Boards warned against growing complacency to cyber security

93 per cent of Australia's largest corporates saying they now feel a degree of confidence that their company is properly secured against cyber threats.

However, just 29 per cent of the leading ASX-listed companies believe their management can detect, respond to and manage an incident with minimal impact on the business. About one in 10 still do not have a documented and approved response, recovery and resumption plan.

The ASX invited the 100 largest listed companies to participate in a voluntary cyber health check in November last year. The health check was a key recommendation of the federal government's 2016 Cyber Security Strategy.

Of the 76 companies that participated in the inaugural health check, four out of every five expected cyber security issues to worsen. The same proportion claim they are doing enough to protect themselves from cyber threats today, but understand they could do more.

When the ASX probed a little deeper, although 92 per cent of respondents said they now included cyber in their corporate risk registers, only 38 per cent had cyber insurance, though a further 16 per cent planned to take out a policy in the coming year.

Thirty-six per cent had considered cyber insurance, and decided against it.

There's further evidence of corporate confidence about cyber threats throughout the region, with fresh research conducted by Frost & Sullivan at the behest of LogRhythm, revealing that 80 per cent of businesses are confident in their cyber resiliency.

Yet 55 per cent of respondents said that they do not conduct risk assessments and 16 per cent of the Australian organisations polled said they did not have an action plan to respond to cyber threats.

Fears at healthcare firms

Regional healthcare businesses considered themselves at greatest risk, particularly as internet connected smart healthcare devices are deployed.

While the healthcare sector seems to be acutely aware of the cyber challenges it faces,

Bill Taylor-Mountford, vice-president of APAC and Japan for LogRhythm, warned against complacency.

"At times there are people who have not experienced a breach who tend to be over confident," he said.

"They have often spent a good deal of money on perimeter defences, but research shows that 65-67 per cent of breaches come from compromised credentials, requiring a different security approach."

He said that senior executives' confidence was "understandable but not excusable", given their traditional lack of IT skills, and warned that more still needed to be done.

ASX chairman Rick Holliday-Smith agrees. Speaking at the launch of the health check he said that while it was reassuring that boards and senior management were spending more time on cyber security, "This is just the beginning of a long journey."

Threats and awareness growing

The threat clearly is not diminishing. The Australian Cyber Security Centre's recently released Cyber Security Survey notes that 90 per cent of all organisations surveyed faced some form of cyber-attack or breach attempt in 2015-16.

In terms of investment in cyber defences most large listed companies (93 per cent) perform vulnerability and penetration assessments, regular internal vulnerability scans (82 per cent) and internal audits of cyber resilience.

However, only a third regularly assess their organisation's cyber security culture and 29 per cent have never assessed it.

Aidan Tudehope, managing director of IT services company Macquarie Government, said that awareness of cyber security had nevertheless "exploded" among senior management and now been normalised at board level.

"They know they are accountable," he said. Indeed 99 per cent of the ASX health check respondents said that accountability for cyber security now lay in the C-suite.

Mr Tudehope, however, noted that while more boards were aware, and were sending the issue to audit and risk committees, many were not necessarily any more able to

answer what to do about it.

Mr Taylor-Mountford agreed there was a "disconnect between the senior executive and what needs to be done."

Gauging investment levels

Macquarie Government is currently developing a model slated for release at the end of the year that will help companies price cyber risk, and hence gauge how much more they should invest to bring that risk down.

In terms of the practical steps that organisations could take to better protect themselves Mr Tudehope said companies should implement the "Essential Eight" recommendations from the Australian Signals Directorate that were released this year.

These recommend that companies:

- Use application whitelisting to help prevent malicious software and unapproved programmes from running;
- Patch applications such as Flash, web browsers, Microsoft Office, Java and PDF viewers;
- Patch operating systems;
- Restrict administrative privileges to operating systems and applications based on user duties;
- Disable untrusted Microsoft Office macros to prevent them being used as malware vectors;
- Block web browser access to Adobe Flash Player (uninstall if possible), web ads and untrusted Java code on the Internet;
- Implement multi factor authentication; and,
- Ensure daily back up of important data.