QCA Corporate Governance Expert Group
Minutes of meeting: 14 January 2014

Held at 4.00pm on Tuesday 14 January 2014
at the offices of Wedlake Bell LLP, 52 Bedford Row, London, WC1R 4LR

Present:	Edward Craft (Chairman)	Wedlake Bell LLP	EC
	Colin Jones	UHY Hacker Young	CJ
	Victoria Barron	Hermes Equity Ownership Services	VB
	Edward Beale	Western Selection Plc	EB
	Rob Burdett	FIT Remuneration Consultants	RB
	Richie Clark	Fox Williams LLP	RC
	Louis Cooper	Crowe Clark Whitehall	LC
	Peter Fitzwilliam	Mission Marketing	PF
	David Fuller	CLA Holdings plc	DF
	Clive Garston	DAC Beachcroft LLP	CG
	Andrew Hobbs	EY LLP	AH
	David Isherwood	BDO LLP	DI
	Nick Janmohamed	Speechly Bircham LLP	NJ
	Sanjay Jha	Hybridan LLP	SJ
	Anita Skipper	Aviva Investors	AS
	Julie Stanbrook	Hogan Lovells International LLP	JS
	Nicholas Stretch	CMS Cameron McKenna LLP	NS
	Peter Swabey	ICSA	PS
	Melanie Wadsworth	Faegre Baker Daniels LLP	MW
	Cliff Weight	MM & K Limited	CW
	Tim Ward	Quoted Companies Alliance	TW
	Kate Jalbert	Quoted Companies Alliance	KJ
Guest Speaker:	Simon Kendall	BIS	SK
In Attendance:	Anna Taylor (minutes)	Wedlake Bell LLP	AT

ACTIONS

1. SIMON KENDALL, BIS – SPEAKING ON THE ISSUE OF CYBER SECURITY

EB welcomed SK and everyone introduce themselves.

Cyber security is major governance concern. The nature of threats ranges from large scale attacks on key international banks to the slow erosion of a business's competitive edge.

According to a breaches survey 93% of companies have experienced some form of breach. For smaller companies the figure is 87%.

Threats can derive from the following:

1.1 Nation States: Cyber attacks are a potentially low risk to the attacker and a largely anonymous means of pursuing:

(a) Economic espionage – by targeting intellectual property and know how; and

(b) Malicious damage to property.

Threats may be very simple or they may be well-resourced and sophisticated.

1.2 Terrorists: Historically they prefer 'real world' events but a shift is being seen towards the use of cyber-attacks.

1.3 Other Criminals: Software designed for cyber-attacks can be sourced internationally and used without detailed technical knowledge.

1.4 Activists: Cyber-attacks can be used as an effective form of humiliation.

Government Response

1.5 Now a tier 1 threat in the National Security Strategy (alongside armed conflict, major natural disaster and epidemic). The Cabinet Office is working alongside GCHQ, MOD, MI5, Home Office and BIS with businesses across the economic spectrum. The main victim of these crimes are businesses who suffer economic loss.

Corporate Governance Program

1.5.1 The Government are keen to raise awareness at Board level of cyber risk and get companies to treat it as a strategic risk.

1.5.2 This is a risk management issue and companies need to determine what their risk appetite is in terms of cyber threats and ask basic questions, such as:

(i) what are our key information assets?;
(ii) who has access to those information assets?; and
(iii) are those information assets adequately protected?

1.5.3 SK noted that companies can add value to business services by demonstrating to clients the importance of data protection and explore ways of minimising risks which accompany opportunities.

Government Actions

1.6 10 steps to Cyber security (publication): SK noted that this document helps companies to understand the basics of cyber security.

1.7 Cyber Security Sharing Partnership: SK explained that this is a platform where you can share information on cyber threats and attacks with other companies.

1.8 Networks and Security Directive: The European Commission would like to mandate companies to disclose any cyber breaches that have happened. The UK Government is pushing back on this and would rather approach this issue from a non-legislative route.

1.9 Cyber governance health check - audit committees of FTSE 350: SK noted that this is a study of the FTSE 350's approach to cyber security. The second part of this study is a diagnostic tool designed to work with companies to better protect against cyber threats.

