AIG

Product Profile

CyberEdge

Cyber Risk Protection for Commercial Entities

With recent data breaches hitting the headlines in Asia and New Zealand, loss of personal and corporate data has far-reaching ramifications that could potentially change the way business is carried out all over the world. Most high-profile stories in the media today address the type of data loss that impacts people on a personal level; credit card numbers, medical records, birth dates, ID/passport numbers and other private personal information.

We should also be mindful of the impact from the loss of corporate data and information such as intellectual property and proprietary information, which in the hands of a competitor or even an extortionist can severely disadvantage business.

Current State of Cyber Liability

The average cost of a breach of Network Security is upwards of US$7m. The average cost per record involved in a breach of network security is US$200. Costs include the restoration of records, notifying the individual that his/her information has been stolen, setting up credit and ID monitoring facilities, etc. The average stock drop for a notification of a breach of Network Security is 5%[1].

More People are at Risk

Virtually all companies handle data and personal corporate information on a daily basis, whether it be identity card numbers and corresponding profiles of employees, credit card information, sensitive demographic information about customers, information on budgets, customer lists, share prospectus or marketing plans. The same companies face very real liabilities if such data falls into the wrong hands or enters the public domain.

[1] Network Security Spending Increases - You can't afford not to. Feb. 3rd 2011 by Hal Stevens CEO

More claims examples equals increased demand

Clients are realising the risk to data and are beginning to request policies with enhanced coverage. AIG has launched the most innovative insurance product in addressing these issues: CyberEdge.

Other Policy Gaps

Most traditional insurance polices do not provide adequate coverage or protection in the event of these evolving exposures:

- Professional Liability
  Broadly worded PI policies are tied to "professional services" and may have a requirement that there be an act of negligence
- Commercial General Liability
  Bodily Injury/Property Damage has potential exclusions/ limitations
- Crime
  Requires intentional acts trigger and only covers money, securities, and tangible property
- Kidnap and Ransom
  No coverage without a "cyber-extortion" amendment
- Property
  Data is not considered tangible property

Cyber breaches in New Zealand that made the headlines

January 2011

- Ex-Telecom staff were reportedly able to access Telecom's databases after they had moved to rival Slingshot, obtaining the personal information and billing details of Telecom customers in an attempt to "win" customers over.

April 2011

- PlayStation Network was reportedly hacked resulting in 77million users worldwide having their personal details including passport numbers and credit card details leaked.

December 2011

- Waikato DHB reportedly had hundreds of on-line job applications stolen by hacker.

March 2012

- ACC reportedly accidently leaked the personal and claim information of 9000 claimants, which in turn was allegedly "extorted" by the receiver in a bid for monetary gain

Coverage

CyberEdge is a specially designed solution which addresses the liability of companies arising from data protection laws, the management of personal data and the consequences of losing corporate information.

This policy provides cover for:

- Personal Data Liability
  Breach of personal information / Data Protection
- Corporate Data Liability
  Breach of corporate information
- Outsourcing
  Breach of Data Protection by an Outsourcer where the Data User or Policyholder is legally liable
- Data Security
  Damage resulting from any breach of duty that ends in:
  - Contamination by Malicious Code of Third Party Data
  - Improper or wrongful denial of access by an authorised Third Party to Data
  - The theft of an access code from premises, Computer System or employees
  - The destruction, modification, corruption, damage or deletion of data stored on any computer system due to a breach of Data Security
  - The physical theft of hardware
  - Data disclosure due to a Breach of Data Security
- Defence Costs
  Both Civil and Criminal, including defense costs in respect of any criminal prosecution brought by a Data Protection Authority.

Key Additional Benefits

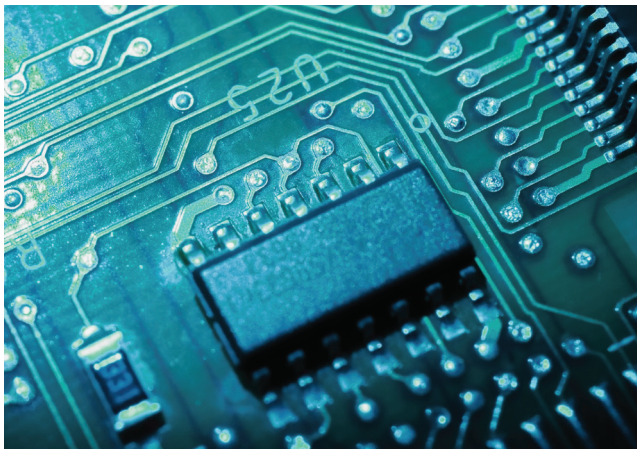
- Data Administrative Investigation
  Provides costs and expenses for legal advice and representation in connection with a formal investigation by a Data Protection or other authority.
- Data Administrative Fines
  Insurable fines and penalties imposed by a government authority, regulator or data protection authority for a breach of data protection laws or regulation.
- Notification & Monitoring Costs
  Provides costs and expenses of the data user for the legally required disclosure to Data Subjects.
- Repair of the Company's and Individual's Reputation
  Reimbursement of costs incurred in relation to Reputational Damage due to a claim covered by this policy.
- Wide definition of Insured
  Including director or partner, in-house counsel, data protection officer, Chief Compliance Officer, employee, estates or legal representatives of any insured.
- Wide definition of Data, Data Protection, Breach of Duty
- First Party & Third Party Loss cover

Optional Extensions

- Media Content
  The collection, creation, release, printing, broadcasting or distribution of media content, advertising and written, printed, video, electronic, digital or digitised content that results in an infringement; plagiarism, piracy or misappropriation or theft of ideas; libel or slander committed without malice; or an intrusion, invasion.
- Cyber Extortion
  Any Extortion incurred as a result of a Security Threat.
- Network Interruption Insurance
  Net Income (Net Profit or Loss before income taxes) that would have been earned; and continuing normal operating expenses incurred, including payroll as a result of a security failure.

