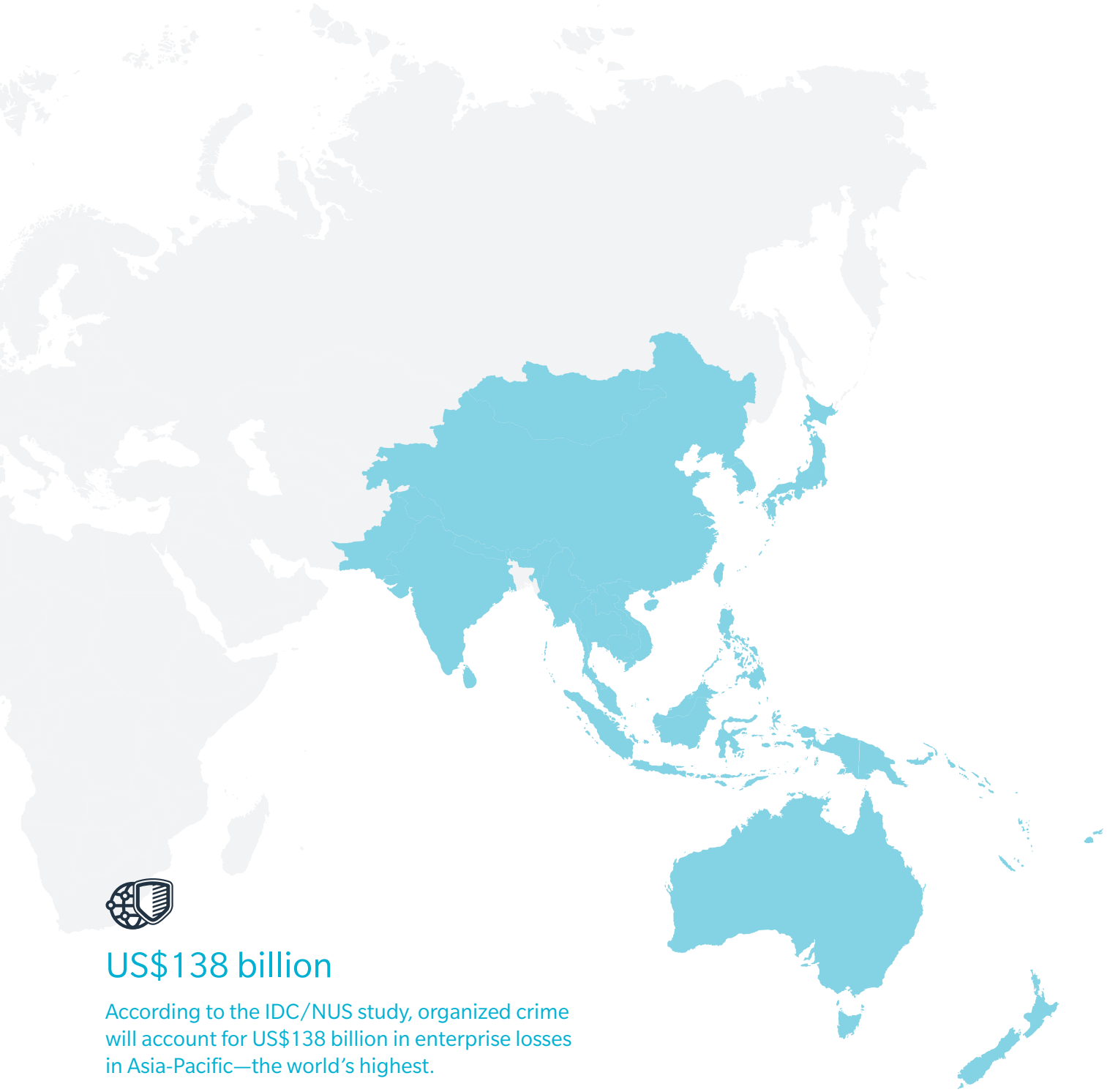
MARSH

CYBERCRIME IN ASIA:
A CHANGING REGULATORY ENVIRONMENT

SOLUTIONS...DEFINED, DESIGNED, AND DELIVERED.

MARSH & McLENNAN COMPANIES



US$138 billion

According to the IDC/NUS study, organized crime will account for US$138 billion in enterprise losses in Asia-Pacific—the world's highest.

