Mitigating and Managing Cyber-Risk: Ten Issues to Consider

Boards of Directors are charged with the responsibility of managing and mitigating risk exposure.

In a recent study conducted by Experian Data Breach Resolution and the Ponemon Institute, it was revealed that companies rank cyber security risks as greater than natural disasters and other major business risks.

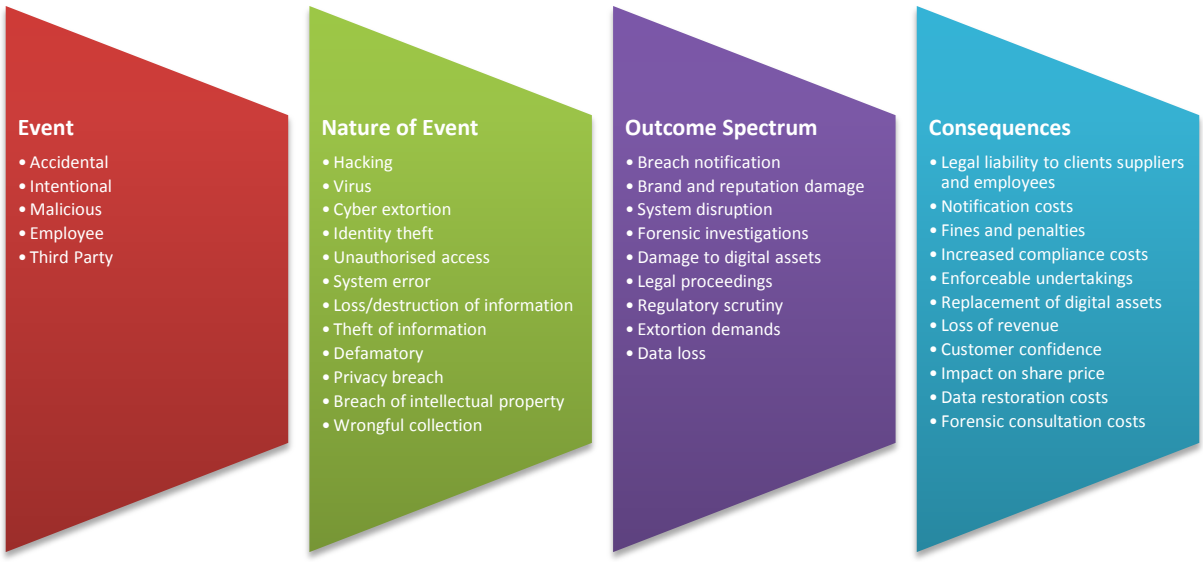
While this rapidly evolving area has its own unique challenges, boards need to consider whether they have discharged their duties by identifying the organisation's cyber risk exposure and exploring risk transfer and mitigation strategies. The following factors highlight key areas that Boards should consider in identifying and mitigating these risks:

1. Understand the risks

Consider your client base. Now consider how your organisation would cope if over three quarters of your clients stopped doing business with you. Should your organisation fall victim to a cyber-attack, this is a very real possibility. Damage to brand and reputation can be irreparable with a recent Unisys survey showing 85 per cent of Australians would stop dealing with an organisation if their data was breached.

A cyber-attack or data breach can take many forms, from deliberate attacks to technology issues and negligence. The perpetrators of these attacks can range from organised crime groups to competitors, from disgruntled employees to politically motivated groups.

Australia's increasing reliance on computing systems, networks and cloud technology has left many organisations open to new exposures. Most risk managers and key decision makers recognise that data breaches represent a major threat to their organisations. However, developing a better understanding of their Network Security & Privacy risk exposures is an important step, in order to align the exposures to appropriate risk transfer options.



2. Data breaches and your share price

The amount of personal and confidential information maintained electronically by public companies increases every day. As a consequence, the likelihood that a material data breach will adversely impact an organisation's reputation, bottom line, and share price is a real exposure. In response to this ever-increasing risk, in the US the Securities and Exchange Commission is requiring greater disclosure related to data security, and it would not be surprising if Australia follows suit in the near future.

3. Prepared for the new Privacy Laws?

Compounding the possible financial, brand and reputational damage which can befall an organisation after a data breach, new Australian Privacy Laws will come into effect in March 2014.