Data Crisis Response Services

- Dedicated hotlines to specialist legal and public relations advisors in the event of an actual or suspected data loss
- Timely advice to help Insured's mitigate or even prevent loss
- Leading professional experts providing global coverage and localised advice
- Direct access to the helpline, no permission required from Insurer
- Services available to individuals and the company



The Cost of Data Breaches

Research[2] has shown that data breach costs tend to be linear; the more records compromised, the greater the costs.

Expenses associated with a large data breach include:

- Detection, Escalation, Notification and Response
  A sophisticated attack by a hacker may take months to uncover after which the full extent of the damage may not be known for several additional months. Once a breach is discovered, affected parties must be notified and steps must be taken to mitigate the damage. Repairing a breach can be expensive and may involve hiring a forensic expert to discover the source of an intrusion.
- Lost Business
  Business can be lost both as a result of customer attrition as well as difficulty in attracting new customers. Lost business is the largest component of the average data breach loss, comprising 63 percent of the total loss, according to the Ponemon Institute a data security research firm. Companies in the financial service and healthcare sectors, where trust and security are cornerstones of the business relationship are especially vulnerable to damaged reputations as a result of a data breach.
- Fines and Penalties
  Fines and penalties can come from a number of sources.
- Damages
  Individuals and businesses that claim to have been damaged as a result of a data breach often seek compensation.
- Lost Productivity
  While difficult to quantify, lost productivity can be a very real cost of a data breach. Depending on the nature of the breach, IT personnel may be pulled off other projects to identify the source of a breach and fix it. Employees will be tasked with identifying affected businesses and individuals; notifying them and responding to questions. Lawyers will often spend a significant amount of time working with regulators and law enforcement agencies. Senior management's time is perhaps the most significant area of loss productivity following a large breach.
- Additional Audit and Security Requirements
  Companies experiencing a data breach may deem it necessary to implement enhanced monitoring and auditing protocols. Regulatory agencies may require heightened security measures and audits as conditions of settlement.
- Miscellaneous Additional Costs
  Additional costs arising from a data breach can include legal fees, consultant fees and various settlement costs.

[2] Advisen Special Report Sponsored by AIG, "An Anatomy of a Data Breach: Disaster - Avoiding a Cyber Catastrophe." 2011

Industries

Industries that will benefit from CyberEdge include all Commercial entities, including but not limited to the following sectors:

- Medical/Healthcare
- Retail/Wholesale
- Manufacturing/Industrial
- Construction/Real Estate
- Telecommunications/Media/Technology/Internet Services
- Transportation/Airlines/Travel Sector/Logistics
- Education (Schools, Colleges and Universities)
- Entertainment
- Professionals (Solicitors, Law Firms, Accountants, Insurance Brokers)
- Telemarketing/ Call Centre/Internet Services/Data Processing (Outsourcer)
- Government and Municipalities
- Any company with offices/operations in EU, Japan, Australia, Korea, Hong Kong, Taiwan, Malaysia and USA where data protection legislation is onerous
- Any other commercial entity that holds personal information and data

Target Market

From small to multinational companies with a minimum revenue/ turnover/ fee income of at least US$100,000 per annum.

Jurisdiction/ Territorial Limit

Worldwide (excluding USA/ Canada)

Documents Required for Underwriting

AIG CyberEdge Proposal Form

Coverage Period

Claims first made against the Insured during the Policy Period

Limits of Liability

Up to $10,000,000 – subject to individual risk assessment CyberEdge

About AIG

AIG is the world's largest insurance organization, serving more than 88 million customers in over 130 countries and jurisdictions around the world. AIG businesses are market leaders in property casualty insurance, life insurance and retirement services, mortgage insurance, and aircraft leasing.

Additional information about AIG can be found at

- www.aig.com
- YouTube: www.youtube.com/aig
- Twitter: @AIG_LatestNews
- LinkedIn: http://www.linkedin.com/company/aig

For more information

Please contact our Professional Indemnity Underwriting team.

Our Claims Promise

We have a proven track record of defending allegations arising from data breaches around the globe. Our local claims teams understand the value of a rapid response, the commerical aspects of business and the importance of mounting the strongest possible defence.

In the event of a claim, each Insured will be allocated a specific claim handler who will assist in the management of the claim and will work with the specialist legal counsel and loss adjusters to limit potential losses and bring the matter to a swift conclusion.

Additionally, in emergency situations our Data Crisis Response Service provides Insureds with direct access to legal and public relations experts who can be contacted even before any claim has been notified to us.

AIG Bring on tomorrow

Auckland
The AIG Building, Level 19
PO Box 1745
Shortland Street
Auckland 1140
Telephone 09) 355 3100
Facsimile 09) 355 3135

Wellington
PO Box 10-238
The Terrace
Wellington 6143

Telephone 04) 385 4737
Facsimile 04) 472 3917

www.aig.co.nz