MARSH

October 2016

# CLIENT BRIEFING

## *CYBER INSURANCE: BETTER INFORMATION WILL GIVE YOU BETTER COVERAGE*

*When it comes to cyber risk, it's said that organisations fall into two categories. Those who have been hacked, and those who will be. Cyber loss, however, doesn't come just from some mysterious hacker, but can equally occur because of system failures and related events.*

While the awareness around cyber and cyber risk management is growing at a rapid pace, so is the understanding that cyber insurance is available to fund losses arising from cyber risks.

As the nature and severity of cyber attacks themselves keep escalating, the options for coverage are evolving, though not necessarily at the same rate. Buying an off-the-shelf cyber policy may satisfy the 'tick box' for coverage, but may still leave your business exposed in a number of ways:

- You might not fully understand how your insurance policy will respond in the event of a loss from a cyber attack, or what the limitations and exclusions are. After the fact is too late.
- Cyber coverage chosen on price alone or based on a benchmark for a specific industry, company size or turnover may miss some unique complexity or feature of your business.
- With the cyber insurance market still evolving, proposal forms from insurers are being frequently updated, taking into account things such as the use of Cloud services and bring-your-own-device (BYOD) practices. Proposal forms can range from the complicated to the overly simple where key information is missed.
- The risk for large organisations that operate globally, or have subsidiary companies or complicated reporting structures, is that cyber risks may not be adequately captured on a standard proposal form. Equally, the questions asked in the proposal forms may not be detailed enough to fairly rate the risk.

To be confident in buying cyber insurance, you need to clearly understand the real potential for exposure within your business. That calls for a structured and risk-based approach so that insurers can underwrite those risks on an informed and competitive basis.

## THE FUNDAMENTALS OF ASSESSING YOUR CYBER RISK INCLUDE:

1. Consideration of your internal and external business environment. What are your key lines of business, your core activities and what key business assets and critical information systems underpin your business, and would create havoc if disrupted?
2. Having a clear understanding of what systems, practices and controls are in place for monitoring, reporting and response should a cyber attack or data loss happen. For example, what level of confidence do you have that your customer data or your intellectual property is secure? And what level of confidence do you have in external vendors who have access or manage your systems or data?
3. A clear outline of your risk tolerance (or appetite) in relation to the various risks that your business could face from a cyber attack or data loss. This could be in terms of financial, reputational, business interruption, regulatory compliance, service delivery and competitive advantage. There will be differing impacts under each category but they need to be assessed and rated from catastrophic through to somewhat inconvenient.

## ESTABLISH A RISK ASSESSMENT TEAM

A robust risk assessment process will need to include staff from across the business. For each potential cyber loss exposure, the team needs to identify where the threats could come from and what this could mean for key business assets and/or critical information systems.

For example, failure of key IT infrastructure could be due to age or the failure of temperature monitoring/control system. For a system breach, the scenario may come from a virus being introduced by a staff member connecting remotely via a mobile phone, or equally by a disgruntled employee deliberately importing a virus.

For each identified scenario, the team needs to review the current controls and practices in place to manage each threat source and risk driver and rate them. This helps in pinpointing where potential gaps may lie. For all identified threats or risk events, it is recommended you assess the likelihood or relevance of the event both qualitatively and where possible, quantitatively to better prioritise those risks.

## OPTIONS FOR COVERING CYBER LOSS

For each threat source or identified risk driver, you can now confirm what options you have in place should a loss occur. This will include reviewing the current insurance policies you have in place to understand coverage and exclusions, in terms of both first and third party response.

For any identified gaps, a tailored cyber insurance policy may make the difference between a catastrophic loss and a time-consuming inconvenience. No matter what the nature of the loss, you can be certain that it will cause disruption to some degree – but it's your degree of preparedness that will decide how you recover.

It should be noted that not all key risk events identified may be insurable. Some, such as certain contractual failures, and the failure of aged hardware may not be fully insurable, if at all. In this case, you could review any vulnerabilities for such events and develop strategies and initiatives to improve systems and controls.

## BETTER INFORMATION. BETTER COVERAGE

In going through the previous stages, you should have amassed a rich source of information for your insurance broker or insurer when negotiating cyber insurance policy cover, limits, pricing and terms.

This allows the risk to be underwritten on an informed basis, and allows your insurance broker to negotiate best available cyber insurance policy cover, limits, pricing and terms.

Marsh has developed considerable experience in the cyber risk area, both in risk consulting and developing tailored cyber insurance coverage for its clients.

*Chris Beh is a Principal for Marsh Risk Consulting in New Zealand and works with clients across all sectors and industries in cyber, project, enterprise, business continuity, liability and property risk management.*

## FOR FURTHER INFORMATION

For more information on this topic or advice on your risk and insurnace programme please call us on **0800 627 744**

marsh.co.nz

**Disclaimer:** Statements concerning legal matters should be understood to be general observations based solely on our experience as insurance brokers and risk consultants and should not be relied upon as legal advice, which we are not authorised to provide. All such matters should be reviewed with your own qualified legal advisors.

The information contained in this publication is based on sources we believe reliable, but we do not guarantee its accuracy. This information provides only a general overview of the subjects covered. NZM_16-2971

Copyright 2016 Marsh Ltd. All rights reserved.