FINANCIAL NEWS

March 24-30, 201

Cybercrime loses its right to silence

Simon Bushell and **Gail Crawford**

New disclosure rules are likely to increase reports of internet security breaches

In 2012, the director general of MI5 revealed that a London-listed company had lost £800 million as a result of a state-backed cyber attack. The company in question has not been publicly identified and no disclosures were made to the market. Why was the market not notified?

That question is one that is likely to gain in importance. In a sign of how seriously the authorities are taking the threat, the Bank of England last month published a report on an exercise carried out last year to test the response of the banking sector and the financial markets to a simulated cyber attack by a hostile foreign state.

The threat is not just theoretical. The UK's Department for Business, Innovation and Skills reported in April last year that 93% of large organisations surveyed had experienced a security breach, yet we have few examples of any listed companies making a market disclosure.

In the US, disclosure of data breaches to customers (and therefore the public) is frequent – driven by state-level reporting rules for breaches of personal data security – and this has resulted in complacency among individuals who receive frequent notifications. In addition, the US Securities and Exchange Commission has issued guidance to US-listed companies about how and when they must report cyber security issues, although companies are reticent when it comes to reporting breaches in any great detail.

By comparison, although there are mandatory and recommended notification requirements on UK businesses that apply to both listed and non-listed companies under the data protection legislation and financial services regulations, they focus on material incidents and require notification to the individuals only where there is a significant risk of harm.

Listed companies also have a requirement to disclose information "likely to have a significant effect on the price" of the company's shares but not clear guidance on how cyber attacks should be treated.

Price sensitive

Details of cyber security breaches could in many cases amount to price-sensitive information, yet you will be hard pressed to find many cyber security-related announcements issued by UK listed companies.

One rare example was the statement made by mining firm ENRC on 23 May 2013, which disclosed the theft of a laptop in a domestic burglary and a subsequent "intrusion into the group's electronic systems by a third party".

The paucity of disclosures is surprising given the apparent scale of cyber security problems reported by the BIS survey. Then again, the significant financial losses that might be incurred in litigation resulting from security breaches could be partly responsible for the considerable reticence towards public disclosure.

Getty Images

Lack of evidence: a dearth of disclosure makes it hard to judge the price sensitivity of cyber breaches

FINANCIAL NEWS

March 24-30, 2014

The dearth of disclosure means there is little evidence to gauge the price sensitivity of information relating to cyber breaches. Therein lies the main problem. If you don't know the impact of a breach, it is hard for a company's board to make a call as to whether it warrants disclosure, and no two breaches are ever the same.

For example, Sony's share price fell by $1.61 (5.4%) to $28.11 in 2011 after it disclosed the loss of significant amounts of PlayStation user data. By comparison, Apple's February 2013 announcement that it had been hacked resulted in a negligible movement in its share price (it dropped 0.2%).

Of course, there are many factors that might influence the size of a share drop, so it is often difficult to ascribe it to a single event or disclosure.

The question of the price sensitivity of a given security breach is likely to depend on the nature of the breach and its significance to the company's business, particularly in respect of operational risks and disruption to business, in addition to reputational damage.

Tougher line

In the US, the SEC has begun to take a tougher line on cyber security, requiring that registrants incorporate cyber security issues, where relevant, in their filings. This may lead to greater scrutiny by the UK authorities, particularly if the EU goes ahead with its proposed Network and Information Security Directive, which will require certain types of companies, including operators of "critical infrastructure" in the fields of energy, transport, banking, stock exchanges and health, to notify the national competent authority of "incidents which have a significant impact on the security of the core services they provide".

The national authority may then make a public disclosure or require the company to do so.

While cyber security breaches affect all industries, the nature of companies in the financial sector makes them particularly attractive targets for cyber criminals. Given the importance of the sector to the UK economy, the government has placed particular focus on the security defences of banks and market intermediaries; the Bank of England's simulated cyber attack exercises, the second of which took place in November 2013, have helped identify any existing security weaknesses.

The UK government considers that more disclosure and information sharing will help with cyber security issues, and the Bank of England report, published last month, found that there was no "formal communication co-ordination within the wider [financial] sector". The report's recommendations included the identification of a single co-ordination body to manage communications, and that financial firms "should be aware of the need to report major incidents to their respective regulators as soon as possible".

At the same time, the UK is in the process of setting up CERT-UK, an organisation to improve co-ordination of national cyber incidents and share technical information between countries to encourage disclosure. Investors, like the companies affected, are finding it difficult to assess the impact of cyber crime, but businesses should not rely on a lack of precedent to justify inaction.

As the number of claims brought as a direct result of cyber security problems grows, so too will the obligations of businesses as the market becomes better equipped to assess the impact of attacks on the bottom line.

Simon Bushell is a partner in the litigation department and Gail Crawford is a partner in the corporate department of Latham & Watkins, London