CLYDE&CO

Update

Asian Cyber Wars; The New Frontier

Cyber Risk: The Dawn of a New Age

The idea of a wave of attackers, getting ready to commence their assault against heavily fortified defences, sounds like a Hollywood movie, or an on-line role playing game. However, in a situation where fantasy is becoming closer to reality, this is exactly what is happening on a daily basis against corporations across the world. The "treasure" is personal data, which can be sold on to third parties, or used to access personal accounts. The loss of this data, can not only cost companies millions in terms of direct compensation, it can lead to severe fines and penalties. Countries across Asia, keen to be seen to be taking steps to address cyber-attacks are rolling out increasingly more onerous legislation. Companies, and their Directors, need to be aware of these new exposures, and consider the new insurance products that are available to meet them.

In August of this year, account details for millions of game players were stolen in a hack attack on 'Blizzard', the maker of various online role-playing games. Players in Southeast Asia as well as the US and Canada were advised to change their login details and security questions. The risk was highlighted that if (as commonly occurs), users adopt similar security procedures and questions across all of their personal accounts, a wholesale change of users' security inputs may be required.

The 'Blizzard' attack followed on from the high profile hacking of the Sony PlayStation Network in April 2011. The associated costs amounted to approximately US$173 million which took into account the cost of increased customer support services, notification costs, legal fees and a drop off in sales due to a loss in consumer confidence.

However, it isn't just the gaming industry that is under attack, advances in information technology have revolutionised the ways businesses attract, retain and interact with customers. Heavy reliance on information technology is making businesses ever increasingly exposed to data breaches and cyber attacks. According to global research by data security software maker Symantec, 5.5 billion cyber attacks were blocked in 2011.

Cyber attacks are becoming increasingly prevalent and highlight the increasing awareness of, and need for, cyber-liability insurance products across Asia to cushion the liability exposure of companies that process and retain personal data of their clients.

This article highlights the potential liability and compliance exposures of companies in Asia and recent trends in cyber crimes.

Cyber crime on the rise

Marsh's report, "Cyber Risk in Asia", stated that in 2010, 75% of Asia Pacific businesses experienced cyber attacks, costing them as much as US$763,000 annually. Reports of data or network sabotage, virus and Trojan infections, computer fraud, laptop theft and network scanning are said to be widely on the increase. 42% of mailboxes targeted for attack are high-level executives, senior managers and people in Research & Development.

In Hong Kong, according to statistics published by the Hong Kong Government Information Security ("InfoSec") website, between the years 2009 to 2011, the number of computer crimes rose from 1,506 to 2,206 and the financial losses due to computer crimes rose from HK$45.1million to HK$148.52 million.

In Singapore, according to Symantec's study, 1.2 million people fell prey to cyber crime in 2010, suffering US$195 million in direct financial losses and an additional US$675 million in time spent resolving the crime- a total cost of US$870 million

Small businesses are becoming more desirable targets than larger organisations, due to generally weaker security. Symantec's research shows that since the beginning of 2010, 40% of all targeted attacks have been directed at small and medium sized businesses, compared to 28% directed at large corporates.

Cyber attacks have wider implications and can affect 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.

Impending laws and regulation in the Asia region

It is because of this wave of cyber attacks that governments in Asia are beginning to step up the regulation and enforcement of personal data privacy. Asian Governments appreciate the need to bring their countries' data protection standards in line with the standards set by the Organisation for Economic Co-Operation and Development. This is an essential part of protecting their own people's personal data, but also to promote inter-national trade and ensure consistency in regulation.

Hong Kong

Hong Kong has one of the more robust and active regimes in Asia in the protection of personal data privacy and the fight against cyber crime. The protection of personal data is largely governed by the recently amended Personal Data (Amendment) Ordinance ("PDPO") (expected to take effect from 1 October 2012). This Ordinance gives statutory effect to internationally-accepted data protection principles that require personal data collection to be lawful, held securely, up-to-date, and used only for the purpose for which it is collected.

