KPMG

ACI FTSE100 conversation about cyber risk

Audit Committee Institute

A conversation about cyber risk with Sir Iain Lobban, Partner at *Hakluyt Cyber* 14 September 2017

Sir Iain Lobban provided a fascinating insight into the cyber security landscape, describing some of the key perpetrators and drawing out the means that board members may already have at their disposal to help mitigate the risk. He closed the discussion by highlighting a number of key areas that board members may find beneficial to test with the executive.

The threat and its impact:

Sir Iain talked about the threat in terms of its impact upon Confidentiality, Integrity and Availability (C/I/A). Cyber-attacks involve a company's systems being compromised in one or more of these areas.

Confidentiality may involve stealing a business's private data, or exposing private information e.g., opinions from hacked emails against the organisation or an individual. Candid, privately held views, such as those exposed during the US election campaign, may end up in the public domain, destroying credibility.

Integrity relates to the health of data: damage to its integrity can cause adverse consequences. Organisational records or processes where data accuracy is key (e.g., health data or chemical recipes) can suffer major disruption by critical values being hacked and altered.

Availability of systems is key to business success. We live in a faster, more instantly available world than ever, and customers expect a quick, available on-line experience. On-line shopping for example, a customer may be prepared to wait a couple of seconds, but too long and patience is lost and custom taken elsewhere. Slowing down systems can cause enormous damage. Impact may go well beyond disruption into denial or even destruction.

The perpetrators:

Cyber attackers take many forms, from teenage computer 'geeks' to state actors, organised criminal groups and patriotic hackers, and often the lines between the groups may be blurred. Even in terms of official intelligence agencies, there are those regarded as 'good'; and 'bad' agencies. Western media reports will often speculate about the involvement of state actors in cyber-attacks – particularly in relation to Russia, China and North Korea.

The threat from insiders should not be underestimated. In large organisations with significant numbers of employees, there are likely to be, at any one time, a percentage of employees who are disenfranchised, potentially criminal or subject to criminal influence, or simply lacking in judgement. An understanding of employee attitudes together with monitoring their access to systems and activity can help mitigate the threat. Staff surveys may be a useful lens on their overall mood, but whatever mechanisms are used to garner information, consider reviewing the conclusions in the light of significant events. For example, a business announcing redundancies is a potential candidate for fresh exposure to disillusioned staff.

Mergers and acquisitions can create vulnerability even for organisations whose own cyber arrangements are very much in order, making the due diligence around systems an important part of the overall best practice for a merger. Following an acquisition, consolidation of data centres can provide an organisation with the very unwelcome surprise of reacquiring all of the malware that they had previously cleaned up, at a huge cost.

A few key areas to probe by non-executives:

— The frequency, depth and amount of time spent discussing cyber at ExCo and at board level.

— Organisational structure – where do accountability and responsibility lie for cyber security.

— The extent to which board/ExCo review and learn from high profile situations that other organisations have faced.

— The value of each of the different categories of data that an organisation might hold, and consideration of the impact, if confidentiality, integrity or availability are impacted through an attack.

— Understanding the organisation's third party relationships, and what controls exist around those with potential access to an organisation's proprietary data.

— Exploring involvement in industry-wide alliances, where organisations work together to detect and combat cyber-crime.

— The regularity with which a company's incident response plans are rehearsed and whether the scenarios are up to date - e.g. for ransomware.

— Regularity of and key findings from independent assessments of the company's systems.

— Number and nature of policy breaches in the last period, and the consequences both for the organisation and for individuals.

Forthcoming breakfast events

FRRP activity
Wednesday 1 November 2017

Our annual assessment of the current state of corporate reporting in the UK. We take a look at the findings of the FRC's overview of their Corporate Reporting Review (CRR) activities, draw out some of the main issues encountered during the past year and highlight those matters we have identified as potentially important in the next financial reporting period.

We will start with tea and coffee at 7:45am, sit down for breakfast at 8:00am and finish our discussion by 9:15am.

Conversation with a chairman
Wednesday 15 November 2017

Richard Burrows, chairman of British American Tobacco, joins us to give a board chairman's perspective on the audit committee.

We will start with tea and coffee at 7:45am, sit down for breakfast at 8:00am and finish our discussion by 9:30am.

Both breakfasts will take place at Number Twenty, Grosvenor Street, W1K 4QJ.

To reserve your place at either breakfast please email us or contact us on 0207 694 8855.

Tim Copnell
Chairman of the UK Audit Committee Institute
T: +44 (0)20 7694 8082
E: tim.copnell@kpmg.co.uk

kpmg.com/uk

Produced by CREATE I Document number: CRT088248A