# Table of Contents

**Introduction**  
What is cyber risk?  
3

**2014 cyber exposure and solution trends**  
New technologies and emerging threats  
5  
Mobile devices, cloud computing, big data and social media  
5  
Cyber-crime, hacktivism, cyber espionage and cyber warfare  
7  
Incidents in Asia  
7  
Costs of security breaches continue to increase  
9  
Legal and regulatory developments in Asian countries  
10

**Country specific cyber issues:**  
Singapore  
12  
Malaysia  
13  
South Korea  
14  
Hong Kong  
15

**Risk management process related to cyber risks**  
The role of the risk manager  
17  
Aon’s cyber clarity process  
18  
Comprehensive cyber risk management programme  
18  
Aon’s proprietary Cyber Risk Discovery Process  
19  
Review of IT use policies  
19  
Third-party exposures  
19  
Vendor/supplier management  
20  
Contractual considerations, including allocation of liability  
20  
Vendor and supplier audits  
20  
Education on legal exposures  
20  
Coordinated approach  
21  
Data breach management policy  
21  
Exposure clarity phase  
22  
Coverage and gap analysis under existing insurance policies  
22  
Transferring risk through cyber insurance  
22  
Cyber exposure spectrum  
24  
Current cyber market  
24  
Adding cyber coverage to traditional insurance  
27  
Captive cyber reinsurance  
29  
Stand-alone risk transfer product  
30  
Cyber claims  
30  
The future of cyber insurance  
32
Cyber Exposures and Solutions in Asia
Risk Management and Insurance to Protect Your Financial Statements

Introduction: The evolving cyber landscape in Asia

Successful businesses throughout Asia use technology to increase sales, maximise efficiency and reduce expenses. Evolving technologies such as cloud computing, mobile devices, social media and “big data” analytics have helped them become more competitive in the global economy. Meanwhile, the array of threats to cyber security continues to grow and evolve, and Asian companies are considered by many to be the most likely targets in the world. Cyber theft, fraud, sabotage, espionage, and hacking (including from governments) are more frequent in the social media age and the associated costs with information security breaches are increasing for entities in every industry sector – from retail, financial institutions, healthcare, hospitality, media, communications, technology, consulting and professional services to manufacturing, government/public sector, energy/utilities, critical infrastructure and transportation. The legal exposure, reputational harm and business interruptions that may result can wreak havoc on a company’s bottom line.

Global executives meeting at the Word Economic Forum in Davos, Switzerland in January 2014 addressed the increasing costs of data theft and the difficulty in countering criminals who are intent on stealing data.1 Citing security breaches such as those at Japan based Mt. Gox, the largest Bitcoin exchange, and Target Corporation, the second largest U.S. retailer: the Davos executives noted the serious risk and high cost of security breaches, and expressed concern that further major disruptions due to security breaches could become commonplace.

“Technology is going to create significant opportunities, but how we as humans adapt to the changes will be very important.”2

The continent of Asia technically encompasses a widely varied landscape with dramatically diverse legal systems and commercial environments. As of March 1, 2014, an increasing number of these countries have some type of privacy, data security, cross-border transfer or other breach disclosure law.3 This paper attempts to:

- Outline some general 2014 cyber exposure and solution trends applicable to most Asian countries
- Explore in-depth cyber issues specific to Malaysia, Singapore, Hong Kong and South Korea
- Offer a risk management process to identify, understand, quantify, mitigate, and transfer cyber risks

2 Kris Gopalakrishnan, President, Confederation of Indian Industry (CII); Vice-Chairman, Infosys, India; Co-Chair of the World Economic Forum Annual Meeting 2014
What is cyber risk?

The number of Asian countries with data protection laws is growing. Companies doing business within these Asian jurisdictions will need to demonstrate that they are capable of meeting the requirements of these new laws, which are intended as a way to increase commerce and protect personal privacy. By instituting legislation protective of individual privacy, but still flexible to business needs, these countries open opportunities for businesses to compete in the global marketplace.

Apart from ensuring compliance in their domiciles, risk managers of Asian companies have to ensure compliance with directives/guidelines pertaining to breaches of Network Security if they are listed in jurisdictions such as US or are engaged in cross border transfer of data. More entities address cyber exposures in their 10-Ks, such as the following:

“We are increasingly dependent on information technology systems and infrastructure; system inadequacies, operating failures, or security breaches could harm our business.”

Risk managers for Asian-based companies are becoming more focused on how to assess and limit risks that are related to data security and other IT-related risks. They work with their company’s leadership to implement a cyber risk management plan and educate employees on how to reduce cyber risks. Responsible corporate leaders will focus on and devote resources to effective programmes to manage information security matters. They will mitigate their risk by engaging experts to place specialised cyber insurance coverage, with language tailored to address their specific needs and exposures.

---

4 SEC cyber exposure disclosure guidance issued in 2011. It is worth noting that the SEC will hold a cybersecurity roundtable on March 26, 2014 to address how public companies are addressing cyber concerns; SEC Comment Letters note entities’ failure to include adequate risk factors related to cyber exposures; State Attorneys General, FTC and other regulators have brought actions against companies for lax data security practices; Spread of foreign jurisdiction data breach disclosure laws and related penalties.

© 2014 Aon Risk Solutions, Asia
2014 cyber exposure and solution trends applicable to most Asian countries

New technologies and emerging threats

Asian countries are now seen as the most likely targets of cyber-attacks in the world. Recent research by FireEye Labs identified the ten most targeted Asian countries during 2013:

1. South Korea
2. Japan
3. Taiwan
4. Thailand
5. Hong Kong
6. Philippines
7. India
8. Australia
9. Pakistan
10. Singapore

Indeed, recent history reveals a wide array of incidents, from various causes, throughout all the countries of Asia (see list of selected incidents, below). Within Asia, FireEye Labs identified the following industries as having experienced advanced persistent cyber-attacks during 2013, in order:

1. Financial Services
2. Government (Federal)
3. High-Tech
4. Chemicals / Manufacturing / Mining
5. Services / Consulting
6. Higher Education
7. Telecom (Internet, Phone and Cable)
8. Energy / Utilities / Petroleum
9. Entertainment / Media
10. State and Local Government

Without question, Asian corporate leaders must recognise their businesses’ vulnerabilities to intentional attacks and take appropriate steps to prepare, prevent and mitigate the damage from such crimes.

While cybercrime, hacktivism and espionage are growing threats, companies must also deal with the risk of security breaches that are inherent in the use of evolving technologies. As companies seek new technological tools to make their businesses more automated, responsive and profitable, they encounter novel risks. Technological developments in recent years, such as increased reliance on cloud computing, mobile devices and social networking, have contributed to the dramatic increase in security risks. Such developments necessitate that each entity develop consistent corporate policies and contractual allocation of liability guidelines as primary risk mitigation measures, to the extent possible.

---

Meanwhile, the cost of a security breach continues to climb, both globally and within Asia. During 2013, Asian companies averaged 2,958 security incidents, up from 2,444 in 2012. The financial losses due to these security incidents averaged USD 1.6 million per company in 2013, up from USD 1.25 million in 2012. Despite the increasing likelihood of a costly security breach, it is estimated that only 46% of Asian chief executive officers believe that their company has an effective data protection security plan in place. Given that the digital revolution has created new cyber risks that can significantly affect an entity’s financial condition, corporate leaders have an obligation to protect their company’s assets and stock prices by anticipating data breach security incidents and taking steps to minimise their exposure.

Asian companies seem to realise that investment in information security is important. Of those surveyed, 60% intend to increase their security budgets over the next 12 months. Most companies have a senior level executive who communicates the importance of security (69%) and have a management process for responding to security incidents (66%). However, only 37% have a policy for security risk assessment and only 29% have a policy for end-user security awareness training.

Mobile devices, cloud computing, big data and social media

Among the technological advances that have contributed to the increased security risks are the countless types of personal tools – USB/thumb drives, smartphones, tablets, and other devices – that employees use in connection with their work. South Korea, Singapore, and Hong Kong have long led the world in early adoption of new technologies. Use of mobile devices is extremely high in Asia, with some Asian countries having the highest penetration of mobile phone usage in the world. However, these tools were initially developed and enjoyed widespread use before employers focused on the security implications that accompany them. Often, the devices are purchased by the employees themselves, used for both personal and work-related matters, and are not encrypted or tracked in appropriate fashion by the employer’s IT department. The security implications are endless – as varied as the seemingly infinite choice of brands, models and applications available. Many workers consider their mobile devices to be indispensable for both personal and work-related use, which brings further challenges in controlling the related associated security risks.

In Asia, like the rest of the world, companies more frequently outsource their computer services to third parties – such as “cloud providers” – as a cost-effective approach for centralised computing and to meet growing data storage demands. Because users are generally geographically separated (sometimes in different legal jurisdictions) from the cloud providers, the services are accessed via the internet. Asian businesses are expected to increasingly adopt cloud computing, which will undoubtedly lead to additional exposures. The sharing of private data between the customer and the cloud host companies is seen as creating potential exposure, since the cloud provider may freely access the private data. However, cloud providers with superior technology can reduce the overall privacy and security risk of its individual customers due to the implementation of continuously updated state-of-the-art IT security and mitigation procedures (compared to the customer’s attempt to maintain its IT security as a non-primary part of its core business). A key consideration with cloud providers may be severity as opposed to frequency due to the aggregation of risk where one breach could affect many customers.

Big data is another technological trend that carries additional risk due to the potential severity of a breach (more data breached equals greater potential severity). Research firm International Data Corporation, predicts that the market for big data will grow to USD 16.1 billion in 2014, which represents a growth rate six times that of the overall IT market. These enormous accumulations of often unstructured data, sometimes hosted outside a company’s IT department, are potentially less secure because they are outside the company’s internal controls. The outsourcing contract should ideally include an indemnity clause triggered by the negligence, privacy breach or security incident of the outsourced

PWC Survey 2014.
PWC Survey 2014.
PWC Survey 2014.
PWC Survey 2014.
PWC Survey 2014.
PWC Survey 2014.
PWC Survey 2014.
PWC Survey 2014.
PWC Survey 2014.
PWC Survey 2014.
PWC Survey 2014.
PWC Survey 2014.
PWC Survey 2014.
provider and specifically request evidence of insurance from the outsourced provider to back the indemnity. An added benefit of obtaining evidence of insurance from the outsourced provider is that in order to obtain such insurance, the outsourced provider would have been scrutinised by an insurance underwriting expert.

