Cyber Security: Corporate insights for companies and their directors

> You would never dream of a CFO not coming to a board meeting. In addition, you would never see a CFO passing up using external audit or teams of external advisors. The same diligence has to be assigned to cyber security.
>
> Val Rahmani, Non-Executive Director, Aberdeen Asset Management.

1. Introduction

1.1 Cyber security is one of the most significant issues facing today's governments, companies and individuals, and accordingly has been the subject of much political attention in the US and UK in recent years. In 2015, President Obama pledged an additional $14bn to the US annual cyber security budget for the 2016 fiscal year. It has also featured heavily in the current US election debates between Hilary Clinton and Donald Trump. In the UK, there has been a flurry of government reports on the issue over the last few years – most notably, the "FTSE 350 Cyber Governance Health Check Report" (the "**Report**").[1] The UK Government has classified cyber security as a "Tier 1" threat, alongside international terrorism. Cyber security has emerged as a key issue on the world political stage; we suggest that it is treated likewise in the boardroom.

1.2 The increased focus on cyber security is unsurprising. Cyber attacks are increasing in scope and sophistication at a time when businesses are moving their key assets and systems to the digital sphere. Cyber crime is estimated to cost the UK £27bn a year[2] and the average cost to a large organisation of a security breach more than doubled between 2014 and 2015 to between £1.46m and £3.14m.[3] Furthermore, companies that fail to maintain adequate cyber security may be subject to claims by stakeholders and affected individuals as well as fines by regulators.

1.3 In our view, although some companies are taking action, companies are still not doing enough to secure their cyber safety. Although the Report shows some progress compared to previous years, there are worrying signs of complacency. Directors should accept that cyber security is neither a business "buzz word" nor a technological issue relevant only to IT teams. It is vital for the continued success and growth of business and thus deserves consideration at board level. By failing to implement robust risk and crisis management protocols, directors may expose themselves and their companies to significant legal risks, including potential breaches of directors' duties, corporate governance and disclosure obligations.

[1] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/521484/Cyber_Governance_Health_Check_report_2015.pdf.
[2] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60943/the-cost-of-cyber-crime-full-report.pdf.
[3] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/432413/bis-15-303_information_security_breaches_survey_2015-executive-eummary.pdf.

Executive Summary

(A) Directors should take action to protect their companies from the risk of cyber attacks. Their failure to do so could expose them and their companies to legal, financial and reputational risks.

(B) Directors should implement a robust and proactive cyber security policy, combined with a disciplined and rigorous board oversight process and which is appropriate to their company.

(C) To meet these objectives, a company should:

(i) appreciate which of its assets and systems are at risk of cyber attack and what the ramifications of such an attack might be;

(ii) assess and develop systems to protect these assets and systems; and

(iii) monitor the specific cyber threats that the company faces.

Doing so will help companies not only to mitigate commercial and legal risks, but also to drive commercial growth by better utilising new and existing technologies.

(D) Companies with a clearly defined cyber security policy will be well placed in the increasingly complex regulatory landscape.

2. The Report

2.1 The Report, which was published by the Department for Culture, Media and Sport ("**DCMS**") in May 2016, assesses the extent to which boards and audit committees of the top 350 UK listed companies engage with cyber security threats to their business. The Report serves as a benchmark of the progress that companies made in 2015, compared to the previous surveys in 2014 and 2013.

2.2 The Report shows that respondents recognise the scale and importance of cyber security. Almost half (49%) of businesses place cyber risk as a top risk faced by the business and 90% of respondents felt that cyber risks were either reasonably or clearly described in the company's risk register.

2.3 However, this apparent awareness of the importance of cyber security has not prompted proper engagement with the issue. Response rates to the Report in 2014 and 2015 have fallen by 50% (compared to 2013, the first year of the survey). Furthermore, only 12% of main boards indicated that they regularly and thoroughly review their key information and data assets. Only 6% of boards were described by their audit chairs as "fully informed and skilled" in respect of cyber security.

2.4 The disconnect between the importance of cyber security issues and the response from companies may be due to complacency or a lack of familiarity with the area. Regardless of the reasons, this disconnect should not persist.

