Allens › ‹ Linklaters

Insuring against cyber-risks

A changing landscape

JULY 2015

As cyber-attacks on Australian businesses increase, many companies are discovering they are not adequately prepared or insured to handle a cyber-attack. Companies should review their cyber-risk profile, analyse the scope of their existing insurance coverage, and consider tailored cyber-insurance products to more thoroughly protect against cyber-risks.

Partner Andrew Maher and Senior Associate Stuart Packham examine the issues.

Introduction

According to the Australian Securities and Investment Commission's March 2015 report 'Cyber Resilience: Health Check' (the ***Report***),[1] cyber-attacks on Australian businesses are increasing. The loss, theft, hijacking or destruction of valuable electronic data and assets, including intellectual property, systems, databases and privately held information (and associated reputational damage) caused by a cyber-attack, can have a significant adverse impact on a company's bottom line.[2] This can occur as a result of 'first party' losses, 'third party' liabilities, and regulatory liability, for example, under the *Privacy Act 1988* (Cth).

A 2013 study commissioned by Symantec put the cost of cyber-crime to Australia at $1.06b per year,[3] with the average cost of a data breach reaching $2.16m in 2011.[4] In 2013, over 552 million identities globally were compromised through cyber-attacks, putting a range of personal information, including credit card details, birth dates and medical records, into the criminal realm.[5] In a 2015 report, the Association for Financial Professionals noted that one in three companies had been the target of cyber-attacks over the past 18 months and that 60 per cent of companies did not have a response plan in place to respond to a cyber-breach.[6]

A recent high-profile example of cyber-crime concerns the Target Corporation in the United States. During the 2013 holiday season, hackers stole credit card, debit card and other personal information of approximately 110 million customers. 114 customers brought putative class action against the retail store chain, relying on causes of action based in negligence, breach of contract, bailment and unjust enrichment. In December 2014, a District Court denied a motion to dismiss.[7] By March 2015 the case had settled, with Target Corporation agreeing to pay $10 million, and each plaintiff receiving up to $10,000 each.

The statistics and cases demonstrate that now, more than ever, companies need to understand their cyber-risk profile and take appropriate measures to protect themselves from these attacks. The ASIC Report highlights the importance of 'cyber resilience' to Australian companies and sets out ASIC's expectations of Australian companies (and their directors) in guarding against cyber-risks. Among other things, the Report questions the adequacy of existing corporate insurance programs in covering these risks and emphasises the importance of specialised cyber-risk insurance to companies, depending on their risk profile. A comprehensive insurance program, with appropriate cover for cyber-risks, is a key element of a prudent risk management regime.

The purpose of this paper is to discuss, at a high level:

- the types of losses and liabilities that a company may suffer or be exposed to following a cyber-breach;
- the extent of coverage generally available (and corresponding coverage gaps) for such losses and liabilities under conventional business insurance policies; and
- the coverage gaps that can be filled by cyber-risk insurance policies.

First-Party Losses and Third-Party Liabilities

First party losses resulting from a cyber-breach that a company may suffer include:

- business interruption losses due to a network or system shutdown, or a 'denial of service' (***DoS***)[8] attack;
- the costs of rectifying harm done, including forensic investigation costs, repairing and restoring systems that have been damaged by malicious acts, and re-creating lost intellectual property;
- the costs of improving cyber security and undertaking forensic investigations to identify the source of a cyber-attack;
- reputational damage and the costs of managing a reputational crisis, for example, by engaging a public relations firm, often at very short notice;
- extortion costs, such as paying ransoms to hackers in order to return, unlock or 'un-corrupt' valuable company data; and
- costs associated with complying with regulatory requirements such as mandatory data breach notifications. (In March 2015, the Australian Government agreed to introduce a mandatory data breach notification scheme to be effective by the end of the year.[9])

A company may also become liable to third-parties as a consequence of a cyber-attack, including, for example:

- liability in negligence or contract for failing to properly protect personal (eg customers') information against cyber-attacks or misuse;
- liability for misleading or deceptive conduct that may arise out of a failure to comply with the company's own privacy policy;

1 Australian Securities and Investment Commission, 'REPORT 429: Cyber Resilience: Health Check' (March 2015) 16 [27].

2 McAfee, Center for Strategic and International Studies, 'The Economic Impact of Cybercrime and Cyber Espionage' (July 2013) .