Key provisions of the PDPO include:

- The offences of disclosure of personal data without the data user's consent that cause monetary/ property gain to the hacker, monetary/ property loss to the individual or psychological harm to the individual. The courts may impose a fine of up to HK$1,000,000 (US$130,000) and imprisonment for up to five years.
- A definition for 'data processor' (which had previously not been expressly defined). A data user is required to adopt contracts with their data processors to monitor the timeframe in which data is kept by the data processor and prevent unauthorised or accidental access, processing, erasure, loss of any personal data. Failure to comply means the Privacy Commissioner can issue an enforcement notice.
- Increased power to impose enforcement notice and increased penalties which includes (i) heaver penalties for repeat offenders being increased with a fine of up to HK$100,000 (and a daily fine of HK$2,000 and imprisonment for up to two years; (ii) a new offence for contravening the enforcement notice after initial compliance which would attract a fine of up to HK$50,000 (and a daily fine of HK$1,000 for a continuing offence) and imprisonment for up to two years.
- The Privacy Commissioner is empowered to provide legal assistance for aggrieved individuals who have the right to claim compensation for damages suffered as a result of a data user's contravention of the PDPO.

It is not just the PDPO that provides statutory provisions to tackle the risks associated with cyber crime, the Computer Crimes Ordinance, enacted in 1993 has, through amending the Telecommunications Ordinance, Crimes Ordinance and the Theft Ordinance, created some new offences and broadened the coverage of existing offences. Key provisions are:

- Telecommunications Ordinance, section 27A: prohibiting unauthorised access to computer by telecommunications. Contravention would attract a HK$20,000 fine.
- Crimes Ordinance, sections 59 and 60: extending the meaning of criminal damage to property to include misuse of a computer program or data. Maximum penalty of 10 years' imprisonment.
- Crimes Ordinance, section 161: prohibiting the access to computer with criminal or dishonest intent. Maximum penalty of 5 years' imprisonment.
- Theft Ordinance, section 11: extending the meaning of burglary to include unlawfully causing a computer to function other than as it has been established and altering, erasing or adding any computer program or data. Maximum penalty of 14 years' imprisonment.
- Theft Ordinance, section 19: extending the meaning of false accounting to include destroying, defacing, concealing or falsifying records kept by computer. Maximum penalty of 10 years' imprisonment.

Singapore

Currently in Singapore there are many Acts that together contain over 150 privacy and data protection provisions. There also exists a number of private sector codes that attempt to provide minimum standards for businesses such as the Direct Marketing Association of Singapore Code of Practice.

A draft Personal Data Protection Bill (the "PDP Bill ") had its first reading on 11 September 2012. Prior to its first reading the Ministry of Information and Communication and Arts ("MICA") published a consultation report on the proposed PDP Bill on 19 March 2012 . Further submissions were called for from the public for which the deadline closed on 30 April 2012.

The PDP Bill outlines a number of main developments in the law, which include:

- A Personal Data Protection Commission will be established ("DP Commission").
- The PDP Bill will establish a 'Do Not Call' register.
- The PDP Bill is to work concurrently with existing legislation to act as the "baseline law" for data protection in Singapore.
- The definition of "personal data" will be broad and will include electronic as well as non electronic data.
- The PDP Bill will apply to all private organisations located in Singapore and also to those overseas organisations collecting, processing or disclosing information within Singapore, even if they are not physically present in Singapore. It will apply to private organisations that collect data with a 'Singapore link'. This is to ensure that data transferred overseas is afforded the same protection as if it remained in Singapore.
- The PDP Bill will not apply to public agencies or organisations acting on behalf of a public agency.

Importantly, the PDP Bill intends to impose a number of fines and enforcement mechanisms which will be overseen by the DP Commission with the right to appeal to the New Data Protection Appeal Panel. It is intended that the DP Commission will be able to issue directions to ensure compliance with undertakings made by private organisations, settlements with wronged consumers and it will be able to prosecute offending private organisations, depending on whether the breach arises under any other applicable legislation. Currently there is no express notification requirements but it is likely to be a feature of directions issued by the DP Commission.