Asia-Pacific enterprises are expected to spend US$230 billion to deal with cyber security breaches in 2014—the highest for any region—according to a study conducted by International Data Corporation (IDC) and the National University of Singapore. As the extent of commerce transacted over cyberspace continues to grow, along with increasing reliance on information technology to derive cost-efficiencies, the risk exposures to enterprises have increased.

Asia also accounted for 8 of the top-10 countries most vulnerable to cybercrime, according to the *2013 Security Threat Report* published by cyber security company Sophos.

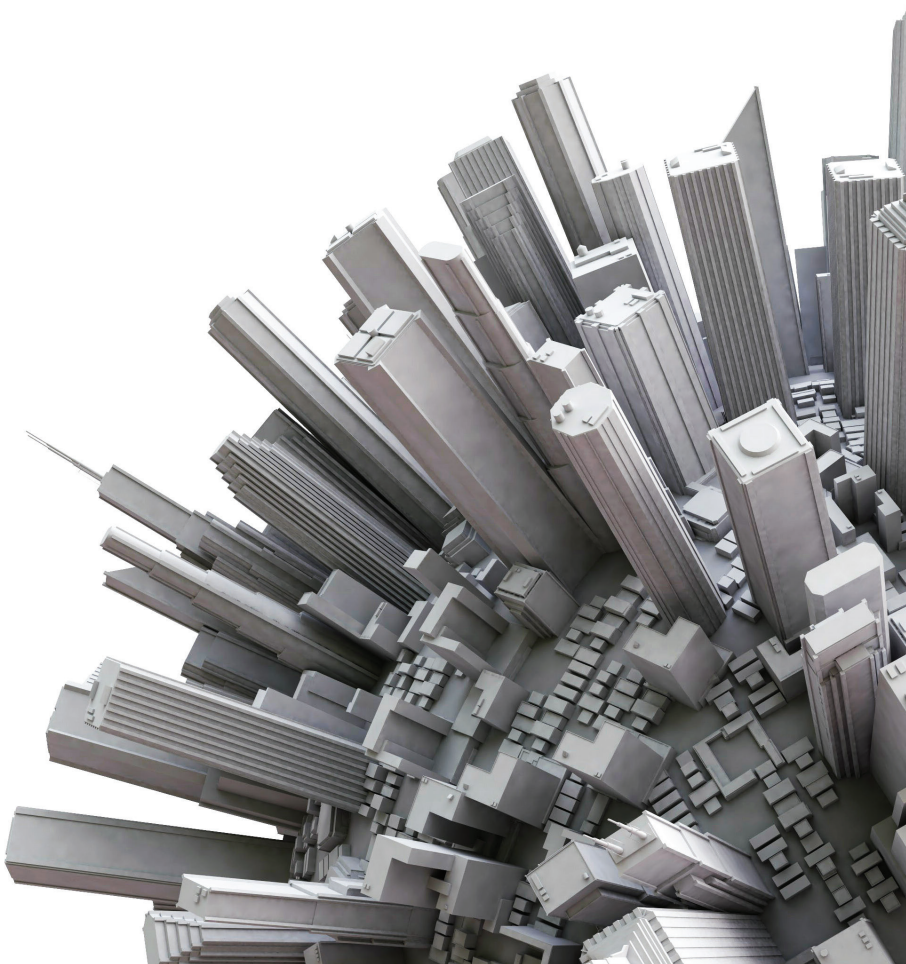
TODAY'S RISK ENVIRONMENT

Years ago, cyber threats came from viruses and relatively unsophisticated hackers. Over time, however, the techniques employed by hackers have become more and more sophisticated. Hackers have kept pace with advances in technologies and have continued to beat efforts to firewall them out.

Cyber risks can take many forms. A massive data breach can invite litigation, cause regulatory fines, and instigate law enforcement investigations. A distributed denial of service (DDoS) attack can halt a company's operations or cause technology or software outages, thereby having a direct impact on its revenue, and worse still, its reputation. Companies also face the risk of losing business trade secrets or competitive information.

At the same time, governments around the world are grappling with threats to their confidential information. It has been estimated that costs associated with malware from pirated software could cost governments around the world more than US$50 billion.

There have been a number of cases around the world in the last year where sensitive customer information has been compromised. In one case, hackers successfully siphoned data from credit and debit cards that were collected at point of sale systems. Even technology companies, which should be at the forefront in implementing advanced protective tools, are not immune. A major software company early this year reported that hackers stole the source codes to some of its most popular software applications, as well as data relating to millions of its customers.