The continued popularity of social media brings additional security concerns. While these tools are valuable for recruiting employees, communicating with customers, and compiling marketing data, they also expose companies to potential human relations problems (e.g., harassment claims), privacy violations, false advertising and consumer fraud issues, defamation actions, copyright infringement claims and the like. By their very nature, social media communications are less formal, and companies tend not to manage these outlets as well as they should. Therefore, risk managers can make sure employees review their employee handbooks and implement a social media policy to ensure employee use of social media is clearly aligned with acceptable company policy and ultimately in accordance with the law.

Cybercrime, hacktivism, cyber espionage and cyber warfare

Attacks upon companies' networks continue to occur with such frequency that no business should consider itself immune. Increasingly creative, invasive and costly, these attacks can cripple an organisation's activities and devastate profits. Businesses in some industries are particularly vulnerable to hacktivism due to the unpopularity of their products or actions with certain groups. For instance, recent hacktivist attacks throughout the world have targeted energy companies, agribusiness, political parties, media outlets, educational institutions, religious groups, governmental entities, and, ironically, even organisations devoted to cyber security. Foreign governments and groups engage in espionage and destruction through electronic means. Cybercriminals continue to enrich themselves through exploiting security weaknesses, as they seek to steal credit card accounts, bank accounts or other information of value. It is estimated that more than half of all cyber-attacks originate in Asia, specifically, 55% from China and Indonesia. Moreover, Asian companies are frequently the targets of increasingly sophisticated and costly attacks.

Incidents in Asia

The following are just a few of the many recent incidents that have impacted companies operating in Asia:

- **February 2014** – Bitcoin’s leading exchange, Japan based Mt. Gox, suffered another security breach and filed for bankruptcy in February 2014, partially due to lack/inadequate insurance (previous breaches caused, among other things, account data including username, email address and an encrypted password to be publicly available). There have already been class action lawsuits filed against Mt. Gox alleging lack of adequate security.

- **January 2014** – A computer contractor working for Korea Credit Bureau stole 105.8 million customer information files personal data for over 20 million customers (more than 40% of South Korea’s population) from three Korean credit card companies, KB Kookmin Bank, Lotte Card and NH Nonghyup Card and sold it to marketing firms. Each of the three companies was fined 6 million won and has been banned from issuing new cards for three months.

- **Dec 2013** - Personal information of about 130,000 customers of Citibank – Seoul, South Korea and Standard Chartered - Seoul, South Korea was recently discovered to have been leaked by insiders, triggering alarm over inadequate security systems at financial institutions. The leaked information included names, addresses, phone numbers, account numbers and loan interest rates.

- **November 2013** – Someone claiming to be part of the hacker group Anonymous threatened the Singapore government that it would “unleash a legion of Anonymous” upon the “tiny little island and infrastructures.” While the government agencies increased vigilance, no attacks appeared to occur.

---


© 2014 Aon Risk Solutions, Asia
• August 2013 – Health records of 68 patients’ were lost when nurse of Hong Kong hospital lost a USB drive with personal details of dozens of patients’ treatment information. In addition to names, dates of birth and identity card numbers of the 68 there were 55 records of tests, 10 patient information change notifications and three study cases.

• June 2013 – Hong Kong found to be home to two computer servers spreading the Citadel Botnets computer virus, used by cybercriminals to infect computers, monitor keystrokes, and relay customer account information. Hong Kong received more attacks from the Citadel Botnets than any other country.

• May 2013 – Yahoo! Japan detected unauthorised to its web portal resulted in the theft of up to 22 million user IDs.

• July 2012 – An estimated 8.7 million customers of mobile carrier KT had their personal information (names, mobile phone numbers, resident registration numbers, handset, payment plan, account switch date) stolen over a five-month period by a mobile phone dealer intending to use the information for marketing mobile phones.

• November 2011 – Unidentified hacker stole personal data (IDs and passwords) for over 13 million users of Nexon MapleStory, Korea’s second largest online game website.

• August 2011 - A wave of DDoS attacks crashed the regulatory disclosure website of Hong Kong Exchanges and Clearing (HKEx). Investors were not able to access company announcements. That also forced the suspension of shares in seven firms with a combined market value of HKD 1.5 trillion, including blue-chips HSBC Holdings, HKEx itself and Cathay Pacific Airways. Trading was also halted on a listed debt security and 419 warrants and derivatives linked to the suspended stocks.

• August 2011 – Personal information on 92,408 customers of Citi Cards Japan, the credit-card subsidiary of Citigroup, was stolen and resold.

• July 2011 – Social networking sites Nate and Cyworld, operated by SK Communications, were hacked, resulting in disclosure of 35 million users’ personal information, including ID, password, name, and resident registration numbers.

• June 2011 – The LuckyCat cyber espionage campaign used malware to target India, Japan and Tibetans. These hackers in China were trying to steal military secrets, spy on Tibetan activities and mine information from companies in the energy, shipping and aerospace industries.

• April 2011 – The massive Sony PlayStation Network data breach exposed personal and password information of an estimated 77 million people. Sony Computer Entertainment and Sony Network Entertainment acknowledged that an "unauthorised person" had stolen the following kinds of information that was provided by PlayStation and Qriocity customers: “Name, address, country, email, address, birth date, PlayStation and Qriocity password and login and handle/PSN online ID.” Sony was compelled to take its PlayStation Network offline in the wake of this massive data breach.

---

• April 2011 – Records belonging to 420,000 customers of Hyundai Motor Group and GE Capital, were stolen by hackers from the Philippines and Brazil over a two-month period. The hackers then attempted to blackmail the company by asking for money in exchange for not releasing the customers’ information for the plaintiffs (including one case in which SK Communications was ordered to pay 200,000 South Korean Won in compensation to each of 2,882 plaintiffs)
• 2010-2013 – User data from China’s online payment platform, Alipay, was stolen and sold to other e-commerce firms and market research companies in 2010, but not discovered until 2012
• October 2007 – Hanaro Telecom sold 500,000 customers’ personal data to telemarketers, and between 2008 and 2010, customers filed class-action lawsuits. In 2011, a Seoul court ordered SK Broadband to pay a combined 400 million won to 2,300 customers

It is no secret that governments spy on one another. A great deal of attention has recently been devoted to the existence of programme allowing the U.S. government, specifically the National Security Administration (NSA), to access certain data for national security purposes through its PRISM programme. Many questions remain about what information was shared, how it was shared, and how it may have been used, but it is no longer a secret that information about individuals’ internet and phone use is being requested, gathered, used, and shared. Leading internet-related entities seek more government transparency, but deny that officials were given unfettered access to their systems. As governments’ tools become more and more sophisticated, the potential for overreach seems greater. Companies will continue to grapple with their competing obligations to their governments versus their customers and employees. Although details of surveillance programmes in other countries, including Asian countries, are somewhat sketchy, the United States is not alone in electronic data collection.

Costs of security breaches continue to increase

Year after year, the costs incurred by companies experiencing data breaches continue to climb. The most recent analysis, the 2013 Ponemon Cost of Data Breach Study, released in May 2013, evaluated a range of business costs relating to data breaches. Globally, the average cost of a single data breach is estimated to be USD 136 per record in 2012 (up from USD 130 per record in 2011.) While each situation is unique, based upon the amount and type of data involved, it is clear that the cost can range from serious to astronomical. In the U.S. and Europe, settlements and expenses reach into the millions in some of the more serious breach situations, and government-imposed fines may be levied on top of that. Likewise, some Asian countries may impose fines as well as provide for private rights of action – including class action lawsuits – for a range of damages.

Research indicates that the cost of cybercrime continues to be a growing global concern. The direct global cost (USD 113 billion) and the average cost per victim (USD 298) increased in 2013. In Singapore, the cost per victim increased from SGD 826 in 2012 to SGD 1,448 in 2013. The overall cost of cybercrime during 2013 was estimated to be SGD 1.25 billion in Singapore, USD 1 billion in Japan and USD 37 billion in China.

Litigation is a predictable and expected cost in the U.S. While Asian countries are historically less litigious than the U.S., that may be changing. A number of Asian countries have extended to individuals the right to bring a legal action against data handlers who violate their laws. Throughout Asia, businesses are encountering laws, increased enforcement, enhanced penalties and the increasing likelihood of litigation.

31 The Ponemon Study included Japan, where the average cost of a single data breach is $700,000 USD and India, where the average cost was reported to be $300,000 USD.

© 2014 Aon Risk Solutions, Asia
A recent survey indicated that 76% of Asian companies have created a board risk committee to oversee privacy and security matters. This is encouraging, because protecting the company’s assets from cyber risk is a board level issue.

Risk management is sometimes mistakenly viewed as a cost center rather than a corporate asset. As a result, risk managers are often directed to reduce expenses (e.g., insurance premiums) with lack of appropriate regard for the total cost of risk (e.g., potential catastrophic losses not covered by insurance). However, the digital revolution raises new cyber risk concerns that can significantly affect an entity’s financial statements. The onus is upon the company to seek coverage for potential risks to its’ electronic data. The world’s data is expected to grow 50-fold in the next decade and information assets are now considered extraordinarily valuable, cyber insurance purchases remain well behind traditional property and casualty insurance. Thus, a prudent board will consider directing its management to:

- Qualify and quantify its cyber exposures, including the potential effect upon the balance sheet
- Management must ‘buy-in’ and support the network security and privacy team in order to ensure its success
- Mitigate cyber exposures, including due diligence and contractual allocation. Note that insurance underwriters will rely on third party security assessments when conducting due diligence to quote a premium and coverage for cyber insurance
- Prepare updates to written policies and procedures with ongoing training assists in creating a culture of best practices.
- Conduct actuarial modeling to determine whether to assume and/or transfer such risks

Risk managers, therefore, must become more educated on matters relating to the financial impact of cyber exposures. Risk managers can assist corporate directors and officers in satisfying their fiduciary duties to protect their company’s assets. As the 2014 derivative shareholder class action against the Target Corporation Board of Directors demonstrates, the next wave of shareholder class action litigation is predicted to be against boards of directors that have not satisfied their duty of care to manage such exposures.