The current proposal is that a penalty of up to SG$1 million (US$800,000) can be imposed for refusal to allow access and/or correct information and a fine of up to SG$100,000 per offence (US$80,000) for any evasion breach which is significantly higher than many other jurisdictions in the region.

Private civil actions are able to be brought against a private organisation in addition to any investigation by the DP Commission but only after the DP Commission has made its final decision with no further right of appeal.

The PDP Bill makes it clear that individuals as well as organisations will be subject to these fines and penalities which will be of concern to those holding positions as Directors and Officers.

Philippines

The Philippines Senate passed the Data Privacy Act of 2011 on 15 August 2012 which took effect on 8 September 2012. This coincides with the Cyber-crime Prevention Act of 2012. The Data Privacy Act of 2012 imposes a privacy regime similar to the European Union Directive. Included in the Act are notice, consent and data breach notification requirements. The Act established a National Privacy Commission which is able to issue cease and desist orders and/or impose a temporary or permanent ban on the processing of personal information if it is detrimental to national security and public interest. Importantly for private organisations it is able to recommend the imposition of penalties to the Department of Justice for non-compliance. The penalties include imprisonment for a period of 1 to 6 years and fines up to 5 million pesos (US$120,000).

Malaysia

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 Malaysian government has now indicated it is considering bringing the Act into force without a Commissioner. There are many criminal offences within the Act including the failure to obtain a data subject's consent prior to the processing of personal data when required to do so which is punishable by a fine not exceeding RM300,000 (US$96,000) or imprisonment for a term not exceeding 2 years or both. Directors and officers have potential joint and several liability under the Act.

Liability exposure for data user companies

The loss of data through a cyber attack can have far reaching ramifications for a company. A wide range of issues such as violation of privacy laws, intellectual property infringement, defamation (libel and slander), negligent transmission of a computer virus to any clients or business partners are touched upon.

There are high costs associated with responding to a cyber or data breach. These costs can potentially include:

- Business interruption;
- Investigation and response costs;
- Reporting costs;
- Repair of the computer system or website and restoration of data following a computer virus;
- Replacement of computer equipment during criminal or regulatory investigations;
- Legal expenses;
- Data administrative fines and penalties;
- Third party claims and losses;
- Cyber-extortion.

Directors and officers are the ones most exposed to potential claims and have to make it their business to understand what information their company holds, where it is located and how it is protected. Boards need to analyse the potential impact a breach could have on the organisation and its likelihood of occurring, and be part of the effort to design and implement a far reaching program to both prevent breaches and prepare the organisation to respond properly if one occurs. They must be able to answer to shareholders, customers, suppliers, business partners and authorities.

The advantages of cyber risk insurance

The Asian insurance industry are recognising the increasing importance of protecting companies against the risks that are connected with a cyber attack and are looking to offer solutions to help mitigate such risks.

Cyber risk is a modern concept and 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 a number of exclusions.

The following are some key points that highlight the gaps in coverage between traditional liability policies and cyber risk policies:

