

Cyber Insurance Research Paper

Sponsored by AIG



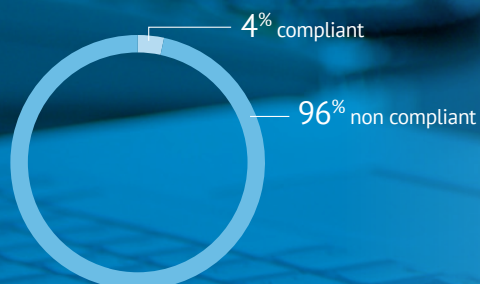
Contents

- 2 Introduction
- 3 Legislative Environment
- 4 Other Jurisdictions
- 5 Cost of a Data Breach
- 6 Incident Response
- 7 What is Cyber Insurance?
- 8 Insurance Benefits and Considerations
- 9 Decision Points
- 10 Conclusion

→ **59%** of respondents to a survey conducted by McAfee were unaware of the recent major changes to the Privacy Act (source: *State of Privacy Awareness in Australian Organisations* survey 2013)

→ **65%** of SMEs said that, in general, their organisations' sensitive or confidential business information is not encrypted or safeguarded by DPL technologies (source: <http://about-threats.trendmicro.com/us/threatencyclopedia#malware>)

Payment Card Industry Data Security Standard compliance status based on last assessment*



*Verizon caseload only. Largely based on victims' claims re their status.
(Source: P.56, Verizon 2012 Data Breach Investigations Report)

Introduction

Technology has transformed the way business is conducted from providing services online to customers, to storing data in the 'cloud' while accessing information from tablets and smart phones. This brings benefits to large and small businesses alike. It also brings risk. According to the Australian Bureau of Statistics, Australian businesses received orders worth an estimated \$237 billion via the internet in 2011/12, an increase of 25% from the previous year. It is expected this increase will continue. Statistics New Zealand has also revealed that with 80% of homes having an internet connection, 50% of the population made an online purchase in 2012. As these changes have evolved, so too has the responsibility for the protection of privacy and personal data fallen on business.

With millions of consumers transacting with businesses online each year, it is an organisation's obligation to put mechanisms in place to stop the loss of personally identifying information of its customers, which includes both sensitive personal information such as a person's name, address, login details, credit card details, unique identifiers such as a Medicare number; and also transactional data and information which can be combined to paint a picture about the user, including system identifiers such as IP addresses, and machine identifiers such as MAC addresses. Should such a loss occur, it is also the business's responsibility to respond in an efficient and effective manner.

A common misconception amongst businesses that don't consider themselves to be online organisations is that they are immune to cyber attacks, however these businesses are likely to have files and records stored on computers connected to the internet, and are therefore responsible for the protection of that information. Another misconception is that only high profile multinational companies are at risk of a cyber attack; however evidence continues to show that small and medium size businesses are increasingly being targeted by cyber criminals. Often

**In 2012, 7,300 incidents reported to CERT Australia
Mid-August 2013, 8,500 incidents already reported.**

Source: CERT Australia, Australian Security Magazine, 21 October 2013

these smaller organisations do not have sophisticated cyber security policies and procedures implemented, yet they still hold valuable information and are seen as "low hanging fruit" by online criminals for the riches they hold.

The Centre for Internet Safety at the University of Canberra was created to foster a safer, more trusted internet by providing thought leadership and policy advice on the social, legal, political and economic impacts of cyber crime and threats to cyber security. With organisations in Australia and New Zealand facing business disruption, loss of clients, distrust amongst stakeholders, legal action and a damaged reputation following a cyber attack, it is integral that managers and directors are aware of the threats they face and the mitigation exercises they can impose to reduce the risks. The aim of this research paper is to explain what exposures are posed by existing and proposed legislation, what cyber insurance is and highlight the potential issues that may arise if relying upon traditional insurance products to address the evolving threats of cyber liability.



Organisation's need to make informed decisions surrounding cyber risk and should ask questions such as:

- What are the organisations tangible assets?
- Can the organisation survive without them?
- Is the organisation principally B2B or B2C?
- Does the organisation manage any fully automated IT systems?
- What are the privacy and data breach laws for the markets the organisation operates in?

Legislative Environment

As businesses and individuals navigate the shifting online risk landscape, they face a range of evolving challenges including privacy, security and intellectual property liability. For organisations that collect, store and use information, there is yet another level of scrutiny. When these organisations deal with personally identifiable information, private health records or commercial trade secrets, you can guarantee that there are cyber criminals somewhere in the world who will see this information as a valuable target.