THE NEW FRONTIER FOR CRIMINALS

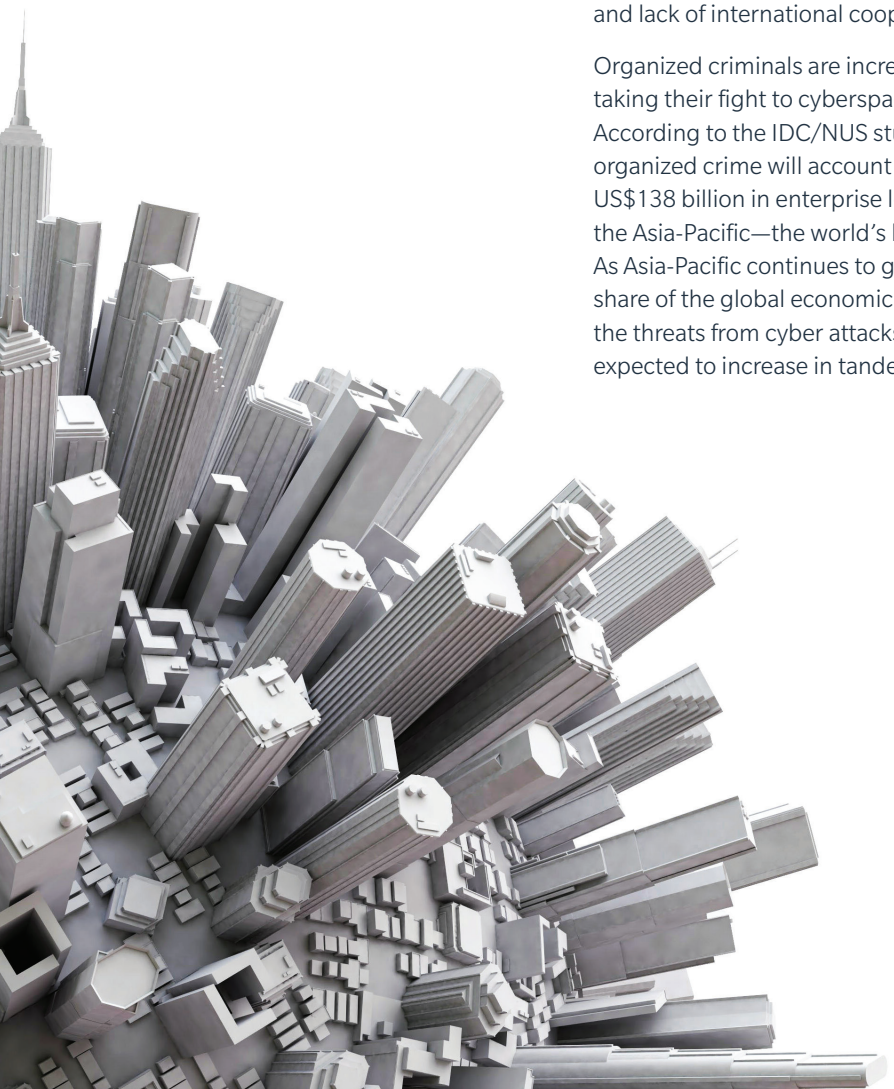
As organizations increasingly embrace emerging technologies, new areas of risk exposures are being created. Mobile devices and cloud computing present new data security exposures, for example. The obvious threat from tablets and mobile phones is that the devices themselves could be stolen, along with the valuable data they hold. Cloud computing is a particularly perplexing area as data can be now be stored in any part of the world. Besides the fact that they are more vulnerable to attacks, the issue is further complicated by varying privacy laws from territory to territory and lack of international cooperation.

Organized criminals are increasingly taking their fight to cyberspace. According to the IDC/NUS study, organized crime will account for US$138 billion in enterprise losses in the Asia-Pacific—the world's highest. As Asia-Pacific continues to grow its share of the global economic pie, the threats from cyber attacks are expected to increase in tandem.

Regulators have two major challenges confronting them. The first is that of protecting the privacy of individuals and their personal information; the second is the more encompassing challenge of data security—protecting the integrity of systems and the data they contain, including that relating to their customers. Regulators have the mandate of ensuring that commercial and government organizations put in place the necessary infrastructures to protect individuals' data. Regulatory structures across Asia vary in terms of their approach as well as the stage of development they are in.
The authorities are being put to the test significantly due to the efforts of groups such as the international network of hackers called Anonymous.

