PURCHASING A CYBEREDGE POLICY)

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

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



# 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 annual CyberEdge premium**



## Employee CyberSecurity Training

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



## Security Ratings

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



## Cyber Maturity Report

Upon completion of the AIG application form businesses can obtain insights into the cyber risks they face and the threat likelihoods via a comprehensive report including risk reducing qualities of their controls.



## 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 annual CyberEdge**



## Phishing Simulator

Part of the eLearning tool, the phishing simulator delivers real world scenarios to reinforce learning and remediate behaviors. Identify susceptible users & 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 black-list automation to reduce risk.



## Infrastructure Vulnerability Scanning

Clients can select up to 250 of their IP addresses 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



Complimentary Services

# Coverage Sections

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



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 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, co-ordinate a PR Advisor to mitigate reputational damage and Cyber Extortion Advisor for extortion or ransomware.

## What's New:

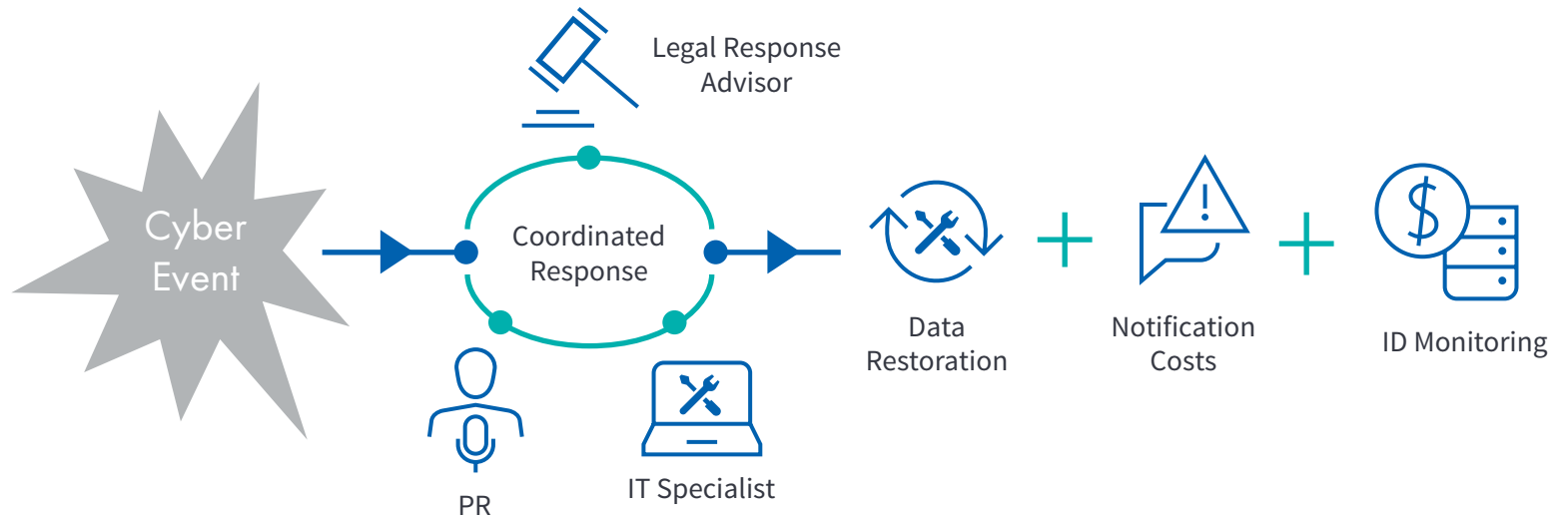
- Clarifies access to AIG's incident response vendors.
- First Response is the process of how a cyber incident is managed.



# 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 system.
- Can cover replacement of obsolete/unavailable system components with upgraded ones.
- Includes devices owned by employees used under a “Bring Your Own Device” policy.