- Geography - many traditional policies have geographical limitations, however with cyber policies, given the global nature of the internet, coverage is offered for loss anywhere in the world.
- Investigation and enforcement costs - traditional policies reflect the principle that it is contrary to public policy for a company to be insured against liability for his own criminal conduct including the payment of fines. In light of the trend of enforcement and fines against breach of data privacy sweeping across Asia, it may be the case that many of the fines imposed on companies would not be covered by their traditional policies. Whereas, many cyber policies specifically seek to provide cover for legal advice and representation costs in connection with regulatory investigations and also the fines that a company is legally obligated to pay upon the discovery that there has been a breach of data privacy legislation.
- Coverage of the costs of repairing the "damage" - traditional policies may not cover economic loss, or the costs of the fees that may be incurred in fixing the problem, and then restoring the injury to the company's reputation. Many cyber risk policies are designed to pay for the professional fees of a forensic cyber risk specialist, and the costs of hiring a public relations consultant to advise on media strategy, and crisis consulting.
- Extortion - an interesting additional element of coverage in some new cyber policies is for the coverage of extortion, which is where threats are made to a company demanding payment of money. In many of these policies, there is a proviso that the company has to keep this element of coverage confidential so as to prevent people from thinking the company has deep pockets and resulting in a flood of threats.
- Third party loss - coverage may not exist for third party losses due to computer viruses or unauthorised access to private and confidential information in traditional policy. Cyber policies specifically seek to provide cover for such claims.

Some issues that insurance companies might need to consider in their policies:

- New or Unknown Definitions - cyber crime is essentially any crime that takes place using computers or the internet - everything from credit card fraud, to hacking to cyber warfare and terrorism. As cyber-crimes become more sophisticated and varied, the challenge for Insurers is in providing a product that continually adapts to meet those exposures. There are grey areas to various potential categories of loss and difficulty may arise in trying to insure against these threats. There are also various commonplace exclusions which may need consideration over time. Most policies, for example, exclude acts of warfare and terrorism. However, as noted in the FBI's Statement before the Senate Judiciary Committee, "*Countering efforts by foreign countries to steal our nation's secrets, evaluating the capabilities of terrorists in a digital age, and fighting cyber crime are the FBI's highest priorities. It is difficult to overstate the potential impact these threats pose to our economy, our national security, and the critical infrastructure upon which our country relies.*" At what stage does "cyber warfare" become "war"? No doubt,

it would require an outbreak of hostilities between two nations, but it is not unimaginable that a cyber-attack between two states could involve targeting of an Insured's company if it held important financial or technical information or was relevant to a country's security. Perhaps more of concern, what are the risks of a financial institution, or a company with ties to a particular government or religion or idealogy, becoming victim of a cyber terrorist attack?

– Intangible property - digital property is becoming increasingly valuable and there is a growing demand in Asia for developments in this area. In China, there have been attempts to insure players of Blizzard's massive multiplayer online role-playing games, World of Warcraft, when they experience lags in gameplay, long queues, or system down time. Beijing based Sunshine Insurance Group Corporation in partnership with the online game operator Gamebar, are offering players monetary compensation for the loss or theft of virtual possessions such as land, loot or digital currency. A key question arises as to how insurance companies are able to prove the value of virtual goods.

Conclusion: a sea of change

A successful cyber-attack can cost millions and cause multiple exposures for an organisation as it may incur direct costs and losses in dealing with the problem, consequential losses in terms of business interruption and damage to goodwill, and finally (just when you think the problem has all been resolved) fines and penalties from the country's regulator.

The threat is very real, and likely only to get worse. The United States currently has some of the most onerous data protection requirements. Europe is reviewing new proposed draft legislation, and the advent of changes in data privacy legislation in Asia shows that Asian governments are becoming increasingly concerned with this cyber threat.

Insurance companies are introducing cyber insurance policies to the Asian market to address some of the exposure gaps that traditional policies cannot cover. In such an environment, it is important that organisations in Asia are mindful of the incoming laws and that they take preemptive action to put in place their own internal data protection policies which are consistent with the proposed legislation as well as making sure that their insurance coverage meets their potential exposures.

Further information

If you would like further information on any issue raised in this update please contact:

Patrick Perry
E: patrick.perry@clydeco.com.hk

Melissa Russell
E: melissa.russell@clyde.com.sg

Isabelle Ma
E: isabelle.ma@clydeco.com.hk

Clyde & Co
58th Floor, Central Plaza
18 Harbour Road
Wanchai, Hong Kong

T: +852 2878 8600
F: +852 2522 5907

Further advice should be taken before relying on the contents of this summary.