INSURANCE - CANADA

Developments in cyber-risk insurance coverage

October 27 2015 | Contributed by McMillan LLP

Coverage for cyber risks
Cyber-liability policies
Comment

AUTHOR

Carol Lyons

Coverage for cyber risks

At one time, organisations may have assumed that losses due to cyber risks were covered under their commercial general liability policies. However, today broad policy exclusions with respect to a host of data-related losses are commonplace. Except for 'Y2K' data exclusions which arose at the turn of the century amid fears that electronic devices would fail to distinguish between century years, exclusions with respect to data loss and liability for data loss were generally not contemplated. The typical broad form exclusions found in modern commercial general liability policies have developed partly because of the relative newness of the cyber-risk phenomenon – making it difficult for insurers to quantify the risk and therefore necessary to exclude them – and partly because of the recent proliferation of high-profile and costly incidences. Unlike what turned out to be unfounded fears of a cataclysmic Y2K event, the likelihood of experiencing cyber-attacks, privacy breaches or data loss incidents are now said to be a matter of when and not if. As a result, if an organisation wishes to obtain comprehensive insurance coverage for cyber-related risks, the insurance – to the extent available – must be thoughtfully and deliberately sought.

Cyber-liability policies

Fortunately, due in part to general overcapacity in the global insurance marketplace, insurers and reinsurers are looking to new products as avenues to increase business, and some are willing to take on cyber risk, at least to a limited extent. Specialised cyber-risk insurance policies are now available, and in some instances may specifically be designed to respond to a number of losses due to a cyber-attack or privacy or data security breach. In fact, many are calling cyber-risk coverage one of the fastest-growing insurance products today. However, the scope and limits of coverage will necessarily be subject to the underwriter's overall risk appetite and ability to quantify the nature and extent of the risks that it is assuming. Therefore, coverage for some types of risk may simply not be available – or the limits offered may be inadequate to cover the organisation's potential risk exposure.

Although policy coverages are rapidly evolving and adapting, a cyber-liability insurance policy may cover:

- loss of income due to the incident (eg, cyber-attack or privacy or data security breach);
- loss of profits that the organisation would have earned had the incident not occurred;
- in the case of an interruption in business, recoupment of expenses that must be paid even though the business is not operating;
- costs for notification to customers and/or others for privacy and data security breaches, certain associated legal costs and, where applicable, costs related to monitoring the credit of affected customers and/or others for a period of time following the incident;
- costs incurred to avoid claims that, if made, would be covered under the policy;
- where legally permitted, costs of regulatory actions and investigations;
- fines and penalties;
- legal liability to third parties arising from hacking attacks or malware or due to a privacy or data security breach; and

- cyber-extortion, such as ransomware (a type of malware that prevents an organisation from accessing its own computer system until a ransom is paid), including payment of a ransom.

On the other hand, the policy will contain a number of exclusions, such as the following:

- bodily injury and property damage;
- undisclosed data risk (ie, with respect to any data that is materially different);
- IP rights infringement;
- intentional acts by directors and senior officers (eg, including chief compliance officers, data protection officers or general counsel);
- securities claims;
- trading losses; and
- unauthorised trading.

Some insurers also offer a suite of cyber-risk related services, including through third-party vendors (eg, breach consultation, forensic analysis, notification services, call centre services, credit and identity theft monitoring, fraud consultation and credit and identity restoration services).

Comment

Insurance specific to cyber risk remains a new and relatively uncharted territory. The fact that cyber-security laws are still developing and changing also makes it difficult for risk managers and insurers to measure the parameters of the risk environment. Some stakeholders are considering how a collaborative cyber-incident data repository could help to meet the information requirements of insurers to assist them in providing more insurance at lower rates. In any event, it appears that organisations are apprehending the seriousness of the risk and that the insurance industry is stepping up by providing thought leadership, tangible services and insurance protection. Since many insurers are still assessing their risk appetite for cyber insurance and may not be willing to offer the scope of coverage that some organisations may require or desire, brokers are likely to play a key role in helping to design programmes for their high-risk clients – for example, involving a number of insurers and layers of coverage.

For further information on this topic please contact Carol Lyons at McMillan LLP by telephone (+1 416 865 7000) or email (carol.lyons@mcmillan.ca). The McMillan LLP website can be accessed at www.mcmillan.ca.