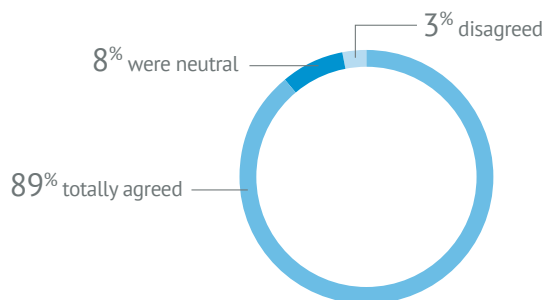
The Office of the Australian Information Commissioner's 2013 Community Attitudes to Privacy Survey revealed that Australians are becoming more concerned about privacy risks and expect the organisations they deal with to take effective steps to safeguard their personal information. In a similar survey conducted for the New Zealand Privacy Commissioner in 2012, 89% of respondents stated that they felt businesses should notify them if their personal information had been breached. Breaches that result

in the loss of proprietary or confidential business information can make an organisation look ill-prepared, careless or incompetent, which leads to a loss of customer trust and ultimately, damages corporate reputation.

In Australia, the Privacy Amendment (Privacy Alerts) Bill 2013 has been designed to amend the Privacy Act 1988 in order to introduce mandatory data breach notification provisions for government agencies and private sector organisations. If this new legislation is passed, the amendments will see organisations fined for data breaches and will force them to notify the Commonwealth Privacy Commissioner and affected consumers when data breaches occur. The legislation will introduce a new level of consumer privacy protection for Australians, compelling organisations that retain personally identifying information to keep personal customer information more secure. The proposed legislation will also encourage agencies and private sector organisations to improve their data security practices.

In addition to the aforementioned legislation, from 12 March 2014 new Australian Privacy Principles will apply to organisations (with revenue greater than \$3m per year), allowing for a harmonised set of guidelines that will regulate the handling of personal information by both Australian government agencies and businesses. These changes will allow the Privacy Commissioner to accept enforceable undertakings, seek civil penalties in serious or repeated breaches of privacy, and conduct assessments of privacy performance for both Australian government agencies and businesses.

Question: If a business loses my personal information, should they tell me?



Source: Individual Privacy & Personal Information Report, UMR Omnibus Results April 2012



In New Zealand, the Privacy Act 1993 controls how 'agencies' collect, use, disclose, store and give access to 'personal information'. The Privacy Act has twelve information privacy principles, which apply to government departments, companies of all sizes, religious groups, schools and clubs. These privacy principles govern the collection of personal information; the way personal information is stored; give individuals the right to access and correct information about themselves; place restrictions on how people and organisations can use or disclose personal information; and govern how unique identifiers, such as bank account numbers, can be used.

The New Zealand Privacy Act contains a number of privacy codes of practice, specifically applying to health, telecommunications and credit reporting. Like Australia, New Zealand has a set of voluntary guidelines reflecting international best practice, which are designed to assist New Zealand organisations that are faced with managing the privacy aspects of a data security breach. Also similar to Australia, the New Zealand Law Commission has recommended that notification should be mandatory in cases where notification will enable individuals to take steps to mitigate a risk of significant harm, or where the breach is a serious one. Mandatory notification is important because it gives organisations an incentive to ensure they have adequate security arrangements in place for the personal information they hold. The implementation of such legislation in Australia and New Zealand will also make complying organisations more trustworthy with consumers.

The New Zealand Privacy (Cross-border Information) Amendment Act 2010 amended sections of the Privacy Act 1993 and focuses upon trans-border data flows and the operation of a privacy law in a globalised economy. In particular, the Act ensures individuals can exercise access rights when outside New Zealand, enables the Privacy Commissioner to more effectively cooperate with overseas privacy enforcement authorities, and enables enforcement actions in certain cases involving transfer of information to another jurisdiction. These privacy laws are being reviewed and it is likely that they will follow suit with similar strengthening of privacy legislation around mandatory notification as has been proposed in Australia.

Whilst the introduction of new legislation surrounding data breaches will be a key step in the reform of privacy laws in Australia and New Zealand, it will only be truly effective if a company's organisational management and if applicable, the Board of Directors, ensure that the company is meeting legislative requirements and ensure that consumers are provided with actionable advice. Prompt notifications issued by organisations following a breach will allow individuals to take action to protect themselves against the misuse of their personal information, which may include credit reference monitoring, resetting passwords, cancelling credit cards and improving their online security settings.

