Managing cyber risk – proactive planning and risk transfer through cyber insurance

As custodians of an ever-growing pool of valuable data assets, organisations need to put in place proactive measures to manage a potential cyber event, including a data breach. As is often said, it is not a matter of 'if' a data breach will happen but 'when' and how severe the financial and reputational impacts will be for the organisation.

Cyber Risk Management Framework

Being able to respond effectively to a cyber event or incident requires having a carefully developed internal privacy and data risk management framework.

Such framework ought to include (among other things):

- a thorough understanding of an organisation's own cyber risk perimeter, including what data assets exist and what data flows occur within and outside the organisation;
- robust internal and external data privacy policies, systems and procedures;
- a data breach response plan and associated toolkit;
- a requirement to undertake privacy impact assessments for new projects or initiatives involving the handling of personal information; and
- a review of key supplier agreements to ensure that there are sufficient protocols in place addressing data breach containment, remediation and notification issues.

.

Cyber Insurance

Organisations should also consider whether they require cyber insurance as part of their broader systems and polices to manage cyber risk. Cyber Insurance can be a useful financial backstop, providing funds for the cost of implementing those measures as well as providing cover for other costs and liabilities.

Cyber risk can have immediate consequences and whilst going through the process of having a claim accepted and paid will often not solve the immediate or broader problem, it can offer several benefits.

What can Cyber Insurance offer?

Generally, dedicated cyber insurance policies provide two areas of cover:

- First party losses, meaning losses incurred by the insured party itself. This can include:
    - Cost of replacing and restoring lost or damaged data following a cyber attack;
    - Loss of net income following a cyber event (business interruption);
    - Cost of PR and legal support in the event of a data breach;

    - Cyber extortion costs.

- Third party losses, meaning the liability of the insured party to third parties for a cyber incident. This can include:

    - Liability to third parties for failure of network security practices which result in a loss to a customer or client;

    - Compensation to individuals affected by a data breach.

Insurable losses can also include liability to pay fines and penalties which are generally insurable where there is no element of deliberate breach or intentional actions.

Buying a cyber insurance policy

The nature of cyber cover can be quite technical and some policies contain a broad operative provision while others provide cover for specifically defined risks. The needs of the individual business will determine which type of policy is most appropriate. Because of the unpredictable and evolving nature of cyber risks, it may be beneficial to opt for cover with a broadly drafted operative provision.

These points can be illustrated through a simple example. Assume that due to a cyber attack (for example, social engineering) human error leads to a loss of substantial funds to the attacker. In that case, there may not be any damage to or compromise of the system or network of the insured business, but it has suffered a loss. However, some cyber insurance policies may only provide cover if there has been a system compromise or damage, so something to consider.

Cyber insurance policies may also exclude certain losses such as those caused by portable devices, loss of data entrusted to a third party (such as a cloud provider), and regulatory investigation costs and fines. Depending upon the risk profile of the business, cover may be required for these risks and could be purchased through an appropriate insurer.

In short, buyers must have a clear understanding of the organisational cyber risk before settling on a particular insurer and policy wording.

How we can support you

McCullough Robertson and our insurance advisory service, Allegiant IRS can provide comprehensive Cyber Insurance policy checks and analysis to ensure your cover is adequate and to assist you to navigate through the complex Cyber Insurance market. McCullough Robertson can also assist you with the design and implementation of a comprehensive cyber risk management plan.

For further information on any of the issues raised in this alert please contact:

- Stephen White on +61 7 3233 8785

- Brad Russell on +61 7 3233 8786

- Matthew McMillan on +61 2 8241 5644

- Adam Battista on + 61 7 3102 5666