Barbarians at the gate – Cyber-security and the board

Description

This famous book title is an apt description of the unprecedented challenge faced by organisations as they deal with the exponentially growing level of cyber attacks. Every hour of the day, organisations, large and small, are suffering non-stop attacks ranging from denial-of-service attacks, malware and social cyber attacks. These attacks if not successfully prevented or managed, can result in major damage to an organisation and its customers ranging from financial loss, reputational loss, loss of customer data, regulatory breaches and loss of intellectual property & sensitive organisational data. According to EY's 2014 Global Information Security Survey, 53% of organizations note that the lack of skilled resources and cybersecurity skills is one of the main roadblocks they face. Less than 20% of organizations have real-time insight on cyber risks, and cybersecurity tasks are generally not adequately resourced or performed by skilled people.

Despite the high profile in the media of cyber-security, a significant majority of boards have and continue to struggle in fully accepting that cyber-security is no longer just a component of the IT department silo and has now become a very major area of responsibility for the board in ensuring that the organisation has an overall effective cyber-security strategy in place and appropriate strategies to deal with cyber attacks. Progressive high-quality boards increasingly understand that cyber security is a risk management issue that affects the entire organization and requires board oversight. However, although directors know that they need to stay informed about cybersecurity, keeping up with it in the complex, rapidly evolving world of IT is often a challenge. Many audit committees simply do not have the technical expertise to provide proper risk oversight to deal with cyber-threats.

Best practices for boards in the area of cyber-security consist of the following ;

Acceptance by the board of their responsibility in Cyber-security

- Boards must ensure that cybersecurity is viewed as an enterprise risk issue, not just an IT topic, and that discussion of cybersecurity gets adequate time on the board agenda and with management.

Set expectations for executive management

- Boards need to ensure that they are adequately briefed about the organisation's security model and vulnerabilities
- Briefings should occur on at least a quarterly basis, and if the management of cyber risk is allocated to a committee, the full board should also be briefed at least semi-annually.

Understand your organisation's cyber-risks

- Assess technology, regulatory & legal risks
- Prioritise assets and systems
- Consider cyber-insurance

- Identify risks from third parties (both existing partners and new third parties)
- Anticipate change (particular focus on times of significant change – new markets, technologies etc)

Board oversight of overall cyber-security capabilities and plans

- Does executive leadership have a clear and consistent understanding of cybersecurity relative to the business?
- Does management understand its responsibility for cybersecurity and have an adequate system of controls in place?
- Is the cyber security budget appropriately funded?
- Is the organization’s enterprise risk management program appropriately staffed and resourced given the types of risk assessed?
- Are there clear policies and procedures in place in the event of a breach?
- Is the company’s disclosure response in line with regulatory guidelines and shareholders expectations?
- Identify an external cybersecurity forensics expert that has done an independent review of the cybersecurity risk management and can be brought in in the event of an emergency

Date Created
27/03/2017