Is cyber safety the biggest risk for investors?

Cyber risk can take billions off a company's bottom line and valuation. ***Vivian Chow****,* ***William Cox*** *and* ***Mathew Garver*** *explain how investors can take account of the risks.*

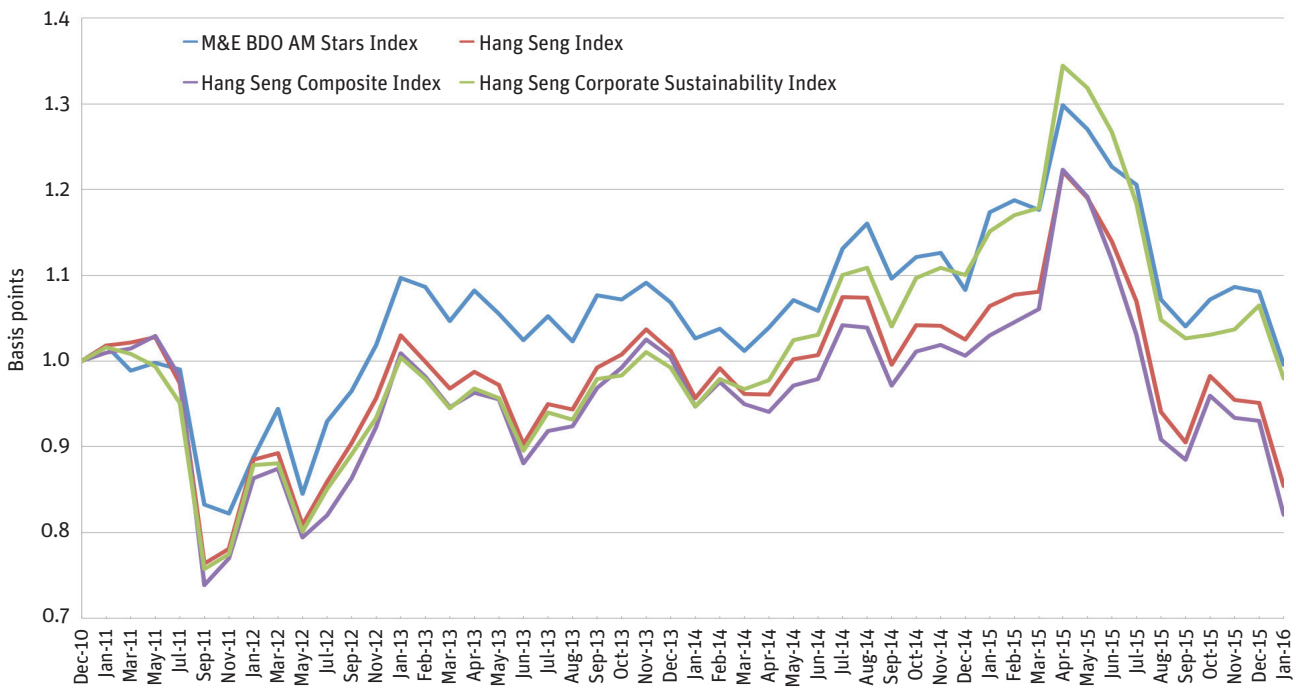
Have you considered the exact impact of unknown cyber risks on your investment or company? Most cyber crime aims at stealing the intellectual property (IP) of companies, which can change the competitive position of a company by giving rivals decisive advantages. The company value then declines massively and quickly, not to mention the disruptive effects of cyber crime on operations.

Estimates put damages from cyber crime worldwide in 2014 at between $375bn and $575bn, which is more than the GDP of most countries, with some estimates as high as $1tr, according to the Center for Strategic & International Studies (CSIS). Cybercrime is valued at 1.6% of German GDP, 0.63% of Chinese GDP and 0.64% of US GDP. And the problem is only getting worse.

A 2015 study of 350 large companies in 11 countries by the Ponemon Institute shows an increase in the cost of cyber breaches of 23% between 2013 and 2015.

Not that only large companies are at risk. In the UK, 93% of large companies and 87% of small companies reported cyber breaches in 2014, with each cyber event costing a large company $1.4m and small companies over $100,000 on average, according to CSIS data.