All entities that handle personal information, including employee and customer information will be affected by the amended laws.

The major impacts include greater accountability of the entities and significant penalties for organisations and directors. Additionally, there are Privacy Commissioner powers to conduct audits and issue enforceable undertakings; and all Australian entities must ensure overseas counterparts comply with the Australian Privacy Laws.

4. ASX disclosure obligations create a number of challenges

As well as the proposed provisions under the Privacy Act, it could be argued that continuous disclosure obligations affecting listed companies apply to data breaches. Pursuant to the Corporations Act and the ASX Listing Rules, listed companies must disclose information that is not generally available and that might reasonably be expected to have a material effect on the share price of the entity.

5. Mandatory notification is on the horizon

The next phase in regulating privacy and protecting personal information will be the introduction of mandatory notification of data breaches. If approved by the Senate, the bill will introduce mandatory data breach reporting obligations for entities regulated by the Privacy Act 1998 (Cth) when a "serious data breach" occurs.

Where a breach reporting obligation arises, the entity must prepare a disclosure notice providing the nature of the data breach, the information at risk and steps that an individual can take to mitigate the effects of the breach of their information.

Failure to notify the Commissioner or affected individuals when required to do so can trigger enforcement rights under the Privacy Act, including penalties such as a) compensation to affected individuals, and b) civil penalties of up to A$340,000 for individuals and A$1.7million for corporations.

6. Australian Prudential Regulation Authority expects that if you are a regulated institution you have implemented processes that ensure compliance with data risk management requirements.

APRA has released a Prudential Practice Guide PPG 235 Managing Data Risk (PPG 235).

The management of data risk is important for a broad range of business outcomes, including meeting financial and other obligations to beneficiaries. Hence, Boards and senior management of an APRA regulated institution need to have an understanding of the risks associated with the management of data, including its collection, retention and use, and of the practices that would safeguard data quality across the data life-cycle.

7. Hackers are already two steps ahead of you

Some organisations mistakenly believe that because they have a firewall, a quality IT team, or antivirus protection, they will not be targeted. Major organisations around the globe have all been victims of cyber-crime in recent years, experiencing significant data and security breaches which have impacted millions of customers.

Bank accounts, medical records and confidential business information are among the data which has been breached, exposing these companies to litigation and liability, significant financial recovery costs, loss of future business and reputational damage.

8. Cyber threats can pose merger risks

Boards need to closely consider the risks should inadequate cyber security and other data protection measures not be taken in the context of corporate M&A activity. If a company acquires a target with a malware-infested IT system, there is a potential for a wide range of liabilities. Cyber security and other data protection methods should be added to the list of criteria a board should consider when evaluating a potential acquisition and acquisition documents should consider and provide for appropriate representations, warranties, and indemnities related to cyber risks.

9. Have you considered the legal and risk governance issues around data hosting and jurisdiction?

Australian entities are outsourcing software applications, technology platforms and/or infrastructures to third-party hosts which raises a number of new legal issues. Businesses must balance the flexibility and potential cost savings of cloud computing with the risks inherent in storing data, infrastructure and platforms offsite, beyond the company's direct control, and possibly even in a foreign country with different laws.

Obtain detailed information from cloud providers concerning their security programs, including who can access the data, where it will be located (country of jurisdiction, for the evaluation of legal obligations), technical aspects of the infrastructure, and what steps the provider has taken to protect the integrity and security of the data.

10. Insurance coverage is available through tailored cyber risk policies

Ramifications of a breach can be very costly to a company's business, both fiscally and for brand and reputation. In addition to notification costs (PR, call centre costs and credit monitoring services), investigations response and compliance, and compensation to affected individuals, there are additional concerns such as engagement of forensic experts, and defence of claims for misleading conduct, negligence, breach of contract, breach of confidence and interference of privacy.

Most of these exposures are not covered under conventional insurance. It is, therefore, important for firms to thoroughly evaluate existing exposures and insurance coverage and consider purchasing tailored Network Security & Privacy insurance to cover identified gaps.

Eric Lowenstein
Aon Risk Solutions
t: +61 2 9253 7445
m: +61 402 103 633
e: eric.lowenstein@aon.com