1.10 Compliance and standards: SK explained that the Government is releasing an organisational standard on cyber security. Government departments will have to put the standard in place, and eventually companies that want to do business with the Government will need to have this standard in place, and therefore, could affect public procurement.

1.11 Investors: SK noted that BIS is liaising with investors in order to help them understand the threats and get them to ask companies that they invest in about their approach to cyber security.

1.12 Law Enforcement: SK noted that the National Cyber Crime Unit (SOCA and Metropolitan Police) has been developed.

2. POINTS RAISED AND RESPONSES

2.1 EC asked about verifying the degree of compliance and agreed that it was difficult to self-evaluate. He also raised questions about business' willingness to share information relating to cyber threats in competitive markets.

SK response: There is an industry understanding of the value of sharing real time information. The focus is on establishing a best practice of sharing information relating to cyber threats - not commercial secrets. So far around 250 organisations have signed up to the CISP. Technical experts are then able to analyse anonymous data and create products for members of CISP.

2.2 TW raised the point that the approach to cyber security must not be a 'box ticking' exercise. There needs to be a fundamental change in people's attitudes and behaviours (for example, instilling a culture in companies that encourages people to put their hand up when they may have downloaded something by mistake.

SK response: A culture is required from the top-down, which encourages employees to be alert to cyber security and to report any issues. The aim is to avoid creating a blame culture.

2.3 SJ raised questions about the quality of in-house expertise and whether businesses rely on IBM and Cloud (and equivalent) security systems, in which case how alert are these organisations to cyber threats?

SK response: Where there is a reliance on outsourcing contracts with external security, businesses must ensure they have sufficient technical capabilities to enable them to assess the standard of protection those contracts afford them and understand how those contracts interact with internal security measure. Effective due diligence must be carried out on contractors, particularly when they have access to the business' most commercially sensitive information.

2.4 AS queried whether cyber security is so important that businesses should be compelled to comply?

SK Response: BIS has a non-legislative approach and does not want to make companies disclose necessarily. Instead it sees the value in fostering best practice in this area.

2.5 VB raised the new SEC Guidance in the United States on this and how in more general terms the business supply chain should respond.

SK Response: SK emphasised the need for the 'second tier' (lawyers, accountants, etc.) to protect their clients and add value to the services through advising on cyber security. BIS is considering introducing training with the Law Society next year.

VB also queried what smaller organisations can do to address this issue.

SK Response: There is an SME version of the 10 Steps guidance. There is also currently a National Information Awareness Campaign called 'Streetwise'. 'Innovation Vouchers' worth £5,000 are also available to enable businesses to protect against cyber threats.

2.6 DI noted that there must be a move away from the yes/no approach to cyber security and a move away from over-reliance on IT departments. The issue of cyber security must be addressed by all company personnel.

2.7 LC noted that independent evaluation of cyber security measures may not remedy cultural attitudes, but it nevertheless is an effective means of ensuring the most commercially sensitive assets are sufficiently protected.

2.8 EB queried whether other organisations will introduce a security standard as the government proposes to.

SK Response: There is a move towards self-certification and independent evaluations with increasing international support.

2.9 EC queried what the Government standard on cyber security entailed.

SK Response: Corporate evidence was gathered in a survey last year. BIS are currently drawing from existing standards to produce a 'standard' and an 'assurance framework' appropriate for all business enterprises. Decisions need to be made as to what 'normal activity' looks like.

2.10 NJ asked how active insurers are in relation to cyber security.

SK Response: The risks are very difficult to quantify and there is little actuarial data beyond the results of breaches surveys. The impact has not been fully assessed.

2.11 SJ queried whether cyber threats are part of a natural progression from espionage seen 20 years ago and asked whether cyber threats could really be prevented.

SK Response: Cyber-attacks are a modern form of traditional espionage in many respects. The threat cannot be excluded completely but there are different levels of compromise. It is not a risk which can be eliminated but it can be managed.

2.12 EC noted that it would be useful to add questions to the next survey of the QCA/BDO Index broadly based on the questions raised in the FTSE 350 Cyber Government Health Check. For example:

2.12.1 What levels of training exist?
2.12.2 Can key assets be identified?
2.12.3 Who has access to key assets?
2.12.4 Where does ultimate responsibility lie?

