



November 1, 2011 03:56AM

By: Joseph Menn

A war marked by fatalism and denial

It is possible to win battles easily and cheaply, explains Joseph Menn

While large companies around the world realise that cybersecurity weaknesses are a growing threat, they are not increasing spending to meet the challenge, according to recent surveys.

In a PwC poll of thousands of executives, just over half the respondents expected their companies to spend more next year on technology security, just as they had the year before.

Yet the confidence of those information technology executives and PwC clients in their organisations' defences has sunk to the lowest point since the survey began six years ago.

The apparent contradiction raises troubling questions about the state of the technology, corporate governance, and the ability of company leaders to act in a complex and evolving arena without a short-term crisis or similar motivation.

The apparent paralysis has deep but distinct roots. "There is fatalism, and there is complacency, and there is denial," said Sir Kevin Tebbit, former permanent under secretary of state at the UK ministry of defence and, before that, director of GCHQ, the nation's signals intelligence agency.

In October, Sir Kevin spoke at a conference in London promoting links between cybersecurity and the wellbeing of businesses and the broad economy, and showing how good practice can be a competitive advantage.

A conference convened this week by William Hague, the UK foreign secretary, expected to draw attendees from 60 countries, will tackle that issue and others. Such efforts can become an uphill battle.

In part, that is because senior executives feel the fight is hopeless, consultants say. Big defence contractors such as Boeing, ManTech, and Northrop Grumman have all been compromised in the past two years.

So, too, have leading security companies, including top security software vendor Symantec and EMC-owned RSA, the leading maker of tokens to authenticate computer users.

The more educated many professionals become about how such high-end attacks are carried out, the more alarmed they become.

Often attributed to hackers working with the military or other government agencies in China, those attacks are often described as "advanced persistent threats" (APTs).

They can combine tricking an employee by posing convincingly as a colleague, with programs that take advantage of vulnerabilities in software, known as zeroday exploits.

Such campaigns were initially aimed at government agencies and are moving to embrace military suppliers and more recently other industries, according to Mandiant, a US firm that has conducted investigations on behalf of many of the highest-profile victims, including Google.

"Mandiant has seen a growing number of commercial entities compromised," the company wrote recently in a trends report, noting that it has been involved in cases in energy, banking, mining, automotive and even the hospitality industry.

Executives have taken note, telling PwC in large numbers that APTs are the driving force behind their defensive spending. Unfortunately, only 16 per cent of them say they have the right policies in place to ward off such threats. Some key capabilities, from alert management processes to awareness training, are actually in declining use.

"Companies wonder: 'Is there really anything I can do about it?'" says Henry Harrison, cybersecurity director at BAE Systems' UK-based Detica unit. "But management is at least having those conversations." The fatalism is a mistake in the view of Mr Harrison and many others.

Companies can raise the odds against the worst kind of data-loss - trade secrets, masses of customers' information, and the like - if they put in the effort. Among other things, it requires redefining what winning is, says Mandiant. The bad guys are going to get in, but they can be stopped from getting data out.

In addition, most hacking attacks are not carried out by evil geniuses, but by young criminals using readily available tools and scanning for holes in the system that allow them to gain access. The \$170m attack on Sony and others this year used a technique called SQL injection, which can be pre-vented cheaply. A recent analysis by Imperva, a security firm, of internet conversations on one popular hacking forum found SQL attacks were the second most popular topic of discussions, after denial-of-service-attacks, which need even less skill. Indeed, fewer than 1 per cent of the infections Microsoft detects are via security holes breached by zero-day events, the software group said last month. Republicans in the US House of Representatives, who are proposing broad legislation to improve the country's security, said in October 90 per cent of attacks could be avoided with "good hygiene". If executives know that, why are they not insisting on good practices? It may be the rewards for success and the

penalties for failure are too low. Because chief executives expect security teams to avert catastrophes, the absence of a successful attack is rarely grounds for a bonus. And the increasingly common reports of breaches at big companies have reduced the stigma attached to victims of successful attacks and the security figures who work there.

The danger is that the very frequency of such reports could lead to complacency. Even when the attacks are serious, the damage is often unclear.

The breaches may not be reported to authorities or to customers, so not immediately harming the brand. They may prompt little more than security enhancements that fall within a reasonable overall technology budget and are unlikely to lead to a firing. The potential exists for outright and very public disaster, but it is still small enough that the third prong of Sir Kevin's problem statement comes in: denial. It is human nature to avoid hard work aimed at avoiding something that has only a small chance of a career-shortening bad outcome, veterans in the industry say.

A few things would help break out of the stasis many politicians, defence leaders and security professionals say is putting the economy at risk. One would be simpler choices, such as the option of more affordable and comprehensive cyber-insurance.

Something that made it easier to sort through the morass of marketing hype around security software would also be a boon. Some of the biggest all purpose technology providers, including Hewlett-Packard and Dell, have bought security firms in the past year and might be on the road to giving thorough protection as a service. But the attempted fix that is likely to arrive the soonest is increased mandatory disclosure. In a lengthy public statement from its staff released in mid-October after pressure from members of Congress, the US Securities and Exchange Commission said cyberattacks that could be material should be revealed to shareholders of publicly traded companies. "Although no existing disclosure requirement explicitly refers to cybersecurity risks and cyber-incidents, a number of disclosure requirements may impose an obligation on registrants," the staff wrote. Potentially material costs could include increased security spending, reputation damage and lost revenue.

Since the new guidance also encompasses disclosures of risk factors, John Reed Stark, a former SEC internet enforcement specialist, says he expects the number of the largest 500 companies reporting cyberthreats to soar from today's handful.

"There isn't a regulated entity out there that on any given day isn't subject to attack," says Mr Stark, who heads the Washington office of Stroz Freidberg, a digital forensics firm. "It's certainly going to be a large number that are vulnerable to this."

The hope of those who pushed for the SEC action is that it will make cyber issues command the attention of chief executives, as well as the public. That could lead to more strategic thinking on the issue, both inside corporate hacking targets and at large.

Frequent reports of breaches at big companies have reduced the stigma attached to victims.