AIG®

What's Inside CyberEdge®

Start

For full pdf features, please view in Adobe Acrobat.

What's Inside
CyberEdge®

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.

What's Inside
CyberEdge®

Cyber Claims Expertise

Our specialist Cyber claims team is one of the most experienced in the insurance market, with backgrounds in insurance, law and industry. They have handled all types of cyber incidents including ransomware, business email compromise and breaches of personal information.

Our specialist Cyber claims team is one of the most experienced in the insurance market, with backgrounds in insurance, law and industry. They have handled all types of cyber incidents including ransomware, business email compromise and breaches of personal information.

From the first notification of a cyber event we work closely with CyberEdge clients to resolve the incident and effectively manage any insurance claims which result from the breach including Business Interruption or Cyber Extortion.

What's Inside
CyberEdge®

- Cyber Claims Expertise
- Cyber Maturity Report
- Cyber Services
- Coverage Sections

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.

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 Executive report

View sample

Maturity reports are available in New Zealand.
Ask an AIG underwriter for additional information to

Smart Application Movie

What's Inside
CyberEdge®

Cyber Services

CyberEdge includes a host of complimentary and discounted tools and services to provide knowledge, training, security and consultative solutions for clients purchasing CyberEdge and spending more than $7,500 in premium.

To access these services please visit **www.aig.com/cyberriskconsulting** and complete the contact form, or email us at **cyberriskconsulting@aig.com.**

Employee Cybersecurity eLearning and Phishing Simulations

Managed training and compliance service for employees tailored to employee roles to reinforce clients' cybersecurity best practices. **Learn more**

Blacklist IP Blocking and Domain Protection

Enables companies to mitigate exposure to criminal activity by leveraging threat intelligence, geo-blocking, and blacklist automation. **Learn more**

Infrastructure Vulnerability Scan

Expert examination of up to 250 of a client's selected IP addresses to identify vulnerabilities to cyber criminals, with a follow up scan 90 days later.

Darknet Credential Exposure

Identifies domain-level cyber risks from enterprise data that is exposed on the darknet with reports customised to the client's specific domain. **Learn more**

Identity Risk Assessment

An identity risk assessment of the client's active directory infrastructure with a technician consultation to help interpret the findings. **Learn more**

AIG Cyber Loss Control Orientation

One hour with an AIG cybersecurity expert to address questions about client's risk posture and introduce other preventative services. **See a sample client report**

CyberMatics®

Patented technology service helps clients verify their organization's cyber risk posture, prioritise risk-reducing controls and investments. **Learn more**

Cybersecurity Information Portal

24/7 online access to current cybersecurity information, including best practices checklists, claims data and a breach calculator. **Learn more**

Security Ratings

Clients can see how their internet security posture and network score from an "outside looking in" perspective, with easy-to-understand scoring systems.

24/7 Cyber Claims Hotline

Our Claims Team will coordinate the response plan and engage the necessary vendors to identify immediate threats, and start restoration and recovery.

What's Inside
CyberEdge®

AIG

Coverage Sections

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

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

What's Inside
CyberEdge®

Coverage Sections

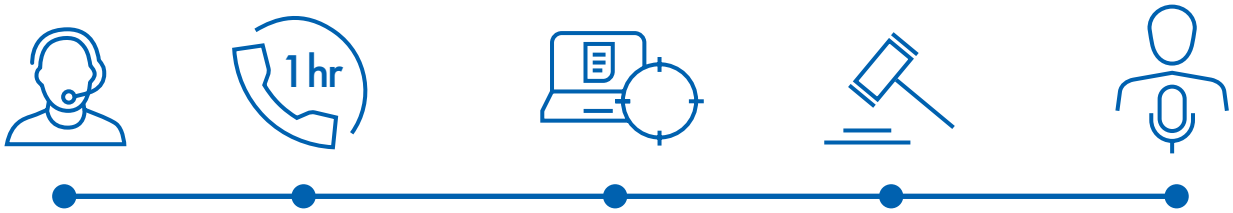
What's New:

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

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 incident response within approximately 1 hour of ringing our hotline.

The coordinated response is provided for 48 or 72 hours depending on the policy terms. 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.

The First Response Advisor will contact you within approximately 1 hour of a call-back service request to take initial details of the incident and advise on next steps as well as assisting with the coordination of the response.

