SPECIAL REPORT:

CYBER RISKS

34 **Cyber attacks**
Cyber insurance policies have evolved, but cyber threats, which are on the rise, can still sneak up from many sides

35 **Big Data**
Large volumes of data can be difficult to manage, but the benefits are huge

MARSH

This report is sponsored by Marsh

Under attack

Asian risk managers are assessing the growing cyber threat to businesses

FROM *GOLDFINGER* TO *THE Man with the Golden Gun*, James Bond has faced some tough nemeses in his time. But in the latest of the Bond movies, *Skyfall*, the world's most famous fictional spy is pitted against a real danger of the contemporary world: cyber terrorism.

In the film, cyber attacks on the British government are launched from a deserted island in the Far East, where the villain is surrounded by computers. The scene bears some resemblance to reality, says Symantec director of security technology and response Kevin Haley.

"Cyber criminals are known to base their operations in less developed countries more lax on policing online security. With their servers protected by bulletproof hosting in these countries, the attackers are free to operate from anywhere," he says.

But while the film's antagonist boasts of his abilities to control national infrastructure at the push of a button, Haley says in reality it's not quite this easy. But he adds: "Computer worms like Stuxnet have already demonstrated their power to disrupt on an industrial scale. In 2010, hackers got into an Iranian uranium enrichment facility and programmed the cylinders in the facility to spin so fast, they cracked and broke."

It's clear that the cyber risk landscape is changing. Increasing state-sponsored criminality, data security and hactivism are among today's dangers. On 20 March 2013, for example, almost 50,000 computers and servers in South Korean broadcasters and banks were shut down in a co-ordinated cyber attack. The initial investigation pointed to a North Korean military spy agency.

A week later, the global community was hit by the largest ever cyber attack of its kind, resulting in a slowdown of internet speeds around the world. The attack – the result of a row between anti-spam organisation Spamhaus and a Dutch web-hosting firm – ranks as the biggest known distributed denial of service (DDoS) attack. DDoS attacks are among the most common to take place and involve overloading a target site with so much traffic that it is taken offline. Such attacks largely concentrate on customers in the business and financial services sector.

So do these high-profile events signal the start of a new cyber-based terrorism war?

Many risk managers in Asia are still assessing the potential impact of cyber issues on their businesses, as DFS Group Hong Kong-based vice-president, risk management, Bob Sweeney explains: "I'm still investigating it, and trying to determine what our exposures are. I am in the midst of a project right now with senior management trying to develop an approach to gathering the overall realm of information security. It goes beyond cyber. A better way of describing it is information security."

But are security systems keeping ahead of the curve? Experts agree that the cyber threat is growing.

The year ahead will feature increasingly sophisticated means to capture and exploit user data, escalating battles over the control of online information and continuous threats to supply chains from global sources. So says 2013's *Emerging Cyber Threats Report* from the Georgia Tech Information Security Center (GTISC) and Georgia Tech Research Institute. According to the report, specific threats over the coming year include:

1 Search history poisoning

Cyber criminals will continue to manipulate search engine algorithms and other automated mechanisms that control information presented to internet users. Moving beyond typical search-engine poisoning, GTISC researchers believe that manipulating users' search histories may be a next step in ways that attackers use legitimate resources for illegitimate gains. "If you compromise a computer, the victim can always switch to a clean machine and your attack is over," says GTISC director Wenke Lee. "If you compromise a user's search history, the victim gets the malicious search results no matter where he logs in from."

2 Cloud-based risks

Most businesses are more focused on the benefits of cloud-based services than the risks. According to the GTISC report, it will be critical for cloud service providers to spell out their responsibilities towards user data. A study by the Ponemon Institute found that 69% of cloud providers thought the customer was responsible for data kept in the cloud, while only 35% of cloud users agreed.

3 Mobile browser and wallet

Last year, global shipments of smartphones surpassed that of PCs, and mobile devices became the most popular way to access the internet according to the GTISC report. This shift in the way employees work and access information can have serious impacts for businesses as the personal and professional use of devices increasingly merge. GTISC's Lee points to the "explosive proliferation of smartphones". This, "will continue to tempt attackers in exploiting user and technology-based vulnerabilities, particularly with the browser function and digital wallet apps".

4 Malware counter-offensive

"The developers of malicious software will employ various methods to hinder malware detection, such as hardening their software with techniques similar to those employed in digital rights management and exploiting the wealth of new interfaces and novel features on mobile devices," the GTISC report says. It also points to Mac users' false sense of security and says attackers are honing their ability to compromise Mac operating systems and mobile-device platforms.

Protection against cyber dangers is becoming increasingly important on several levels, according to Marsh Financial and Professional Risks (FINPRO) Practice leader, Asia, Stella Tse.

"Cyber insurance coverage is increasingly being seen as a must-have by organisations. Historically, coverage was triggered when companies were the victims of data breaches or hacking attacks. But as cyber insurance policies have evolved, many now provide coverage for a broad range of technology failures," she says.

"It's important to remember, however, that cyber insurance should never be seen as a replacement for sound risk management.