Coverage Sections

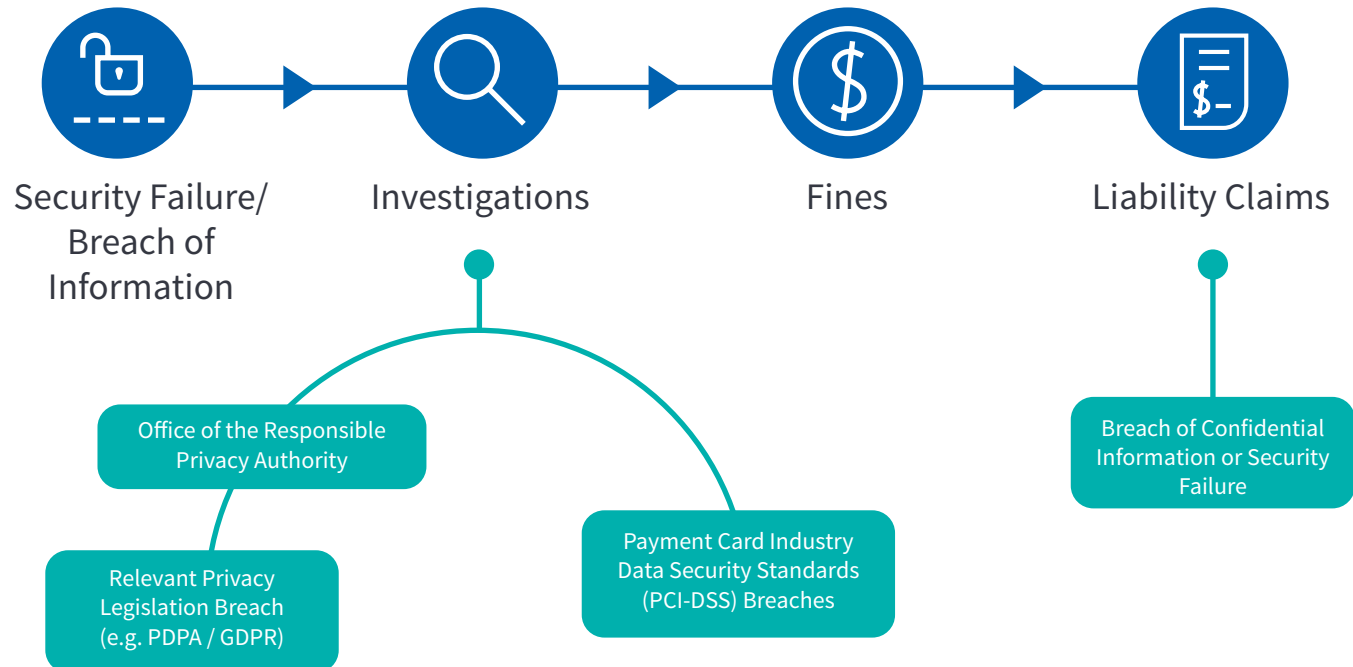




# Security & Privacy Liability

Our Security and Privacy Liability module responds to third-party liabilities resulting from breaches of confidential info, 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 ICO to its equivalent across worldwide jurisdictions.



## 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.



Coverage  
Sections



# Cyber Extortion

As one of the more increasingly prevalent cyber threats facing businesses, CyberEdge covers an extensive range of specialist services to combat the use of ransomware for cyber extortion. From conducting investigations to validate a threat, to containment and negotiations to end an extortion event through to 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 such cryptocurrency in order to pay a ransom.