At least 52% of U.S. companies and 12% of European companies purchase cyber insurance coverage and that proportion is steadily increasing. With each highly-publicised breach, companies rush to buy coverage. Evidence suggests that Asian countries lag behind their counterparts abroad in obtaining coverage for these risks.

Legal and regulatory developments in Asian countries

Asia is experiencing tremendous economic growth and, as a result, is seeing an increase in the need for privacy and data security regulation. The legal landscape varies widely from one country to the next, which results in a complicated patchwork of different privacy and data protection laws throughout Asia, as well as throughout the rest of the world. Uncertainty about legal obligations can hinder international trade if, for instance, a business in one country is hesitant to outsource work to a business in another country because it fears data protection might be inadequate. Thus, to fully benefit from global economic opportunity, countries should encourage the promulgation and enforcement of data protection laws. If Asian countries wish to receive outsourced data, they will need to ensure that this data will be protected.

Many Asian countries already have, or are in the process of, adopting data protection rules. Others are tightening their existing privacy rules. In most cases, the penalties for noncompliance are increasing. Some, but not all, countries regulate cross-border transfers of data. The concept of privacy varies from one Asian country to another. Some countries have breach notification provisions, while others do not.

From the start of the current decade, governments in Asia have shown a marked tendency to tackle the concerns relating to data privacy or misuse issues through a multipronged approach of promulgation of various specific laws, to setting up

---

of central/national data protection authorities and recognising the rights of individuals whose privacy may have been compromised to seek legal redress. Though Japan can be rightly called the forerunner in this sphere; Japan’s Personal Information Protection Act was promulgated on May 23, 2003 and became fully effective on 1st April 2005 extending its purview even to the private sector; in the last couple of years other countries have also rapidly caught up and now there are significant enactments in many Asian countries. Whether one tends to dwell on the Singapore Personal Data Protection Act of 2012 or the Data Privacy Act or the Cyber Crime Prevention Act in Philippines, most of them have adopted in larger or smaller measure the six Data Protection Principles (DPP) enunciated in Hong Kong and reproduced below.

- **DPP1**: personal data shall be collected for a purpose directly related to a function and activity of the data user; lawful and fair collection of adequate data; data subjects shall be informed of the purpose for which the data are collected and to be used
- **DPP2**: all practicable steps shall be taken to ensure the accuracy of personal data; data shall be deleted upon fulfillment of the purpose for which the data are used
- **DPP3**: unless the data subject has given prior consent, personal data shall be used for the purpose for which they were originally collected or a directly related purpose
- **DPP4**: all practicable steps shall be taken to ensure that personal data are protected against unauthorised or accidental access, processing or erasure.
- **DPP5**: formulates and provides policies and practices in relation to personal data
- **DPP6**: individuals have rights of access to and correction of their personal data. Data users should comply with data access or data correction request within the time limit

These are also reflected in the Malaysian Personal Data Protection Act 2010 which enunciates the following Personal Data Protection Principles under Section 5 of the Act.

**Section 5:**

(1) The processing of personal data by a data user shall be in compliance with the following Personal Data Protection Principles, namely:

a) The General Principle  
b) The Notice and Choice Principle  
c) The Disclosure Principle  
d) The Security Principle  
e) The Retention Principle  
f) The Data Integrity Principle  
g) The Access Principle,

In general, companies that operate in Asia should expect data protection laws to be strengthened and for enforcement to become more rigorous in the foreseeable future.

---

40 Source Notice/ Copyright 2001 Office of the Privacy Commissioner for Personal Data, Hong Kong).

41 A number of Asian countries are members of the Asia-Pacific Economic Cooperation Forum (APEC), which issued a privacy framework for its 21 members. These voluntary associations create useful, but non-binding principles.
Cyber issues specific to Malaysia, Singapore, Hong Kong and South Korea

Singapore

Singapore has historically taken a business-friendly approach to data protection. There was no data protection law before 2012, when Parliament passed the Personal Data Protection Act of 2012 (PDPA). The law becomes effective in three phases, with the main provisions going into effect on July 2, 2014. The PDPA does not contain a fundamental right to privacy, but it does purport to enhance an individual’s right to control his or her personally identifying data.

The PDPC issued “Advisory Guidelines on Key Concepts” and “Advisory Guidelines on the Personal Data Protection Act for Selected Topics,” on 24th September 2013. In addition, on 26th December 2013, the PDPA issued “Advisory Guidelines on the Do Not Call Provisions.” These non-binding guidelines set forth information on how the PDPC will interpret certain provisions of the PDPA.42

The law applies to companies (both inside and outside of Singapore) that use, collect or disclose data in Singapore. Unless exempt, companies may collect or disclose personal data only for reasonable and appropriate purposes and only with the affected individuals’ prior knowledge and consent (subject to specific exceptions). Like the European Data Protection Directive, individuals have the right to access data relating to them and to correct it. Unlike the European Data Protection Directive, however, there is no separate definition of sensitive personal data (such as information about race, health, religion, sexual orientation, political opinions etc.). The law permits transfer of data outside Singapore only if the jurisdiction of the transferee organisation provides comparable protection as the Singapore PDPA. Affected businesses (of all sizes) are required to designate (by publishing contact information) a data protection officer, who is responsible for ensuring the business’ compliance with the law. Covered businesses are required by the law to protect personal data by making reasonable efforts to protect the security of the data from unauthorised access, collection, use, disclosure, modification, or other risks. The law does not state specifically what measures are required, but does impose a general obligation. More detailed industry-specific regulations are likely to follow. The law does not contain any reference to a right of privacy.

Nothing in the PDPA or other laws requires breach notification to authorities or individuals. There are some situations in which it may be prudent or required for companies in particular industries to notify authorities.43

The PDPA also includes a “do not call” registry allowing individuals to opt out of receiving marketing contacts through telephone, SMS, MMS or fax. This legal limitation on electronic marketing applies both to messages sent from Singapore and messages received in Singapore.

The Personal Data Protection Commission is the authority in Singapore that implements the law. The Commission may direct a company to stop collecting, using or disclosing data, to destroy personal data collected in violation of the law, to provide or refuse access to the data, and/or to pay a penalty. The Commission’s orders may be registered with the Singapore District Courts to obtain the force of law (similar to a court order). Penalties for violations of the PDPA include fines up to SGD 1 million. The Commission may initiate investigations on its own. Affected individuals also have the right to file a complaint with the Commission or to bring a private civil action. In a private action, unless the Commission has already made a decision, the individual may obtain injunctive relief, declaratory relief, monetary damages and any other relief the court deems proper.

In light of the possible financial penalties and exposure to lawsuits, it is strongly recommended that affected individuals be notified promptly of a security breach. This, and other remedial steps, may be used to mitigate exposure to damages or to lower the penalty assessed by the Commission.

---

42 The Guidelines are available on the PDPC’s website: [http://www.pdpc.gov.sg/resources/advisory-guidelines#sthash.iRdsSKpH.dpuf](http://www.pdpc.gov.sg/resources/advisory-guidelines#sthash.iRdsSKpH.dpuf) Included in this guidance is a discussion of the use of “cookies,” distinguishing between active consent and the mere “failure of an individual to actively manage his browser settings.”

43 For example, financial institutions that process data containing specified personal information required to be encrypted pursuant to Monetary Authority of Singapore (MAS) Circular No. SRD TR 01/2009 are directed to notify MAS within one hour of a security breach. See MAS Notice 664, issued 21 June 2013, and MAS Technology Risk Guidelines, June 2013.
Malaysia

Stock market operator Bursa Malaysia Bhd's website was the target of a distributed denial of service attack (DDoS) in February 2012, whereby the site was overloaded with excess traffic from multiple sources, which is not addressed by the following Malaysia laws. For instance, Malaysia’s Personal Data Protection Act 2010 became effective on 15th November 2013. Data users have three months to comply with the PDPA and regulations. The law applies to all data used in commercial transactions, so it applies to virtually all companies – including financial institutions, law firms, accounting firms, hotels and retailers. The Malaysian PDPA has many similarities with the European Data Protection Directive. It applies to persons established in Malaysia and to those not established in Malaysia but who use equipment in Malaysia for processing personal information. The PDPA does not apply to personal data processed outside of Malaysia, unless that data will be further processed in Malaysia.

Malaysia’s PDPA does not contain any data breach notification requirement. It does contain the seven data protection principles found in the UK PDPA. The Malaysian PDPA requires users of data to comply with a number of principles, the General Principle, the justification for the processing, such as consent; the Notice and Choice Principle, the right to be informed about the purposes for the processing; the Disclosure Principle, no disclosure except in connection with the purpose; the Security Principle, the obligation to take practical steps to protect data; Retention Principle, not to keep the data for longer than necessary; Data Integrity Principle, ensure that data is accurate and up to date; and the Access Principle, an individual’s right to have access to his or her data. The Malaysia PDPA requires prior written consent from a data subject in order for his or her data to be processed (and “process” is defined very broadly). The data may not be disclosed to a third party without consent. A data user is required to take appropriate steps to protect personal data from being lost, misused, modified, or accessed without authorisation. The Malaysian PDPA also distinguishes between personal data and sensitive personal data, with more stringent requirements applying to the latter.

