Cyber Risk

As the benefits of new technology increase, so do the risks. Cyber Risk is the downside to the remarkable gains made in recent times by the adoption of new technology.

Most cyber risk is related to software and data, but there are recorded incidences where it has affected the "real" world and caused physical damage. The most publicised example of this is the Stuxnet virus, which affected the Iranian nuclear program. However, there have been others where safety systems have been overridden leading to overheating and fires.

The more common risk is closer to home and nowhere near as noteworthy – a hacker stealing data or a virus locking a computer accompanied by a ransom demand. There are countless real examples of these things happening and they are gaining more and more attention in the media.

Cyber risk is a business risk, not an IT risk.

Key Risks

The risks can be broadly categorised into First Party Risks and Third Party Risks. While both will impact on your business and could ultimately be your responsibility, the difference lies in who is initially affected and whether you will pay the costs up front or have to respond to a claim against you by a third party.

First Party

This includes the actual downtime where your business cannot trade due to disruption to your system, as well as the ongoing losses caused by damage to your reputation. Points worth discussing:

- How reliant are you on your system – could you trade if your system was unavailable for an extended period?
- How reliant are others on your system – if your customers rely on your system for their business will they continue to pay the monthly costs for a system they can't use?
- What plan do you have in place following a cyber event, for example notifying affecting parties, mitigation of the damage (redundant systems, data backup, restoration costs) and steps to prevent a recurrence?

Third Party

These are claims made against you by affected third parties which could include your customers or suppliers. Anyone who relies on your system or you hold data about could potentially be affected.

- Privacy breach – just because data appears innocuous, it doesn't mean someone won't want to steal your data and the affected parties won't want compensation.
- How many parties depend on your business to operate as these could all lodge a claim against you for their losses caused by the disruption
- Commercially sensitive information – do you hold any third party information which could be considered commercially sensitive and therefore be a target for hackers?

Risk Management

The risks need to be reviewed regularly and ideally a board member should be responsible for cyber risk. Most businesses have some form of network security in place and employee policies around passwords and access to information. While these are a good start there needs to be more thought put into proactive steps such as retaining expertise to deal with cyber threats (either in-house or outsourced), penetration testing by cyber security specialists and regular reporting on activity.

Risk Factors

While all businesses have a degree of cyber risk the magnitude will vary depending on a number of factors. The amount of third party data held isn't the only risk factor, the type of data held will impact as well. Consider a hospital holding medical records compared to a patent attorney holding commercially sensitive information which supports patent applications.

The stage of your business also has an impact. Is your business developing new products, which aren't yet in the market or is there a highly sensitive sale and purchase taking place?

How connected is your business to the world, and what systems are in place if that connection is lost? Can systems work offline or will the business shut down until they are restored?

What effect does regulation have on your business? This is particularly relevant if you are in multiple jurisdictions as you may have to comply with different rules in each jurisdiction.

How good is the security used by your customers and suppliers?

Insurance Solutions

All businesses should have IT security in place which is appropriate given their risk profile. A major benefit of a Cyber insurance policy is the 24/7 response as that can minimise the damage caused.

Cyber Insurance

This policy will cover all the risks outlined above. It has been specifically designed for these risks, and more importantly provides the emergency response capability so the company can react quickly.

Professional Indemnity / Technology Liability

These policies will respond to most of the third party losses and may have limited cover for the first party losses. None have a Cyber Exclusion yet, but there are indications that these may appear. Most have a War & Terrorism exclusion which will exclude some claims depending on the facts of the case.

Directors & Officers (D&O) Liability
This policy may respond to some of the third party claims and may have some cover for first party (reputation, crisis response) costs. There is currently no cyber exclusion in D&O policies but the War & Terrorism exclusion may apply. Note that some D&O policies have a "Failure to Maintain Insurance Exclusion" which may also apply as Cyber insurance becomes more common.

Key Points

There are some key points to remember when assessing and dealing with Cyber Risk in your business

- Cyber risk is a business risk, not an IT issue
- There needs to someone senior in the business who is responsible for staying on top of the risk
- It is important to retain the expertise, whether in-house or outsourced, to properly address the risk
- Identifying the risks is only half the battle, you must then decide what to mitigate, transfer or accept

We are always available to work with you to identify and assess the risks in your business.

To discuss further or for any queries, please contact:
Natasha Tennent
Phone **021 666 428**
Email **Natasha.tennent@apexinsurance.co.nz**

Claims examples:

- **Recently a sports club had their server hacked and their data was held to ransom. This was certainly not what one would regard as a "target market" for hackers however unless a ransom payment was made the data would be destroyed and the costs to recreate from scratch would have been substantial. The club had cyber cover and the ransom was paid under the extortion extension built into the policy.**
- **A government department in New Zealand sent out a large number of clients' personal information by email to the wrong address. This led to that information being publicized and those affected were able to sue for damages alleging a breach of privacy. The damages and defence costs would have been covered under a cyber policy.**
- **A very well-known case in the not too distant past involved hackers obtaining access to an adult dating site. The personal information was released on the web and this led to massive damages claims from those whose information had been released alleging inadequate security of the website - most of these claims were for humiliation and distress. The website had cyber cover which provided indemnity for both defence costs and damages which were massive.**