Financial Lines

CyberEdge
Cyber Risk Protection for Commercial Entities

With recent data breaches hitting the headlines across the Asia Pacific/Oceania region, 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 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 businesses.

Current State of Cyber Liability

A study commissioned by Symantec put the cost of cybercrime to Australians at $4.5 billion per year with the average cost of a data breach reaching $2.16 million in 2011. The majority of the cyber liability insurance claims payments are found to go towards legal costs including regulatory fines, compensation claims and forensic and legal counsel.

Our technology-dependent world is changing constantly; liability policies do not cover every invading army of cyber risk exposures. There is clearly a need for advancing the scope of coverage for cyber liability that addresses the full breadth of cyber risks.

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 liability issues if such data were to fall into the wrong hands or enter the public domain.

Research has found that:

- Over the last three years, there has been a 2000% increase in cyber attacks, with more than 45% originating in the Asia Pacific/Oceania region.
- In Australia, cybercrime is the second most commonly experienced crime, just behind asset misappropriation.
- 30% of Australian organisations experienced cybercrime in the last 12 months, significantly higher than global (23%) and Asia Pacific (22%) levels.

More Claims Examples equals Increased Demand

There are more cyber risk stories in the media every day, most notably the following high profile examples:

- In January 2012, Australia’s second-biggest online broking business, ANZ Bank’s ETrade, was forced to shut down over the New Year period by a denial-of-service attack launched from overseas. Following the attack, access to the site was unavailable for some customers for nearly two weeks.

- Former Woodside Petroleum CEO Don Voelte warned in 2011 that cyber attacks were a major concern and that the company had been attacked “from everywhere”, particularly Eastern Europe, Russia and China.

Such examples are making clients realise the risks that personal and corporate data create, and are beginning to request policies with enhanced coverage. AIG has launched an innovative insurance product in addressing these issues, CyberEdge.

CyberEdge is an insurance solution specifically designed to address 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, corporate data liability, outsourcing liability, data security liability, data administrative investigations, data administrative fines, repair of the company’s reputation, repair of individual reputation, notification and monitoring costs, electronic data and defence costs. CyberEdge also includes optional coverage for media content, cyber extortion and network interruption.

1  ABC radio ‘AM’ 8 Sep 2011.
2  Akamai, State of the Internet Q3 2011.
3  Ibid.
Where other Policies can Fall Short

Whilst most traditional insurance policies claim to offer a comprehensive solution for cyber risks, it is important to be aware that they generally do not provide adequate coverage or protection in the event of these evolving exposures:

- **Professional Indemnity/Professional Liability (PI)** – Broadly worded PI policies are tied to “professional services” and may have a requirement that there be an act of negligence
- **Commercial General Liability** – Injury has potential exclusions/limitations around financial loss
- **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

What CyberEdge will Cover

CyberEdge provides coverage for personal data liability, corporate data liability, outsourcing liability, data security liability, data administrative investigations, data administrative fines, repair of the company’s reputation, repair of individual reputation, notification and monitoring costs, electronic data and defence costs. CyberEdge also provides optional coverage for media content, cyber extortion and network interruption.

- **Personal Data Liability** – Breach of personal information/data protection
- **Corporate Data Liability** – Breach of corporate information
- **Outsourcing** – Breach of data protection by an outsourced provider 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** – Defence costs in respect of any litigation brought by a data protection authority
Key Additional Benefits

- **Data Administrative Investigations** – Provides costs and expenses for legal advice and representation in connection with a formal investigation by 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 regulations.

- **Notification and Monitoring Costs** – Provides costs and expenses of the insured for the legally required and voluntary disclosure to data subjects.

- **Reputational Repair of the Company and Individual** – 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**

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 loss 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.
What are the Exposures?

The Internet has spun a whole new “Web” of liability exposures. Creating a website is simple, the exposures that come with it are not so straightforward. Whether you meant to or not, you are creating a portal for external access into your internal systems.

The risk category includes privacy issues and the theft of data, the infringement of intellectual property, virus transmission or any other serious intrusion that may be passed from first to third parties via the Web.

Exposures Are Continuously Morphing and Becoming Harder to Defend Against:

- Hacking of data stored on your website and servers
- DDoS attack (other forms of extortion)

These Exposures Can Result in the Following:

- SQL injections
- Viruses and trojans
- Liability from slander/defamation
- Employee error/rogue employees
- Loss of laptop/USB drive
- The industry of “advanced persistent threats” is growing rapidly.

7 InsureNewMedia, “Cyber Liability Explained.” 2011.
First and Third Party Potential Losses

- It can take years to build a good reputation and book of business, but a single data breach can instantly change everything, leading to loss of clients and potentially the devaluation of company stock
- Small companies which are dependent on larger sites as a platform for shared hosting services may lose their partnerships, limiting distribution avenues and opportunities
- Costs associated with notification of data breaches and credit monitoring facilities may arise
- Regulatory investigations can require companies to shut down their systems for forensic purposes, limiting potential production
- Network hijackings can often require systems to be shutdown over extended periods of time as issues are resolved. This could lead to loss of business and the ability to conduct business as usual
- Cyber extortion can cost a company considerable time and money to quantify the potential damage of leaked information and weigh it against the cost of paying any ransoms

Legal Exposures

Regulatory Action

2011 has been identified as a watershed year for data protection in the Asia Pacific region8

In 2009 New Zealand, Hong Kong, Taiwan, South Korea, Japan and Macau enacted data privacy laws. Since then they have been joined by India and Malaysia, but just as important, South Korea and Taiwan have made major changes to expand and strengthen their laws. Australia and Hong Kong are in the process of so doing and New Zealand has made significant changes in order to obtain an ‘adequacy’ rating from the EU. Even Singapore has promised a law and China and Vietnam have introduced piecemeal protections.

