SECTOR VIEW

TECHNOLOGY, MEDIA & TELECOMMUNICATIONS

Tech firms wise up to new exposures

While fire and explosion remains a top risk for all firms, **cyber and technology exposures are becoming increasingly complex**

IT WAS AN INDUSTRIAL mishap that would have ordinarily gone unnoticed. On 4 September 2013, a fire engulfed a substantial portion of a computer memory chip production plant in Wuxi, China.

But this wasn't just any production plan.

Owned and operated by SK Hynix, the plant produced between 10%-17% of the world's supply of dynamic random access memory (DRAM), a memory chip used in computing electronics from laptop computers to mobile phones. The company supplied everyone from Apple and Dell to Lenovo and Sony.

So just how bad was the fire and business interruption?

The effects of the incident were instant: the price of a benchmark unit of 2-gigabit DRAM jumped some 20% to $1.90 the following day, a three-year high. One research firm estimated that the shipment of some 10 million smartphones and 11 million laptops were delayed as a result of the fire, while HP took the threat of supply-chain disruption seriously enough for senior management to clear their calendars for two days.

Beyond the immediate supply chain disruption and delays, the case "totally changed the concept for fire risk in the technology, media and telecommunications (TMT) industry", says Willis Asia head of TMT, managing director, Sirikit Oh.

SK Hynix was one of the top claims in the TMT industry, which cost insurers about $860m.

It's cases like these that have ensured 'fire and explosion' comes close to the top of almost any firm's risk register.

But the risk priorities for TMT companies have evolved in the past two years (see box out, right).

Today, the focus also prioritises cyber and technology risks.

This is because TMT companies typically operate on complex IT networks, depend heavily on web-based solutions, hold and work with a large amount of customer data and often host data for their clients.

Indeed, David Ralph, senior vice president of risk management at Hong Kong-based telecommunications company PCCW Limited, says: "Not only do we rely on IT for billings and aspects like that, but the underlying infrastructure is IT-based for everything we are providing."

Ralph says his IT knowledge has also assisted when people have tried to inform him that a certain area of technology has minimal, or no, risks.

"I have a reasonable amount of respect and authority when it comes to discussing what the risks actually are, and it enables me to work more closely with the technical teams," he says.

Willis's Oh explains that TMT firms are more "vulnerable to cyber and technology-related risks, including hacking, denial of service attacks, or data breaches causing potential expenses, liabilities and regulatory concerns".

She says: "Companies in the TMT industry should take proactive measures in safeguarding their IT systems and intellectual property so as to ensure that their brand and reputation in the market is protected.

"Besides taking physical protective measures, their risk mitigation strategy should include risk sharing and risk transfer through various insurance products."

The cyber insurance market in Asia is still emerging, however, with both insurers and clients grappling with cover and capacity issues.

"In Asia, every country (whether developing or developed) is trying to find their footing in handling internet and cyber security issues. It is a very delicate balance between regulation and allowing cyber developments to take place at the right pace," Oh says.

But Zurich Insurance Global Corporate Asia-Pacific chief executive Keith Thomas says the region needs a more coordinated response to increase its cyber resilience.

"Asia currently lacks an overarching framework to deal with cyber risk," Thomas says.

The region has recently seen some promising steps forward in this area, however. For example, Singapore recently established a Cyber Security Agency and Hong Kong established a Cyber Crime Unit.

But Thomas is calling on regional bodies such as ASEAN and APEC to lead a unanimous response for the region.

"Companies cannot turn a blind eye to the prevailing risks of cyber attacks," he adds. "Besides the potential damage caused from such events, there are also serious reputational risks associated with cyber security. The topic needs to be a priority and escalated to a boardroom level issue."

KEY RISKS FOR TMT COMPANIES IN ASIA

Supply chain and contingent business interruption
TMT companies are increasingly dependent on a complex supply chain, including alliances with third party providers of services, content or other strategic partnerships. Problems in the supply chain can have adverse financial and reputational consequences for the company if not managed adequately.

Catastrophic service interruption
In many countries there is an absolute requirement for telcos to provide continuous services.

Non-physical business interruption (BI)
An interruption or interference to key IT systems from events such as a cyber attack or network failure, can lead to revenue loss and increased costs that may not be covered under a traditional (BI) policy.

Mergers and acquisitions
The TMT industry is consolidating, as large cash-rich companies seek to expand and grow by acquiring companies that enhance strategic value. There are inherent risks involved in both the acquisition process and post-integration stage i.e. inherited liabilities.

Intellectual property/patents
TMT companies are often owners of large amount of intellectual property rights.

Human capital risk
TMT companies often employ large work forces across diverse territories, entailing large salary and benefits costs. Employers' liability and talent management are key exposures.

Contractual liabilities and performance-related risks
As TMT companies move along the value chain or increase the amount and type of services they provide, they encounter an increased range of new and performance and contractual-related risks.

Cyber, data privacy and network security risk
Most TMT companies operate or depend on IT networks, and hold large amount of data. This makes them vulnerable to cyber and technology related risks including hacking, denial of service attacks, or data breaches causing potential expenses, liabilities, and regulatory concerns.

Executive risks
TMT companies are facing increased directors' and officers' exposures with greater scrutiny from regulatory authorities and shareholders than ever before.

International operations and globalisation risks
As TMT companies expand into new markets in search of higher growth, they may face new exposures related to political risk, trade credit and global and local compliance.

Reputation/brand
TMT companies are key brands in the local as well as global economy and the failure to manage an incident correctly could have negative impacts on the brand.

THOUGHT LEADERSHIP

Why TMT firms face heightened cyber risks

SIRIKIT OH
managing director, Asia head of technology, media and telecommunications (TMT), Willis Towers Watson

Companies in the Asia telecommunications, media and technology (TMT) industry face a plethora of risks across almost every aspect of their operations – examples include supply chain, business continuity, mergers and acquisitions plans, data and network security, and intellectual property, as well as threats to key executives and human resources. A serious risk incident to the company in any of these areas can debilitate its business.

The risk exposures for Asian TMT companies have broadened and magnified in recent times. While systems can be rebuilt and business interruptions can be temporary, the biggest risks often relate to a company's reputation and brand.

One area that almost every country in Asia is grappling to manage is cyber security. Fraud, cyber theft, hacking and other forms of sabotage can result in losses to intellectual property, client information and employee data. Business interruptions have a significant impact on the bottom line. We are no strangers to news of such incidents at even national levels with state-of-the art government systems being compromised.

What worries me is that many companies take cyber security for granted and they view it as "other people's problem" – until it hits them. This belies their lack of appreciation for the considerable damage that can be caused by lapses in cyber security. This worrisome situation is further compounded by a lack of understanding and awareness among companies on the type of insurance products available. Senior decision-makers need to be apprised of the means by which they can protect themselves. It is the responsibility of the risk manager, as well as other stakeholders, to ensure that cyber security risks receive board level attention.

A well-designed insurance programme can assist in stretching the dollar spend on companies' risk transfer strategies. While the risk manager is often seen as the gatekeeper for risk management, today practically every department and everyone within a company has a role to play in mitigating the risks.

The really positive news is that the insurance industry is now developing sophisticated risk modelling tools to help companies understand their cyber risk exposures better. In parallel, the quality, limit availability and pricing of Cyber insurance cover have evolved significantly, and are now very well aligned with the requirements that many companies have.

Willis Towers Watson