Some countries have, for years, had data protection laws in place which focus on individuals' personal information. These laws are now being extended further, as ensuring data privacy cannot be accomplished without considering the larger issue of data security.

The following pages include a summary of recent cybercrime cases in Asia, as well as government responses to the issue.



CHINA

Cybercrime statistics

- It has been estimated that the annual cost to China's economy from cyber attacks is in the tens of billions of RMB.
- In the first eight months of 2013, more than 20,000 China-based websites were hacked, and more than eight million servers hijacked by Zombie and Trojan programs controlled from overseas.
- Police arrested a 10-member gang in Beijing and Shanghai for illegally obtaining and selling close to one million records of personal information, and making RMB320,000 in illegal profits.
- Employees of a leading Shanghai courier firm sold millions of items of personal information, including customer names, addresses, telephone numbers, and transaction serials numbers to online traders.
- The employee of a local taxation bureau in Wuhan copied and sold millions of items of personal data extracted from the Intranet to third parties.

Government & regulatory responses

While China has one of the world's largest team of hackers by numbers, ironically when it comes to fighting cybercrime, it lags behind the US, Europe, and even some Asian countries, such as Hong Kong and Singapore.

However, this is expected to change as Chinese President Xi Jinping announced in February 2014 that he will spearhead the fight against cybercrime by putting himself in charge of a newly formed body to coordinate cyber security. This new body will draft policy for boosting the country's defense against cybercrime as well as expanding and improving Internet access.

Relevant laws

- The P.R.C. Tort Liability Law.
- The Criminal Law and its Amendment VII.

RMB320,000

Police arrested a 10-member gang in Beijing and Shanghai for illegally obtaining and selling close to one million records of personal information, and making RMB320,000 in illegal profits.

HONG KONG

Cybercrime statistics

- While overall crime rates in Hong Kong fell to a 10-year low in 2013, cybercrime cases, by contrast, grew by 70%.
- Losses from corporate email scams increased three fold in 2012, to HK$760 million, the most significant of which amounted to HK$75.2 million.
- Hong Kong police have acknowledged that cybercrimes are the hardest to detect and the most difficult to solve.
- One of the most telling instances with regards to the seriousness of cybercrime is the case of a major international bank which, in 2008, lost a computer server containing the transaction details of 159,000 account holders. Many of the affected customers subsequently moved their accounts to other banks.

Government & regulatory responses

Hong Kong was one of the first Asian territories to institute comprehensive data privacy regulation—in 1996. Following a prominent direct marketing scandal in 2010, Hong Kong implemented further regulations in 2013 and put in place what is today considered to be one of the most rigorous regulations of direct marketing in the world.

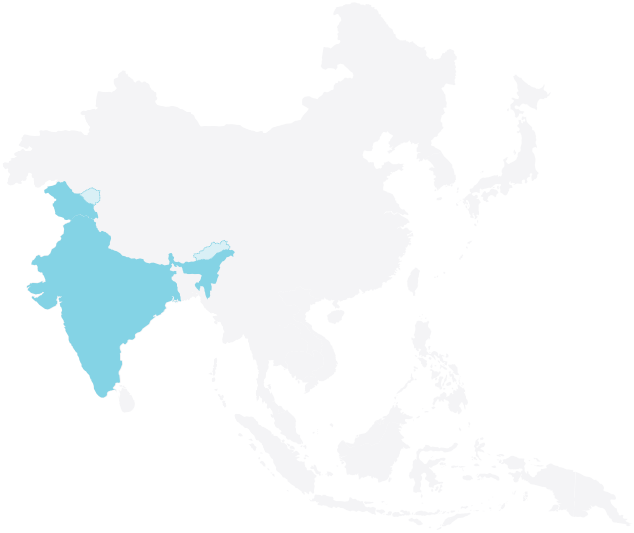
Relevant laws

The primary legislation in Hong Kong against computer crime is the Computer Crimes Ordinance. In recent years, through amending the Telecommunications Ordinance (Cap. 106), Crimes Ordinance (Cap. 200), and Theft Ordinance (Cap. 210), some new offences have been named as crimes and the coverage of existing offences broadened as follows:

- Obtaining unauthorised access to computers has been included in the Telecommunications Ordinance S. 27A, Cap. 106.
- Under Crimes Ordinance S. 59, Cap. 200, the meaning of property has been extended to include any program or data held in a computer or in a computer storage medium.
- Under Crimes Ordinance S. 59 and 60, Cap 200, the meaning of criminal damage to property has been extended to include misuse of a computer program or data.
- Obtaining access to a computer with intent to commit an offence or with a dishonest intent has been included under Crimes Ordinance S.161, Cap 200.
- Under Crimes Ordinance S.85, Cap. 200, the meaning of making a false entry in a bank book has been extended to include falsification of the books of account kept at any bank in electronic means.
- Under Theft Ordinance S.11, Cap, 210, the meaning of burglary has been extended to include unlawfully causing a computer to function other than as it has been established and altering, erasing, or adding any computer program or data.
- Under Theft Ordinance S.19, Cap. 210, the meaning of false accounting has been extended to include destroying, defacing, concealing, or falsifying records kept by computer.

Other relevant laws include:

- The Electronic Transaction Ordinance.
- The Personal Data (Privacy) Ordinance.



INDIA

Cybercrime statistics

- India has been ranked among the top-5 countries to be affected by cybercrime, according to a report by Symantec. In addition, a Norton report named India as the "ransomware capital of the Asia Pacific."
- A recent government commission report said cybercrime cost India US$4 billion in 2013.
- The e-commerce industry in India has become the second largest target for distributed denial of service (DDoS) attacks by hackers, with a 2.6% increase in attack traffic in the first quarter of 2014.
- As of June 2013, 78 government websites have been hacked. Some of the attacks allegedly emanated from Pakistan.
- According to the Norton report, Indian citizens and corporations lost Rs 50,400 crore to cyber fraud in 2012. The report also said that 63% of smart phone users in the country have experienced some form of mobile cybercrime in the 12 months preceding the report's release.
- In 2013, two Indian-based companies that processed credit card payments for Middle Eastern banks were described as the "weak links" that enabled hackers to make a US$45 million global cyber heist by manipulating balances and withdrawal limits on bank accounts.
- India's Central Bureau of Investigation (CBI) caught its first cyber criminal ever in 2013. Amit Vikram Tiwari is allegedly the owner of two websites providing services that include breaking into email accounts.

Government & regulatory responses

The Information Technology Act of 2000 addresses a range of cybercrimes, such as hacking, viruses, email scams, DDoS, forgery, cyber terrorism, identity theft, phishing, and e-commerce fraud.

In 2013, the government went one step further by announcing a National Cyber Security Policy aimed at setting up an agency to protect the public and private infrastructures from cyber attacks and safeguarding the personal information of web users, financial and banking information, and sovereign data. How this policy will be executed remains to be seen. India is also working on a new piece of legislation on privacy, which provides for the protection of data and personal privacy.

Relevant law

- The Information Technology Act, 2000.
- Information Technology Act Amendment (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.
- RBI Regulation: DBOD.COMP.BC. No. 130/07.03.23/2000-01.

US$45 million

In 2013, two Indian-based companies that processed credit card payments for Middle Eastern banks were described as the "weak links" that enabled hackers to make a US$45 million global cyber heist by manipulating balances and withdrawal limits on bank accounts.

INDONESIA

Cybercrime statistics

- *The Security Threat Report 2013* published by Sophos ranked Indonesia number one on the list of countries most vulnerable to cybercrime.
- A group identifying itself as Anonymous Indonesia hacked into and defaced more than 12 government websites in 2013.
- In October 2013, 25 foreigners and three Indonesian women were arrested for their involvement in an email scam totalling Rp30 billion.

Government & regulatory responses

Indonesia's current legal framework to deal with cyber security is weak. The two acts that are in place—the Telecommunication Act No. 36/1999 and the Transaction Act No.11/2008—are lacking in detail, especially in the context of the plethora of cyber risks that are emerging in the country. To deal with cybercrime, other acts are frequently relied upon.

Relevant law

- The Electronic Information and Transaction Act.

Rp30 billion

In October 2013, 25 foreigners and three Indonesian women were arrested for their involvement in an email scam totalling Rp30 billion.

JAPAN

Cybercrime statistics

- According to Tokyo's National Institute of Information and Communications Technology, there were 12.8 billion cyber attacks in 2013, the highest ever in the country's history.
- The hacktivist group Anonymous has warned the country of cyber attacks if it continued with whaling activities. Anonymous has on several occasions threatened or carried out attacks on consumer giant Sony, targetting its popular Playstation network.
- "Drive by downloads," which refer to cyber attacks launched by just visiting seemingly innocuous websites (without the need to click on anything on the website), are more active in Japan than in any other country in the world. In the first half of 2013, there were twice as many cases than for the same period in 2012. Such attacks target individuals' financial assets and personal information.
- Mitsubishi Heavy Industries and Japan's parliament, space agency, and foreign and finance ministries have all been targets of cyber attacks since 2011.

