Are company boards sleep-walking in the face of un-relenting cyber-threats and potential catastrophic damage to their organisation ?

Description

On a weekly basis, I am genuinely taken aback by the complacency & naivety of company boards when it comes to the serious threats posed by cyber-attacks and their potential to cause serious operational, financial & reputational damage to both the company and their customers. When it comes to risk management, you would normally see a trend of the larger companies having a more sophisticated approach and maturity level. Cyber-security is an exception where even the largest company boards often have a blind-spot in terms of both the level of threat posed by cyber-attacks and the critical role the board have in working with the executive team and the entire organisation to protect both the organisation's infrastructure and sensitive customer data.

How many board members are aware of the critical importance of updating the organisation's software with the latest security patches ? Security firm Verizon estimates that 85% of successful cyberattacks are caused by just ten known bugs that any organisation could readily patch and protect themselves from. Even adding this one KPI to the overall KPI set in the board pack that the executive responsible for IT & cyber-security would update the board on would be a very valuable practical step. At this stage, no board member anywhere in the world, irrespective of the size of the organisation, could claim that they are not aware of the risks posed by cyber-attacks. Yet, in a recent study by PwC, they found that less than half of the boards surveyed had any involvement in their cyber-security strategy.

At the recent World Economic Forum in Davos, Jim Hagemann Snabe, Chairman of A.P. Møller-Maersk, the global shipping company, gave a very honest and insightful account of how his organisation was impacted by the NotPetya ransomeware outbreak last year. " I'll never forget, It was the 27 of June when I was woken up at 4 o'clock in the morning. A call came from the office that we

had suffered a cyberattack," Snabe said. "The impact of that is that we basically found that we had to reinstall an entire infrastructure," Snabe continued. "We had to install 4,000 new servers, 45,000 new PCs, 2,500 applications." . Snabe also said his company estimated the damages caused by NotPetya to between $250 and $300 million. This is similar to the damages cost that both US pharmaceutics giant Merck and US-based international courier service FedEx also put on the NotPetya aftermath.

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
- Identify and partner with specialist cyber-security firms who can support your internal IT department on a 7×24 basis
- 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 there a specific executive with overall responsibility for cyber-security that briefs the board on a regular basis ?
- Have the executive team put in place the structure to test the organisation's cyber-defences with "red teaming", where outside security experts mount live hack attacks on your network to expose weaknesses and identify the key areas that need strengthening ?
- 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

As the pace of technology innovation and disruption continues to accelerate, every new advance in key areas such as IoT, artificial intelligence, and financial technology infrastructure brings with it substantial new cyber-risks. It is virtually impossible for any organisation, irrespective of its scale, to be immune from cyber-attacks. However the board of directors have a fundamental role and responsibility to their shareholders & customers in ensuring the organisation is optimally protecting its infrastructure, reducing the potential for a serious cyber-attack, mitigating the level of cyber risk and importantly being prepared to respond to a breach rapidly and in a very coherent manner.

Kieran Moynihan is the managing partner of ***Board Excellence (https://boardexcellence.ie & https://boardexcellence.co.uk)*** *– supporting boards & directors in Ireland, UK and Europe excel in effectiveness, performance and corporate governance.*

Date Created
19/02/2018