Any person or entity storing or processing personal data is potentially subject to investigation and enforcement action by local regulators under these increasingly strict legal regimes. Additionally, they may face significant fines and defence costs in the event of a data breach, regardless of whether any third party suffers loss or chooses to take legal action.

The cross border reach of many data protection regimes, coupled with an increasing tendency towards international outsourcing of data processing services, means that few businesses can be confident that their systems and processes are not subject to regulation and enforcement by overseas authorities.

Further, even in countries with no specified data protection or data privacy law or regulator, businesses may find their data processing activities increasingly subject to scrutiny under local criminal law and other regulatory requirements, which may be markedly stringent.
Civil Liability

In addition to the likely regulatory investigation and enforcement action occasioned by a data breach, a business may also face civil liability in the form of damages and costs to individuals and corporate entities whose data has been compromised.

Claims arising from personal data breaches may be comparatively low in quantum at the individual level. In the context of thousands or even millions of records being lost, disclosed, corrupted or illegally sold, the prospect of group or class actions creates an exposure of a magnitude with defence costs to match.

Similarly, a breach of corporate data has the potential to give rise to financially significant and complex commercial litigation that may be costly and time-consuming to resolve.

Cause of Data Loss

Through 2010, theft/loss/improper disposal of computers, hardware and portable media accounted for 32% of reported data breach incidents. Many of these incidents could have been avoided with the implementation of appropriate security procedures such as encryption.

The increase in web/network exposure, hacking and malware has grown exponentially with industries including telecommunications, retail, professional services and education being most heavily affected by percentage of total breaches. Financial institutions and retailers were traditionally the biggest targets, however advanced network security enhancements within these sectors have now made professionals and small businesses the leading threat.

Cyber crimes are perpetrated by governments, organised crime syndicates, rogue investors and even competitors. The threat of human/system error continues to be one of the biggest threats to network security. By sector, non-profits, financial services and governments are most heavily affected by human/system errors by percentage of total breaches. Malicious insiders are a growing pandemic and can affect any industry.9

Cause of Data Loss vs. Industry:

Number of acknowledged incidents as % of total for 2010 (January – June)

[Diagram showing data loss causes by industry]

Rogue Employees

In 2011, Accenture surveyed 1,500 companies across 19 countries and found that employees (48%) and business/system failures (57%) were cited most often as the source of data breaches across the world. This finding is in stark contrast to common perception that external forces are the biggest threat to privacy and security. The number of rogue employee-related incidents are expected to grow unless the proper security procedures are in place.

Research has also found that:
- A direct correlation exists between the increased number of insider thefts and the increase in unemployment
- 46% of insider incidents are committed using company email
- 22% of incidents involved the theft of hard copies
- 9% of insiders used USB drives or CDs
- Insiders steal mostly financial information, business plans and client data
- 70% of insiders take the information to competitors
- 23% use the information to start a competing business
- 1% sell the data
- 93% of malicious insiders leave the company before their acts are discovered
What Industries are Being Attacked?

- Healthcare
- Insurance
- Financial services
- Professional services
- Technology

By Sector: Number of incidents as a % of total for 2010

By Sector: Number of records/people affected as a % of total since 2007 (to June 2010)
What is Being Taken?

- Personally identifiable information
- Government ID numbers
- Medical records
- Credit/debit card details

By Type: Number of records/people affected in 2010 (January – June)

NB. This graph shows the number of records exposed per data type. Note that some records lost/stolen may expose one or more data type.

Source KPMG 2010
The Cost of Data Breaches

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

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 should 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% of the total loss, according to the Ponemon Institute, a data security research firm. Three types of organisations are more vulnerable to reputational risk and consequently lost business as a result of a data breach. 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 lost 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.

Avoiding a Data Breach Disaster

For loss of sensitive records, once a breach has been discovered and the appropriate people within the organisation have been notified, an effective response should include:

- Identifying and fixing the cause of the breach. The timing and method of the fix will depend upon the nature of the breach (e.g. a system is hacked requiring more robust laptop security protocols)

- Notifying law enforcement officials

- Notifying critical vendors and business partners

- Notifying regulatory agencies (e.g. Privacy Commissioner)

- Notifying data subjects

- Notifying other stakeholders such as investors

- Implementing activities such as credit report monitoring services to mitigate potential future harm

- Notifying the cyber liability insurer and activating coverage
What Industries can Benefit From CyberEdge

- Medical/Healthcare
- Retail/Wholesale
- Manufacturing/Industrial
- Construction/Real estate
- Telecommunications/Media/Technology/Internet services
- Transportation/Airlines/Travel sector/Logistics
- Education
- Entertainment
- Professionals (Solicitors, Law firms, Accountants, Insurance brokers)
- Telemarketing/Call centre/Internet services/Data processing
- Government and municipalities
- Any company with operations in Australia, EU, Japan, New Zealand, 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

Jurisdiction/Territorial Limit
Worldwide (excluding USA/Canada)

Documents Required for Underwriting (to be reviewed and accepted by Underwriters)
- CyberEdge proposal form

Coverage Period
Claims first made against the Insured during the policy period

Limits of Liability
Up to AU$10,000,000 – subject to individual risk assessment
How AIG can Help?

About AIG
American International Group, Inc. (AIG) is a leading international insurance organisation serving customers in more than 130 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.

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.au. Products and services are written or provided by subsidiaries or affiliates of American International Group, Inc. Not all products and services are available in every jurisdiction, and insurance coverage is governed by actual policy language. Certain products and services may be provided by independent third parties. Insurance products may be distributed through affiliated or unaffiliated entities. 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.