RISK FINANCING
DIGITAL RISKS

Evolving cyber cover

As awareness of digital risk grows, insurance options from a burgeoning cyber market are becoming more sophisticated

CYBER CRIME IS GROWING. IN THE UK IT COSTS £27BN (€32bn) a year, according to new statistics collected by Detica for the UK government, and is one of the country's biggest emerging threats. *The Information Security Breaches Survey* by PricewaterhouseCoopers found that security breaches had doubled or tripled from 2008 to 2009, and in that survey over 90% of organisations with more than 250 staff revealed they had experienced at least one security incident at that time.

Some of the big stories of recent years included the attack on Sony Playstation that affected 77 million customers and brought down the network for an entire month in 2011, attacks on Google that were found to originate in China in 2010, and since then various attacks on government websites around the world.

In a technological age, most organisations are exposed to some cyber risk and, with growing awareness of this exposure, an increasing number are considering taking out bespoke cyber insurance policies.

"It was previously thought as something that was much more of an IT risk – something the IT department handles," Lockton's assistant vice-president of the global technology and privacy practice, Tom Draper, says. "But after the large breaches we've seen in the last two or three years, there's a dawning realisation from a lot of boards that this is actually a company risk and a corporate governance risk."

While many recent headlines involving cyber attacks and data theft have involved large multinationals (and unlike publicly listed organisations, limited companies are not required to issue public statements on their breaches, so we do not have the entire picture), companies of all sizes and from all sectors are vulnerable. Cosmetics firm Lush had its website repeatedly hacked last year, breaching thousands of customer credit card details. In Australia, an attack on web-hosting firm Distribute.IT affected the websites of nearly 5,000 SMEs.

"It's amazing to see that it really is across the board," says ACE European Group technology and cyber liability underwriter Iain Ainslie. "I've looked at lawyers, online trading, insurance, retail, carpark payment companies, accounting software, trade bodies, e-training, charities, recruitment consultants, pawnbrokers, florists – it goes on and on. It does seem that cyber is something that affects any company in any industry, because it is all about computer systems and the content you publish and the data you hold."

The burgeoning cyber insurance market provides a wide range of covers, some of them more expansive than others. But they all provide covers that cannot be found in traditional policies. "Your standard property policy won't cover any of the liabilities, won't cover any of the first-party costs, and won't cover any of the regulatory costs associated with the data breach," Draper says.

While the market is competitive, insurers are starting to become more risk selective. Vendor risk and portable media risk are some of the key concerns at present, as these have been responsible for a number of recent claims. "As the cover develops, we will see some insurers putting on unencrypted portable media exclusions," Draper reveals. "So unless the company can show that all their portable media is encrypted as standard, the insurer won't pick up the claim when it comes around."

Only nine insurers in the UK (ACE, Kiln, Brit, Barbican, QBE, CNA, Beazley, XL and Hiscox) have specialist cyber divisions, compared to 30-40 in the USA, where the market is substantially more developed. All are bespoke products and include elements of first-party and third-party liability and, as yet, there are no off-the-shelf solutions or standard wordings. "The general basic cover is offered by most," Ainslie says. "It's really whether people choose to expand that to bring in more of the liability aspects or the first-party costs associated with data breach."

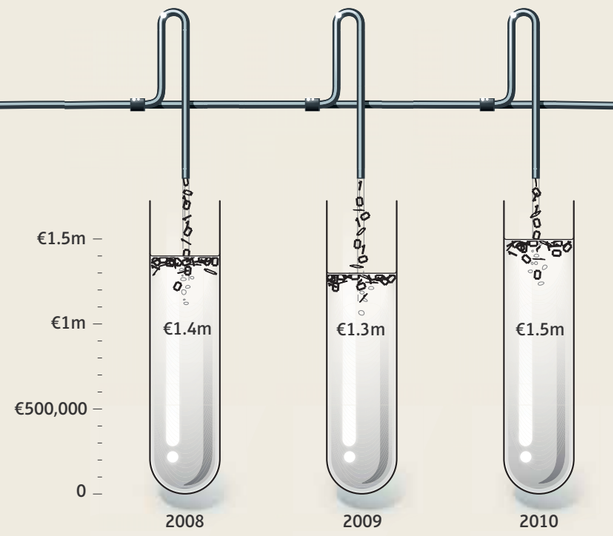
The first-party aspect of the policy typically covers the cost of hiring IT and legal specialists, loss of revenue during an IT failure and crisis management, including the PR and notification costs. But it is the third-party claims arising from the loss of external parties' sensitive data that can be most costly for organisations, and this is where sophisticated liability products come into their own.

Organisations should choose what cover to take out based on their size and scope. While many smaller companies may want to focus on the first-party costs, those dealing with large volumes of data – such as an online retailer – will need third-party liability. "If you're a multibillion-dollar organisation, the actual value of lost revenue from cyber failure might be quite large, but in the overall scheme of things it's not that big," Ainslie says. "When you look at an SME, if they're only taking £25m in revenue a year, a week's loss is a large amount of money."

"Whereas the larger companies may have more of a leaning towards the liability insurance, because they're holding an awful lot of data and content, for the SME the combined offering of first and third party together is making more people interested in the product, because it does encapsulate all the cyber-related risks they have." **SR**

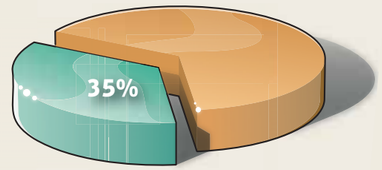
'After the large breaches we've seen in the last two or three years, there's a dawning realisation that this is actually a company risk and a corporate governance risk'

Tom Draper Lockton



Cost of a data breach

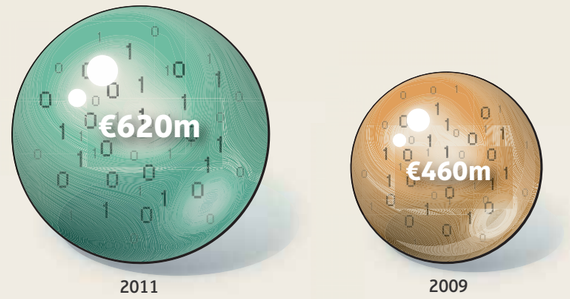
Source: Ponemon Institute, 2010 Annual Study: UK Cost of a Data Breach



How many companies purchase cyber insurance?

Source: Advisen, October 2011

Illustration: Jamie Sneddon



Size of the cyber insurance market

Source: www.betterley.com

EDUCATION PROCESS

WHILE AWARENESS OF CYBER RISK IS GROWING, THERE IS still a long way to go. While headlines about big firms such as Sony do raise awareness, there is still a misconception that these kind of attacks only happen to large multinationals.

"People deliberately made an effort over a period of time to hack Sony," ACE European Group technology and cyber liability underwriter Iain Ainslie says. "What I say to people is that there's an awful lot more hacking done through scripting. If it gets into your system and finds any data of relevance – credit card data or names and addresses – it will take them."

"More are becoming interested in the product, and the number of enquiries has increased over the last 12-15 months," he adds. "A lot of that is down to the general press coverage of data breaches and government regulations. Consumers are more aware of the value of data and how they can be harmed, so a whole combination of things are making directors and chief executives realise that it could affect them."

The other factor likely to drive UK companies to better manage and finance their cyber risks is regulation and fines. At present, the Information Commissioner's Office can level fines of up to £500,000 for data breach. But it is the FSA, thinks Draper, that is emerging as a much bigger force to be reckoned with. "The FSA is the entity that we've seen being the most aggressive about fines for data breaches," he says. "They fined Zurich £2m for their data breach two years ago."