Malaysia also issued regulations for implementation of the PDPA. These regulations require certain organisations to register as data users, including:

- Banking and Financial Institutions
- Communications Service Providers
- Tourism and Hospitality Providers
- Insurers
- Real Estate Firms
- Education Bodies
- Direct Marketing Organisations
- Transportation Firms
- Utility Providers

There are also provisions on transfers of data out of Malaysia, which allow users to transfer data to a place specified by the Minister for Information, Culture and Communications, or in accordance with one of the exemptions, e.g. with the individual’s consent or for the performance of a contract.

Malaysia’s new law carries fairly heavy penalties for noncompliance. If convicted of a violation of any of the seven principles, the violator could face a fine of up to 300,000 Ringgit or imprisonment of up to two years. Failure to register (for the organisations listed) could result in a fine of up to 500,000 Ringgit and imprisonment of up to three years.

---

44 The Malaysian PDPA was initially scheduled to go into effect on August 16, 2013, but was delayed for technical reasons, so the operative date was also postponed. The PDPA did finally become effective on November 15, 2013, with compliance required by January 1, 2014. “Data protection act gazetted, effective today,” The Malay Mail Online, by Melissa Chi, November 15, 2013, http://www.themalaymailonline.com/malaysia/article/data-protection-act-gazetted-effective-today
45 Personal Data Protection (Registration of Data User) Regulations 2013, http://op.bna.com/pl.nsf/id/dapn-9dmq6k/$File/Personal%20Data%20Protection%20(Registration%20of%20Data%20User)%20Regulations%202013.pdf
South Korea

South Korea is in a particularly precarious situation because of the attacks from North Korea that has caused computer networks at major South Korean banks and top TV broadcasters to crash simultaneously. In late 2011, the government of South Korea enacted one of the most stringent data protection laws in Asia, the Personal Information Protection Act (“PIPA”), to prevent and address security breaches leading to the disclosure of personal information. Among other obligations, companies are obligated to protect unique identifying information, such as resident registration numbers and foreigner registration numbers, through encryption. The Minister of Public Administration and Security (MOPAS) is responsible for executing PIPA.

The PIPA differentiates between personal data and sensitive personal data. Except for narrow exceptions, data may be obtained only after the individual has been informed of, and has consented to, its purpose and use. PIPA defines “sensitive personal data” as information that relates to a living person’s thoughts/creeds, membership in a political party or labor union, political views, health and sexual life, and other data anticipated to intrude seriously upon the privacy of the person (through the Enforcement Decree, this now includes genetic information and criminal record).

A public institution (such as a government agency) which collects personal data is required to register with MOPAS the name of the personal data file, the basis and purpose of the personal data file, the items of data contained in the file, the method of processing the file, the period the file will be retained, the person who receives the data, and other matters. The Presidential Decree added the following required registration: the name of the institution which operates the data file, the number of subjects in the data file, the department of the institution in charge of processing, the department handling the personal data subjects’ requests to inspect their data, and the scope of the data inspection.

The amended IT Network Protection Act became effective 18th August 2012. It prohibits the collection of a Resident Registration number unless the Data Handler has been designated as an identification institution by the KCC or there are special provisions under other laws. Under the IT Network Act, every IT Service Provider is required to designate a director or chief officer in charge of handling personal data as a data protection officer.

If a Data Handler under PIPA or an IT Service Provider under the IT Network Act intends to obtain personal data from an individual or IT service user, it must first notify the data subject or IT service user of the vital information prescribed by the law, and obtain their prior consent to such collection (except under rare cases). Consent for sensitive personal data must be separately obtained.

Article 16 of South Korea’s Personal Information Protection Act (effective September 30, 2011) was amended on 6th August 2013 to incorporate an affirmative obligation on the part of a personal information processor, requiring notification to data subjects that data subjects may deny consent for the collection of any personal information other than for any purposes under Article 15(1). This continues South Korea’s stringent efforts to promote data privacy, and provides another instance of South Korea’s articulation of a minimum data collection regime.

Following the 2014 Korea Credit Bureau data breach incident, the South Korean Government, specifically the Financial Supervisory Service (FSS), began conducting on-site inspections of a variety of financial institutions. Among the targets of these inspections are banks, investment companies, credit card companies and insurance companies – all of which are known to handle large amounts of personal information. In addition, FSS has requested the status of protection of customer information from over 3,000 financial institutions via a checklist report. Based on the results of this information, more FSS audits are expected. If violations are uncovered, heavy sanctions may be imposed on the responsible corporate leaders, including chief executive officers. As a follow-up to the FSS checklist and self-audit, companies should consider taking the measures:

1. Companies should review whether their standard of "satisfactory" or "inadequate" as applied in responding to the FSS checklist is consistent with the relevant laws, the position of the financial authorities and the overall industry situation.

2. The FSS is still working out the details on how and when to conduct field inspections based on the audit results it received. Therefore, in the interim companies should prioritise their action plan and focus their efforts on improvements that can be implemented immediately. For example, companies should check whether there are IT or security improvements that can be implemented right away under the existing hardware and software system (e.g., optimising the rule sets of existing security solutions to tighten internal control.

strengthening the monitoring of logs), and at the same time establish mid to long-term improvement plans. In some cases, companies may consider adopting a low-cost solution for the time being (e.g. utilising security features included in Microsoft Windows) while reviewing and evaluating mid to long-term solutions.

In Korea, companies and their responsible employees/executives are subject to criminal sanctions (under the Personal Information Protect Act and the Act on Promotion of Information and Communications Network Utilisation and Information Protection) for the chief executive officer, chief process officer and responsible employees, as well as severe disciplinary measures by the FSS for responsible employees.

Hong Kong

Hong Kong’s Personal Data (Privacy) Ordinance (Cap. 486), first passed in 1996 and amended in 2012, governs the collection, accuracy, retention, use, security and access to personal data. The law addresses the use and transfer of personal data for direct marketing (requires consent) and the requirements that data processors take steps to prevent unauthorised access. The Ordinance also contains cross-border rules that prohibit the transfer of personal data outside of Hong Kong except under limited specified circumstances.

The Ordinance is enforced by the Privacy Commissioner for Personal Data (PCPD), which issues guidance to Hong Kong companies to assist with compliance. The PCPD has the authority to assess fines of up to HKD 500,000 and three years in jail for most violations. For violations in which personal data is illegally disclosed for personal gain, a fine of HKD 1 million and five years in jail may be imposed. Individuals harmed by a security breach may seek assistance from the PCO. In 2013, privacy complaints to the PCPD increased by 43% over the prior year.51

There is no data breach requirement in Hong Kong, although the PCPD does recommend that users maintain a breach notification system.52 While the PCPD has no power to impose fines or penalties for failure to notify subjects or authorities of a breach, evidence of prompt notification may be offered in mitigation of damages if private litigation were to be commenced.

Reports suggest that cyber-attacks in Hong Kong are on the rise. In the first six months of 2013, the Hong Kong Computer Emergency Response Team (HKCERT), a government-backed watchdog, reported a 12% increase compared to the same period in 2012.53 Approximately half of those attacks resulting from hacking and botnets, with the remaining incidents involving phishing, viruses, spyware and the like. The number of security incidents had increased by 30% from 2011 to 2012. HKCERT reports that the number of malicious software incidents has increased from about 1,000 in 1991 to “millions” in 2012.54

The Hong Kong Privacy Commissioner has highlighted some activities and areas of data privacy practice likely to attract his attention in 2014 and signaled an intention finally to bring the restrictions on international data transfers into force.55

1. **New protections for international data transfers proposed**
   The most eye-catching - and long-awaited - announcement by the Privacy Commissioner was that the issue of international data transfers will be one of his three strategic focuses for 2014

2. **Greater emphasis on good corporate governance**
   The Privacy Commissioner announced that he will assist organisations to adopt more robust data protection policies as part of their corporate governance responsibilities, saying that organisations need “to treat the subject seriously”

---

53 PCPD Guidance Note on Data Breach Handling and the Giving of Breach Notifications, June 2010. The Guidance Note contains specific advice on what the notice should contain and other matters.
3. **Direct marketing**
   The introduction of new direct marketing rules in April 2013 (under the Personal Data (Privacy) (Amendment) Ordinance) led to a significant increase in the overall number of complaints, enquiries and potential cases for prosecution received by the PCPD in 2013 as compared to 2012, as organisations in Hong Kong got to grips with the new laws. Interestingly, though not surprisingly, around a third of the complaints received by the PCPD in 2013, and just over a half of enquiries, received by the PCPD in 2013 related to the new direct marketing rules.

4. **Data user return scheme postponed**
   The Privacy Commissioner announced that it plans to put the implementation of the Data User Returns Scheme (DURS) on hold until data privacy reforms in the European Union are finalised.

5. **Self-initiated investigations and data breach notifications**
   The number of self-initiated investigations by organisations through voluntary notifications to the Privacy Commissioner increased in 2013, demonstrating that businesses are becoming increasingly concerned with personal data protection, from both a compliance and reputational perspective.

6. **New technologies**
   The number of complaints relating to the use of new information and communications technologies also rose in 2013.

7. **High risk industry sectors**
   In 2013 organisations in the financial services, telecommunications and property management sectors were the subject of most complaints to the Privacy Commissioner. In 2014 businesses in these sectors are likely to be under increased scrutiny from the PCPD, and thus face greater pressure to ensure compliance with the PDPO.

8. **High risk activities**
   Organisations in Hong Kong are still getting it wrong when it comes to notifying individuals about how and why their personal data will be used.