3 Symantec, '2013 Norton Report: Total Cost of Cybercrime in Australia amounts to AU$1.06 billion' (16 October 2013).

4 Ponemon Institute LLC, '2011 Cost of Data Breach Study: Australia' (March 2012) 5.

5 Symantec, 'Internet Security Threat Report: Volume 19' (April 2014) 5.

6 Association for Financial Professionals, '2015 AFP Risk Survey, Report of Survey Results' (January 2015) .

7 *In Re Target Corporation Customer Data Security Breach Litigation*, MDL No, 14-2522 (PAM/JJK), United States District Court, District of Minnesota.

8 A DoS attack is a malicious attempt to make a server or a network resource unavailable to users, usually by temporarily interrupting or suspending the services of a host connected to the internet.

9 Senator the Hon George Brandis QC and the Hon Malcolm Turnbull MP, 'The Australian Government has responded to the inquiry of the Parliamentary Joint Committee on Intelligence and Security (PJCIS) into the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014' (3 March 2015).

- fines imposed by regulators (eg the Information Commissioner or ASIC) on companies or individual directors;[10] and
- claims by third parties arising from failure to disclose market-sensitive cyber-risk information in prospectuses or disclosure documents, or failure to comply with continuous disclosure obligations (relevant to listed companies).

Traditional business insurance policies versus cyber-insurance

Companies typically maintain a suite of insurance policies, including:

- public and products liability insurance;
- professional indemnity insurance (where professional services are provided);
- commercial crime insurance;
- directors' and officers' liability insurance (***D&O insurance***); and
- property damage and business interruption insurance.

While some of these policies may, between them, cover losses or liabilities consequent upon a cyber-breach, some significant losses or liabilities may fall through the gaps.

Public and products liability insurance

Public and products liability insurance covers amounts that the insured becomes legally liable to pay as compensation for personal injury or property damage.

'Property damage' is generally defined as physical damage to, or loss of, or destruction of *tangible* property. Under Australian law, tangible property is unlikely to extend to computer software and other data.[11] Accordingly, the 'property damage' limbs of such policies would likely be of no assistance where a company is liable to pay compensation due to, for example, the destruction of a client's valuable data. Even if 'tangible property' was interpreted to include electronic data, some policies specifically exclude coverage for 'information technology hazards', being hazards arising from or connected to an insured's internet operations, or property damage to computer data or programs connected to the use of computer hardware or software, including damage caused by any computer virus.

Public and products liability insurance also covers compensation for personal injury, which is often defined to include an 'invasion of privacy'. However, given that potential Australian claimants are restricted to claims in negligence or contract, due to the lack of a personal cause of action in Australia for invasion of privacy, it is difficult to see this being helpful to insureds in the context of cyber-attacks.

Professional indemnity insurance

Professional indemnity insurance provides protection against claims for financial loss arising from an act, error or omission in the performance of professional services covered by the policy.

Generally speaking, the types of liabilities arising from cyber-attacks will not have arisen in the course of performance of professional services. Professional indemnity policies may however be helpful, for example, in protecting an information technology company providing services such as creating and maintaining firewalls and other network security, in the event that such services were deficient and lead to a cyber-attack. However, for the victim of a cyber-attack itself, any acts, errors or omissions will likely not have occurred in the performance of professional services.

Commercial crime insurance

Commercial crime policies indemnify the policy holder for losses resulting from 'criminal acts', which is generally defined to include 'computer fraud'. 'Computer fraud' generally means loss caused by a third party's fraudulent or dishonest misuse or manipulation of computer or funds transfer systems or programs owned or operated by the insured.

However, 'loss' is often narrowly defined to the *direct* financial loss of any property, money or securities, and generally exclude consequential losses such as business interruption, contractual penalties, court attendance costs, data reconstitution costs, investigation costs, legal expenses, or the costs of hiring a loss investigator or a public relations consultant.

Accordingly, many kinds of losses consequent upon cyber-attacks may not be covered by commercial crime policies, particularly where they fall within the scope of *consequential loss*. For example, a DoS attack which prevents a business from operating would arguably not cause any *direct* loss of any money or property, and would therefore be unable to trigger a business interruption extension, even if the company had taken one out.

A crime policy may however be useful in the case of a cyber-extortion attempt, where a hacker threatens to damage or destroy the computer systems of a company unless the hacker is paid a ransom. Cover for extortion is generally broadly worded enough to cover these threats to computer systems, although companies should be aware that such coverage is typically offered as an extension of cover rather than as part of the standard insurance offering.

D&O insurance

D&O insurance is liability insurance payable to the directors and officers of a company indemnifying losses resulting from claims made against insured persons in relation to alleged wrongful acts that were carried out in their capacity as directors and officers. D&O insurance policies also generally cover 'security claims', being wrongful acts with respect to the purchase, sale, transfer, or ownership of securities from, by or to the company.

