Deloitte.

The Deloitte Academy
August 2016

Governance *in brief*

Cyber risk – how are boards responding?

Headlines

- The third annual FTSE 350 health check survey shows board awareness of the nature and impact of cyber risk is improving, reflected in a marked increase of companies who have elevated cyber to a top Group risk in their risk registers.
- However, not enough FTSE 350 boards have defined their organisation's cyber risk appetite to promote consistent and well-informed strategic and operational risk decisions.
- Insufficient numbers of FTSE 350 boards receive robust and timely intelligence that allows the board to critically challenge and evaluate management's oversight and approach to this critical risk.

Background

The barriers to launch and execute sophisticated cyber attacks are continually decreasing, revealing significant vulnerabilities, as recently highlighted by the $81 million Bank of Bangladesh breach. In the last year, UK companies have suffered a number of high profile, successful cyber breaches including attacks on many household names, and on a daily basis, businesses are reacting to the increasing proliferation of threats such as ransomware where affected parties are extorted to regain access to their own files.

Against this backdrop, the UK government ran the third annual FTSE 350 UK Cyber Governance Health Check, over the first quarter of 2016, the results of which were published in the second quarter. This is part of the UK's strategy to lead in digital innovation and cyber security. The Health Check was sent to Audit Committee Chairs for completion, with the aim of promoting awareness and providing insight into how boards are strategically managing and responding to cyber risk.

Recognising the challenge

There are clear signs that board awareness of cyber risk continues to improve. Almost half of Audit Committee Chairs (49%) confirmed that their board now has a clear understanding of the impact of a loss or disruption to their key information and data assets in the event of a cyber incident, a material improvement compared to 2013 (33%). Feedback during interviews that were conducted to collate responses for the FTSE 350 survey suggested this greater awareness stems from visibility of incidents within respondents' own organisations or at other companies, coupled with industry and government education programmes.

This increase in understanding of cyber is reflected across FTSE 350 risk registers where the Health Check revealed a significant increase in companies highlighting cyber as a primary Group risk (49%) compared to the 2014 survey (29%). The majority of respondents (71%) are expecting net cyber risk to increase over the next year.

Responding to the challenge

77% of companies are setting aside a specific budget to ensure the adequacy of the protection of consumer data, demonstrating an increased awareness of security and data privacy concerns and legislation. Interestingly, three quarters of budgets that have been set aside are held by IT departments. While IT spend will likely be the greatest contribution to any cyber related budget, management and boards should ensure that, as a pervasive business risk, there is adequate engagement and budget set aside for non IT-specific investment such as employee education programmes, wider business resilience activity and cyber insurance.

Boards are reviewing their own composition and support mechanisms to prepare themselves for the extent of the challenge, with 49% of respondents indicating that the board now has the right skills and knowledge to a 'significant degree' to manage innovation and risk in a digital world. From our own experiences, several boards have sought to inject technology skillsets through direct recruitment, although experienced technology experts with sufficient board or management experience are in short supply. Other routes adopted have included boards obtaining more extensive external advice or allocating a specific director to take responsibility for cyber risk who becomes more immersed in understanding management's activity, allowing them to inform the board and take a more active role.

An improvement on prior surveys maybe, but there is a recognition that much more can be done as only 6% indicated that their boards were 'fully informed and skilled'.

Maintaining the momentum

While evidence is emerging that boards are starting to play a greater role in supporting management to strategically define the cyber risk agenda, various indicators suggest boards could do more.

Although an improvement from 2014, cyber risk appetite has only been clearly set for one third of FTSE 350 boards. With the speed of digital innovation and the commoditisation of cyber threats, a well-defined cyber risk appetite will help management make appropriate and consistent operational decisions. This will support the company's ability to determine the right balance of risk against its capacity to innovate and take advantage of new market opportunities. Failure to set the cyber risk appetite may mean that the organisation makes decisions that expose the company to unnecessary cyber and operational risk; or conversely in the event of an overly risk averse management team, strangles the organisation's development and growth.

Although we have seen that great strides have been made to improve cyber risk awareness, the majority of boards do not yet regularly consider cyber risk with only 23% of respondents indicating that frequent discussions on the topic actually occur; and 55% saying their board discusses cyber risk bi-annually or only when incidents occur. Many respondents highlighted that a presentation on cyber risk was given to the board only after specifically requested by a board member. Coupled with this, less than a quarter of FTSE 350 companies described the threat intelligence and cyber related management information they received as comprehensive or robust. Often cyber related management information is conveyed in technical terms and is not readily understood by a non IT-specialist audience, thereby reducing its value to the board.