M&E BDO ASIAMONEY HONG KONG STARS INDEX VS HANG SENG INDEX, HANG SENG COMPOSITE INDEX AND HANG SENG CORPORATE SUSTAINABILITY INDEX



SOURCE: M&E; BDO

That said, some industries are more vulnerable than others. Sixty two percent of cyber attacks are concentrated on three sectors: finance and insurance, information and communications, and manufacturing.

And the costs of recovering data and restoring operations can be 10x that of the initial damage. For example, the US retail chain Target is said to have incurred losses of $420m from a recent cyber-attack, according to CSIS.

INVESTORS IN THE DARK

Cyber crime often not only steals IP, it can compromise the data and lives of hundreds of millions of individuals worldwide. In December 2015, three million accounts of the Hong Kong-based hosting company Sanrio Digital were attacked. A company spokesperson told Reuters at the time that: "It would have been extremely easy for a bad guy to take the data," he said. "Extremely easy. Almost as easy as downloading a web page."

This is not an isolated case. The Hong Kong Productivity Council's Computer Emergency Response Team Coordination Centre (HKCERT) claimed a 103% jump in cyber breaches in Hong Kong in 2014.

But unlike the example above, most cyber breaches are not made public, which leaves investors in the dark about the real condition of their investments. This is perhaps not surprising as CSIS calculates that when breaches are made public, stock prices normally drop by 1% to 5%. Yet given the long term effects of cyber crime, particularly if valuable IP is stolen and given to a competitor, a company's stock price is likely to suffer long term and substantial damage.

Cybercrime probably extracts 15% to 20% from the entire value added generated by the internet, making it a huge and growing added tax. Therefore, one general way to calculate the value-at-risk to a company from cyber crime would be to subtract 15%-20% of the economic value produced by the internet and cyber networks for that company. In the cases of retail companies, the risk level could easily be higher than the entire value of a company.

UNKNOWN DOWNSIDE

Against this background, conventional approaches to calculating the risk and return of companies and investments break down. What is worse, most cyber breaches go undetected. Companies often do not even know if they have been compromised or whether their data is being stolen. Never have unknown risks been greater for investors and executives. In addition, cyber breaches, governance and internal process risks can easily multiply the required return on capital several times over.

While technology is needed to avert attacks, the main risk comes from people. IBM cites that 31.5% of the bad guys committing cyber crimes are malicious insiders with an axe to grind. Employees have knowledge of a company's security systems and can access its data so as a result their attacks are the least likely to be detected.

Indeed, most cyber breaches are rooted in or facilitated by weaknesses in the management and governance structures of the attacked companies. An American client of M&E with operations in Asia was severely breached because its governance policies only covered opening hours in the US and not those of its Asian subsidiary.

As a result, the market for policy and compliance measures addressing cyber crime has grown at over 20% annually, according to CSIS.

Cyber security needs to be a strategic priority of top management, assigning a C-level officer to co-ordinate between the IT, governance and compliance areas of the company. Moreover, that person needs to speak both languages — that of the IT specialists and of management. The first step should be to calculate the value-at-risk of all assets in danger, particularly IP.

> *While technology is needed to avert attacks, the main risk comes from people. IBM cites that 31.5% of the bad guys committing cyber crimes are malicious insiders with an axe to grind.*

SHUNNING THE CYBER SECURITY ISSUE

Yet executives often shy away from technological issues, referring them to the IT department. In a survey of Indian executives by KPMG last year, 94% of executives believe cyber crime is one of the major threats being faced by organisations. However, only 41% state that it is part of the board agenda even though 63% of cyber attacks are known to have led to financial loss.

One likely reason for executives' failure to act on such a significant threat is that cyber threats are often not expressed in financial data such as value-at-risk or return-on-investment (RoI) covering cyber risks, costs and the upside of cyber security efforts.

The benefactors of cyber breaches are not only the cyber criminals themselves. The International Data Corporation estimates that the market for cyber security products had already grown to $58bn in 2013, with $10bn being added annually. For example, the specialists who developed and implemented software after 9/11 to effectively detect cyber breaches within the US Government recently set up their own shop called Punch Cyber. The software is supposed to detect close to 100% of all historic breaches and indicate weaknesses in companies' systems. ■

William Cox is CEO of Management & Excellence and received his PhD from the London School of Economics. Mathew Garver is President of Management & Excellence Global Inc., a company which specialises in calculating Cyber ROI. Vivian Chow is an executive at BDO Financial in Hong Kong, which works with M&E to offer various RoI services.