9. **Increased enforcement actions**
   In 2013, the number of enforcement notices issued by the Privacy Commissioner more than doubled, and investigation reports published by the Privacy Commissioner have received widespread media coverage and invoked the sanction and discipline of public scrutiny.
Risk management process to identify, understand, quantify, mitigate, and transfer cyber risks

The role of the risk manager

Risk managers advise companies regarding potential risks to the organisation. They identify and assess threats, develop policies and strategies for risk management and decide how to avoid, reduce, allocate and transfer risks. While proactive measures to mitigate risk can be costly and time-consuming, they are far less demanding than the consequences of a serious breach, which can require dealing with a seemingly endless list of critics, including the company’s General Counsel, data privacy authorities, prosecutors, politicians, customers, patients, students, aggrieved employees, shareholders, plaintiffs’ class-action lawyers, the media and the public. Moreover, having a robust, well-documented programme to monitor network privacy and security matters may provide favorable evidence of the company’s efforts, thus reducing liability should an incident occur. A network security and privacy risk mitigation programme should start with the following:

1. Identify, classify and quantify the use of information assets and electronic methodologies, including reliance on third party outsourced service provider
2. Implement risk management best practices, such as IT security, corporate policies and procedures
3. Critically evaluate the contracts with customers, outsourced service providers and other relevant entities (external data processors) to ensure compliance with the regulations, and ascertain appropriate contractual allocation of liability
4. Train and monitor employees, subcontractors, third party outsourced service providers and other channel partners regarding such best practices
5. Model the range of potential frequency and severity of losses from network security and privacy incidents for your unique industry and entity specific circumstances
6. Determine the entity’s risk appetite to retain, mitigate and transfer network security and privacy exposures compared to the entity’s overall enterprise risk management strategy
7. Analyse existing insurance policies for possible partial network security and privacy coverage
8. Consider customised network security and privacy insurance to stabilise the entity’s financial statements and mitigate the risk of breach of fiduciary duty of management and the board of directors

[56 http://one.aon.com/shiftin-landscape-cybercrime]
Aon’s cyber clarity process

**Introduction**
- Understand a framework for viewing cyber risk
- Gain a high-level understanding of your company’s risks

**Exposure Clarity**
- Gain a deep understanding of your company’s cyber risks and the:
  - Scenarios that they could create
  - Potential financial impact
  - Maturity level of your current risk management approach
  - Insurability of your cyber risk

**Advisory**
- Translate your exposure clarity into actionable insight and prepare for risk transfer strategies
- Measure the gap between existing insurance and cyber risk scenarios
- Receive ongoing advisory and support on cyber issues
- Examine actual incident case studies

**Insurance**
- Transfer cyber risks through insurance
- Ensure best in class programme through:
  - Proprietary and consistent programme analytic tool
  - Global peer purchasing data
  - Qualitative and quantitative evaluations of available insurers
  - Global market leverage

Comprehensive cyber risk management programme

In light of the increased significance of cyber risk management matters, it is essential that corporations develop a comprehensive programme. A team consisting of Information Technology, legal, risk management, Chief Information Officer, IT security, human resources, product development, sales, marketing and other pertinent personnel should be involved in developing and executing the programme. Risk managers are responsible for managing the risks to the company, its employees, customers, reputation, assets and interest of stakeholders. Risk managers are responsible for coordinating a cyber risk management plan that protects the company from specific risks.

An effective cyber risk management programme will not be static, but rather will be subjected to regular re-evaluation and improvement. Risk managers need to be aware of changes in the company’s business because these may require modifications to the programme. Virtually every corporate transaction should be evaluated for potential cyber security implications. For example, should an acquisition occur, the cyber security situation of the acquired entity should be made a priority in the due diligence process, and necessary improvements may be required to bring the acquired company in line with the security standards of the acquiring company.

Once a programme is developed, it is essential that it be well-documented, so that it can be used as evidence of good faith should a breach occur.
Review of IT use policies

Risk managers need to audit and regularly review the company’s reliance on different forms of technology (i.e. tablets, smartphones, iPads, USBs) and ensure that various uses of such technology (i.e., work, social media, personal use) are appropriately regulated in company IT and/or social media policies and guidelines. In particular, the increased use of mobile devices carries security risks for corporate networks. Data breaches caused by smartphones are becoming more common than lost or stolen laptops.  

Third-party exposures

Businesses may take great care in protecting their own electronic systems but utterly fail to take into account the vulnerabilities in the systems of the various third parties with whom they share confidential information. Vendors, suppliers, consultants, IT providers and a range of other third parties have occasion to access various types of confidential corporate information. A number of steps can mitigate the exposure in these situations.

---

Vendor/supplier management

A risk assessment should be conducted for each third party provider and, depending on the type of data being shared, additional steps should be considered to prevent security breaches: The more sensitive the information being shared, the more thorough the steps to be taken.

Risk managers must appropriately assess, measure, monitor and control the risks associated with third party relationships. Risk assessment is fundamental to the initial decision whether to enter into a third party relationship. The first step is to ensure the relationship is consistent with the company’s overall business strategy. Next, risk managers should analyse the benefits, costs, legal aspects and the potential risks associated with the third party. The last step is to estimate the long-term effect of the proposed third party relationship.

Throughout the third party relationship risk managers must continue to analyse the risks associated with the interactions. Third party providers that are found to have lax security procedures should be replaced or given a relatively short period of time to bring their practices within acceptable standards.

Contractual considerations, including allocation of liability

Corporate counsel should assist clients with mitigating cyber exposures by developing consistent contractual language to be used in vendor agreements. Third parties should, at a minimum, be expected to accept inclusion of language in which they warrant that they are in compliance with applicable laws relating to information privacy and security. Clients should also expect that third party providers will commit contractually to follow the client organisation’s privacy policies. Depending upon the type of information to be shared, contracts may also include specific provisions outlining the vendor’s security procedures that require the vendor to conduct regular risk assessments and report to the client. In some situations, it may be useful to specify that the client has the right to engage an outside firm to audit the service provider’s security infrastructure. In all cases, contracts should contain a clear requirement that any security breach be reported to the client immediately upon discovery.

Many third party contracts contain indemnification provisions that commit the third party providers to indemnify the client should a security breach occur due to the vendor’s negligence or intentional act. Where possible, such indemnification should be sought, and should be as broad as possible, including all direct and indirect costs associated with a breach. Clients should inquire about, and perhaps insist upon, third party providers maintaining adequate levels of cyber insurance to cover the cost of potential breaches. Where such coverage is required, clients may wish to require that the client be named as an ‘Additional Insured’ on such policies. It may also be advisable to specify that disputes be resolved through arbitration rather than litigation in the courts, given the sensitivity of some of the information involved.

Vendor and supplier audits

Organisations may be unaware of which vendors and suppliers have access to their confidential data, such as personally-identifiable information on customers and employees, or proprietary information about the company’s products. The first step in implementing a system to manage this exposure is to identify the various suppliers and vendors and to determine precisely which type of information each third party entity is being sent (or otherwise accessing). A robust audit is essential. These audits should examine not only the outsourced IT service providers, such as data processors, but also any other type of third party organisation or individual who might have access to corporate data. The audits should be conducted regularly and systematically so that both existing and all new third party providers are tracked and monitored. For each provider identified, careful consideration should be given to whether the level of access is appropriate and necessary in light of the service being provided or whether more limited disclosure may be warranted to avoid exposing data unnecessarily.

Education on legal exposures

Risk managers must work with corporate counsel to educate the organisation regarding the evolving legal exposures in the area of cyber security. Fortunately, corporate leaders now recognise data protection as a top concern.

Coordinated approach

Corporations may be asked to share information with law enforcement or national security agencies. It is essential that the appropriate corporate personnel be assigned to oversee these interactions so that the company’s legal obligations are satisfied without unnecessarily risking disclosure of confidential company data. Legal oversight is essential, as these issues often require an extremely sophisticated and difficult balancing of competing legal obligations. There is also an argument that, in the event of a security or privacy incident, legal counsel, rather than the risk manager or insurance broker, should engage forensics, investigative and other third party experts to enable attorney-client privilege protection.

Data breach management policy

Risk managers should work with the company to develop a Data Breach Management Policy (also known as a Data Breach Response Plan) to address and outline internal corporate prevention, detection and incident response processes in response to a security breach. It could help in defending an allegation that the company failed to take reasonable care in handling a data security breach.

The first step in creating such a policy is defining a ‘breach.’ Everyone understands that when criminals hack into a company’s network that a security breach has occurred. However, a security breach occurs virtually every time an employee loses a cell phone or has a laptop stolen. A useful policy must define what a breach is, and set forth a process designed to respond effectively to each specific incident based on the specific circumstances of the breach and the precise nature of the information compromised. Different measures are required depending on the sensitivity of the information involved. Failure to respond promptly, effectively, and in compliance with applicable laws can expose a business to material liability. Furthermore, insurance underwriters assume that nearly every entity will suffer some type of security or privacy incident at one time or another and reducing the impact of a breach is essential. Therefore, insurance underwriters focus almost as much on the robust data breach incident response policy as on the prevention measures.

---

Exposure clarity phase

Each step builds on the previous, creating clarity of cyber exposures faced by the client

<table>
<thead>
<tr>
<th>Service</th>
<th>Core Characteristics</th>
<th>Deliverable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk/ Exposure Assessment</td>
<td>- Tailored to the client/bespoke</td>
<td>- Report identifying and prioritising cyber risks tailored to client</td>
</tr>
<tr>
<td></td>
<td>- Interviews with key employees (IT, Risk/Insurance, Operation, etc.)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Detailed report with prioritised cyber risks and recommendations</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Identification of <strong>cyber scenarios</strong></td>
<td></td>
</tr>
<tr>
<td>Scenario Quantification</td>
<td>- Matching cyber scenarios to business impacts/consequences</td>
<td>- Report quantifying cyber risks impacts tailored to client</td>
</tr>
<tr>
<td></td>
<td>- High level estimation of impact based on available data</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Quantification of consequences</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Detailed, quantitative assessment of business interruption due to cyber risks</td>
<td></td>
</tr>
<tr>
<td>Risk Mitigation &amp; Maturity Review</td>
<td>- Web-based “health check” questionnaire with detailed questions about client’s current cyber risk mitigation processes and practices</td>
<td>- Report evaluating the maturity and effectiveness of client’s current controls</td>
</tr>
<tr>
<td></td>
<td>- Follow-up with Aon Global Risk Consulting to validate results and provide high level recommendations</td>
<td></td>
</tr>
<tr>
<td>Insurability Review</td>
<td>- Analysis of insurability of identified scenarios (follow-up after cyber risk assessment)</td>
<td>- Report detailing insurability of previously identified scenarios and risks</td>
</tr>
<tr>
<td></td>
<td>- Analysis of a typical policy response</td>
<td></td>
</tr>
</tbody>
</table>

Bespoke services (by Aon or in connection with subcontractors) can be designed around the needs of specific clients at additional cost

Coverage and gap analysis under existing insurance policies

Companies should work with their insurance broker to analyse property, crime and general liability insurance policies and determine any potential gaps in existing coverage. Companies should consider specific network security and privacy insurance to fill any obvious gaps.  