Reliance on third parties

Only 16% of respondents indicated that their boards have a clear understanding of how their company's assets and information are shared with third parties. With third party relationships becoming ever more prevalent and complex against the backdrop of wider industrial movements of outsourcing; proliferation of cloud and online technology; and the need for ever more specialist services; the cyber risk profile associated with third parties is only magnified. Vulnerabilities at third parties potentially not only expose your organisations' systems directly to risk, often acting as a stepping stone to your systems environment; but also put your reputation on the line as those third parties may be processing your sensitive and customer data. Recent cyber incidents such as the successful appropriation of $81 million previously referred to are stark examples of where weaknesses in a participant bank's technology environment have raised wider questions around the reliability of the payment ecosystem and jeopardised the reputation of related payment processers and providers.

What should the board be doing?

If a board does not regularly consider cyber risk and receives poor threat intelligence information, how can the board effectively discharge its duties to direct the affairs of the company? In this digital networked age, consideration of cyber risk should be embedded into any strategic discussions concerning the business including exploration of new and existing market opportunities, product development decisions and major structural changes such as potential acquisitions, mergers or divestments. Failing to do so will expose the company to an unnecessary and unknown level of cyber risk.

The board should gauge its understanding of the organisation's cyber risk profile and seek to understand management activity through asking itself questions such as these:

- Are we aware of what indicators and metrics management use to gauge and measure cyber risk?
- What does the threat profile of the organisation look like and how this is impacted by potential changes in the internal and external environment?
- How many cyber incidents has the company experienced in the last year? How many of these are attributable to the same root cause?
- What cyber capability is available within and to the organisation? Where do we need help?
- Is cyber risk being treated solely as an IT risk, reflected through decisions such as how cyber budgets are allocated and how cyber leadership roles across the organisation are defined. Do all cyber leadership roles sit in IT?

Third party cyber risk – questions to support the board's understanding:

- Do we know which third parties and vendors have access to our systems?
- Which suppliers have access to personal or sensitive commercial data?
- Which third parties are exposing us to the highest level of potential cyber risk?
- How are we monitoring the cyber security capabilities of relevant third parties?
- Which of our third parties have experienced cyber incidents?

Deloitte View

- Cyber is a complex pervasive risk across the organisation that cannot be addressed via a point solution or in a linear fashion. Consideration and mitigation of cyber risk needs to be built into the DNA of an organisation's governance and decision making processes supported by strong leadership.
- We welcome the clear signs of improved awareness of cyber risk across FTSE 350 boards, however as the threat profile continues to grow, there is a need for boards to become more engaged to accelerate the board's involvement in driving the strategic response to this risk and there is a need for boards to become "cyber-intelligent".
- The board should challenge itself as to whether it has sufficient capability and understanding to drive the cyber risk agenda through reviewing the board composition; ensuring existing board members are receiving sufficient training and briefings and potentially nominating a specific director to take a lead.
- Boards should now seek actively to define and shape the company's cyber risk appetite. This requires regular and frequent dialogue with management on cyber risk supported by review and critical challenge underpinned by robust information.

Further information

Details of the 2015/2016 FTSE 350 government health check can be found at **https://www.gov.uk/government/publications/cyber-governance-health-check-201516**.

Contacts – Cyber Risk

Deloitte's Cyber Risk Practice assists organisations throughout the public and private sectors with their cyber challenges, including cyber risk assessment and strategy, implementing cyber-defences, providing threat intelligence and managed cyber services and helping organisations deal with the aftermath of a breach. For further information about the survey or the wider practice and to speak to a member of our team, please contact:

Phill Everson – 020 7303 0012 or **peverson@deloitte.co.uk**
Nick Seaver – 020 7303 7097 or **nseaver@deloitte.co.uk**
David Wallis – 020 7303 7739 or **dxwallis@deloitte.co.uk**

The Deloitte Academy

The Deloitte Academy provides support and guidance to boards, committees and individual directors, principally of the FTSE 350, through a series of briefings and bespoke training. Membership of the Deloitte Academy is free to board directors of listed companies, and includes access to the Deloitte Academy business centre between Covent Garden and the City.

Members receive copies of our regular publications on Corporate Governance and a newsletter. There is also a dedicated members' website **www.deloitteacademy.co.uk** which members can use to register for briefings and access additional relevant resources.

For further details about the Deloitte Academy, including membership, please email **enquiries@deloitteacademy.co.uk**.

Contacts – Centre for Corporate Governance

Tracy Gordon – 020 7007 3812 or **trgordon@deloitte.co.uk**
William Touche – 020 7007 3352 or **wtouche@deloitte.co.uk**
Corinne Sheriff – 020 7007 8368 or **csheriff@deloitte.co.uk**

Designed and produced by The Creative Studio at Deloitte, London. J8288