Ultimately, new data breach legislation in Australia and New Zealand is a long overdue measure for ensuring any organisation's readiness when addressing cyber risk.

Other Jurisdictions

Data breach notification laws are a feature of the US privacy law landscape. They were pioneered in California in 2003 and exist in approximately 45 other States, as well as Federally.

Under European law, personal data can only be gathered legally under strict conditions and for a legitimate purpose. Persons or organisations that collect and manage personal information must protect it from misuse. Under the revised ePrivacy Directive (2009/136/EC), when a personal data breach occurs, the provider has to report this to a specific national authority. The provider must also inform the concerned subscriber directly when the breach is likely to adversely affect personal data or privacy.



Cyber insurance is a part of a stepped risk management process. Organisations should:

1. Map their cyber risks, including interdependencies, measuring impact and probability
2. Implement protection procedures and conduct regular audits
3. Identify residual risk and seek to transfer this to an insurer

Cost of a Data Breach

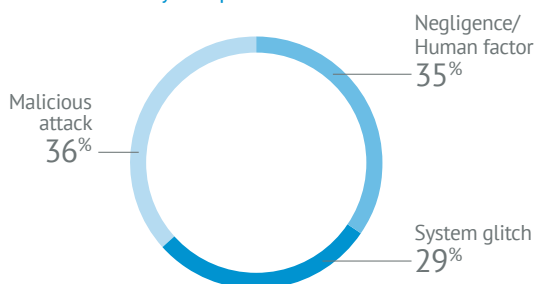
Individuals can suffer identity theft and fraud when personal information relating to their finances is compromised as a result of a data breach. They can also suffer embarrassment and distress when personally identifying information is publicly revealed. Whilst most data breaches involve loss of personally identifiable information such as credit card details which can easily be turned into money, there are also a vast number of breaches that seek an organisation's intellectual property and classified data.

There is a constant stream of media coverage regarding organisations, public and private and of all sizes, suffering a data breach. In October 2013, the security team of software maker Adobe discovered sophisticated attacks on their network, involving the illegal access of customer information as well as source codes for numerous Adobe products. Details from approximately 2.9 million Adobe customers were believed to be stolen, including names, credit and debit card numbers, expiration dates, and information relating to customer orders.

Another high profile example of a data breach in a large organisation occurred in February 2013, when the Australian Broadcasting Corporation (ABC) revealed the personal details of almost 50,000 internet users had been exposed online after a subsidiary program website was hacked. This incident follows data breaches in recent years at Telstra, Medvet and Roses Only.

There have also been many recent data breach incidents in New Zealand, with a notable example being the Accident Compensation Corporation's 2012 breach of 6,748 clients details, which is currently being investigated by The New Zealand Privacy Commissioner. The Commissioner's comments were that the Corporation displayed an "almost cavalier attitude" towards data protection.

The main cause of data breach for nine country samples



Source: Ponemon Institute/Symantec 2013
Cost of Data Breach: Global Study

Not all data breaches are equal. The impact of a data breach can be wide ranging; from financial implications via liability to third parties, fines and expenses, through to less tangible impacts such as reputational damage and the disruption caused by being involved in a regulatory investigation. Some breaches are more devastating than others to an organisation's reputation and brand image, with the loss or theft of customer information arguably the most devastating. A data breach may occur in a number of scenarios, such as following a malicious breach of an organisation's IT systems by a hacker; an accidental loss, such as IT equipment or hard copy documents; or through a negligent or improper disclosure of information. Also critical is the loss or theft of confidential financial business information and intellectual property critical to an organisation's operations.

The 2011 Ponemon Institute Reputation Impact of a Data Breach Study reported that whether the result of lost laptops, misplaced thumb drives, malicious software or system glitches, data breaches carry very serious financial consequences, with the average loss in the value of the brand ranged from \$184 million to more than \$332 million.

The 2013 Verizon Data Breach Investigations Report found 75% of all attacks were opportunistic – not targeted at a specific individual or company; whilst 62% of all breaches took months to discover. Of these breaches discovered, 69% were found by an external party and 9% were spotted by customers.