3. Directors' duties

Directors who fail to appropriately manage cyber security risk may infringe their legal duties to promote the success of the company and to exercise reasonable care, skill and diligence.

Duty to promote the success of the company

3.1 The duty to promote the success of the company requires directors to promote an increase in the long-term value of the company, having regard to, among other things, the interests of the company's shareholders, employees, customers and suppliers. As part of their duty to promote the success of the company, directors must consider the impact of the company's operations on the community.[4] We believe that a board's failure to understand and mitigate cyber security risk could entail a breach of this duty.

3.2 Cyber attacks – which often entail the loss of commercially sensitive and valuable information, disrupted logistics, damaged reputations and expensive remediation programmes – can seriously harm a company's long-term value.[5] The 2015 Information Security Breaches Survey, commissioned by DCMS, put the average cost to a large company of dealing with their worst single breach at between £1.46m and £3.14m.[6] The damage can, however, be much worse. Target Corporation, following an attack in 2013 that compromised the financial and personal information of 110m customers, saw a 46% drop in profits during its fourth quarter of 2013. Sony lost a reported $171m[7] following the security breach of the PlayStation Network in 2011 and another £35m (in order to restore financial and IT systems) as a result of the cyber attack it suffered in November 2014.[8] TalkTalk was also hit with an estimated £60m loss following the attack on its business in October 2015.[9] Although the Report indicates that an increasing number of companies appreciate the link between securing critical information assets and shareholder value (up to 65% from 54% in 2013), this does not appear to be reflected in the way boards approach cyber security.

3.3 Poor cyber risk management could also jeopardise sensitive information to the detriment of shareholders, employees, customers, suppliers and the wider community. Data breaches often lead to follow-on crimes, such as theft and identity fraud. Where sensitive information is compromised on a particularly large scale, the repercussions can reverberate deep into the community. Many banks, following the cyber attack on Target Corporation, decided to limit overdrafts, re-issue credit and debit cards and monitor account usage in respect of those customers that may have been affected. Where the information accessed is commercially sensitive, it may be used to make financial gain, thereby disrupting the proper functioning of the capital markets.

[4] Section 172, Companies Act 2006.
[5] http://www.forbes.com/sites/maggiemcgrath/2014/02/26/target-profit-falls-46-on-credit-card-breach-and-says-the-hits-could-keep-on-coming/.
[6] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/432413/bis-15-303_information_security_breaches_survey_2015-executive-eummary.pdf.
[7] http://www.forbes.com/sites/insertcoin/2011/05/23/sony-pegs-psn-attack-costs-at-170-million/
[8] http://www.eweek.com/security/sony-pegs-initial-cyber-attack-losses-at-35-million.html .
[9] http://www.ft.com/fastft/2016/02/02/cyber-attack-cost-talktalk-up-to-60m/.

Duty to exercise reasonable care, skill and diligence

3.4 The duty to exercise reasonable care, skill and diligence requires directors to exercise the same care, skill and diligence that would be exercised by a reasonably diligent person with the knowledge, skill and experience that may be reasonably expected of: (i) a person carrying out the same functions in relation to the company as the director and (ii) the actual director in question.[10] Consequently, directors who fail to manage cyber risk adequately will not be able to defend their actions on the basis that they acted according to their own understanding and abilities, if more could reasonably be expected of directors in their position. Further, the standard to which the directors will be held in respect of the management of cyber risk will depend not only on the value of the company's digital assets, but also the extent to which the company relies on online systems. For instance, there may be a higher standard of care and skill expected in the management of cyber risk from the board of a technology or financial services firm than from a board operating in the construction industry.

3.5 Nearly all businesses have assets in the digital sphere and in 2015 90% of large companies suffered a breach.[11] This makes cyber risk an inescapable part of business. In 2015 the Financial Policy Committee stated that cyber security is not a technical issue and that the board of directors must drive a culture of resilience throughout their business.[12] Although directors need not acquire cyber expertise on an individual level, prudent oversight requires that such expertise is present at a suitably senior level within the organisation.

