MARSH

Financial and Professional Liability Practice (FINPRO)

NETWORK & SECURITY LIABILITY PROTECTION

CYBER IS AN ENTERPRISE-WIDE CONCERN

In today's marketplace, cybersecurity is no longer just an IT-department issue. It is an enterprise risk issue that must be considered and addressed by the many stakeholders throughout the organization. In Asia, organizations are facing increasingly complex network and security risks. An ever-evolving environment of threats, regulatory reforms, and potential litigation has broadened the spectrum of risk and deepened the potential loss that organizations face in their daily operations.

KEY CYBER RISKS

Operational Disruption – When criminals attack an organization's core systems, whether it be at the point of sale for a retailer, the billing system for an insurance company, the information processing system at a financial institution, or the automated machine line at a manufacturer, it can lead to disruption of daily operations and business processes, supply chain and vendor communication issues, as well as loss of revenues and trust.

Employee Exposures – If an organization only focuses on external cyber risks, it will miss a good portion of its exposure. A misplaced laptop or an unencrypted email sent by a good employee can reveal a large amount of sensitive data. The damage done by a rogue, disgruntled employee can be even greater.

Lawsuits and Reputational Harm – Asia is becoming a growth area for litigations; a thorough breach response plan can help retain trust in an organization and mitigate the damage that such litigations can do to its brand reputation and bottom line.

Regulatory Implications – A number of regulators across Asia are starting to look at all aspects of cyber risk, from how an organization prepares for to how it responds to a data breach. No board can afford to be caught without a plan for a cyber breach or attack. The potential for fines and reputational damage has increased the responsibility on senior executives to put the right governance structure in place before a cyber event happens.

Who it's for

- All organizations that collect data or confidential information
- All organizations that utilize a computer network in the operation of their business

What you get

- Policies that can be customized to include any or all of the following coverages
  - Network & Security Liability
  - Information Asset Coverage
  - Business Interruption Coverage
  - Cyber Crime Coverage
  - Cyber-Extortion Coverage
  - Crisis Management Coverage

GAPS IN TRADITIONAL INSURANCE

The evolution of privacy and computer security risks has left many of the traditional forms of insurance unable to adequately respond to these exposures.

General Liability policies often do not provide coverage for damage to electronic data, criminal or intentional acts of insureds or its employees, or pre-claim expenses (i.e., notification costs and regulatory defense).

Property policies typically limit coverage to damage to / loss of use of tangible property resulting from a physical peril and damage to tangible property at specific locations. Some insurers have expressly excluded coverage for any damage to data.

Fidelity policies limit coverage to direct loss from employee theft of money, securities, or other tangible property. Even with a computer crime extension, coverage is limited to the cost of recollecting or restoring the damaged or corrupted data.

Professional Indemnity policies often limit coverage to claims arising from negligence in performing specifically-defined services and exclude coverage for criminal acts of insureds or its employees and first party loss expenses associated with a privacy breach or cyber attack (i.e. business interruption, crisis management, and cyber extortion).

NETWORK & SECURITY LIABILITY INSURANCE

Network and security liability insurance can fill the gaps in traditional insurance, as well as provide direct loss and liability protection for risks created by the use of technology and data in an organization's day-to-day operations. These insurance policies are flexible, allowing a customized programme to provide protection for the following key exposures.

NETWORK & SECURITY LIABILITY

- Protection for claims arising from an actual or alleged failure of computer security to prevent or mitigate a computer attack.
- Protection for claims arising from a disclosure or mishandling of confidential information.
- Coverage applies whether the information is electronic or hard copy.
- Coverage includes protection for the entity for the intentional acts of rogue employees.
- Vicarious liability for a privacy breach occasioned by third party vendors or business process outsourcing firms.
- Coverage for the costs associated with complying with privacy breach notification statutes, including legal and forensic expenses.
- Coverage for defense of regulatory actions – including affirmative coverage for assessed fines and penalties.

MARSH FINPRO'S PRACTICE

Marsh is a leading risk management advisor and thought leader in the network and security risk space. From the creation of the first "cyber" policy forms to helping insurers develop the new privacy coverage, Marsh continues to move and shape the market on behalf of our clients. As part of our service offerings, Marsh is able to assist our clients in evaluating their network and security risks through coverage gap analyses and risk assessments.

INFORMATION ASSET COVERAGE

- Reimbursement for actual and necessary costs incurred to restore or recollect an organization's information and computer system assets that were damaged or corrupted by a computer attack.

BUSINESS INTERRUPTION COVERAGE

- Reimbursement for lost revenue – including extra expense resulting from a failure of technology, computer system outage, or computer attack.

CYBER CRIME COVERAGE

- Difference-In-Conditions coverage fills the gap for "theft of data/information" in crime policies as well as indemnification for theft of information or computer system assets.
- Coverage can sit excess of a computer crime policy.

CYBER-EXTORTION COVERAGE

- Payment of ransom or investigative expenses associated with a threat to release, divulge, disseminate, destroy, steal, or use of confidential information; introduction of malicious code into the computer system; corruption, damage, or destruction of the computer system; or restriction of access to the computer system.

CRISIS MANAGEMENT COVERAGE

- A fund for public relations and crisis management in connection with any crisis event relating to a failure of computer security or breach of privacy resulting in a covered loss or claim under the policy.

To learn more about our experience with network and security protection or to discuss your organization's unique risks, please contact:

DOUGLAS URE
Managing Director
+65 6922 8233
douglas.ure@marsh.com

ARATI VARMA
Senior Vice President
+65 6922 8028
arati.varma@marsh.com

NAUREEN RASUL
Senior Vice President
+852 2301 7206
naureen.z.rasul@marsh.com

KEGAN CHAN
Vice President
+852 2301 7205
kegan.kc.chan@marsh.com

PH 17-3264_ASM