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

Initial legal advice will be required to notify regulators and individuals.

If required, AIG will co-ordinate a PR Advisor to mitigate reputational damage and provide access to a Cyber Extortion Advisor for extortion or ransomware.

Additional Information

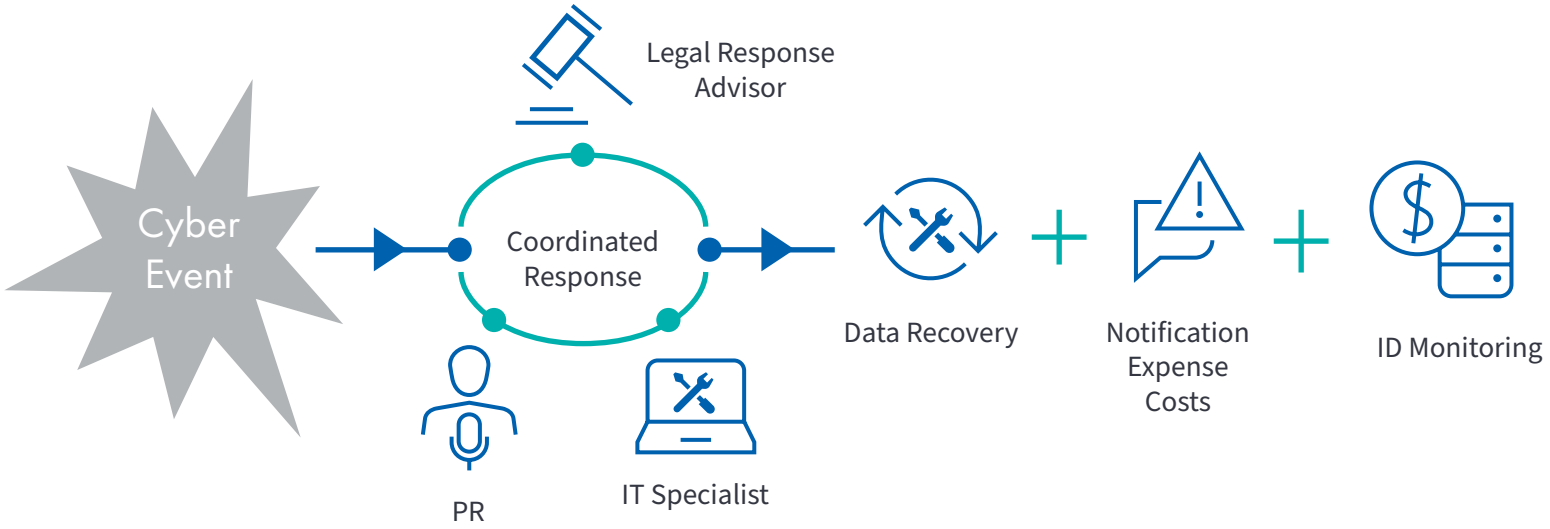
What's Inside
CyberEdge®

Coverage Sections

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 Recovery and Notification Expense 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"