Government & regulatory responses

As of March 2014, the government has been considering a new law granting the National Information Security Centre (NISC) and the Government Security Operation Coordination team (GSOC) with powers to cut through bureaucracy when dealing with cyber threats.

While the government has divided responsibilities among the various ministries, the NISC will be reorganized to become the authoritative Cyber Security Centre by 2015. By 2020, the government intends to double the size of the domestic information security market, and also address the dearth in talent in this area. The NISC's Cyber Security Strategy, released in June 2013, details the roles of the government, infrastructure providers, companies, individuals, and other operators in combating cybercrime.

Relevant laws

- The Act on the Protection of Personal Information.
- The Act on the Prohibition of Unauthorized Computer Access.

12.8 billion

According to Tokyo's National Institute of Information and Communications Technology, there were 12.8 billion cyber attacks in 2013, the highest ever in the country's history.

MALAYSIA

Cybercrime statistics

- In the first six months of 2013, losses due to lapses in cyber security and online fraud were in the region of RM1 billion.
- Cybercrime recently surpassed drug trafficking as the most lucrative type of crime. In addition, 70% of commercial crime cases are now categorized as cybercrime cases.
- Several dozen Nigerian nationals were arrested in a series of raids in December 2013 for cybercrimes, such as online fraud and scams.
- Types of cybercrimes in Malaysia consist of (in order of frequency) fraud, security breaches, spam, and virus attacks.

Government & regulatory responses

In order to keep legislation against cybercrime current, Malaysia is considering amendments to the Penal Code, Criminal Procedure Code, Evidence Act 1950, Computer Crimes Act 1997, and Cyber Crimes Act 2003.

Relevant laws

- The Communications and Multimedia Act 1998.
- The Personal Data Protection Act 2010.
- The Computer Crimes Act 1997.

RM1 billion

In the first six months of 2013, losses due to lapses in cyber security and online fraud were in the region of RM1 billion.

PHILIPPINES

Cybercrime statistics

- According to the Department of Justice, almost 9 out of 10 Internet users in the Philippines have been the victims of or targeted by cybercrime at some point.
- In August 2013, the police arrested 35 foreign nationals and 30 Filipinos in raids on cybercrime rings across Manila.
- In August 2012, more than 350 Chinese and Taiwanese nationals were arrested in what is considered to be the largest cybercrime crackdown in the country's history. The operation scuttled a massive bank account takeover scam targeted at individuals in China. Those arrested were charged with violating the Philippines Access Device Act, whereby the perpetrators used internet connected computers to call phones in mainland China posing as Chinese police to say their bank account has been used for money laundering. They then encouraged victims to transfer funds into a "safe account," which was provided by the scammers.

Government & regulatory responses

The Cybercrime Prevention Act of 2012 addresses legal issues concerning online interactions and the Internet in the Philippines, specifically, cyber squatting, cybersex, child pornography, identity theft, illegal access to data, and libel. However, the sections of the law criminalising libel came under heavy criticism as a restriction on freedom of expression, and subsequently, the Supreme Court (SC) issued a temporary restraining order stopping implementation of the Act for 120 days, pending further orders from the court.

In February 2014, the SC upheld the constitutionality of the provision criminalising online libel. The SC further ruled that only the source of a malicious email, or post on a social media can be held liable under the act. Other key provisions that the court declared to be constitutional included the sections penalizing illegal access, data interference, cyber squatting, computer-related identity theft, cybersex, child pornography, and allowing search and seizure of computer data.

The Cybercrime Prevention Act further repealed the penal provisions/clauses relating to hacking or cracking under the Electronic Commerce Act of 2000, providing for a more comprehensive list of offenses and penalties relating to the confidentiality, integrity, and availability of computer data and systems, other computer-related offenses, and content-related offenses, among others.

In March 2013, the Philippine National Police formed the Anti Cybercrime Group (ACG) to spearhead efforts in this area. The new unit is focused on cybercrime offenses, computer-related offenses, and other content-related offenses, including unsolicited commercial communication.

