Barring the cyber criminals

The increasing frequency and severity of cyber attacks and their impact on business can no longer be ignored. But insuring against exposures from a security breach requires more than an extension to a traditional property or liability policy. By Lee Coppack

More money is said to be made from cyber crime than the illicit drugs trade. Personal information, credit card details and project plans held on computer networks are virtual gold bars for cyber criminals. Research from both sides of the Atlantic shows the number of attacks is rapidly rising.

A cyber incident is likely to be expensive and damaging. Business may have to come to a halt while the company traces and repairs the weakness in its network. The 2011 Cost of Cyber Crime Study of 50 companies by the US Ponemon Institute found each suffered more than one successful attack each week of varying severity in 2010. The average time to resolve an external cyber attack was 18 days, and average cost was $416,000.

But repairing the damage from cyber attacks can take much longer, and cost much more. Sony took about 40 days to restore fully its PlayStation and other entertainment systems after discovering it had been hacked earlier this year. The US-based Heartland Payment Systems, which processes credit card payments, revealed that a security breach cost the company $114.9 million after insurance recoveries.

"It isn't easy to say what the impact on the business will be following a major event," says Simon Milner, a Partner within JLT Specialty's Financial Risks division. "The company is almost certainly going to lose money for one quarter and probably two."

Surveys from the UK and the US indicate that most businesses suffer security incidents. Glyn Thoms, an Associate within JLT Specialty's Financial Risks division, points out that companies that do not do business direct with the public still hold sensitive personal details on their employees. Neil Hare-Brown, CEO of QCC Information Security, notes that B2C company executives and sales people frequently use company credit cards, which can be vulnerable to cyber attack.

> "It isn't easy to say what the impact of a major event will be."
>
> Simon Milner, Partner JLT Specialty Financial Risks

Cyber insurance

Coverage offered by dedicated policies includes:

- first party damage to data
- business interruption
- privacy and security liability, including notification and credit monitoring costs
- brand reputation
- cyber extortion
- technology professional liability
- multimedia liability
- payment Card Industry Data Security Standard (PCI DSS) compliance
- cyber terrorism.

Insurance

Traditional business insurance policies were designed long before the arrival of the internet. Even with a cyber risks extension, they will not cover all the exposures a business will face

Attacks by insiders are less frequent but can cause more damage

Cyber case studies

Sony PlayStation
In April 2011 Sony reported it had been hacked through its Sony PlayStation Network. More than 100 million accounts including Personal Identifiable Information were compromised.

Hacking causes bankruptcy
The Dutch Certificate Authority DigiNotar filed for bankruptcy in September 2011 after a hacking attack caused it to issue fake online security certificates, and contracts were cancelled.

Hackers tax HMRC
Phishing emails reported in August 2011 to the UK tax office, HMRC, rose by nearly 300 per cent to 24,000 for the month alone. Hackers send genuine-looking emails to taxpayers saying they are due a tax refund. Anyone who replies is directed to a fake site, which collects their personal details and uses them for fraud.

The high cost of hacking
Heartland Payment Systems, which processes credit card payments, revealed that a security breach cost the company $146.1 million between 20 January 2009 and 31 December 2010, reduced by insurance recoveries of $31.2 million. Of the total, $114.7 million was for the settlement of claims, including with credit card issuers, while legal fees, investigation costs, remedial action and crisis management cost $31.4 million.

from a security breach, says Chris Newton, Managing Director of Principia Underwriting. Notifying customers is just one of many costs – the company will need expert advice to restore the damage and manage the impact, and sales may cease while systems are under repair. "There are a number of trigger points, not least of which is the lost income," Newton adds.

Milner says that the market for cyber risks insurance is maturing, and today, there are stand alone cyber insurance products with modular structures, so that it is possible to select which covers to buy.

Policies are now available for smaller and medium-sized business that will wrap around their existing property and third party insurance programmes. This is a first party cover that includes the cost of forensic technical and legal advice and compliance with credit card issuer requirements.

Key considerations

Businesses seeking protection from cyber crime must consider their exposure carefully, choosing insurance cover that meets their needs. What is the waiting period on the business interruption before coverage will apply? Forty-eight hours, even 36 hours? This should be six or eight hours, and at worst ten or twelve. Business interruption insurance can offer a 12-month indemnity rather than just loss of revenue while your network is temporarily unavailable.

Attacks by insiders are less frequent but tend to take much longer to repair so companies should consider taking out insurance that specifically covers the acts of employees and sub-contractors.

While not all companies are yet legally required to notify customers of compromised data (although EU legislation is set to change this) companies often want to voluntarily notify their customers to limit reputational damage. Voluntary notification coverage can help. Credit file monitoring cover will also help restore your customers' trust if they have fallen victim to credit card fraud or other crime because of a breach in your systems.

Lastly, with the services of experts needed to undertake a forensic investigation perhaps the most significant expense, it is worth considering covering this cost with insurance. Legal costs including the means to defend a privacy breach action brought by regulators can also be covered, significantly reducing the risk of major outlays should the worst happen. RS

Simon_Milner@jltgroup.com

Lee Coppack is Editor of *Catastrophe Risk Management* **and** *InfoRM*.