



SEC Filings: Businesses told to reveal true scale of losses

November 1, 2011 3:56AM

SEC filings Fresh guidelines are likely to be a burden for US companies, writes Joseph Menn

One of the difficulties in fighting cybercrime is the uncertainty about how much it costs companies, countries and individuals.

Without this information, it is hard to determine what should be spent to combat the problem - let alone who should be spending the money and on what. For annual global losses, estimates range from below \$100bn to as much as \$1,000bn, an industry report's ballpark figure that has been cited by Barack Obama, the US president.

This figure includes lost intellectual property, which could be worth far more to the inventor than to the thief, but it does not include national security, which is hard to put a price on.

But many more professionals are about to start making educated guesses about the costs to specific companies, potentially helping both top executives and society as a whole understand what they are up against.

On October 13, the staff of the US Securities and Exchange Commission issued extensive guidelines to companies that are publicly traded in the country, spelling out when and how both past cybersecurity breaches and the risk of future ones should be disclosed in regulatory filings viewable by anyone.

That will prompt many, if not all, of the several hundred largest companies to start opening up about what they have lost and what they stand to lose, says John Reed Stark, a former SEC official and now managing director of Stroz Friedberg, a digital security firm.

Even if companies do not leap to adhere to the agency's mandate that they avoid vague language - such as a retailer warning that all industry databases of customer data could theoretically be targets - laws that reward whistleblowers will encourage employees and others to tip off the SEC about serious breaches.

"The SEC has issued an all points bulletin to any whistleblower out there: 'Let us know and you may be able to get up to 30 per cent of whatever fine we levy'," Mr Stark says.

"It is terrific that the SEC has come in, but it is going to be a tremendous burden for public companies," he adds.

Companies will now have to cover specific security issues in the "risk factors" section of their regular filings. System compromises that have a material impact on results or financial conditions, or that are likely to do so, must be reported in management discussions of recent performance.

They could even potentially be included in so-called 8K filings, which describe special events.

The combined disclosures should "provide sufficient disclosure to allow investors to appreciate the nature of the risks faced by the particular registrant", the SEC wrote, adding that reputational damage, loss of customers and strategic trade secrets would all be factors to consider.

Though a fair number of companies have mentioned hacking threats in passing, thus far very few have disclosed actual breaches and their financial consequence.

Intel, the US microchip group, and Google did so early last year, after the internet company announced that hackers based in China had tried to gain access to the accounts of political dissidents.

However, these companies have not put a dollar value on the impact.

As regards extended outages and credit card thefts, some disclosures have been more precise. Sony, the consumer electronics group, said it stood to lose about \$170m after its online gaming networks were attacked repeatedly this year.

TJX, the US retail group that owns TK Maxx, and Heartland Payment Systems, a payment processing company, said that being victims in some of the largest credit and debit card number thefts yet reported had cost them more than \$250m and \$140m respectively.

US laws force companies to warn customers when they lose sensitive data about them, which can trigger lawsuits and provisions for settlements.

But, so far, the loss of trade secrets has generally not required disclosure.

In the past, some companies that were hit by hackers chose not to learn what data were taken, according to Henry Harrison, technical director at BAE Systems' Detica,

the information security company owned by the defence equipment group. This is confirmed by veteran contract investigators in the US.

William Beer, a director of the cybersecurity practice at PwC, the professional services firm, comments: "It is a bit of a Pandora's box. You could discover some pretty nasty problems, so the easy option is to keep the lid shut."

However, a policy of deliberate ignorance might be untenable in the wake of the SEC policy.

If companies start to admit dire events - such as software vendors disclosing the loss of source code for key programs - they could face stock sell-offs by investors.

Security veterans disagree about how often such things might occur, but say that anything beyond a few public statements about events on this scale will encourage a public debate and could force stalled security laws through legislatures.

Richard Clarke, the former White House cybersecurity chief, says more disclosure is not only fairer to investors, but could galvanise Congress into more helpful action.

"If you are a company and 90 per cent of your revenue comes from three drugs and the formulas are gone and they are being knocked off in India, what, really, is your worth?"