Cyber Attacks Prove Costly

Simon Landrigan
Principal
Marsh Pty Ltd

Cyber attacks on Australian organisations increased by 20 per cent in 2014 according to the Australian Signals Directorate; this is a timely reminder of how cyber threats are growing. Moreover, the Australian Crime Commission reported in June last year that Australians lost an estimated $110 000 every hour to cyber criminals, or more than $2.6m every day.

This demonstrates how serious cyber security is for every business. As such, it is critical that law firms are aware of the growing risk of cyber intrusions and are implementing steps to reduce this risk.

At Marsh we have observed many rising threats, some include criminals targeting data by stealing or disclosing personally identifiable or financial information, modifying or corrupting data or blocking legitimate users' access to systems. However, it's not only these external threats from hackers that organisations need to be aware of; many perils are actually internal.

For instance, a culture of trust within a workforce, traditionally thought to be a benefit, now creates a threat. Many high quality phishing emails appearing to be legitimate correspondence from banks, the Australian Taxation Office (ATO) and other trusted sources may inadvertently be opened by employees, exposing the business to hackers. Therefore employees must be trained to spot and delete such communication to thwart the intended intrusion.

Some of the other internal risks are known as 'man in the middle' intrusions. These are where attackers electronically eavesdrop undetected on email conversations and alter communication between parties who believe they are writing to each other in confidence.

It was anticipated that mandatory data breach notification laws would be in place by the end of 2015. While this did not happen, the recommendation for data-breach notifications by the Joint Parliamentary Committee on Intelligence and Security remains. As such it is expected that data breach notification legislation will be introduced into Parliament in 2016.

Additionally, the advent of the Internet of Things is introducing new cyber perils. Worryingly, it's likely that many businesses are overlooking vulnerabilities in devices such as printers, video conferencing equipment, mobile phones and thermostats.

While many firms now understand that potential cyber threats expose them to financial regulatory and reputation repercussions, many don't appreciate some of the other, more serious consequences of a cyber intrusion. For instance, ratings agency, Standard & Poor's, has noted that a major cyber-attack on a financial institution could put its credit rating at risk.

It is important for law firms to explore ways to protect their electronic ramparts in light of the growing risks around cyber. As part of this, it's important not to overlook third party vendors or customers when it comes to cyber security, with the massive Target breach in December 2013, attributed to a vulnerability in an air-conditioning contractor's system. It's also essential to seek assurance from third party vendors or customers on their level of cyber security resilience and ask for a Cyber Insurance Certificate of Currency from them. You may also be asked to provide documentary evidence that your firm purchases cyber insurance. While we are still developing a detailed understanding of the full spectrum of threats to Australian networks, a number of trends will manifest globally in the near future, as outlined in the Australian Cyber Security Centre Threat Report 2015[1]. Importantly, the number of cyber criminals and their sophistication is likely to increase, making detection and response more difficult.

[1] Australian Cyber Security Centre, 'Threat Report: 2015', <https://www.acsc.gov.au/publications/ACSC_Threat_Report_2015.pdf>.

We also expect incidences of spear phishing will continue to grow and the use of ransomware will continue to be prominent.

What this shows is that cyber intrusions are a growing and increasingly complex peril businesses must face. It's essential for every law firm to recognise this growing problem, and put robust mitigation strategies in place to reduce the risk of cyber threat undermining or even destroying their businesses.

Cyber security and privacy risk is heightened for any organisation which collects and stores personal data along with confidential client information.

If you wish to discuss Cyber Insurance or conduct an analysis of the potential exposure for this emerging risk, please contact your Marsh representative.

Potential main cost and loss items

Legal liability

Defence and settlement costs connected to:

- Consumer class actions
- Consumer protection actions
- Contractual liability to third parties

Regulatory

Defence costs and financial penalties imposed by:

- The Australia Information Commissioner's Office
- An overseas regulator where applicable
- An industry regulator

Damage loss items

Cost to replace or repair:

- Data that has been corrupted or destroyed
- Software that has been corrupted or destroyed

First party

Incident response costs incurred in connections with:

- Forensic IT investigation and remediation costs
- Legal advisory costs
- Notifying affected individuals
- Establishing a customer contact centre
- Providing credit monitoring service to affected individuals
- Engaging a public relations/crisis management consultancy

Network interruption loss items

An interruption to your computer system results in:

- Loss of revenue
- Additions cost of working

Key insurance coverages

Network Security liability

Liability to a third party as a result of:

- Destruction of a third party's electronic data
- Your network's participation in denial-of-service attacks
- Transmission of viruses to third party computers and systems

Data privacy liability

Liability to a third party as a result of:

- Unauthorised disclosure of personally identifiable information
- Unauthorised disclosure of third party confidential information in your care, custody or control
- Defence against regulatory actions

Crisis management

Expenses to respond to a personal data breach event including:

- Computer forensic costs
- Notification costs including call centre costs
- Credit monitoring and identify theft protection costs
- Public relations and crisis management consultancy costs

Cyber extortion

A genuine threat to the computer network or data leads to payment of:

- Expert fees to negotiate with the hacker
- A ransom

Cyber Attacks Prove Costly

Network business interruption

The interruption or suspension of computer systems resulting in:

- Your potential loss of income
- Extra expenses incurred to mitigate an income loss

Resulting from:

- A network security breach
- A network failure

Data asset protection

The corruption, destruction of data or computer| programs incurs:

- Replacement, restoration or rectification costs
- Costs to determine that data or programs cannot be replaced

Multimedia liability

Liability arising from online content, stemming from:

- Infringement of intellectual property rights
- Invasion of privacy
- Defamation
- Negligent publication or misrepresentation

Summary of the Society's recent advocacy activities

- Letter to Chris Cox – Delay in Returns
- Letter to Police Commissioner – Infectious Diseases
- Letter to Health Department – Guardianship of Adults Bill
- Meeting with Corrections
- Attended Criminal Justice Forum
- Attended CDU School of Law Prize Night
- Attended legal services forum
- Hosted Law Week
- Attended making justice work forum
- Attended NT Justice Review meeting