Factors which contribute to electronic attacks:

- Exploitation of misconfigured operating systems
- Unpatched or unprotected software
- Inadequate staff training
- Poor organisational security culture
- Lack of security technologies
- Remote access and/or connectivity to IT systems
- Inadequate levels of security of 3rd party computer networks



Incident Response

Whilst legislation in Australia and New Zealand does not impose an obligation on entities to notify the respective Commissioners or any individuals whose personal information has been compromised in the event of a data breach, Privacy Acts in both countries do require government agencies and organisations to take reasonable steps to maintain the security of the personal information they hold. The Office of the Australian Information Commissioner currently has in place a voluntary guide for entities giving advice on how to handle a data breach. It is a similar situation in New Zealand with practical guidance given by the Office of the Privacy Commissioner.

Data breaches can be caused by a variety of internal and external factors, affect different types of personal information and give rise to a range of actual or potential harms to individuals, agencies and organisations. Figure one lists the impact of various kinds of cyber attack against industry sectors. As such, there is no single way of responding to a data breach. Each breach will need to be dealt with on a case-by-case basis, undertaking an assessment of the risks involved, and using that risk assessment as the basis for deciding what actions to take in the circumstances.

Organisations should develop and regularly test an incident response plan which will list actions that are proportionate to the significance of a breach, as well as identifying whether it was a systemic breach or an isolated event.

Figure One
Impact of various kinds of cyber attack against industry sectors.

■ Low impact
■ Medium impact
■ High impact

	Arts & Entertainment	Agriculture	Banking & Finance	Construction	Defence	Education	Government	Health	Hospitality	Manufacturing	Media & Telecommunications	Mining	Not for Profit	Retail	Transport	Utilities
Degradation of network performance	Low	Low	High	High	High	Low	High	High	Low	Low	High	High	Low	High	High	High
Denial of service attack	High	High	High	Low	High	Low	High	High	Low	Low	High	Low	Low	High	High	High
Computer facilitated financial fraud	Low	Low	High	Low	High	Low	High	High	Low	Low	High	Low	Low	High	High	High
Interception of telecommunications	High	High	High	Low	High	Low	High	High	Low	Low	High	Low	Low	High	High	High
Malicious software attack	Low	Low	High	High	High	Low	High	High	Low	Low	High	Low	Low	High	High	High
Phishing scams	High	High	High	Low	High	Low	High	High	Low	Low	High	Low	Low	High	High	High
System penetration by outsider	Low	Low	High	Low	High	Low	High	High	Low	Low	High	Low	Low	High	High	High
Theft of physical device	High	High	High	High	High	Low	High	High	Low	Low	High	Low	Low	High	High	High
Theft of PII	High	High	High	High	High	Low	High	High	Low	Low	High	Low	Low	High	High	High
Theft or breach of information	Low	Low	High	High	High	Low	High	High	Low	Low	High	Low	Low	High	High	High
Unauthorised access to information by insider	Low	Low	High	High	High	Low	High	High	Low	Low	High	Low	Low	High	High	High
Unauthorised privileged access	High	High	High	High	High	Low	High	High	Low	Low	High	Low	Low	High	High	High
Website defacement	High	Low	High	Low	High	Low	High	High	Low	Low	High	Low	Low	High	High	High

Incident 1

Background

The insured was a national apparel retailer with hundreds of stores.

Incident Overview

At the start of a busy holiday weekend, security failure prevented both in-store and online credit card sales being processed and also disrupted the time management system for individual stores and in-store communication systems for nearly 48 hours.

Damage

The insured experienced huge delays in processing payments, leading to frustration and customer walk-outs.

AIG worked closely with the insured to retain a forensic accountant to calculate the lost sales resulting from the system disruption/failure, recognising that weekend sales are normally higher and that damages were compounded by the disruption occurring during a holiday weekend.

Incident Costs

Approximately US\$1,400,000 of profit was lost, in excess of the applicable waiting period for system failure (optional coverage) in the Network Interruption coverage section of the insured's policy.

AIG successfully processed the reimbursement in full.

What is Cyber Insurance?

The number of exposures businesses face continue to increase and as organisations become more globally networked and complex, insurance policies need to adapt to the changing environment. Some organisations have discovered gaps in what is and what isn't covered after an attack. Unfortunately for them, by then it is too late. The Sony Playstation case is currently before the courts in the US as a result of a traditional liability policy not responding to a cyber attack.

Cyber insurance is a tailor made insurance offering providing comprehensive cover for liability and expenses a business may incur arising out of unauthorised use of, or unauthorised access to, physical and electronic data or software within an organisation's computer network or business. Cyber insurance policies can also provide coverage for liability, costs and expenses arising from network outages, the spreading of a virus or malicious code, computer theft or extortion.