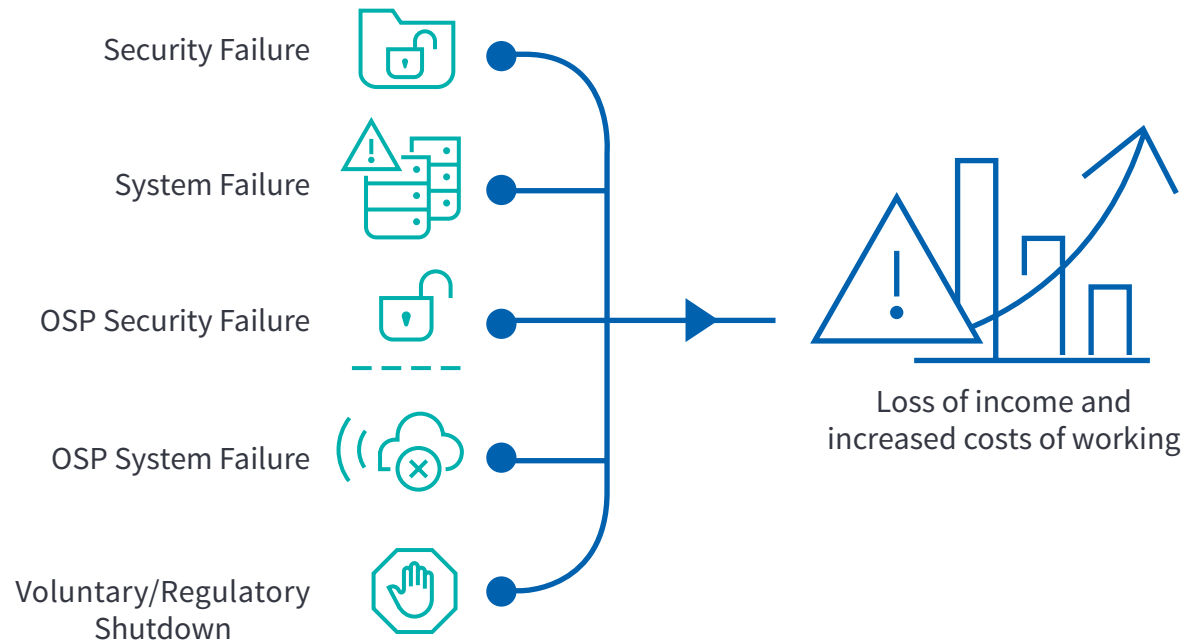
# Network Interruption

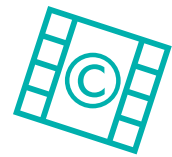
Network Interruption covers loss of income, mitigation expenses and forensic accountant' costs to quantify the loss when business operations are interrupted by a selected peril including cyber-security breach, system failure and voluntary shutdown to contain a cyber incident.

The module can also be extended to cover losses from security breaches or system failures at Outsourced Service Providers (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.

## What's New:

- “Hour Zero” NI 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 system to contain an incident

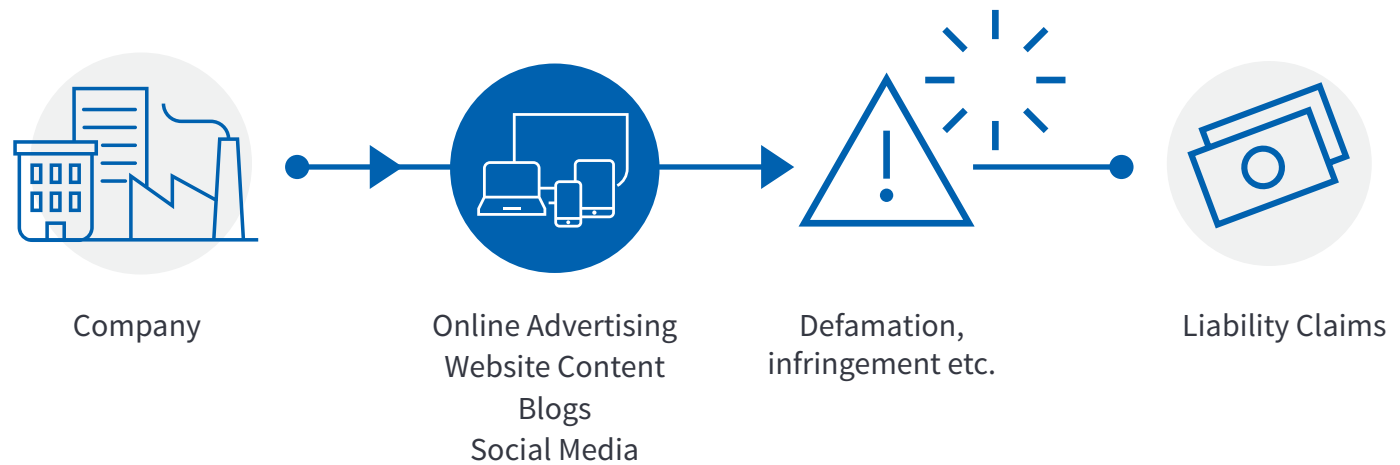




# Digital Media Content

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.



