Are boards fulfilling their duty of care on cyber security?

By Grant Barker, Managing Director, Protiviti

- Proviti survey shows higher security performance in companies with strong board engagement.
- Cyber-security risk should be formally integrated into the organisation's audit plan and reported to the board or risk committee.
- Governance professionals should work with CIOs and IT security executives to ensure that the business context of IT risk is clearly articulated and discussed in a non-technical manner.

With cyber attacks and data breaches routinely making media headlines, you'd assume companies are making cyber-security and data privacy a top priority.

Companies still struggling with cyber security

But the results of the latest *Protiviti IT Security and Privacy Survey* which incorporates responses from more than 340 CIOs, chief information security officers, and other IT executives and managers in late 2014, indicate that many organisations have still done little to safeguard against such potential crises. And worse, they are ill prepared to mitigate them if they should strike.

More than one-third of survey respondents said they do not have a written information security policy, and 41 per cent lack a data encryption policy. Such findings are startling, considering the *Privacy Act 1988* imposes significant penalties on organisations that mishandle or expose personal information.

An engaged board is the key

On the upside, the survey gives insights into the factors that help organisations build a robust IT security and privacy profile. It found that the common denominator among entities with strong cyber-security frameworks is an engaged board of directors that genuinely understands security and privacy issues.

Seventy-eight per cent of organisations with boards demonstrating a high or medium level of engagement and understanding of security risks had all 'core' information security policies in place. That doesn't mean boards must be aware of every security practice in detail. However, those that set high expectations and send a strong message about the significance of data security, will spur their organisations to plan and implement more robust cyber-security measures.

The survey repeatedly shows striking differences in security performance between companies with strong board engagement and those without it.

For example, with data volumes growing almost exponentially, it's paramount for companies to classify their data based on importance and sensitivity, and apply appropriate retention and destruction policies to each type, according to regulatory and legal requirements or industry standards. After all, not all data is equal. Some of it is useful or valuable, and some, critical. A clear data classification scheme and policy, allows companies to identify data according to whether it is sensitive, confidential, non-sensitive, or public and to allocate security resources in a more targeted, economical and effective way.

Yet, here again, there's a clear divide: 87 per cent of companies with boards that are highly engaged in information security have a clear data classification

> …87 per cent of companies with boards that are highly engaged in information security have a clear data classification policy, compared with 64 per cent for those lacking board engagement.

policy, compared with 64 per cent for those lacking board engagement.

Likewise, although all companies can fall victim to hackers, those with a board that's more engaged in information security are likely to recover more quickly after an attack: 77 per cent of these companies have a formal and documented crisis response plan that would be executed in such an event. By comparison, only 47 per cent of companies without high board engagement in information security are similarly prepared.

Companies need to understand that even the most secure organisation cannot expect to prevent all breaches. And that's why it's critical to have a documented crisis response plan which articulates responsibilities and the actions to be taken in the event of a cyber attack, and which is tested at least annually to ensure it's up-to-date and effective.

Why board engagement matters

Why does high board engagement on information security make a difference? In our experience, operational teams are compelled to tackle IT security issues attentively as a result of oversight and direct questioning from directors. Put simply, board engagement raises the accountability stakes. These organisations are also likely to be producing meaningful metrics and communicating more effectively with the board, which in turn predisposes management to provide more funding for security measures.

The clear message is that an engaged board leads to a security-conscious environment that fosters a true understanding of an organisation's capabilities — and, just as importantly, its limitations.

Tips to get your board IT-engaged

With reports of cyber attacks cutting across multiple industries on an unprecedented scale and resulting in the loss of intellectual property, business intelligence and reputation, directors are quickly beginning to understand that IT and data security is a business security issue — and not just a narrow IT issue.

Australian boards have traditionally not been strong on IT expertise. While this is gradually changing, governance professionals should work with chief information officers (CIO) and IT security executives, to heighten the board's awareness and knowledge of cyber-security risk to ensure board members remain highly engaged and up to date on the changing nature and strategic importance of cyber-security risk.

Here are some tips to advance the focus on cyber security at board level.

- Work with management and the board to develop a cyber-security strategy and policy.
- Seek to have the organisation become 'very effective' in its ability to identify, assess and mitigate cyber-security risk to an acceptable level.
- Leverage board relationships to raise the board's awareness of cyber-security risk.
- Ensure cyber-security risk is formally integrated into the organisation's audit plan and reported to the board or risk committee.
- Develop and keep current, an understanding of how emerging technologies and technological trends are affecting the company and its cyber-security risk profile and periodically keep the board abreast of these trends.
- Make cyber-security monitoring and cyber-incident response a top management priority. A clear escalation protocol can help make the case for and sustain this priority.
- Address any IT staffing or resource shortages which can hamper efforts to address cyber-security issues.
- Recognise that with regard to cyber security, the strongest preventative capability requires a combination of human and technology security — a complementary blend of education, awareness, vigilance and technology tools.

Talking to the board about IT risk

Boards often lament that the quality and quantity of information they receive from management fails to give them a sufficient understanding of the IT risks facing their organisations.

To ensure key information about the organisation's IT profile is communicated in a way that optimises board engagement, governance professionals should work with CIOs and IT security executives to ensure that

the business context of IT risk is clearly articulated and discussed in a non-technical manner. To facilitate positive dialogue with the board, IT discussions should always do the following.

- **Demonstrate an understanding of the business:** The board needs to understand how the IT-related objectives and plans support the over-arching business growth and risk mitigation goals of the organisation.
- **Address business impact and metrics, not simply IT impact and metrics:** Any performance metric should provide an end-to-end view and focus on business consequences. A metric like '99 per cent of our systems are patched in ten days' does not address business issues, such as what data is at risk or the consequences of service failure.
- **Focus on the board's needs:** The board has little interest in the intricacies of how the IT function is managed so stick to the business 'big picture'.
- **Target the audience:** Seek insight about the background and personalities of the various board members either from the board committee chair or others 'in the know' to help tailor your discussions.
- **Keep it pithy:** Directors do not want the whole nine yards. Focus purely on what they need to know and share sophisticated knowledge carefully.

There is a clear, positive correlation between a high level of board engagement in information security and an organisation's ability to acceptably manage cyber-security risk. Governance professionals, IT executives and risk managers who galvanise their efforts to enhance their board's appreciation of the risks in terms that resonate with the business, will be far better placed to mitigate the inevitable threat of a future security breach.

Grant Barker can be contacted on (03) 9948 1206 or by email at grant.barker@proviti.com.au.