Cyber attack

"Companies in Asia are becoming increasingly concerned about the potential for a cyber attack or data breach to cause reputation damage to their firms and are planning to become more proactive in managing their cyber risk exposures," says Tse.

"According to a survey of insurance buyers, conducted by Marsh at the Advisen Cyber Liability Insights event held in Singapore in April, risk managers are increasingly concerned about the perceived threat of cyber attack to their organisations, with 86% naming the risk as 'critical'. Asked to identify the top issue stemming from a cyber attack or data breach, 44% said that reputation damage was their number one concern, followed by financial loss (24%) and litigation (18%)."

Attacks on businesses are occurring all the time, wherever a company operates, as Deloitte South-East Asia head of strategic risk consulting Dr Janson Yap says: "When it comes to stealing information, crimes with the intention to harm can be committed virtually, physically and in various different combinations. Most enterprises have experienced security breaches, incidents and attacks to some degree. Many do not even know that they have been hacked or attacked."

The number of cyber attacks around the world is increasing and many emanate from Asia, although the focus is shifting from China to other countries in the region.

The volume of cyber attacks originating from Indonesia almost doubled in the second quarter of 2013 compared with first-quarter traffic, according to Akamai Technologies' latest *State of the Internet* report. Indonesia pushed China out of the top spot.

Furthermore, with Indonesia and China originating significantly more observed attack traffic than any other countries, the distribution of this traffic was heavily weighted towards the Asia-Pacific. In the second quarter, the region was responsible for 79% of observed attacks, up from 68% in the first quarter, and 56% in the fourth quarter of 2012.

The number of DDoS attacks reported by Akamai Intelligent Platform customers in Asia nearly tripled in the second quarter.

Akamai product line director David Belson says that Akamai maintained a distributed set of unadvertised agents deployed across the internet that log connection attempts, which the company classified as attack traffic. "Based on the data collected by these agents, Akamai is able to identify the top countries from which attack traffic originates, as well as the top ports targeted by these attacks," he says. "It is important to note, however, that the originating country as identified by the source IP address may not represent the nation in which an attacker resides."

The report also provides insight into other key global statistics, such as network connectivity and connection speeds, and broadband adoption and availability. It found that extremely large growth rates in broadband adoption were seen in Indonesia and China, as well as Malaysia and Thailand. "All four countries more than doubled their levels of broadband adoption from the second quarter of 2012," Belson says. "The most impressive growth rates were seen in Indonesia, which grew by nearly three times year-over-year, and in China, which was up over 500% during the same period."

Belson says that with the growing number of users online, and as connection speeds improve over time, the importance of security would also grow. "Successful phishing attacks have continued to prove that humans remain the weak link in the security chain," he says. "In addition, revelations over the past few months indicate that encrypting communications may not provide complete privacy of those communications.

"While there is no silver bullet to address any of these issues in their entirety, ongoing education of users and administrators alike, the practice of good network hygiene (including regularly updating/patching systems), and a healthy level of scepticism can help to keep things in check," he says.

The interconnectedness of risk is particularly acute with cyber in a variety of ways as Tse explains: "As risk managers continue to address and mitigate the cyber security risks facing their organisations, they may be overlooking a critical threat: the impact of technology failures on supply chains and general operations.

'Companies should not underestimate the business interruption costs'
Stella Tse Marsh

"Such outages and failures have the potential to cause significant loss of income, increase operating expenses, and damage an organisation's reputation. While data privacy breach is a priority risk, companies should not underestimate the business interruption costs if they have to suspend services due to a hack attack or other technology failure. This has direct cash flow implications, not to mention the potential lasting reputational impacts.

"If unplanned, information technology (IT) outages are the most debilitating source of supply chain disruption, affecting 52% of the companies responding to the Business Continuity Institute's Supply Chain Resilience 2012 report. In fact, IT outages outpaced all other sources of supply chain disruption, including severe weather events, transportation disruptions, and product contamination."

And while getting insurers and other key stakeholders to agree on what is required from cyber coverage can be tricky, there is an opportunity for risk managers to really seize the initiative, according to Franck Baron, general manager for risk management and insurance at healthcare, medical assistance and security services company International SOS.

"It is a wonderful opportunity for risk managers to lead the game, to raise the bar," he says.

"Risk managers can highlight to their management the high degree of sophistication and complexity that goes with the insurance game. It's not just about purchasing a piece of paper, and insurance policy, because cyber starts with analysing each insurance programme in your organisation, and seeing what bits of cyber exposure are already covered, and then you can develop a proposal to try to centralise all this insurance coverage into one vehicle, like cyber liability insurance."

Baron, who is also the Pan-Asia Risk and Insurance Management Association (Parima) chairman, adds: "Risk managers and insurance managers need the appropriate set of skills to leverage this and address this properly in their organisations. It's a wonderful opportunity, but it's a complex one. SR

Big Data

Big Data must be embraced, not feared

THERE IS NO DOUBT THAT the digital age has transformed the way businesses and governments operate. Masses of data are being generated – sometimes unintentionally – bringing to the fore a new technological trend that is believed to be helping businesses gain greater competitive advantage in a new way. It comes in the form of what is known as 'Big Data'.