Relevant laws

- The Cybercrime Prevention Act of 2012 (R.A. 10175).
- The Data Privacy Act of 2012 (R.A. 10173).
- Electronic Commerce Act of 2000 (R.A. 8792).

9 out of 10

According to the Department of Justice, almost 9 out of 10 Internet users in the Philippines have been the victims of or targeted by cybercrime at some point.

SINGAPORE

Cybercrime statistics

- Overall crime rates fell to a 30-year low in Singapore, but remain consistent with the rest of the world. Cybercrime rates spiked in 2013.
- According to a 2013 Norton report, Singapore cybercrime victims had the highest average per capita losses worldwide in 2013, of US$1,158. This is four times the global average of US$287 and twice the figure set 12 months earlier in the country, which indicates the growth of the problem.
- Direct financial losses in Singapore due to cybercrime grew from US$944 million in 2012 to US$1 billion in 2013.
- The hacktivist organization Anonymous, through a member known by the online handle "the Messiah," hacked into various government websites, including the Prime Minister's official website in late 2013. In one single day, 19 government websites were taken down by the hackers.

Government & regulatory responses

Under Singapore's five-year National Cyber Security Master Plan, the Cyber Watch Centre and Threat Assessment Centre are being upgraded, with a view to strengthening critical infrastructures in the country.

The government has also launched an initiative to identify vulnerabilities and gaps in infrastructure, when exposed to cyber threats. In addition, exercises to test critical industry sectors, as well as their cyber security readiness are being planned. Finally, the government agency Infocomm Development Authority is working with Institutes of Higher Learning to incorporate security courses and degree programs into the curriculum.

The Personal Data Protection Act (PPDA) came into full effect in July 2014. This law comprises various rules for the collection, use, disclosure, and care of personal data. One of the key features of the new law is the establishment of a "Do Not Call" registry, which allows individuals to opt out of receiving marketing phone calls, mobile text messages, or faxes. Three basic principles underpin the PPDA: 1) the need for consent from the individual; 2) consistency between the customer and the company of the understood purposes for which the data is collected and used; and 3) reasonableness—the usage of the data in a manner appropriate to the circumstances.

Relevant laws

- The Computer Misuse and Cybersecurity Act.
- The Electronic Transactions Act.
- The Personal Data Protection Act.

US$944 million

Direct financial losses in Singapore due to cybercrime grew from US$944 million in 2012 to US$1 billion in 2013.

SOUTH KOREA

Cybercrime statistics

- Every year since 2010, South Korea has experienced more than 100,000 cases of cybercrime.
- Alleged attacks from North Korea have reportedly cost the country around 800 billion won in economic damages.
- The personal data of 20 million South Koreans (about 40% of the country's population, including President Park Geun-hye and UN Chief Ban Ki-moon) were stolen by a worker at the Korea Credit Bureau, a company offering risk management and fraud detection services, it was reported in 2014. The information stolen included personal identification and credit card numbers. Top level managers at the three banks most affected subsequently resigned. A class action suit was initiated in January 2014 against the credit card providers, expected to be the first of many litigations to come.
- IT systems used by many TV stations and banks crashed on March 20, 2013, supposedly due to the actions of hackers operating out of North Korea.

Government & Regulatory responses

In April 2013, the government announced the National Anti-Cyberterrorism Act, a legislative bill that proposed the establishment of a comprehensive pre-emptive line of defense to detect attacks in advance and address the threats early. The definition of what constitutes cyber terror was also significantly broadened by the act, to constitute any form of cybercrime.

The act provides the South Korean National Intelligence Service with power to create, vote on, and enforce anti-cyber terror policies.

Relevant laws

- The Personal Information Protection Act.
- The Act on Promotion of Information and Communications Network Utilization and Information Protection.
- The Use and Protection of Credit Information Act.

800 billion won

Alleged attacks from North Korea have reportedly cost the country around 800 billion won in economic damages.

TAIWAN

Cybercrime statistics

- In January 2014, after Taiwan launched its electronic freeway toll system, its mobile application was attacked by hackers.
- In the first six months of 2013, hackers launched more than 1 million attacks on the website of Taiwan's National Security Bureau.
- Hackers from mainland China have allegedly targeted Taiwan with data theft attacks for more than a decade.