Effective May, 2014, the Insurance Services Office Commercial General Liability (CGL) template endorsement, which is voluntary – not mandatory, clarifies that “**This Insurance does not apply to: Access or Disclosure of Confidential or Personal Information.**” The result can be self-insured losses of more than $100 million in the cases of SONY, TJX, Heartland and Global Payments. Driving the point home is that, in February 2014, a court found that the Zurich CGL is not obligated to cover Japan based SONY for litigation related to the 2011 hacking of its PlayStation Network.

Transferring risk through cyber insurance

Insurance specifically designed to cover the unique exposures of data privacy and security can act as a backstop to protect a business from the financial statement harm resulting from a breach. While there is an argument that some cyber risks could be covered under traditional insurance policies, such as property (e.g., business interruption from a computer hack) or commercial general liability (e.g. third party data privacy breach litigation), it is wise to consider specialised cyber risk insurance coverage in order to comprehensively cover network security risks.

Traditional policies were developed years ago and typically do not contemplate exposures such as those discussed in this paper. While some categories of losses might be covered under standard policies, many gaps usually exist. In the US, insurers are filing declaratory judgment actions against their insureds to deny coverage for cyber exposures under

---

property, general liability, professional liability and crime policies. Some courts are finding that these traditional policies, such as property policies, do not cover the types of intangible harm that results from data breaches. Coverage may also be denied if intentional acts are excluded from coverage.

Insurers are also denying coverage under professional liability/ers’ and omissions and directors’ and officers’ policies, with mixed outcomes in the courts. With these other types of non-cyber specific insurance policies, the outcome of a coverage dispute is far from certain, and will turn on the precise policy language, the specific circumstances of the claim, the identity of the victim, the nature of the harm caused and the court’s willingness to find coverage where policy language appears to preclude it. For example, in *Eyeblast, Inc v. Fed Ins Co*, 613 F.3d 797 (8th Cir 2010), the Court of Appeals for the Eighth Circuit concluded that coverage existed under the comprehensive general liability (“CGL”) policy despite the insurer’s fairly persuasive claims to the contrary. Eyeblast, the insured, an online marketing company, was sued for allegedly causing the plaintiff’s computer to malfunction due to spyware attached to Eyeblast’s online advertising. Eyeblast submitted a claim to its CGL and professional liability/ers and omissions insurers, but the claim was denied. The insurer asserted that since the CGL policy covered only ‘tangible property,’ and excluded losses resulting from ‘software, data or other information that is in electronic form,’ it was not covered. The insurer also denied coverage under the errors and omissions policy on the grounds that the plaintiff had failed to allege a wrongful act by the insured, since the policy defined a wrongful act as an error, unintentional omission, or negligent act in connection with a product failure. The court disagreed, finding that coverage existed under both policies. The general liability policy was held to cover damage for the loss of the plaintiff’s computer, which was tangible property. The errors and omissions policy provided coverage because ‘error,’ defined as including ‘intentional, non-negligent acts but to exclude intentional wrongful conduct,’ would include actions such as the insured’s causing of software to be installed on the plaintiff’s computer. Though intentional, Eyeblast had disclosed to the insurer that its core business was online advertising, so its actions in causing software to be installed on the plaintiff’s computer was not an intentional wrongful act because it was in the ordinary course of its business. In a case decided 23 May 2013, *The Illinois Supreme Court held that claims based on alleged violations of the Telephone Consumer Protection Act are covered under a traditional general liability policy.*

---

62 Zurich Am Ins Co et al v Sony Corporation of America, et al, Case No 65198, filed 20 July 2011 (NY Sup Ct) https://iapps.courts.state.ny.us/litigation/AS/publicdetails.aspx?caseid=125425 (Zurich sought declaratory judgment that it has no duty to defend or indemnify Sony against class actions relating to hacking of 100 million PlayStation customers under the primary commercial general liability and excess liability policies because, Zurich asserts, the customers’ claims are not covered by the ‘bodily injury,’ ‘property damage,’ or ‘personal and advertising injury’ provisions in the policies); *Arch Ins Co v Michaels Stores, Inc*, Case No 1:12-CV-00786, filed 23 Feb 2012 (ND Ill) (Arch sought declaratory judgment that the general liability policy it sold to Michaels Stores does not require coverage for customer data stolen by tampering with PIN pad terminals. Arch cites the electronic data and breach of contract exclusions, and also claims that the customers’ suits do not claim property damage, bodily injury, or advertising injury, as the policy requires; the case appears to be near settlement on undisclosed terms); *Retail Ventures Inc/DSW Inc v Nat Union Fire Ins Co of Pittsburgh*, PA, 691 F3d 821 (6th Cir 2012) (Insurer sought to avoid coverage under crime policy for losses caused by hacker who stole credit card data, but the Sixth Circuit disagreed, holding that third party losses were covered despite requirement that loss be ‘resulting directly from’ theft, and that exclusion for loss of ‘confidential information of any kind’ would not preclude coverage for theft of credit card information because to allow that result would vitiate the coverage the policy intended).  
63 *Recall Total Info Mgmt, Inc v Fed Ins Co*, No X07CV095031734, 2012 Conn Super LEXIS 227, filed 17 Jan 2012 (Conn Super Ct) (The insured, a third party provider of distribution services for IBM, lost data tapes containing personal data on 500,000 IBM employees, and sought coverage under its general liability and umbrella policies; the Court denied coverage because IBM sought damages for the lost electronic data, not the tapes themselves, and the policy defined covered property as only tangible property). See also *Union Pump Co v Centfrugal Tech, Inc*, Case No 05-0287, 2009 LEXIS 86352 (WD La, 18 Sept 2009) (CGL policy which covered only ‘tangible property’ held not to cover electronic data including design drawings and models).  
64 *Union Pump Co v Centfrugal Tech, Inc.*, Case No 05-0287, 2009 LEXIS 86352 (WD La, 18 Sept 2009) (CGL policy held not to cover claims that insured had used and destroyed plaintiff’s data due to intentional act exclusion).  
65 *State National Insurance claims no responsibility to pay for Global Payments’ breach costs*: http://www.databreaches.net/?p=27378  
66 *Compare United Westlavs, Inc v Greenwich Ins Co*, Case No 09C-12-048 MJJ, 2001 De Super LEXIS 261 (Del Super, June 13, 2011), aff’d, Case No 337, 2011, 2012 Del LEXIS 130 (Feb 28, 2012) (policy intended to cover cyber and technology held not to cover lawsuit initiated prior to policy period involving continuous series of related acts) and *Tagged, Inc v. Scottsdale Ins Co*, Case No JFM-11-127, 2011 US Dist LEXIS 75262 (SD NY, May 27, 2011) (dismissing declaratory judgment action and finding no coverage based on professional services exclusion in the D&O Coverage Section of policy issued by Scottsdale to Tagged, a social networking site targeted to teenage users, because the site falsely advertised that it had features in place to remove sexually explicit and predatory content and conduct from its website) with *St Paul Fire and Marine Ins Co v Compaq Computer Corp*, 539 F3d 809 (8th Cir 2008) (technology E&O policy covered ‘error,’ which as defined included insured’s alleged unintentional selling of defective computers). Another case involving an E&O policy remains pending, See *Vonage Holdings Corp v Hartford Fire Ins Co*, Civ No 11-6187 (US Dist Ct NJ 2012) (Vonage suffered loss over $1M due to server hacking but insurer denied coverage because losses were not tangible property; case remains pending).  
Similarly, in *Retail Ventures*[^68], the Sixth Circuit found third-party coverage under a first party commercial crime policy despite language stating that only direct losses would be covered. However, clients should not take comfort from the Sixth and Eighth Circuits decisions in *Eyeblister* and *Retail Ventures*, because both cases are far from clear and are limited to the unique facts involved in the claims at issue. In light of the high stakes involved, a cyber policy which clearly covers first and third party, non-tangible losses is the prudent choice.

Many insurers also endorse their professional indemnity/errors and omissions policies with typical cyber extensions that attempt to pick up third-party liability exposures that may arise from data breaches typically for financial institutions, IT industry and professional firms. Whilst it is easy to opt for the same, there are certain disadvantages latent in such a practice, not only does it erode/divert limits from core exposures but such approach does not usually grant first party coverages which are in most cases the first to be incurred following a cyber-attack.

Cyber exposures have the potential to affect the entire spectrum of risks – from physical property that is vulnerable to attacks from ‘Stuxnet’ like computer viruses, to products that contain chips with embedded software, to degradation or complete failure of critical infrastructure stakeholders.[^69] As a result, cyber events have the ability to impact numerous lines of insurance coverage.[^70] Consider some of the issues related to insurance coverage afforded under traditional policies of insurance and under cyber policies for a cyber event. Insurers are stakeholders because their coverage obligations may be triggered under various policies of insurance after an accident, disaster, cyber event or the cataclysmic meltdown of national critical infrastructures. Insurers can help manage cyber risks and offer insurance coverage for losses and claims arising from cyber events. However, not all risks or claims are covered and some insurers are limiting or excluding coverage afforded under traditional policies, and even some cyber policies may have narrowly tailored coverages. Thus, all insurance policies and coverages should be thoroughly reviewed and the provisions and conditions for coverage should be understood by all parties to the insurance contract.