Optional extras

What's Inside
CyberEdge®

Coverage Sections

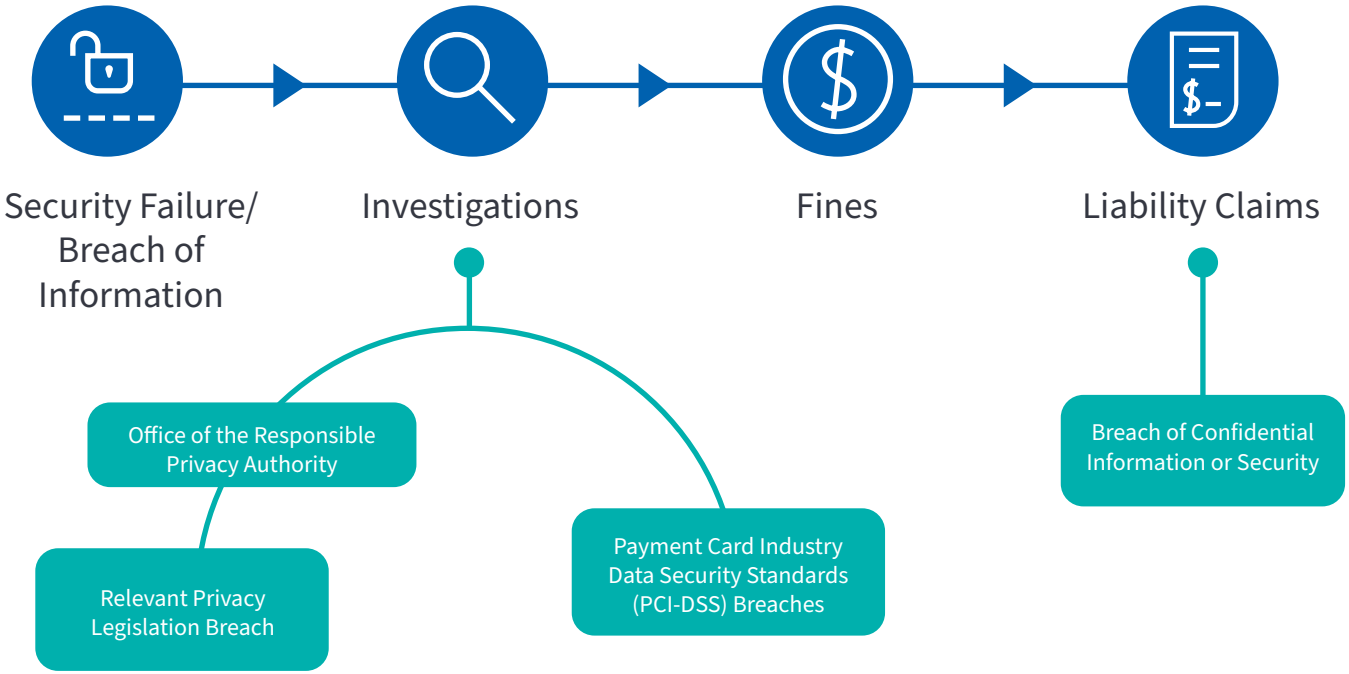
What's New:

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

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 and includes defence costs and insurable fines in relation to any regulator of Data Protection legislation.



What's Inside
CyberEdge®

Coverage Sections

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

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 Inside
CyberEdge®

Coverage Sections

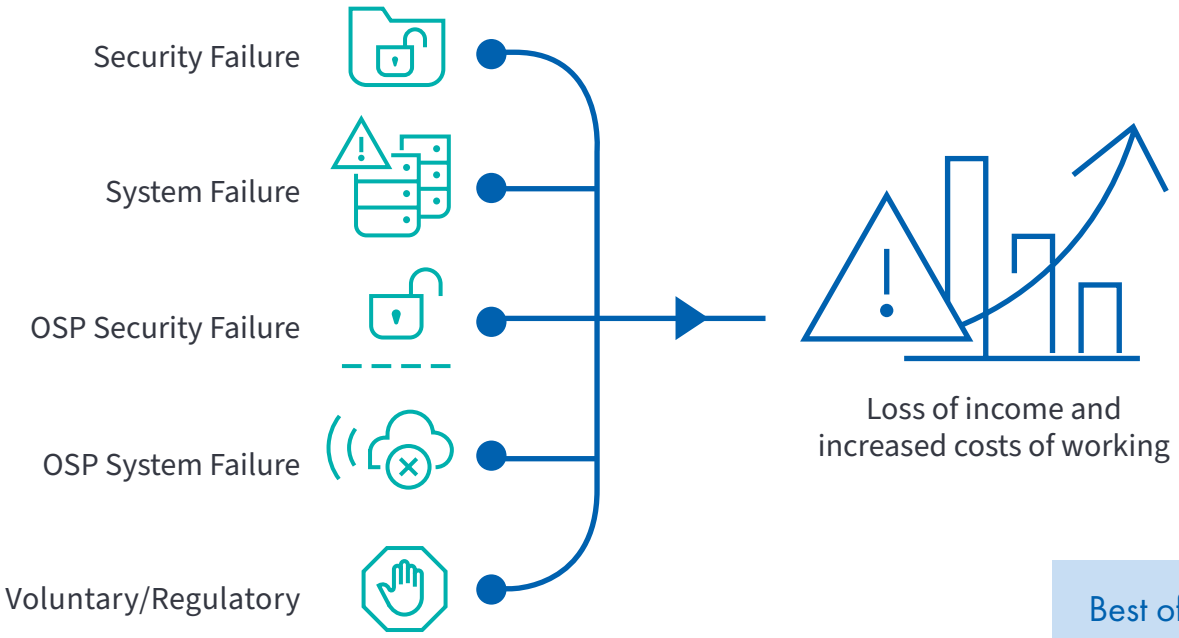
What's New:

- "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 a system to contain an incident.