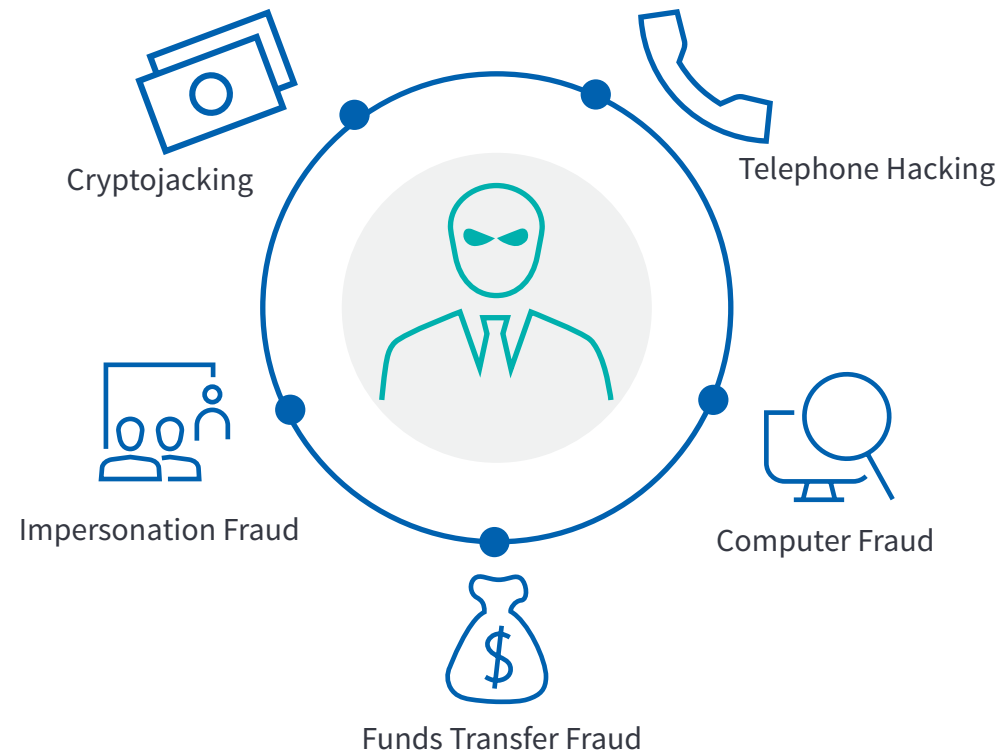


# Cyber Crime



Coverage  
Sections

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:

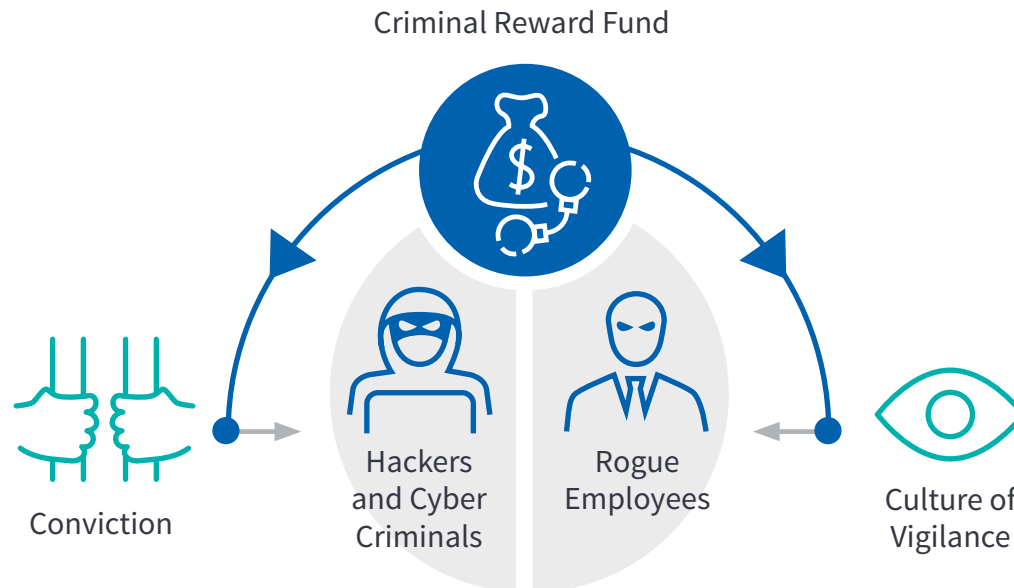




# Criminal Reward Fund

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 includes rogue employees, thus rewarding staff who notice and report suspicious behaviour.



[www.aig.com.hk](http://www.aig.com.hk)

---



American International Group, Inc. (AIG) is a leading global insurance organisation. 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.

Additional information about AIG can be found at [www.aig.com](http://www.aig.com) and [www.aig.com/strategyupdate](http://www.aig.com/strategyupdate) | YouTube: [www.youtube.com/aig](http://www.youtube.com/aig) | Twitter: @AIGinsurance | LinkedIn: [www.linkedin.com/company/aig](http://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 into this material.

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](http://www.aig.com) and at [www.aig.com](http://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.

AIG HK CyberEdge What's Inside Guide 05-2020