Directors and officers of a company that falls victim to a data breach may need to make a claim on this policy if, for example, that company has failed to adequately disclose any high risk of cyber breach to the market.

10 The Australian Information Commissioner has the power to seek civil penalties or apply for civil penalty orders of up to $340,000 for individuals and $1.7 million for companies: ss 13G and 80W(5) of the *Privacy Act 1988* (Cth). Companies should also be aware of potential penalties from ASIC, for example due to a failure to notify ASIC of a breach of its AFS licensee obligations: see s 912D(1B) of the *Corporations Act 2001* (Cth). The maximum penalty for not reporting a significant breach (or likely breach) within 10 business days of becoming aware of the breach (or likely breach) is $42,500 for a company.

11 *Erris Promotions Ltd v Commissioner of Inland Revenue* [2004] 1 NZLR 811; *St Albans City and District Council v International Computers Ltd* [1996] 4 All ER 481.

While D&O insurance may provide coverage in many instances for such wrongful acts, the increasing occurrence of cyber-attacks on companies and the financial impact of such attacks is leading to greater scrutiny from insurers of a company's cyber-risk mitigation strategy and, in some instances, exclusion of cyber-risks from coverage. Insurers may also become less willing to cover cyber-risks under D&O policies when specific insurance exists for that purpose.[12]

Property damage and business interruption insurance

Most businesses maintain property damage and business interruption insurance indemnifying against physical loss, destruction or damage to particular property.

These policies generally insure against business interruption, which provides protection for time element losses caused by the damage incurred. Such policies are however ill-suited to covering cyber-losses, as time element losses typically require a 'physical damage' trigger,[13] being physical loss, damage or destruction occurring to insured property.

Further, regardless of the interpretation of 'tangible property' or 'physical damage', many property damage insurance policies contain general exclusions for losses in any way connected with the destruction, distortion, or misuse or misappropriation of electronic data, or a failure to send or receive electronic data, unless it is caused by a peril such as fire or flood or the theft of the physical computer hardware. Such exclusions would prevent a business from being able to claim, for example, losses suffered due to a DoS attack, or the misappropriation of customer information.

Cyber-risk policies

Noting the gaps in coverage concerning cyber-risks, insurers have devised specific 'cyber-insurance policies'. A typical cyber-insurance policy will cover, among other things:

- liability to pay compensation to third parties in relation to liability arising from a cyber-breach, and the defence costs associated with this, even if arising from the dishonest conduct of employees;
- fines and penalties imposed by government authorities for a breach of data protection and privacy laws (to the extent that such coverage is not prohibited by law);
- reasonable costs incurred in relation to public relations and crisis management to avert damage to the company's reputation;
- costs and expenses in restoring, re-creating or recollecting electronic data, where possible;
- costs of repairing or replacing any IT assets that have been damaged, corrupted or stolen;
- loss of business income resulting from interruption in service or the failure of IT assets; and
- cyber extortion expenses.

Cyber-insurance policies cover a number of the potential cyber-risk specific losses and liabilities, with the application of a single deductible.

It is important for all companies to consider their cyber-risk profile and determine whether their existing policies will be responsive. In considering these issues, it is also important for them to be conscious of exclusions that may apply in their existing policies – for example, a commercial crime policy may require tangible property theft, as opposed to data theft, and business interruption loss may only be covered on the proviso that physical damage is first sustained.

Conclusion

Given the increasing prevalence of cyber-losses and liabilities and the significant damage that they can cause a company, companies should analyse the scope of their existing coverage and, as appropriate, take out cyber-risk insurance. However, regardless of the insurance position taken by companies, it is important to bear in mind that cyber-insurance is no substitute for ensuring that proper risk-management and security measures are in place and are being regularly reviewed.

12 See further Insurance News, 'Directors Warned of D&O gaps for cyber attacks' (22 June 2015).

13 Some United States cases give 'physical damage' a wide definition, encompassing the malicious infection of a computer network with a virus and other destruction of data. We are not however aware of similarly broad cover in the Australian market. 'Physical damage' is also interpreted in Australia rather narrowly. See, eg *Transfield Constructions Pty Ltd v GIO Australia Holdings Pty Ltd* (1997) 9 ANZ Ins Cas 61-336.

Contact

Andrew Maher
Partner
T +61 3 9613 8022
Andrew.Maher@allens.com.au

Louise Jenkins
Partner
T +61 3 9613 8785
Louise.Jenkins@allens.com.au

Malcolm Stephens
Partner
T +61 2 9230 4828
Malcolm.Stephens@allens.com.au

Stuart Packham
Senior Associate
T +61 3 9613 8624
Stuart.Packham@allens.com.au