Government & Regulatory responses

- The Computer-Processed Personal Data Protection Law was amended and renamed as Personal Information Protection Act (PIPA) on May 26, 2010, and came into full effect in October 2012. This law provides protection for individuals' personal information.
- Specifically, PIPA has dramatically increased the civil liability, criminal liability, and administration penalty for breaches, including:
  - Civil Liability—NT$500 to NT$20,000 compensation for each incident, per person, while no evidence of substantial damages shall be proved. The ceiling is NT$200 million. However, if the breach was for profit seeking purposes and damages exceed NT$200 million, the compensation will be calculated according to actual damages amount. Class action is permitted.
  - Criminal Liability—Not more than two years imprisonment and/or NT$200,000 fine, if no profit seeking purpose is proved. Not more than five years imprisonment and/or NT$ one million.
  - Administration Penalty—Not less than NT$50,000 but no more than NT$500,000 fine, then remediation action is completed. NT$20,000 but no more than NT$200,000—over the deadline without completion of remediation action after receiving the demand order each time.
  - The natural persons, juridical persons, groups, and its representative will be subject to the administration fine respectively under the same amount.
  - In addition to the fine, the local city government or Financial Supervisory Commission may also order, at its discretion, to prohibit the natural persons, juridical persons, or groups to collect, process, and use, or order to delete, or destroy personal data, or announce to the public about the violation of the natural persons, juridical persons, groups and their names and the name of the responsible person.
  - The natural persons, juridical persons, and groups should be liable for damages and compensation caused by illegal collection, processing, and use of personal information, or other ways of infringement on the rights of the Personal Information Owner due to violation of this act. However, it does not apply to the situation where the natural persons, juridical persons, or groups can be proved to be unintentional or non-negligent.
  - Class action law suits are also permitted under the act.
  - The provisions of this act are also applicable to the natural persons, juridical persons, and groups when they collect, process, or use the personal information of the citizens of the Taiwan outside the territory of Taiwan, the Republic of China.
  - Taiwan has responded to the attacks from across the Straits with the establishment of four cyber ware units.

Relevant laws

- The Computer-Processed Personal Data Protection Law.
- The Personal Information Protection Act.

THAILAND

Cybercrime statistics

- Thailand was ranked, along with Indonesia and China, among the top-three riskiest countries in the world for cybercrime, in the *Security Threat Report 2013* by Sophos.
- In March 2014, Thai police arrested a hacker wanted by Swiss authorities for compromising computer networks and websites belonging to Swiss banks, causing damages in excess of US$4 billion.
- In January 2013, Thai and American authorities, working together, arrested one of the world's top-20 bank hacking criminal masterminds in Bangkok; an Algerian responsible for defrauding tens of millions of dollars from the computer networks of 217 banks.

Government & Regulatory responses

Thailand does not currently have comprehensive data privacy or protection regulations in place. However, the government is currently reviewing a draft Personal Information Protection Act.

Thailand is also reviewing its Computer Related Crime Act BE 2550 that rolled out in 2007 and has been criticised for not covering a number of issues.

Relevant laws

- The Personal Information Protection Act (draft).
- The Credit Information Business Act.
- The Civil and Commercial Code.
- The Electronic Transaction Act 2001.
- Penal Code of Thailand Section269/1 – 269/7.
- The Consumer Protection Act 2002.

US$4 billion

In March 2014, Thai police arrested a hacker wanted by Swiss authorities for compromising computer networks and websites belonging to Swiss banks, causing damages in excess of US$4 billion.

VIETNAM

Cybercrime statistics

- More than 2,400 websites of Vietnamese government agencies and companies were hacked in the first nine months of 2013, according to a report by the *Vietnam Economic Times*.
- Virus attacks cause damages of around eight trillion dong to consumers every year.
- Vietnam is regularly cited as one of the top-three sources of malware.
- The industry group, Business Software Alliance, has estimated that around 81% of PCs in Vietnam use illegal or pirated software.

Government & Regulatory responses

Vietnam is setting up the National Center for Network Technology, with a US$42-million budget over the next decade. In addition, there are also plans to update laws relating to internet crime and security.

Relevant laws

- The Law on Telecommunications.
- The Law of Information Technology.
- The Law on Electronic Transactions.

8 trillion

Virus attacks cause damages of around eight trillion dong to consumers every year.

MARSH

For more information, please contact your Marsh representative:

CRAIG CLAUGHTON
NSW Manager
FINPRO
+61 2 8864 7788
craig.claughton@marsh.com

JEANNE FENNELL
Principal
FINPRO
+61 2 8864 7671
jeanne.fennell@marsh.com