Victims of hacking stay silent on espionage

HACKERS in China rifled the computers of DuPont at least twice in 2009 and 2010, hunting for the secrets that made the company one of the world's most successful chemical makers.

But investors would have learned nothing on the subject from DuPont's regulatory filings, or from those of other companies victimised by hackers. The documents DuPont submitted to the US Securities and Exchange Commission over the period don't identify hacking as even a significant risk, much less reveal what two US intelligence officials later said was a successful case of industrial espionage.

It is an issue that has raised concerns inside Australia's biggest company, BHP Billiton, as cyber spies from China, Russia and other countries ransack the computer networks of major companies.

The chief executive of BHP Billiton, Marius Kloppers, last year confirmed reports that he is fearful of espionage from China. He was talking in February after the Herald revealed WikiLeaks cables between Mr Kloppers and the US consul-general in Melbourne, Michael Thurston, in which the BHP boss complained that Chinese and industry surveillance was abundant.

"One of the reasons we have pushed so hard for market-clearing prices [for iron ore and coal] is so these sorts of things aren't a concern," Mr Kloppers said.

Mandiant Corp, a US security firm that specialises in cyber industrial espionage, has responded to incidents at 22 Fortune 100 companies, said Richard Bejtlich, the firm's chief security officer.

Mandiant estimates more than 20 per cent of Fortune 500 companies have experienced serious breaches recently, or are dealing with current ones.

The victims of even serious attacks are largely silent, often reporting only breaches that fit narrow legal requirements, such as the theft of credit card numbers.

Beginning in 2009, the networks of at least six major US and European energy companies were breached by hackers in China. The victims included ExxonMobil, Shell, ConocoPhillips and BP.

The hackers stole exploration data and provided the cyber thieves with valuable, confidential assessments of the quality and accessibility of oil reserves, according to Ed Skoudis, senior consultant with InGuardians, a security firm.

In the past five years, cyber spies have raided pharmaceutical companies, cosmetics makers, chip fabricators and mining companies. They have stolen blueprints, manufacturing technology and the chemical formulas of leading products.

Read more: http://www.smh.com.au/business/victims-of-hacking-stay-silent-on-espionage-20120111-1pvap.html#ixzz1kTNFm300