Network Interruption

Network Interruption covers loss of income, mitigation expenses and a forensic accountant's 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.



Best of both worlds

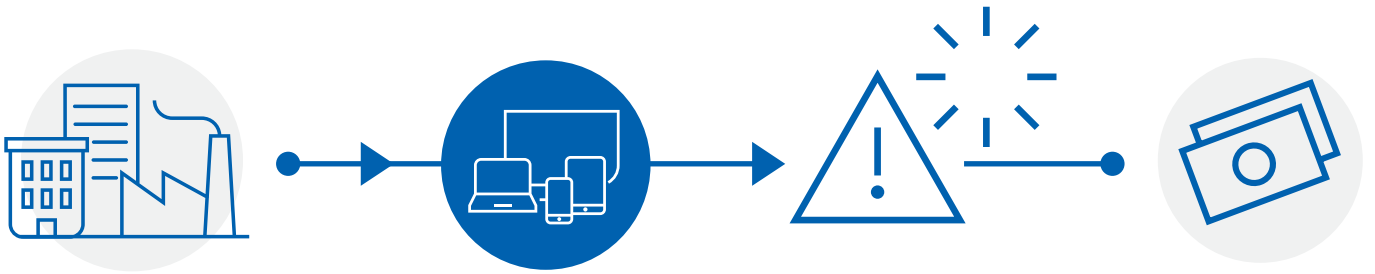
What's Inside
CyberEdge®

Coverage Sections

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 matters such as defamation, unintentional infringement of copyright and misappropriation of ideas in connection with electronic content.



Company

Online Advertising
Website Content
Blogs
Social Media

Defamation, infringement etc.

Liability Claims

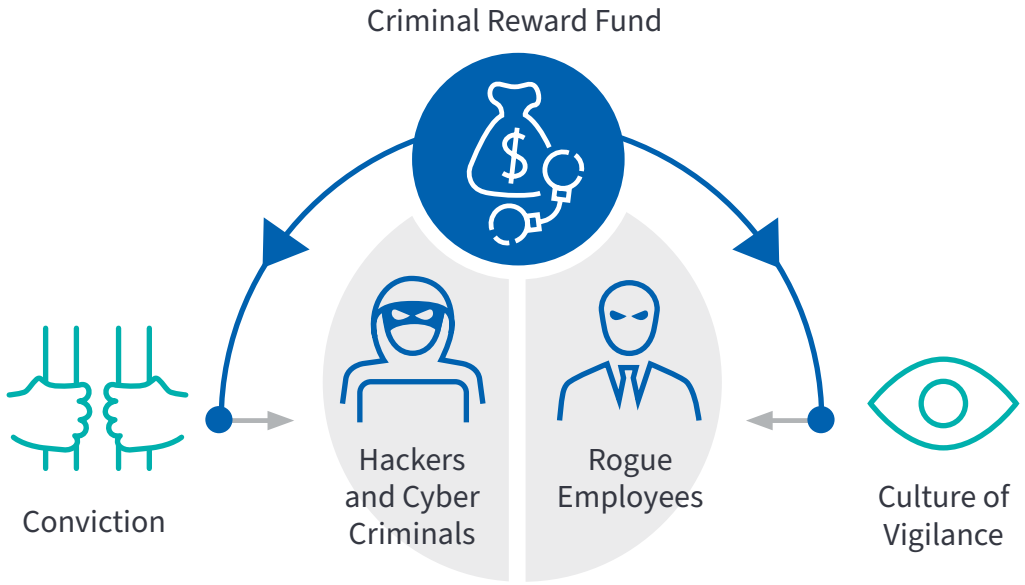
Cyber Crime

There are many types of fraud related to computer crime.
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.co.nz

NZFLCYBERPBBR202405