MANAGING CYBER SECURITY CHALLENGES AT BOARD LEVEL

Dr. Claudia Natanson, FBCS CITP, CISSP
Founder, Security Practitioners

Cyber security can be defined in a number of different ways but perhaps from a business perspective is best described as the body of technologies, processes and practices designed to protect an organisation's information assets from compromise – these assets include computers, mobile devices and cloud-based systems. By compromise, we mean loss of the confidentiality, integrity and availability of the information asset, often leading to reputational damage, revenue loss, and reduced shareholder and customer confidence.

1 billion data records were compromised in 2014 (PWC's 2015 US State of Cybercrime Survey). In the early days of cyber security incidents, organisations were often reluctant to go public if a breach occurred. However, non- or limited disclosure has ceased to be a viable option with the regulatory requirements to notify when a breach has occurred and the rapid spread of information via the press and social media. In addition, 'hacktivists' (those gaining unauthorised access to computer files or networks to further social or political ends), organised crime and malicious perpetrators now often quickly go public following a successful hack as part of their agenda to gain attention. As a result, organisations can be left exposed very quickly.

Changing board involvement

It is, therefore, not surprising that cyber security is now firmly on the agendas of organisational boards. The biggest challenge that boards now face is making necessary adjustments to the way they approach cyber security governance. Historically, boards tended to view security risks exclusively as part of IT risks, rather than making the connection with enterprise-wide risk management. The inability of boards to understand the full extent of risks associated with cyber security governance has meant that key questions have gone unasked, and unanswered. The consequence in some cases has been unexpected security breaches.

To address this, many organisations have now moved to having an independent risk committee that functions outside of the Audit and Risk Committee. This means the organisation is better able to focus on all aspects of risk management right across the organisations that have a relevance to information assets. The fact is that boards need to be provided with the right information and set the risk appetite and culture for the organisation. They must lead by example, and that means keeping abreast by maintaining their own awareness levels and training at an appropriate level.

A number of specific developments are reinforcing the responsibilities of senior management in this area. For example, the much anticipated Senior Managers and Certification Regime (SM&CR) for the financial sector in the UK (due in March 2016), will place a statutory requirement on senior managers to take reasonable steps to prevent regulatory breaches in their area of responsibility. And the latest revision of ISO/IEC 27001 emphasises that accountability for asset security sits at the very top of the organisation.

Boards need to consider if they are asking the right questions, or even seeing the bigger picture regarding cyber risks. The good news culture mentality at board level can mean that finer details are missed. An over-reliance on controls that may have been in place for some time can mean that effective management and monitoring of the original risk are compromised, while many controls are untested, or become part of tick box exercises, which simply get passed up as metrics to the board. Being properly breach-ready has to start at board level.

Defence-in-depth approach

The defence-in-depth (onion ring) approach, in which multiple layers of security controls are placed around information assets, is a good basis from which the board can ask questions. The five layers of defence are: (1) user, (2) application, (3) perimeter (network/physical), (4) server, (5) database in which our assets are stored.

In relation to the user level, the organisation must be able to drill down to look at the privileged user, authorised and non authorised access, and statistics for compliance at this level. Application layers must also deliver statistics on current versions, upgrades, secure coding and access controls. Similar levels of information must be available for all other layers.

Vulnerabilities on servers and the network are extremely important with many organisations still having unsupported systems as part of their day-to-day operations. This makes them easier to attack. The NOPSEC 2015 State of Vulnerability Risk Management report shows that system vulnerabilities and misconfigurations are still the main cause of security breaches. With organisations taking on average 170 days to detect breaches, it is very clear that boards must pay closer attention to the management of vulnerabilities in these areas. Despite having more vulnerabilities per asset recorded, cloud providers recorded shorter remediation times, fixing vulnerabilities in less than 30 days.

It is also important that close attention is given to suppliers. With risk in the supply chain a key security factor, all providers should be held to account to provide evidence of best practice security.

Risk management based on trends

The Cisco 2016 Annual Security Report has shown that, of the 115,000 Cisco devices on the internet, 92% were running software with known vulnerabilities. 31% of these devices were at "end of sale" and 8% at "end of life", meaning they would not any longer be eligible for receiving patch support. These statistics can be viewed alongside the NOPSEC report figures that show it takes on average 103 days for organisations to remedy a security problem, with banks showing an average of 176 days. Boards must take such risks into account and combine them with other associated risks, such as risk in the supply chain, inadequate resource bandwidth, capability and expertise, to create an aggregated risk profile from which to make sound risk decisions, on whether to mitigate, manage or transfer their risk. They must use this information when making decisions on spend, and for strategic business planning especially in the area of IT infrastructure spend.

Boards must also obtain briefings on trends that may be of assistance in implementing proactive risk management. These include Blockchain, the decentralised ledger that allows global computers to become sequentially constructed transactional spreadsheets that are linked together in blocks. Each block is made up of discrete private data and uses a public header and cryptography to link and secure each block. Bitcoin was one of the first applications to make use of this infrastructure and since then many more have come to market. Ripple is the second largest, and is of great interest to the financial community because of its ability to carry our micro transactions at high levels of granularity cost-effectively.

Big Data is now also playing a major role in many organisations. Big Data analytics have often been used to gain insight into customer trends, but also offer considerable potential for future threat correlation and incident handling for cyber security teams.

Key considerations for Boards

• Carry out regular incident handling and response to security breaches as exercises at board level.

• Lead by example in setting the security and risk culture of the organisation.

• Ask the same questions during day-to-day management of cyber security governance as during an actual breach – where are assets, who has access to them, can they be compromised, if so by whom, possible reasons for such an attack, how an incident would be handled, and processes and procedures to be employed during a breach.

• Be aware that the pace of release of vulnerability updates and patches will continue with the large software and system providers such as Microsoft, Oracle and Adobe. Distributed Denial of Service attacks, where a network is brought to its knees by flooding with useless traffic, continue to increase with many senior executives being successfully targeted with fake email campaigns (spear phishing).

• Recognise that security risk should be considered in terms of the enterprise-wide risk framework rather than being seen as purely IT-based.

• End point security will become increasingly important and must be tracked and managed, as freedom of choice in what device to use will also increase. Effective encryption will be very important, but should not result in neglecting other areas of cyber security.

• The physical side of cyber security, as the first line of defence, should not be overlooked and must be part of all reporting procedures.

• Recognise fiduciary responsibilities, including cyber security governance. Track the progress of raising the security maturity level of the organisation, so that it is in a state of continuous improvement and not reactively responding to cyber security requirements.

• Track statistics to ensure security is considered at the start of projects, rather than being bolted on later or even excluded entirely.

• Keep security as a regular board agenda item and apportion adequate time to understand the metrics provided.

• Continue to set up risk committees that are separate to the Audit and Risk Committee, to facilitate looking at cyber security in a more granular way.

75% of UK CEOs are now citing cyber security as the third major threat after over-regulation and geo-political uncertainty, (PwC 2015 security report), and this is being echoed globally by their peers. While third parties can be used to transfer responsibility, liability will remain firmly at the top of the organisation. The ethical responsibility of boards will continue to increase to cover the digital dimension, and the way the organisation manipulates its data, protects and secures it.

Board competence and commitment in meeting these challenges will be vital in ensuring the organisation is breach ready.