Cyber risk in Asia: the dawn of a new age


CLYDE&CO

The insurance industry in Asia is recognising the increasing importance of protecting companies against risks connected with cyber attacks and offering risk-management solutions.

Cyber risk often falls outside the realms of traditional insurance policies. Many professional indemnity or financial lines policies can (often unintentionally) provide cover for certain cyber-risk exposures but this cover is often limited and subject to exclusions.

For example, gaps in coverage between traditional liability policies and cyber-risk policies often arise in relation to geographical limitations, investigation and enforcement costs, coverage of the costs of repairing the "damage" suffered, extortion payments, and third-party loss.

A recent report published by Marsh, "Cyber Risk in Asia", says in 2010, 75% of Asia-Pacific businesses experienced cyber attacks, costing as much as $763,000 annually. Reports of data or network sabotage, virus and Trojan infections, computer fraud, laptop theft and network scanning are said to be increasing. Around 42% of mailboxes targeted for attack are high-level executives, senior managers and people in research and development.

Small businesses are becoming more desirable targets than larger organisations, because of generally weaker security. However, cyber attacks can have wider implications, affecting a whole industry. Recently, hackers targeted the Hong Kong Stock Exchange. The partially closed trading session affected stocks that made up 18% of the Hang Seng index's weight.

The wave of cyber attacks has caused governments in Asia to increase regulation and enforcement of personal data privacy. There is an appreciation of the need to bring data protection standards in line with those set by the Organisation for Economic Co-Operation and Development. This is essential for protecting personal data in the region, but also important for the promotion of international trade and ensuring consistency in regulation.

By way of overview of the regimes in the region:

- Hong Kong has one of the more robust and active regimes in Asia, largely governed by the recently amended Personal Data (Amendment) Ordinance (expected to take effect from October 1, 2012).
- In Singapore, there are many acts that together contain more than 150 privacy and data protection provisions. A draft Personal Data Protection Bill, which had its first reading last month, includes a number of developments including establishment of a Personal Data Protection Commission and the broadening of the definition of personal data to include electronic, as well as non-electronic, data.
- Recent change has taken place in the Philippines, with the passing of the Data Privacy Act of 2011 which took effect last month. This coincides with the Cybercrime Prevention Act of 2012.
- Malaysia's Personal Data Protection Act of 2010 has not yet been brought into force, primarily because the government has not appointed a Personal Data Protection Commissioner as required by the Act. The government has now indicated it is considering proceeding without a Commissioner.

The range of regimes across Asia creates a variety of exposures, from fines and penalties to imprisonment; directors and officers may face personal liabilities arising from data breach. It is therefore critical for organisations to be mindful of incoming laws and take pre-emptive action to put in place internal data protection policies that are consistent with the proposed legislation, as well as ensuring appropriate cover is in place to meet potential exposures traditional policies do not meet. ■

Patrick Perry is a partner and Melissa Russell is a senior associate at Clyde & Co