UK Corporate Governance Code

3.6 Many of the principles that a board must consider in order to comply with directors' duties apply equally in the field of corporate governance. The UK Corporate Governance Code (the "**Code**") requires that the board and its committees have the appropriate balance of skills, experience, independence and knowledge to enable them to discharge their duties and responsibilities effectively. Directors are also expected to assess and mitigate the principal risks facing the company, and UK listed companies must make a statement to this effect in their annual report.[13]

3.7 Although the Code is not legally binding, a company must explain any failure to comply with its recommendations to shareholders, and this obligation should not be taken lightly. The Institutional Shareholder Services' ("**ISS**") UK and Ireland Proxy Voting Guidelines, state that, under extraordinary circumstances, ISS will consider recommending a vote against individual directors for material failures of governance, stewardship or risk oversight. We believe that a failure to implement adequate cyber security systems could represent such a failure. Indeed, following the cyber attack on Target, ISS USA issued a voting recommendation against the election of all members of Target's audit and corporate responsibility committees at the company's annual general meeting on the basis that the executives should have been "more closely monitoring the possibility of theft of sensitive information."[14] Following the breach, Target's CEO and chief information officer both resigned from their roles amid public and shareholder pressure.

[10] Section 174, Companies Act 2006.
[11] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/432413/bis-15-303_information_security_breaches_survey_2015-executive-eummary.pdf.
[12] http://www.bankofengland.co.uk/publications/Documents/fsr/2015/fsrfull1507.pdf.
[13] https://www.frc.org.uk/Our-Work/Publications/Corporate-Governance/UK-Corporate-Governance-Code-April-2016.pdf.
[14] http://www.startribune.com/business/260960251.html.

Mitigating the risk of a breach

3.8 In order to act in a way that promotes the success of the company and demonstrates reasonable care, skill and diligence, directors should show an active and informed engagement with the company's cyber security profile.

3.9 Unfortunately, the evidence shows that it is more common for companies to consider cyber security at Executive Committee, Audit Committee or Security Committee level than at main board level. Few companies view cyber security as sufficiently important to require that a board-level seat be dedicated to someone with relevant expertise, though some FTSE 100 firms are beginning to adopt this approach. For example, HSBC appointed Lord (Jonathan) Evans of Weardale, the former director general of MI5, as an independent non-executive director and a Chairman of the Financial System Vulnerabilities Committee (which has been set up to help the bank identify areas where it could be exposed to financial crime). Interestingly, in 2014 Sir David Walker, former Chairman of Barclays plc, cited cyber expertise on the main board as a "necessary ingredient" of good corporate governance.[15]

3.10 Although delegation of cyber security matters does not, of itself, prevent directors from fulfilling their duties of management and oversight, directors cannot abdicate their responsibility to manage risks that are of significance to the company.[16] Directors who do not deal directly with the matter at board level, should ensure that they scrutinise the role and findings of relevant sub-committees, demand information at appropriate intervals and remain involved in developing the company's cyber security protocols.

3.11 Unfortunately, the Report indicates that this proactive involvement is not commonplace. Only 6% of audit chairs felt that the main board was "fully informed and skilled" in respect of cyber security. This figure is perhaps unsurprising, though not defensible, in light of the fact that only 23% of boards were reported to regularly consider cyber security issues or actively manage their exposure to cyber risks.

3.12 Directors have little excuse for failing to develop an effective cyber strategy, given the proliferation of guidance on the topic. In the UK, for example, the Government has issued "The Ten Steps" guidance,[17] which offers practical steps in areas such as protecting network security, incident management and ICT monitoring systems. The Report shows that this guidance is now used by a majority of respondents. In the US, the National Association of Corporate Directors and the National Institute for Standards and Technology have each published reports which provide companies with a set of industry standards and best practices for managing cyber security risks.