Traditional business insurance policies have tended to only cover "tangible" assets such as PCs, lap tops and other mobile devices. Developing exposures have highlighted that electronic data is not always considered to fall under the definition of tangible assets and is just one area where cyber insurance is designed to fill a gap.

Cyber insurance also provides cover for business interruption and the cost of notifying customers and regulatory investigations or actions in case of a breach, without the requirement for physical damage that is a standard trigger under property policies. When looking at policy options, organisations should consider coverage which addresses these issues.

Policy premiums vary depending on the industry, type of data held, number of data records and the risk management policies and procedures implemented to ensure the security and integrity of that data.

Organisational size by number of breaches (number of employees)	
1 to 10	42
11 to 100	570
101 to 1,000	48
1,101 to 10,000	27
10,001 to 100,000	23
Over 100,000	10
Unknown	135

(Source: P.11, Verizon 2012 Data Breach Investigations Report)



Incident 2

Background

The insured was a Financial Institution.

Incident Overview

An email server and an external hard drive were stolen from the premises of an outside vendor.

Damage

Data that included personally identifiable emails affecting approximately 175,000 individuals were compromised. AIG worked closely with the insured and extended the full policy limit for Event Management coverage for the costs of notification to the affected individuals and the retention of a law firm and public relations firm.

Incident Costs

AIG paid in excess of US\$1,000,000.

Insurance Benefits and Considerations

Cyber insurance can help organisations return to their normal operating status after a cyber attack or a data breach. Cyber insurance policies are designed to address many variables within the online realm and can include:

- The liability of companies arising from data protection laws;
- The management of personal data;
- The consequences of losing personally identifying data or corporate information (including that which may be hosted by third parties on behalf of an organisation);
- Repair of an organisation's reputation;
- Repair of individual reputation;
- Notification and monitoring costs;
- Cyber extortion; and
- Network interruption.

A cyber insurance policy should cover immediate expenses such as crisis management, hiring a public relations firm to manage a data breach incident, forensic analysis, repairing and restoring computer systems and the loss of business income resulting from the incident.

An effective cyber insurance policy will include explicit wording which covers first party and third party claims. First party claims include cost of data recovery notification of affected customers, credit monitoring and legal expenses. Third party claims include financial penalties, customer compensation and reputational damage.

When evaluating the need for cyber insurance, an organisation should consider the following factors in assessing the risks:

- The type and context of personal information transacted and retained;
- The risk of serious harm to the affected individuals;
- The education, training and oversight of employees;
- The level of security of mobile devices that carry sensitive data;

- The level of encryption of sensitive data at rest and in motion;
- Interruption to business-as-usual operations;
- Costs of computer forensic investigations and civil litigation or criminal investigation;
- Service level agreements with any third-party service providers who may be contracted and have access to sensitive data, ensuring they have policies and procedures in place which are tested to ensure compliance;
- Crisis management, public relations and customer notification expenses in the event of a data breach or other online attack.

Too often the subject of cyber risk management and insurance is seen as a matter for the IT department to manage. However, for an organisation to form a comprehensive cyber risk strategy and to have a strong chance of it succeeding, it is imperative that an organisation's key stakeholders including the Chief Executive Officer, Chief Risk Officer and Operations Manager are all involved. Organisations need to make informed decisions, while understanding what their assets are and how the organisation would survive without them.

Cost of data breach



Cost goes up when...

Third party error	(+\$19)
Lost or stolen devices	(+\$8)



Cost goes down when...

Strong security posture	(-\$15)
Incident response plan	(-\$13)
CISO appointment	(-\$8)
Consultants engaged	(-\$5)

2013 Annual Study: Global Cost of a Data Breach - June 5, 2013



The Payment Card Industry Data Security Standard lists a number of common drivers why organisations seek compliance:

- Increased awareness and general concerns over data security and privacy
- Significant fines, penalties and increased transaction processing costs
- Reputation and brand damage leading to loss of revenue
- Regulatory requirements around the privacy of customer data
- Industry peer pressure
- Alignment with corporate risk management guidelines
- Potential inability to process credit cards

Decision Points

The constant evolution of cyber attacks and consequential organisational vulnerabilities means it is easy for companies to underplay the business impact from cyber exposures and the best way to identify and mitigate risk. Cyber risk needs to be part of the broader enterprise risk strategy, ensuring all risks are assessed together in a portfolio approach. Organisations need to make informed decisions regarding the cyber threats facing them and the sector they operate in. Once they assess their exposures, organisations can choose what risks they are willing to accept and what risks they would like to transfer by way of insurance.

