Cyber security wakeup call

Directors should be asking questions about cyber security because their organisations may have already been attacked without them knowing it. **Zilla Efrat** reports.

TOP FOUR STRATEGIES TO MITIGATE TARGETED CYBER INTRUSIONS:

- Application whitelisting of permitted or trusted programs, to prevent execution of malicious or unapproved programs, including .DLL files, for example, using Microsoft AppLocker.
- Patch applications - for example, PDF viewer, Flash Player, Microsoft Office and Java. Patch or mitigate "extreme risk" vulnerabilities within two days. Avoid Adobe Reader prior to version X.
- Patch operating system vulnerabilities. Patch or mitigate "extreme risk" vulnerabilities within two days. Avoid continuing to use Microsoft Windows XP or earlier versions.
- Minimise the number of users with domain or local administrative privileges. Such users should use a separate unprivileged account for email and web browsing.

Source: Department of Defence, Intelligence and Security

"Wake up and smell the coffee!" That was the message from Julie Garland-McLellan, chairman of Oldfields Holdings and a director of Bounty Mining and Kimbriki Environmental Enterprises, to delegates attending the cyber security forum at Company Directors national conference in Singapore last month.

Delegates heard how many organisations were unaware that they had experienced a cyber security breach and that most data breaches were not discovered by the company, but by outsiders.

"All organisations of all forms should never assume their information has no value, because it can be traded or commoditised," warned Nigel Phair GAICD, a director at the Centre for Internet Safety at the University of Canberra.

"A lot of hackers will get into a system and just sit there silently and wait, particularly for competitive intelligence reasons. Sometimes they will want you to know they are there, with some website defacement. Others will want to just monetise [the breach]. They will get in, get the data and get out. And you often won't know about it."

He cautioned that the roll out the National Broadband Network could lead to more malware in cyber space. "Everything will get faster so, of course, the threats will get faster. It will just put them on steroids."

Yet many companies and their boards were not doing enough to mitigate cyber security risk.

Dave Grubman, chief information officer of AIG Property & Casualty, APAC region, pointed to the Carnegie Mellon *Governance of Enterprise Security: CyLab 2012 Report* which revealed that more than half (57 per cent) of respondents were not analysing the adequacy of cyber insurance coverage or undertaking key activities related to cyber risk management to help them manage reputational and financial risks associated with the theft of confidential and proprietary data and security breaches.

"There's an education issue here for boards and then there is an action issue once directors understand what the risks are," said Grubman.

"There is a tremendous amount of information out there for boards. You just have to go and look it. Boards can looks at frameworks, but they have to start asking questions. They also need to start reviewing the budgets of the people [charged with protecting cyber security] to ensure there is actually money to be spent on this.

"Understand how your company is managing this. Are there dedicated individuals associated with privacy risks or IT support or physical security? Weaknesses in physical security can be a big cause of cyber attacks – for example, someone can walk off with a disk. Is there basic training that makes employees aware of the problem and what to look for? Are there customers or other partners that could trip up a suspicion? Is there incident reporting?

"We know this stuff is happening all the time and it doesn't always result in a breach, but if your organisation is telling the board: 'We don't have any problems' or 'No one is trying to penetrate our website', then my guess is that it doesn't have appropriate controls in place."

Garland-McLellan believed that for directors, it was a question of understanding what the risks were and warned directors to be very aware of what their people were doing and how they were doing it. She said the questions for boards were: Do we really know what is going on? Do we really know what the risks are? Are those risks within our appetite? And have we got appropriate people in place to manage those risks and bring them within our risk appetite?

Phair said by using the top four mitigation strategies (see right), out of a list of 35 strategies listed by the Defence Signals Directorate, they could prevent at least 85 percent of targeted cyber intrusions.