[15] http://www.ft.com/cms/s/0/e6cf88ac-7fa4-11e4-b4f5-00144feabdc0.html.
[16] Re Barings [1999].
[17] http://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility/10-steps-summary

3.13 Effective management of cyber risk does not require a company to achieve immunity from cyber breaches. Such an aim would be unrealistic. According to Sadie Creese, Professor of Cybersecurity at the University of Oxford: "We tell managers 'assume you've been compromised.'"[18] Further, the variety of ways in which a company can manage its cyber profile means that there is no objectively correct way of approaching cyber security that all boards should attempt to follow. Although the pace of change and the complex nature of the topic make cyber security daunting for many boards, an informed, proactive and diligent board that takes appropriate steps to ensure that cyber security is appropriately managed should be able to mitigate the risk of issues arising from a corporate governance and directors' duties perspective.

4. Disclosure obligations

4.1 In the context of cyber security, there is a tension between secrecy and transparency. On the one hand, companies are reluctant to admit that they have been hacked for fear of potential reputational damage, loss of customers and litigation. A company may also worry that disclosing a cyber attack could expose its technological weaknesses, thereby making it more vulnerable to further attacks. The desire for secrecy, though understandable, is counterproductive and at odds with the openness expected of UK companies. There are growing expectations that companies should collaborate with one other (and with government agencies) to share information and intelligence on cyber security threats. For example, the Cyber-security Information Sharing Partnership offers a platform for secure online collaboration where government and companies can exchange information to help strengthen their cyber security.

4.2 In contrast to regulators in other jurisdictions, the UK Listing Authority (the "**UKLA**") has not yet issued any guidance for listed companies that specifically addresses cyber security. In Hong Kong, the Securities and Futures Commission and the Hong Kong Monetary Authority have issued recent guidance in respect of cyber security for companies operating within the financial services industry. In Canada, the Ontario Securities Commission has issued similar guidance. Perhaps the most detailed guidance comes from the United States, where the Securities and Exchange Commission ("**SEC**") issued guidance in October 2011 in respect of how existing rules should be interpreted in light of cyber security (the "**SEC Guidance**"). Although the SEC Guidance is not binding on UK listed companies, it offers principles that can be applied analogously to the UK disclosure framework. Even in the absence of clear guidance from the UKLA, we believe that there is a strong case for UK listed companies to disclose significant cyber attacks in three areas: prospectuses, annual reports and under the Disclosure Guidance and Transparency Rules (the "**DTRs**") and the Market Abuse Regulation ("**MAR**"), each of which is considered below.

Disclosure in a prospectus

4.3 Under the Prospectus Rules, a UK listed company that is required to prepare a prospectus prior to raising equity or debt on the capital markets, must set out in the prospectus a comprehensive and specific description of all the risks relevant to the issuer, the industry in which it operates and the securities to be offered or listed. In our view, an issuer would be expected to disclose the risks posed by cyber threats, where such risks are material to the company or its industry and would make an investment in the securities of such company particularly risky. The SEC Guidance

[18] http://www.bbc.co.uk/news/30925696.

is useful (but non-binding) for UK companies when considering their disclosure obligations: "registrants should consider the probability of cyber incidents occurring and the quantitative and qualitative magnitude of those risks, including the potential costs and other consequences resulting from misappropriation of assets or sensitive information, corruption of data or operational disruption."[19]

4.4 If a company considers a cyber threat to be an appropriate risk factor to be disclosed in a prospectus, it is not sufficient for the issuer to include generic "boilerplate" language to describe the risk. Instead, the issuer will be expected to tailor the description of the risk to the particular issuer and its industry so that it provides sufficient insight into the nature of the risk and how it could affect the investment. This may include, where appropriate, the potential costs and other consequences of a cyber attack.

4.5 Companies that fail to provide sufficient information in respect of a cyber attack may attract criticism from shareholders and institutional investor bodies. For example, Betfair Group plc (now Paddy Power Betfair plc) attracted criticism for failing to disclose, in its 2010 flotation prospectus, a cyber attack that occurred six months prior to the flotation which resulted in the theft of more than 3m Betfair account names, 2.9m user names and addresses and details of nearly 90,000 bank accounts.[20] Betfair included a single sentence in its prospectus, which downplayed the severity of the recent cyber attack: "Betfair has experienced a limited number of security breaches in the past… which have not had a significant effect on Betfair's reputation, operations, financial performance."[21] Many commentators expected Betfair to provide more specific and tailored information not only to comply with the prospectus disclosure obligations, but also to minimise adverse publicity.

