A heightened threat

Erin Nealy Cox

Originally published in *Governance and Compliance*
www.govcompmag.com, 29 March 2016

STROZ FRIEDBERG

New legislation compels boards to examine cyber risk

The EU's recent decision to push forward with legislation that will force companies to disclose data breaches is certain to focus board and management efforts on cyber security. Introduced in response to heightened cyber threats and a desire to make essential services 'cyber attack-proof', the legislation will initially apply to organisations in the energy, transport, banking, financial services, health and water supply sectors. The EU has also said that companies who break data protection rules could face significant fines.

In today's digital and connected environment, the question is not if a company will be compromised, but when – so the notion of anything being cyber attack-proof is unrealistic. These mandatory reporting actions illustrate the importance of cyber preparedness and the adoption of an organisation-wide cyber resilience mindset, including in the boardroom.

A company that is cyber resilient is prepared for a potential business disruption caused by cyber attacks. Although historically this kind of risk has been the sole focus of chief information officers and chief security officers, implementing a plan large enough to address the severity of the risk requires the attention and the participation of all company leaders.

Cyber risk will likely drive the board's agenda this year. Resilience starts with a solid cyber security blueprint that helps boards integrate this issue into their management of enterprise risk. The foundation of this blueprint is not technical, yet boards should have an understanding of some of the technical realities, including the problems and solutions.

Although this may require some board education in the short term, it does not necessitate deep technical skill. The board's focus should simply begin with being well informed so it can ask the right questions and better understand how senior executives are addressing the effectiveness of the company's security strategy.

To jumpstart this information gathering process, boards should ask three questions: Has the organisation appropriately assessed its cyber security-related risks, and how are those risks evaluated? Have cyber security risks been prioritised, and are these priorities properly aligned with the corporate strategy and cyber vulnerabilities? What specific actions will be taken to mitigate cyber security risks? Boards can then progress to building a cyber-resilience blueprint around the following six key elements.

1. Involve the full board

Every director must have enough of an understanding of the risk to take an active part in the review process and, given the potentially devastating consequences of a major breach, the dialogue on cyber security risk should preferably take place at every board meeting. To ensure all directors are engaged, expert reports should be delivered free of any jargon and discussions should address issues in the enterprise risk language to ensure a strategy-level focus. Executives will never need to know how to configure a firewall, but there is a lot to learn about the nature and potential impact of cyber attacks, as well as mitigation approaches.

A recommended approach is to establish a committee responsible for cyber security risk, chaired by an executive charged with becoming familiar with the issues and educating the rest of the board where and when appropriate. Establishing a specific committee also fulfils the goal of consistency. The chair can regularly report to the board and arrange further input from relevant internal managers in the IT and security departments, as well as from outside experts who can provide valuable help on topics such as threat intelligence.

2. Be proactive in risk management

Cyber security risk should be introduced into early stage discussions of all business decisions. Whether a decision has to do with corporate strategy, new product launches or new enterprise initiatives, management should always proactively consider cyber security risk. If an issue only emerges later on, it will be far harder to address.

An example of such proactive thinking is when executives are considering an acquisition. M&A cyber security risk has a number of dimensions that should feature in a board's analysis: the M&A process itself should be performed in a cyber-safe manner, the acquisition target should be investigated for its cyber security strengths and weaknesses, and potential cyber risks resulting from post-deal integration must be addressed.

Continued...

3. Prioritise actions based on risk

The number of cyber security measures in which a company could invest is practically limitless – prioritisation is essential. A customised assessment of the most serious threats should be made, considering both the value of assets and the organisation's major vulnerabilities. These are key to a cyber security review and both must be updated as the risks evolve.

Executives must regularly ask what measures are being taken to protect a company's most critical systems, from development through production to distribution. Beyond the most critical, consider what other assets require protection. Customised threat intelligence can also play a valuable role by analysing the network for weaknesses, identifying where sensitive information is stored and how it is protected, and offering an up-to-date view of the wider environment for cyber threats.

4. Human defences are key

Determined hackers can find a way through even the best cyber-defence technology as there is always a weak link – people. Tactics known as social engineering and spear phishing are typically used to exploit staff and breach networks, and the most effective defence against this is education. Programmes such as spear phishing training should be provided on an ongoing basis, with executives taking an active and visible interest in the success of the initiative. Risk prioritisation applies equally to human defences, which should work in tandem with insights from customised threat intelligence.

5. Assess all third-party relationships

As business collaboration surges, the amount of confidential, trade secret and intellectual property information that is being shared among business partners is rocketing. This is creating an electronic flow of mission-critical information ready made for economic espionage. These third-party relationships create further vulnerabilities, as hackers may breach a business partner with weaker security and then use that partner's network access credentials to reach the target company.

Consideration is therefore needed as to how cyber due diligence on third parties is conducted. Boards should assess its business relationships and identify high risk supply chain partners. Where a high risk connection is identified, that supplier's own security preparedness must be reviewed. Cyber security consideration should be included early in the development of a new business relationship, so that appropriate access to information can be ensured under a security regime that is consistent with the company's own security policies.

6. Incident response policies and procedures

In spite of the EU's mandate on critical infrastructure, perfect security may not be achievable and a breach of the network is inevitable. This means boards must ensure their organisations have well-honed policies in place for responding to a breach when it happens. As recent incidents have shown, it is the delayed, bumbling response to a security breach that often leads to increased data loss, exposure to regulatory action and reputational damage. The move towards mandatory reporting of data breaches will increase the importance of getting the response right and suitable preparations should not, therefore, be seen as an admission of a weakness.

Good incident response plans define the roles and responsibilities of the teams involved, such as crisis communications, human resources, legal and IT. Each team should have clear initial actions to complete and people to report to, and the plan should be tested with regular simulation exercises. An incident response plan should engage the entire enterprise, with all employees kept up-to-date as threat intelligence evolves.

Cyber security should not be viewed as the exclusive responsibility of an organisation's IT team. Heightened cyber threats and the severity of data breach legislation are emerging as prime catalysts for boards to ramp up their cyber insight, to ensure they are well-informed and comfortable making cyber risk decisions. Boards must take steps to ensure the goal of cyber resilience is fully understood throughout the organisation as part of the company's enterprise risk strategy, and that steps are being taken to achieve this goal – and not only through technical measures. Although no strategy offers a company immunity from a cyber breach, the appropriate management of risk will go a long way in minimising the potential financial, reputational and regulatory fall out of an attack.

Erin Nealy Cox is an Executive Managing Director at Stroz Friedberg. Learn more at **strozfriedberg.com.**

strozfriedberg.com
Originally published in *Governance and Compliance*
www.govcompmag.com, 29 March 2016