THE AUSTRALIAN BUSINESS REVIEW

Voluntary cyber security health checks: is this enough?

FERGUS BROOKS
THE AUSTRALIAN
1:05PM JULY 14, 2016

The bulk of Australian businesses have not been made to understand their risk of being exposed to a serious cyber threat. Indeed, most of the Australian corporate ecosystem is in a state of relative obliviousness. While media headlines report almost daily about data breaches or cyber security issues, a lack of action and accountability seems to characterise our country's response to a critical and growing threat.

The federal government recently announced its Australian Cyber Security Strategy, including cyber security health checks for the top 100 ASX-listed companies. While the strategy positions cyber security as one of Australia's highest national security priorities, these health checks are voluntary, whereas a similar scheme for listed companies in the United Kingdom is mandatory.

Certainly Australia's top 100 ASX-listed companies should be leading by example. However, these companies are likely the most aware of the impact a cyber event would have on their business. It's the organisations that are unaware of their exposure to cyber threats that pose a far greater concern.

In order to reduce cyber risk across the nation, large businesses falling just outside the top ASX-100 should undertake similar cyber security health checks. This group should encompass companies across all industries and would ideally extend to the next 10,000 to 15,000 largest businesses in Australia. As a priority, we must start with the cyber-critical organisations that are most at risk–the ones that hold sensitive information and stand to see substantial reputational damage following a cyber event. Importantly, a positive mechanism should be put in place to encourage and reward companies that proactively seek an assessment of their cyber security risk.

When the Australian Privacy Principles (APPs) replaced the National Privacy Principles in 2014, the government introduced a positive incentive for organisations to implement practices, procedures and systems that would ensure compliance with the APPs. Similar action could be taken to encourage uptake of the government's voluntary cyber security health checks.

Business and government collaboration is vital

A key tenet of the Australian Cyber Security Strategy is collaboration between business and government in order to improve cyber security across Australia. The recent announcement that IBM plans to open a National Cyber Security Centre in Canberra, with a former AFP technology chief at its helm, is a positive step towards demonstrating that this theory is actionable. IBM's announcement follows a similar, recent move by Optus Business and Macquarie University to establish a Cyber Security Hub.

It's unrealistic to expect the Australian government to have the resources to help every organisation. Consequently, the involvement of private enterprise will be vital to ensuring Australia's entire corporate ecosystem is aware of its security risk profile.

Playing catch-up with data breach notification laws

One of the reasons why Australia is so far behind the United States in taking action to reduce cyber risk is because we do not have mandated data breach notification laws. In most states across America, if a company loses personal information as a result of a technology failure or another incident, the company is required, by law, to notify the individual whose information has been compromised. To date, no similar legislation has been passed in Australia. However, in December last year, the government released an exposure draft of a bill to implement a data breach notification scheme. The scheme will require businesses to report a "serious data breach" to the Australian Information Commissioner and notify individuals whose data is affected by the breach. Indications suggest that the scheme is likely to be legislated within the next six- to 12-months.

Positively, when the mandatory breach notification amendment is passed in Australia it will be federal legislation. By comparison, the US struggles with data sovereignty issues as different states follow different regulations.

A mandatory data breach notification scheme makes perfect sense. It is sure to serve as a wakeup call for Australian organisations that have yet to take action to understand their cyber security risk profiles. In some cases, senior management and board members will be liable for claims following a data

breach. For this reason, data breach notifications are likely to encourage organisational transparency from the top down. All employees will be forced to take responsibility for carrying people's sensitive information. Soon, cyber risk insurance will become a standard part of every company's insurance portfolio. Damage to an organisation's reputation around how information is secured should be the biggest concern.

Forward-thinking companies will take proactive steps now

Cyber criminals are working on new techniques to penetrate the security of organisations to misappropriate funds, cause damage, access sensitive data and steal intellectual property. Organisations that operate critical infrastructure and industrial control systems are being targeted, resulting in destruction to systems and operations technology, property damage and considerable business disruption. A significant data breach can be financially crippling in first and third party costs, while having a damaging effect on a company's brand and reputation. Ranging from business interruption and legal costs, to customer notification expenses and damage to data — organisations can no longer afford to ignore cyber threats.

There are class actions underway in the US where organisations are being held accountable for the fact that they did not have adequate cyber risk coverage, including insurance. Notably, these actions are targeting senior management and boards of directors.

In this increasingly punitive and regulatory environment, forward-thinking companies will take proactive steps now to identify their cyber risk exposure and explore risk transfer and mitigation strategies.

Fergus Brooks is national practice leader, cyber risk at Aon.