Disclosure in annual reports

4.6 Annual reports are another area where UK listed companies should carefully consider their disclosure obligations in the context of cyber security. Under the Companies Act 2006 and the DTRs, a company's annual report should contain a description of the principal risks and uncertainties facing the company and an explanation of the measures the company has taken to manage or mitigate these risks and uncertainties.[22] In our view, cyber threats – whether actual or expected – could constitute a principal risk, depending on the nature and severity of the threat. Investors are keen for companies to disclose not only the theoretical cyber risks, but also those risks that have actually materialised.

4.7 In its 2016 annual report, BT identified security and resilience among its principal risks: "A malicious cyber-attack or breach of our security could mean our data is lost, corrupted, disclosed or ransomed, or that our services are interrupted. A big interruption to our services, from cyber-attack or otherwise, could mean immediate financial losses from fraud and theft; contract cancellations; lost revenue from not being able to process orders and invoices;

[19] CF Disclosure Guidance: Topic No. 2, Securities and Exchange Commission, 13 October 2011, http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.
[20] http://www.telegraph.co.uk/finance/newsbysector/retailandconsumer/8797993/Betfair-is-in-for-a-rough-ride-over-data-theft.html?mobile=basic.
[21] Betfair Group plc prospectus, 2010.
[22] Section 414C(2)(b) CA 06 and DTR 4.1.8(2). This position is supported by investor bodies (e.g. NAPF Guidelines, Appendix 1, Section C, para C.2.1 and Para 2.1 ABI Disclosure Guidelines).

contractual penalties; lost productivity and unplanned costs to restore and improve our security; prosecution and fines"[23] BT is not alone in disclosing cyber risks in its annual report. Almost two thirds (63%) of the UK listed companies who responded to the Report claimed to have outlined their approach to cyber security clearly in their annual reports and on their websites.[24] We expect that this percentage will rise in the future as companies become more familiar with their disclosure obligations.

4.8 By contrast, in the US, disclosure of cyber risks by companies in their annual reports is more prevalent than in the UK. This is due, in part, to the SEC Guidance which notes that an issuer should explain how it expects a material cyber attack to affect its financial position, including liquidity, future cash flows and impairment charges. Where the issuer does not have sufficient information to make a definitive statement, it should rely on estimates which should be re-assessed and revised as appropriate. Following this guidance, banks such as Bank of America, Citi, Wells Fargo and JPMorgan Chase have reported that their systems have experienced cyber attacks in their annual reports.[25]

Disclosure in accordance with the Disclosure Guidance and Transparency Rules and the Market Abuse Regulation

4.9 A UK listed company is under a general obligation to notify the market as soon as possible of any inside information. Inside information is information which: (i) directly or indirectly concerns the company; (ii) is not generally available; (iii) is sufficiently precise; and (iv) if made public, would be likely to have a significant effect on the share price (which is assessed by asking whether a reasonable investor would use the information as part of the basis of his or her investment decisions).[26]

4.10 Ultimately, whether the existence of a cyber attack amounts to inside information requiring disclosure under the DTRs is a judgment call for each company and its advisers.[27] However, our review of US and UK listed companies that have suffered cyber attacks suggests that such attacks may indeed have a significant effect on the share price of the target company (see Table 1), which was recently held to include any effect on price that is more than trivial.[28] For example, the share price of Heartland Payment Systems fell by almost 50% in 2009, following an announcement by the company that its systems had been compromised by a global cyber fraud operation. Although Heartland Payment Systems stands out for the magnitude of its share price fall, the 11 companies noted in our table experienced an average share price decline of 12.5% (one month after the event) – clearly a significant effect on the share price. There were only three examples where the share price decline was less than 5%.