2.13 Expert group members expressed a general concern on the lack of focus on cyber security in mid-size companies.

EC thanked SK for attending and SK left the meeting.

3. APOLOGIES

Apologies were received from Anthony Carey, Madeleine Cordes, Katie Elsdon, David Firth, Nick Greaves, Alexandra Hockenhull, Dalia Joseph, Claire Noyce (who was represented by her alternate Sanjay Jha) and Eugenia Unanyants-Jackson.

4. MINUTES OF THE LAST MEETING (12 NOVEMBER 2013)

4.1 JS queried what further action had happened on proxy advisors. EC noted that the group responded to the consultation on this before Christmas and the aim is to turn this into a document for quoted companies that explains the role of the proxy advisor.

5. CURRENT ISSUES

5.1 Corporate Governance Reporting Review

CJ noted that the aim is to have this document finalised by mid-February 2014 (in time for the 2014 reporting season). CJ explained that he will circulate a draft for the group to comment on shortly. **CJ**

5.2 Progress on revision of Audit Committee Guide for Smaller Quoted Companies (working group being led by CJ)

CJ reported that the first draft is underway and that the working group is due to meet again in February. CJ explained that the group is trying to coordinate with FRC to issue the guide alongside the publication of the FRC's revised guidance on going concern and risk management.

5.3 Work Streams and involvement of the group in these:

This was not discussed.

6. CONSULTATIONS

6.1 FRC: Risk Management, Internal Control and the Going Concern Basis of Accounting: Consultation on Draft Guidance to the Directors of Companies applying the UK Corporate Governance Code and Associated changes to the Code (response date: 24 January 2014)

LC noted that he will have the first draft of the response completed by the week ending 24 January 2014. LC explained that there is a lot of generic information in the revised guidance and that it would be helpful if there was greater clarity and more examples, as appeared in the old guidance. DI noted that some of his clients have mentioned the draft omits some of the more practical guidance from the 2009 document. AS highlighted that there are issues over the definition of a going concern and LC agreed, noting that there is a lack of consistency with the definition used in financial reporting. LC explained that Matthew Howells on the QCA Financial Reporting Expert Group was looking at this area of the response.

KJ will circulate the draft response to the expert group members for comment asap. **KJ**

6.2 **FCA CP13/15 – Feedback on CP12/25: Enhancing the Effectiveness of the Listing Regime and further consultation (Response date: 5 February 2014)**

EC noted that the Legal Expert Group is drafting a response on this. PS noted that the FCA's additional proposal in respect of minority and majority shareholders voting on a delisting is complicated. KJ noted that she will circulate the draft response for comment. **KJ**

6.3 **FRC Draft Plan & Budget 2014/5 (Response date: 28 February 2014)**

NS noted that there was nothing on remuneration in the draft plan. KJ explained that she is keen to know whether anyone has comments on the FRC's Draft Plan that would warrant a response. CJ noted that he was going to open meeting on this at the FRC. **ALL**

7. COMUNICATION/FOR NOTING AND FUTURE MEETINGS

7.1 FRC encourages better comply or explain disclosure and improved investor transparency

This was not discussed.

7.2 NAPF: Corporate Governance Policy & Voting Guidelines

CW noted that ISS and NAPF have ended their commercial relationship, which is interesting to note.

7.3 NAPF/Hermes: Remuneration Principles for building and reinforcing long-term business success

This was not discussed.

7.4 Guest invitations to future meetings

Sarah Wilson, Manifest, is attending 25 February meeting. EC proposed the April meeting would not have a guest speaker and focus on the revised Audit Committee guide.

7.5 Policy update (January 2014) quarterly update

This was not discussed.

8. AOB – NONE

9. ACTION POINTS

ACTION	PERSON	DATE
Circulate draft response to risk management and going concern paper	KJ	ASAP (Before 24 January 2014)
Circulate draft response to FCA CP13/15 – Feedback on CP12/25: Enhancing the Effectiveness of the Listing Regime and further consultation	KJ	ASAP (Before 28 February 2014)
Comments on the FRC's draft plan	KJ	Asap (Before 28 February 2014)

Date for next meeting: Tuesday 25 February 2014 (4pm)

(Venue: Wedlake Bell LLP, 52 Bedford Row, London WC1R 4LR)