The majority of developments to date on the cyber risk transfer front relate to privacy or data breach risk, and specifically, breaches of Personally Identifiable Information (PII). Many breached entities and other responsible parties have been aided tremendously by their insurance policies.[^71] Privacy, however, is only a fraction of the entire cyber spectrum, and companies that are not consumer facing or do not participate in the PII chain are struggling with the insurability of their cyber risk. Consider also that while annual cyber premiums may exceed USD 1 billion on an annual basis[^72], annual commercial property and general liability premiums are in excess of USD 151 billion.[^73] Defined cyber premiums account for a mere 1/151th of property and casualty risk transfer and 1/667th of non-life premiums in an economy where more businesses put a higher value on intangible assets than on traditional assets like plant, property, equipment and inventory.

The insurance industry is continuing to embrace evolving cyber risks in an effort to provide true end-to-end solutions that provide confidence to policyholders that the majority of cyber risk is covered. The insurance industry can serve as a catalyst and facilitator to significantly improve cyber security solutions.[^74]

---

[^68]: See also *Owners Ins Co, v European Auto Works, Inc*, 2012 WL 4052406 (8th Cir Sept 17, 2012) http://caselaw.findlaw.com/ us-8th-circuit/1612035.html (Eighth Circuit required insurer to cover insured’s $2 million settlement in a junk fax class action); and *Landmark Amer Ins Co, v. Gulf Coast Analytical Labs*, 2012 US LEXIS 45184 (Louisiana) (Court denied summary judgment for insurer where a different company’s data had been corrupted).

[^69]: The US Department of Commerce has described cyber security insurance as a potentially ‘effective, market-driven way of increasing cyber security’ because it may help reduce the number of successful cyber attacks by promoting widespread adoption of preventative measures; encouraging the implementation of best practices by basing premiums on an insured’s level of self-protection; and limiting the level of losses that companies face following a cyber attack. http://www.dhs.gov/publication/cybersecurity-insurance

[^70]: The Securities and Exchange Commission requires public companies to report to its shareholders any ‘material losses’ from cyber attacks, plus any information, ‘a reasonable investor would consider important to an investment decision.’ SEC guidance promulgated October 13, 2011 (not mandatory) suggests that such disclosure include the impact of cyber insurance coverage.


Cyber exposure spectrum

- First-party financial loss – the party that experienced the cyber event suffers financial losses or costs associated with the event. The most commonly cited examples include costs associated with data breach response, lost income attributable to network/IT interruption, as well as future lost income and reputational harm. Note that the policy holder should request that the first party business interruption triggers upon partial degradation and not simply a total network outage.

- Third-party financial loss – a party other than that which experienced the cyber event suffers financial losses or costs associated with the event. This could be a customer, business partner or unrelated third-party. Examples of losses in this category include the business interruption losses of users of cloud services should such services suffer outages, or recall costs of clients of electronic component manufacturers should such components malfunction due to the failure of embedded code and not any tangible damage.

- First party bodily injury or property damage – the party that experienced the cyber event suffers bodily injury or property damage.

- Third party bodily injury or property damage – a party other than that which experienced the cyber event suffers bodily injury or property damage.

Current cyber market

- Privacy breach coverage\textsuperscript{75} – policies cover privacy breach notification and crisis management, regulatory defense and civil penalties, and liability resulting from a breach.
  - Premiums are fact specific depending upon deductible/self-insured retention, losses, revenue, scope of business and risk mitigation employed.

In general, Asia based companies are charged significantly less premium per million dollars of limits than their European or United States counterparts. Based on deductibles of USD 25,000 – USD 100,000 for small companies with revenue less than USD 100 million and deductibles of USD 250,000 – USD 10 million for large companies with

\textsuperscript{75} These prices are estimates based on averages. The actual price of policy can vary drastically depending on the industry, size of the company, and specific circumstances.
revenue greater than USD 100 million, we make the following generalisations, which must be adjusted depending upon your specific situation.

In the wake of several massive breaches with claims made in 2014, some classes of business that have seen losses and hold or process a large amount of personally identifiable information, are now viewed as a greater risk. Prior to the Target and Neiman Marcus breaches, standalone cyber insurance capacity was increasing as new carriers entered the market, particularly targeting middle market and smaller organisations. As a result, pricing and availability is competitive for small to medium enterprises’ (SME) (e.g. USD 5,000 – USD 15,000 per million of limits, with some 2014 Q1 SME renewals seeing 5% - 10% premium reductions).

Retailers, financial institutions, hospitality, and payment processors, to name a few, are seeing 10 – 50% plus premium increases from a base of USD 20,000 – USD 50,000 per million of limits. The recent breaches are the first instances where several insurance carriers will pay cyber claims. As a result, a number of insurance carriers have reduced their capacity for any one insured and we are seeing less insurance carrier competition, (particularly for larger entities), plus large retention requests (e.g. increases from USD 1 million – USD 5 million plus) and exclusions from the few carriers that will consider a primary position. Other industry classes, such as manufacturers, non-IT service providers, education, pharmaceuticals and healthcare (although healthcare is suffering increased losses) have not yet felt the same wrath on an industry wide basis. More importantly, insurers are trying to use policy exclusions to deny coverage for fundamental exposure issues that have resulted in damages on average of USD 5.5 million per incident (according to the 2013 Ponemon Report), and average insurance claim payout of USD 3.5 million according to the 2013 Net Diligence Cyber Liability and Data Breach Insurance Claims Report.

However, it is well advised to jointly develop with each unique client a comprehensive list of specific priority coverage grants and dictate such requests to the insurance carriers in the form of a submission priority coverage matrix.

- Application process becoming streamlined whereby multiple carriers will quote pricing, terms and conditions based on one common application.76
- Policy wording is paramount to successful coverage.77 A lot of exclusions and pre-qualifications exist in cyber insurance. Experience in customised wording and claims handling is important
- Ancillary financial loss products – most available policies include first party network business interruption – to cover loss of revenue during network interruption; information asset – to cover restoration costs or loss of value associated with electronic data; cyber extortion – to pay an extortion threat if doing so successfully wards off a cyber event; and Contingent Business Interruption – to cover loss of revenue during the downtime of a critical outsourced IT provider (i.e. cloud services, etc.)
- Future loss of revenue products – currently developing coverage when the event ends and the firm returns to normal operations, but the negative reputational effect from the cyber event produces customer churn and a diminished ability to increase sales
- Property, comprehensive general liability (‘CGL’), crime/bond, director’s and officers, professional liability and kidnap and ransom, insurers should also be notified in the event of a cyber incident. Typical forms respond as follows:
  o General liability: covers bodily injury and property damage, not intangible or economic loss
  o Errors and omissions: covers economic damages resulting from a failure of defined services due to negligence only, and may contain exclusions for data and privacy breaches
  o Property: covers tangible property, which data is not. Loss must be caused by a physical peril while perils to data are more likely to be viruses or hackers
  o Crime: covers employees and generally only money, securities and tangible property. No coverage for third party property such as customer/client data

Review the “Notice” section of each potentially applicable insurance policy to ensure compliance with the timing, form and content of proper notice. Failure to properly notify pursuant to the terms of each policy could result in insurance carriers attempting to deny an otherwise covered claim.

---

Adding cyber coverage to traditional insurance

Beyond these four areas of risk transfer, coverage is either unavailable entirely, uncertain, or unavailable in a quantity that matches the magnitude of the risk. The most concerning area is likely coverage for cyber resultant bodily injury and property damage risks given exclusions found in policies designed to cover those risks – which are intended to exclude claims related to the loss or destruction of electronic data. However, the manner in which such exclusions are construed presents the possibility that they could be used to deny coverage for a loss that originated from a cyber-attack or virus. Consider the following exclusion, which is typically inserted in both property and general liability insurance policies:

**Damages arising out of the loss of, loss of use of, damage to, corruption of, inability to access, or inability to manipulate electronic data.**

---

78Recent cases illustrate the need for careful attention to insurance policies, as businesses battle with their insurers over coverage for network-related losses. Following hackers’ attack on Sony’s PlayStation Network (77 million records exposed) in April 2011, Sony has been engaged in a battle with its insurer, Zurich American Insurance Company, over whether its primary and excess Commercial General Liability (CGL) policy covered such a breach, requiring Zurich to defend or indemnify Sony. The remediation actions alone for the Sony breach are estimated to cost at least $171 million, and this legal battle illustrates why companies should consider separate privacy and security insurance to address these types of exposures. To be clear, the Zurich policies at issue were not ‘cyberliability’ policies, but rather only CGL policies, which are considered weak protection for covering security breaches. A copy of the Complaint for Declaratory Judgment can be found online at [https://apps.courts.state.ny.us/lbem/DocumentDisplayServlet?documentId=tirVqwp3WujFno1EqNuTA==&system=prod](https://apps.courts.state.ny.us/lbem/DocumentDisplayServlet?documentId=tirVqwp3WujFno1EqNuTA==&system=prod)
Based on the defined cyber policies that are available and uncertainty surrounding traditional coverage, the representation of cyber insurability as it currently exists is as follows:

<table>
<thead>
<tr>
<th>Firm X</th>
<th>Third-party</th>
</tr>
</thead>
<tbody>
<tr>
<td>Revenue loss due to network business interruption, information asset loss, first party data breach mitigation</td>
<td>Financial damages or loss due to failure of technology or software to perform as intended, third-party financial damages from a data breach, data breach related regulatory fines and penalties, &quot;contingent regulatory&quot; losses, recall costs where no tangible damage in end product occurs</td>
</tr>
<tr>
<td>Revenue loss due to property damage events</td>
<td>Third-party recall costs associated with tangibly damaged goods or products</td>
</tr>
<tr>
<td>Revenue loss due to theft of trade secrets/intellectual capital and introduction of competing products into marketplace, criminal fines and penalties</td>
<td>Third-party damage or bodily injury losses where products directly cause loss. Should be covered under general liability, products/recall policies</td>
</tr>
<tr>
<td>Covered under property, general liability and workers comp programmes</td>
<td>Contingent bodily injury and property damage losses due to the failure of technology or software products (no direct damage)</td>
</tr>
</tbody>
</table>

This has resulted in vastly disparate cyber insurance purchasing trends. Consumer facing industries have led the charge (mainly specific to ‘privacy’ coverage), and various estimates put adoption rates between 20% - 60% for certain segments – financial, healthcare, retail and hospitality. Beyond those industries, uptake is more limited. Business-to-business firms (predominantly technology centric) that participate in the personally identifiable information (PII) chain can blend cyber coverage into a commercial errors and omissions policy to contemplate a large percentage of the risks, but such firms continue to struggle to identify their exposures and the related insurability. For firms that do not fit this classification, buying drops off precipitously – and while knowing that their cyber exposures are significant, companies in industries such as manufacturing, industrial and critical infrastructure are struggling with the available products as well as the debatable nature of their existing coverage. New vulnerabilities will develop as cars, home appliances and other physical objects become integrated into information networks.