[23] BT Group plc, Annual Report & Form 20-F 2016, page 49.
[24] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/521484/Cyber_Governance_Health_Check_report_2015.pdf.
[25] http://www.washingtonpost.com/world/national-security/more-companies-reporting-cybersecurity-incidents/2013/03/01/f7f7cb68-8293-11e2-8074-b26a871b165a_story.html.
[26] Article 7 and 17 MAR.
[27] DTR 2.2.7G.
[28] Hannam v FCA [2014] UKUT 0233 (TCC).

Table 1: Share price declines of selected major US and UK listed companies following cyber attacks

Company name	Date of announcement of cyber security breach	Drop in share price following breach (%)	
		Three days	One month
Verizon	24 March 2016	0.29%	4.74%
TalkTalk	21 October 2015	14.4%	14.55%
Ebay	21 May 2014	1.48%	7.35%
AOL	28 April 2014	1.70%	23.56%
Target	19 December 2013	2.41%	5.79%
Adobe	3 October 2013	2.91%	4.04%
KT Corporation	29 July 2013	1.30%	5.82%
Ubisoft	2 July 2013	2.48%	2.48%
Betfair Group Ltd	30 September 2011	13.67%	13.67%
Heartland Payment Systems	20 January 2009	46.3%	49.54%
TK / TJ Maxx	17 January 2007	1.82%	6.49%

4.11 Given the frequency of cyber attacks, the relative lack of disclosures of cyber attacks by UK companies is surprising. One notable exception is TalkTalk Telecom Group PLC, which, in October 2015, announced to the market that a criminal investigation had been launched by the Metropolitan Police Cyber Crime Unit following a significant cyber attack on the company's website. This initial announcement was followed by two further market updates in the two consecutive weeks, which together provided the market with detailed descriptions of the extent of the personal customer data that was compromised by the cyber attack.[29]

4.12 Specific disclosures following a cyber security breach are more common (and more detailed) in the US. For example, eBay,[30] Adobe,[31] Target,[32] Home Depot[33] and AOL[34] have all provided extensive SEC filings. We expect that this is due, in part, to the SEC Guidance, which covers the extent of disclosure that is expected of US companies following a cyber attack.

[29] TalkTalk Telecom Group PLC's RNS announcements numbered 1902D, 0464E and 8130E.
[30] http://investor.ebayinc.com/secfiling.cfm?filingID=1065088-14-97&CIK=1065088.
[31] https://helpx.adobe.com/uk/x-productkb/policy-pricing/customer-alert.html#read_faq.
[32] http://investors.target.com/phoenix.zhtml?c=65828&p=irol-SECText&TEXT=aHR0cDovL2FwaS50ZW5rd2l6YXJkLmNvbS9maWxpbmcueG1sP2lwYWdlPTk0MjE2NjAmRFNFUT0wJlNFUT0wJlNRREVTQz1TRUNUSU9OX0VOVElSRSZzdWJzaWQ9NTc%3d.
[33] http://ir.homedepot.com/phoenix.zhtml?c=63646&p=irol-SECText&TEXT=aHR0cDovL2FwaS50ZW5rd2l6YXJkLmNvbS9maWxpbmcueG1sP2lwYWdlPTk4MTA2MTgmRFNFUT0wJlNFUT0wJlNRREVTQz1TRUNUSU9OX0VOVElSRSZzdWJzaWQ9NTc%3d.
[34] http://ir.aol.com/phoenix.zhtml?c=147895&p=irol-SECText&TEXT=aHR0cDovL2FwaS50ZW5rd2l6YXJkLmNvbS9maWxpbmcueG1sP2lwYWdlPTk1NDg0MjgmRFNFUT0wJlNFUT0wJlNRREVTQz1TRUNUSU9OX0VOVElSRSZzdWJzaWQ9NTc%3d.