According to global IT and technology provider IBM, the world emits 2.5 quintillion (10^{18})' bytes of data on a daily basis – so much that 90% of the data in the world today has been created in the past two years alone. It comes from everywhere and anywhere, and takes the form of instant Google search results, mobile satellite navigation, and real-time news through social media streams.

Much of the pioneering work on Big Data is taking place in the US but businesses elsewhere, including Asia, are starting to take notice, as Deloitte South-East Asia's head of strategic risk consulting Dr Janson Yap explains.

»

» "The use of Big Data in analysing voting trends ahead of political campaigns and elections is well documented," he says. "Previous elections in Malaysia underestimated the power of social media, forums and blogs to shape public opinions. Recent elections saw an increased use of such vehicles."

There are varying interpretations as to what constitutes Big Data. Analysts generally talk about it in terms of the three Vs: volume; velocity and variety of structured or unstructured data. For many businesses, Big Data also lies in company records. Fundamentally, it is a means to make accurate predictions about risks and opportunities. It is now possible to assess large volumes of data, identify patterns and infer probabilities with much greater speed and precision. The supermarket loyalty card is a good example: retailers have been able to track their customers' shopping habits, to better target their marketing materials and increase sales.

Data is there to be used and monetised. But some companies may be missing out on profit-making opportunities. The term Big Data is often associated with negative issues such as security or data protection lapses. So, firms may have overlooked its strategic potential by dismissing Big Data as simply the latest buzzphrase.

There are, of course, opportunities and threats associated with Big Data and it is important to understand both elements of this, according to Woolworths Limited Australia head of enterprise risk management Nicky Burns.

He says: "With the increased business opportunities for Big Data, new risk exposures exist that need to be worked through to protect data and manage the brand and new legislative requirements, for example, Privacy."

Taking control of your data is crucial. "So many people have spoken about Big Data. As a result, it has lost its meaning along the way," says US-based information management firm Iron Mountain's head of information risk Christian Toon. "A key risk for businesses is not knowing what data they have and where it is.

"Managing Big Data is no different from managing records around your business. It's these principles that companies need to take through when they approach Big Data."

Management issues

"Similarly, being unaware opens the gateway to possible security attacks because businesses remain oblivious to the data assets that they may need to protect," Toon says.

However, given the sheer volume of data a business must handle, it may not be easy to draw conclusions from the information. It is for this reason that firms are advised to approach the management of Big Data with a single vision.

IBM associate partner and security services delivery leader Brendan Byrne says: "Businesses have to be clear about what they are trying to achieve. Big Data is not something organisations should fear – it is something to be embraced, as there are numerous business benefits. If you have a vision you can focus on specific streams of data that will be most valuable to your organisation.

"It's not easy to start because some companies will have vast amounts of data. Big Data is not a quick win; it's something that needs to be factored into business plans."

The outcomes for some businesses have been groundbreaking, with many putting Big Data to radical new uses. Working towards a single vision has helped one US healthcare organisation to save thousands of lives.

In a project involving 157 hospitals, Premier Alliance – which serves more than 2,600 US hospitals and about 84,000 other healthcare sites – claimed it saved an estimated 24,800 lives and reduced healthcare spending by $2.85bn (€2.13bn).

It achieved this by developing an integrated set of data models with IBM, from which it could analyse clinical and operational data, as well as logistics around medication. As a result, the firm was able to identify the treatments that worked best in particular illnesses, helping healthcare practitioners to deliver quicker and more efficient treatment. SR

SPONSORED WORD

Beyond IT and into the boardroom

The potential ramifications of data security breaches have elevated the issue beyond the IT department and into the boardroom. Data protection has become as much a matter of good governance as it is a technology challenge. It is no longer enough to rely on anti-virus software to keep your company's data safe. A wide range of issues such as violation of privacy laws and intellectual property infringement constitute a much broader scope of cyber exposures.

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

Managing the risk also requires a whole-of-company approach – involving every employee – to effectively defend against cyber-related threats and implement comprehensive protection mechanisms.

It's not only hackers to blame

We are frequently bombarded with news of sophisticated computer hackers and viruses, but breaches can just as easily happen through lost or mishandled files, unintentional security breaches or illegal behaviour by employees.

- **Low tech loss** Data security is breached every day through the simple mistake of misplacing or being robbed of a USB stick or laptop that holds confidential data, and through improper disposal of computers or hard copies.
- **Unintended exposure** Unintentional exposure to 'malware' (malicious software) by employees accessing 'contaminated' websites or emails; emailing confidential business information using unsecured wi-fi hotspots; or using their own unsecure mobile devices and laptops for work purposes: these are all a hacker's dream come true.
- **Malicious insiders** Rogue employees may steal confidential information, business plans, and client data, in either soft or hard copy form, intending to expose the data to competitors, start a competing business, or sell it. The vast majority of these malicious insiders leave the company before their acts are discovered.

The spectrum of cyber and data privacy breaches is constantly evolving, adding another layer of complexity and risk management demands to company executives – especially risk managers – that cannot be ignored.

Stella Tse, Marsh Financial and Professional Risks (FINPRO) practice leader, Asia

MARSH