Another significant problem is limit sufficiency, which is adequate for 90% of organisations, but not high enough to provide catastrophic coverage levels required by large firms involved in critical infrastructure, since the total cyber insurance capacity per insured is USD 200 million to 300 million.

While underwriting for privacy and related financial loss products is good (and usually under one roof), know-how and consistency for more traditional products drops off significantly. This dynamic is further exacerbated by the silo approach at many insurers whereby the cyber underwriters don’t interact with their counterparts in other divisions. This ultimately results in everything ranging from flat out cyber exclusions to shaky coverage extensions and attempted clarifications to responses from traditional underwriters that, “you need a cyber policy for that” – when the fundamental nature of the risk should fall within the boundaries of traditional property and general liability policies (i.e. the yellow areas of the risk quadrant)

---

79 Internet of Things, infrastructure attacks are big security headaches. CIA Director John Brennan, February 2014.

© 2014 Aon Risk Solutions, Asia

28
Captive cyber reinsurance

A few entities have placed broad customised wording cyber insurance through their already established captive. Thereafter, some of such entities have reinsured the placement through traditional Cyber insurers while a few have elected to retain the risk themselves in the captive without reinsurance. Tax, jurisdiction, administrative, legal and claims handling issues must be considered with respect to this type of captive usage.

Stand-alone risk transfer product

Cyber insurance coverage is growing at a brisk pace in those countries where a mandatory data breach disclosure law is in place. There is a significant correlation between the timing of the effective date of data breach disclosure laws, lawsuits by individuals and entities that have been affected, and the subsequent purchase of cyber insurance. As set forth previously, the base coverages generally include:

1st party coverage

- Network business interruption: loss of income and extra expense due to network security failure
- Breach event notification/management costs associated with:
  - Statutory notification requirements, including the hiring of outside law firms and public relations consultants
  - Credit monitoring/protection
  - Notification hot line/call center
  - Forensic costs
  - Identity theft resources
- Cyber extortion

3rd party coverage

- Wrongful disclosure of personally identifiable information, protected health information or confidential corporate information in the client’s care, custody and control via a computer network or off-line (e.g. via laptop, paper records, disks)
- Failure of computer network security to guard against threats such as hackers, viruses, worms, Trojan horses and denial-of-service attacks whether or not resulting from the provision of professional services
- Content liability perils such as defamation and infringement of intellectual property rights arising out of website, marketing and advertising activities
- Security or privacy breach regulatory proceedings (including associated fines and penalties)

Risk managers and legal counsel must take a closer look at how the cyber policy language would respond to specific circumstances, such as following:

- Does the coverage include services with the insurance, such as third party forensics, credit monitoring, crisis management and legal advice in the event of a breach?
- Does the insurance cover liability of the insured due to incidents caused by an outsourced third-party service provider?
- Are regulatory investigations, fines and penalties addressed?
- Is first party business interruption and crisis management included? Are there sub-limits or full limits?
- How do the benchmarking limits compare to peers to help satisfy board fiduciary duties?

An additional development over the past 18–24 months is the growth of cyber insurance policies that include data breach response services within the policy. Instead of the insured having to research and go out and find remediation experts, some insurance carriers provide the following services as part of their insurance solution:
- Breach prevention IT security tools and educational mitigation workshops
- Legal assistance
- Data breach response correspondence fulfillment
- Call center support
- Forensic experts
- Credit monitoring to mitigate Identity Theft risk following a breach

Many smaller entities have found such ‘pre-packaged services’ to be valuable. Contrarily, some larger entities have been surprised to find out that they have given up to their insurer key material decision making authority and control following a breach.

**Cyber claims**

A good guide to an insurance policy purchase decision lies in an analysis of the cyber claims and actual payouts. If we were to analyse by the number of attacks, it would seem that the attacks are concentrated on smaller entities and this could be because of factors including, inadequate resources to put an effective cyber risk management process in place and lack of awareness and attention from senior leadership.

Though mega cap and large cap companies accounted for only 5% of the claim events, they were responsible for 48% of the records exposed, which illustrates the magnitude and severity of cyber claims. Clearly, mega market cap and large market cap companies account for a large percentage of actual claim payouts as evidenced by the graph below.

---

The data relating to Cyber claims is extracted from The NetDiligence Cyber Claims Study 2013.  

---

© 2014 Aon Risk Solutions, Asia
Another interesting finding from the NetDiligence Cyber Claims Study 2013 was in relation to the type of costs that were most frequently incurred by the victims of a cyber-attack. Most companies have claimed crisis management costs from their insurers and this is not surprising given that companies in the immediate aftermath of an attack will look for forensic, legal and public relations services to help them handle the adverse consequences of an attack. Broken down further from the sample size, 75.8% organisations claimed for forensic costs, 63.6% for notification costs, 50% for credit monitoring and/or identity theft remediation and 80.3% for legal guidance.

Whilst many of the Asian regulations do not provide for mandatory notification to data subjects, the necessity of engaging forensic, legal and public relations experts is likely to be felt by organisations irrespective of their geographical and regulatory environments.
The future of cyber insurance

USD 1 billion (or more) of ‘Cyber Complete’ coverage is being developed, which would span the entire spectrum of exposure as identified above, except for areas that are difficult to insure (or entirely uninsurable) such as patent infringement, criminal fines/penalties and the theft of trade secrets and the actual “value” of intellectual capital. Coverage would be structured as catastrophic protection with substantial retentions (equivalent or greater to those taken on property programmes), but firms would maintain the ability to infill such retentions with smaller policies for privacy breach mitigation, defense costs and any other areas where stand-alone policies can be structured.

Given the size of the programmes, we anticipate that a syndicated structure (in the large property model) could work best, with each insurer or re-insurer sharing proportionally in loss from the ground up. As for the rest of the dynamics required in order to create this structure:

- Underwriting approach and expertise – We envision an approach similar to what various top insurers deploy in the property world – engineers that evaluate/assist clients with risk rather than just offering insurance. In this case the approach would involve top IT professionals with expertise tied to the various domains of the underwriting framework as further described below. We believe that this is critically important in order for the participating insurance carriers to gain confidence that risks are being evenly and expertly evaluated, and that the baseline evolves in accordance with the constantly changing nature of the cyber world.

- Underwriting and policy compliance framework – The underwriting and policy compliance framework needs to be enterprise-wide and inclusive of both physical and IT security. This will allow for a far better and more comprehensive analysis; rather than focusing on granular elements such as firewalls and anti-virus software, the approach needs to evaluate critical domains such as enterprise assets, cyber governance, external threats, internal threats, regulatory compliance and event preparedness. The framework needs to constantly evolve based on the changing threat climate; this will not be a standard that is instantly outdated and one that gives firms the ability to achieve minimum compliance and ‘check the box.’ Additionally, and as further described below, the framework will form the basis for dynamic interaction between insurers and policyholders.

- Link to reputational risk – It is important that the framework needs to tie to, and therefore evaluate the reputational profile of the Insured. Aon’s research shows that firms with outstanding reputational rankings that suffer significant cyber events will recover far more quickly and effectively than firms that rank poorly.

- Information sharing and dynamic interaction – We believe that the insurance industry sits on a treasure trove of information that, if used appropriately with the right precautions, could be utilised for the benefit of all parties involved. Numerous insurers underwrite the cyber risk of firms across all industries and see claim activity in close to real time and have more insight into the macro cyber climate than most security providers who generally focus on narrow verticals. This data should be used to evolve the framework and by establishing certain compliance thresholds, policyholders would be incented to continually improve their security posture in order to maintain coverage.

Given the exposures and constantly evolving risks associated with cyber events that could cripple companies, industries and critical infrastructures, prudent insureds should review their insurance programme with their insurance broker and seek out professionals who understand the cyber insurance market before those catastrophic cyber events take place. Relying on traditional insurance to protect against cyber events is wishful thinking. Due diligence and due consideration should be undertaken so that all companies can understand the insurance coverage they have and just as importantly, understand what cyber insurance coverage they deliberately decided not to purchase for their cyber liability risk management programme. Additionally, the financial strength of the insurers should be considered because in the event that multiple critical infrastructures are taken down, an insurer may be have to pay too many or a number of large claims that may impact its surplus and impede its ability to pay all claims. A competent insurance broker can help companies understand the options and alternatives for cyber insurance thereby giving the insured the proper information to make an educated decision as to what type and how much insurance will be in place for the next big cyber catastrophe.

---


Authors

Kevin P. Kalinich, Esq.
Global Practice Leader – Cyber Insurance
Aon Risk Solutions
kevin.kalinich@aon.com

Uttara Vaid
Regional Director – Aon Financial Services & Professions Group
Aon Risk Solutions, Asia
uttara.vaid@aon.com

This report is for general informational purposes only and is not intended to provide individualised business or legal advice. The information contained herein was compiled from sources that Aon considers to be reliable; however, Aon does not warrant the accuracy or completeness of any information herein. Should you have any questions regarding how the subject matter may impact you, please contact your legal, financial or other appropriate advisor.