FTSE100 Chairs' conversation about managing through a crisis

Audit Committee Institute

Conversation about managing through a crisis with Baroness Dido Harding – 27 September 2016

We were delighted that Baroness Dido Harding joined us to share her experience of crisis management – most notably managing through the October 2015 TalkTalk Plc cyber-attack.

Dido provided a brief overview of the crisis and its aftermath, noting how what initially appeared to be an issue about digital responsiveness and service interruption evolved into a major *"national incident"* involving, amongst others, GCHQ and the Metropolitan Police. With four million customers potentially affected, the TalkTalk board made the unprecedented decision of going public about the breach within just a day of the attack - with Dido fronting the media response. The initial parliamentary select committee report on cyber security[1] which the attack triggered recognises *"the strong crisis management response by TalkTalk and the prompt response and leadership shown by Dido Harding."* During the inquiry following the attack, Dido is also noted as acknowledging that *"Cyber security is a board level issue, and I am responsible for it."*

The following points arose from the discussion:

1 – An organisation can emerge from a difficult crisis with stronger brand value. *"It took a long time, it cost us a lot of money, it wasn't a good thing to happen, but my business is now stronger"*. Customers (and other stakeholders) value open and honest communications (even if it means admitting mistakes) and such an approach can be a powerful catalyst for re-gaining customer trust. [Customer opinion polling shows that TalkTalk customers trust the company more now than they did before the attack.]

2 – Whilst it is important for boards to seek expert insight and advice, ultimately boards are accountable for their own actions and must determine the appropriate course of action based on the specific circumstances, facts and culture of the organisation. Sometimes this may run contrary to the expert advice they receive.

3 – Inherited legacy systems - often de-prioritised and under-invested - present a cyber-security weak spot.

4 – The way that boards challenge needs to be fit for purpose and that may mean probing deeper than at present in less familiar areas. Questions such as *"Are we OK in terms of cyber security?"* or *"Are our systems safe?"* are unlikely to elicit responses that will provide the board with sufficient information about the risks and mitigating actions for effective decision making. Ultimately boards have to take difficult decisions because when it comes to cyber security there is no such thing as 'safe'. Dido provided an example, namely when would it be deemed safe to put the systems back on-line post-attack? Too soon and the security risks to customers may still be too high; too late and the delay in service and operations could irreversibly damage the business.

5 – *"Battlefield appointments"* can be made to ensure the right expertise, time and resources – unhindered by business as usual activity - are dedicated to crisis management.

6 – Crisis situations provide boards and management with a different perspective on colleagues' skill sets. Whilst some individuals thrive in an everyday 'peace-time' leadership role, they may be less effective in a crisis. Conversely, others who perhaps do not necessarily stand out on a day-to-day basis, may really come into their own and display amazing latent talent under conditions of adversity.

7 – Organisations may have expertise within the business that can be drafted into a crisis-management team on a secondment basis. For example, TalkTalk boosted their crisis communications team by co-opting people with a communications background into a central response team.

8 – Crisis planning, scenario testing and rehearsed protocols help businesses and boards respond more effectively to large-scale crises. Understanding who will do what and when, the decision-making process, communications with stakeholders and how the media response will be addressed are all important. *"Dealing with the business section of the newspaper is very different to being on the front page."* Whilst the precise response to any given crisis will be different, the preparedness of the board members and the steps to follow may prove easier if they have already rehearsed their response to a simulated pressure situation.

[1] The Culture, Media and Sport Committee first report for session 2016-17 "Cyber Security: Protection of Personal Data Online" Monday 20 June 2016.

9 – Learning from difficult situations is important - not just in terms of remedial actions and implementing controls to prevent future issues, but also in changing behaviours and implementing improved ways of working *per se*. For example, working through a crisis may drive greater emphasis on 'completer-finisher' behaviour. Dido described how the entire business is now focused on being *"more rigorous"* and in turn the board is providing more robust challenge to the audit and risk committee.

10 – A crisis can result in traditional reporting lines being rethought. For example, post-attack, TalkTalk have separated their Chief Technology Officer and Chief Security Officer roles to provide more dedicated support, challenge and assurance across both areas.

11 – While an understanding of technology and the agility to manage the consequential opportunities and risks are vital to the success of most companies, technology expertise is typically an under-represented area in the boardroom. IT talent can be hired at an executive level, but boards still need to be able to *"ask the right questions"* and just as important, *"understand the answers"*.

Members in attendance	
Tessa Bamford	Wolseley
Steve Barber	Next
Ian Barlow	Smith & Nephew
John Bason	Compass Group
Alexander Filshie	World First UK
Shirley Garrood	Hargreaves Lansdown
Kevin Parry	Standard Life
Caroline Silver	PZ Cussons

KPMG hosts	
Tim Copnell	Audit Committee Institute
Bill Holland	KPMG
Jon Mills	KPMG
Simon Richardson	KPMG
Tracey Stead	Audit Committee Institute
Adrian Stone	KPMG
Amanda Tickel	KPMG

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

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.