Creating effective IT security is about taking practical approaches. A secure IT system is one aspect, but often people are the weakest link. Many cyber risk issues are not the result of technology, nor the policies and procedures, but rather the internal and external people implementing them. Even the most sophisticated IT systems will not prevent breaches. Social engineering will continue to occur and whilst the risk cannot be eradicated, it can be reduced to an acceptable level.

There are ways to reduce cyber liability insurance premiums. The creation, implementation and ongoing testing of a cyber security policy and procedures benchmarked to best practice will not only reduce insurance costs, but will also decrease an organisation's chance of falling prey to cyber attacks, including data breaches. Competent organisations will have well-developed, well-communicated and tested plans and practices in place to prevent a data breach from occurring. They will also have developed a crisis management process that governs what to do in the event of a cyber attack.

Before purchasing an insurance policy, organisations should first self-analyse to determine what controls are in place and what risks need to be managed.

According to the Australian Bureau of Statistics, in 2011/12:

- 91.9% of businesses had an internet connection
- 44.6% of businesses had a web presence
- 55% of businesses placed an order via the internet
- 28% of businesses received an order via the internet

There are many parties who may be responsible for a cyber attack against an organisation, including employees, ex-employees, criminals and state parties. Likewise there are many reasons for carrying out such an attack, including illicit financial gain, using system resources for other activity, a competitor seeking commercial advantage, a foreign government seeking political advantage, personal grievance, unsolicited malicious damage or just an indiscriminate attack.



Conclusion

It is accepted even with the best-designed systems, that mistakes can happen and vulnerabilities will be found. As part of a data security policy, an organisation should anticipate what it would do if there were a data breach. Considering cyber insurance as part of this process will allow organisations to accurately map the various risk factors, such as:

- Does your organisation have a definition which specifies what a data breach is?
- Does staff at all levels understand the implications of losing organisational data or personally identifying information?
- What actions has your organisation implemented to reduce the risk of a cyber attack?
- How would your organisation know it has suffered a data breach?
- What would your organisation do if it suffered a data breach?
- Is it clear in your risk management plans who is responsible for dealing with an incident?

Mitigating cyber risk is not only about spending money on IT security, more importantly it is about identifying risks in people and procedures and developing a security-aware culture. In addition to the regulatory involvement and enforcement action resulting from 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.

Cyber insurance will become part of standard business insurance purchases in the next five years, and customers, suppliers, boards and investors will insist organisations they do business with have an appropriate level of cover.



Incident 3

Background

The insured was a professional services firm which operated a computer network comprising 22 desktop workstations, two virtual servers and ancillary devices including printers. Anti-virus software was installed on servers and all desktop workstations. Anti-virus definitions were up-to-date.

Incident Overview

A virus infection was discovered on the computers and the insured's IT service provider dispatched staff to assist. Initial attempts to eradicate the virus were unsuccessful. Eventually, the infection was eradicated by wiping and reinstalling all computers on the network. The insured incurred service costs and was unable to operate for several days.

Damage

The virus left the insured's computer systems impaired, requiring clean-up work to restore normal operation. There was no apparent loss of data or privacy breach. The incident was contained by quick action in conjunction with the AIG CyberEdge Data Crisis Response Team. AIG's quick response time prevented subsequent reputational damage or harm. The insured may have missed business opportunities and income during the period of business interruption (three days).

Incident Costs

This incident was minor relative to many cyber claims, due in part to the speed of response. No legal or reputational costs were incurred, but costs related to data restoration and business interruption were still significant given the size of the company.

Costs Covered by AIG:

Restoration of data including fees for forensic partners: NZ \$15,265

Estimated Network Loss: > NZ \$20,000



Centre for Internet Safety

About the Centre for Internet Safety

The Centre for Internet Safety at the University of Canberra was created to foster a safer, more trusted Internet by providing thought leadership and policy advice on the social, legal, political and economic impacts of cybercrime and threats to cybersecurity. For more information visit www.canberra.edu.au/cis

About AIG

American International Group, Inc. (AIG) is the world's largest insurance organisation, serving customers in more than 130 countries. AIG companies serve commercial, institutional, and individual customers through the most extensive worldwide property-casualty networks of any insurer. For more information visit aig.co.nz

Acknowledgements: AON, Marsh, NCC Group