4.13 It is difficult to determine the reason for the relative scarcity of announcements by UK listed companies following a cyber attack. It may be that companies are concluding that information in respect of a cyber attack does not constitute inside information. It is arguable whether this conclusion is supportable in all instances. Companies may also be reluctant to reveal sensitive information.[35] Further, companies are permitted to delay disclosure in two circumstances. First, when faced with an unexpected and significant event, such as a cyber attack, an issuer is allowed a short delay prior to disclosing inside information in order to clarify the situation, provided that the issuer releases a holding announcement where there is a danger of inside information leaking before the facts and their impact can be confirmed.[36] Second, a UK issuer may delay the public disclosure of inside information to avoid prejudicing its legitimate interests, provided that such omission would not be likely to mislead the public and the confidentiality of the information can be guaranteed.[37]

4.14 It is arguable that a UK issuer may be permitted to delay disclosure of a cyber attack while it conducts tests to investigate the extent of the damage, and bolsters its defences. Further, there may be situations where the company's response should be kept confidential until developments are at a stage when the issuer can make an announcement without prejudicing its legitimate interests. The permitted delays in disclosure do not entitle companies to avoid disclosure indefinitely, although companies are not expected to disclose information which may render them vulnerable to further cyber attacks. The US regulator made a similar point in the SEC Guidance, in which it said that the SEC is "mindful of potential concerns that detailed disclosures could compromise cyber security efforts – for example, by providing a roadmap for those who seek to infiltrate a registrant's network security – and we emphasize that disclosures of that nature are not required."[38] Even so, companies should not use the concern about compromising cyber security efforts as an excuse for disclosing inadequate information following a significant cyber attack.

[35] http://www.bloomberg.com/news/articles/2012-11-04/coke-hacked-and-doesn-t-tell.
[36] DTR 2.2.9G(2).
[37] Article 17(4) MAR.
[38] CF Disclosure Guidance: Topic No. 2, Securities and Exchange Commission, 13 October 2011, http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

Focus: Key Findings of the Report[39]

> **Company boards are improving their understanding of cyber risks and taking them more seriously than ever before. However progress needs to be made in understanding where key data is shared with third parties and the impact if this goes wrong.**
>
> Ed Vaizey, former Minister of State for Culture and the Digital Economy.

Since the Government first published its Cyber Security Strategy in 2011, the official figures have largely painted a positive picture, of companies becoming better at dealing with cyber threats and boards apparently more engaged than ever before with the issue. Indeed, the statistics suggest that there have been some significant improvements since the publication of the 2014 FTSE 350 report.

63% of boards
clearly set out their risk management approach in their annual reports

33% of boards
have clearly set and understood their appetite for cyber risk
up from 18% in 2014

16% of boards
have a very clear understanding of where the company's key information/ data assets are shared with third parties
up from 11% in 2014

49% of businesses
place cyber risk as a top risk (compared to other risks faced)
up from 29% in 2014

49% of boards
have a clear understanding of the potential impact of loss/disruption of key information and data assets

77% of businessess
have allocated budget specifically to protect consumer data

[39] Contains public sector information licensed under the Open Government Licence. The full report can be found at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/521484/Cyber_Governance_Health_Check_report_2015.pdf

However, these improvements mask the more concerning findings of the latest Report, which in our view demonstrate that there is still a large gap between the principles for establishing and maintaining effective cyber security systems and how organisations engage with cyber security issues in practice.

Decrease in responses from board chairs	In 2015, there were no responses to the survey from those who were the Chair of the main board (down from 85% in 2013 and 25% in 2014) – this decrease suggests a desensitisation to the issue following a period of engagement, which is further indicated by the fact that in 2015 only 113 companies responded to the survey (down from 218 in 2013).
Decrease in response rates generally	Worryingly, response rates in most sectors (with the exception of technology, communications and healthcare and consumer goods) have fallen considerably in comparison with 2013, with only the technology, financial services and utilities and resources sectors improving on 2014 responses.
Failure to review key information and data assets	Only 12% of main boards regularly and thoroughly review their key information and data assets. Although this has increased on previous years, of particular concern is the fact that the majority of main boards rarely (41%) or never (19%) do so. In addition, over 60% admit to rarely or never reviewing such information to confirm the risk management, legal, ethical and security implications of retaining them.
Limited understanding of supply chain and data sharing arrangement risk	Only 46% of the main boards have a basic understanding of key information and data sharing arrangements with third parties (e.g. suppliers).

© Slaughter and May 2017

This material is for general information only and is not intended to provide legal advice.
For further information, please speak to your usual Slaughter and May contact.