Taking the pulse: what we can learn from the latest FTSE 350 Cyber Health Check?

March 2019

The UK Government has published the FTSE 350 Cyber Governance Health Check 2018, its annual "barometer of how corporate Britain is responding to the ongoing challenge of cyber threats." The report demonstrates an increasing awareness of cyber risk at board level, but also that there remains key practical steps to take to embed cyber security into organisations and avoid it becoming merely a tick box exercise.

As the UK strives to become a world-leading digital economy at the forefront of digital innovation and security, the Government continues to look at ways to help businesses, and their boards, understand and manage cyber risk.

The latest annual FTSE 350 Cyber Governance Health Check gives an insight into how the UK's leading companies are prioritising and managing cyber risk, and good practices companies can follow to increase their cyber readiness.

What is the FTSE 350 Cyber Governance Health Check?

The Government's annual survey of the UK's leading 350 companies has been an important part of its cyber security strategy since 2013. In 2018, 94 businesses from a range of sectors (in particular financial services and consumer goods companies) responded to a survey designed to illustrate the maturity of their cyber risk management. The survey is used by Government as an indicator of the health of the broader economy, and gives companies an insight into what others are doing to manage an evolving cyber risk.

The report at a glance

Increased awareness

The report shows that cyber is now a board level issue, with the majority of respondents from the UK's top companies rating cyber risk as high or very high (up from 25% in 2013 to 72% now). Almost all respondents now have a cyber strategy, and board understanding regarding cyber security continues to increase. For example, more boards than last year understand both their business's critical information, data assets and systems, and the potential impact from loss or disruption to these (although some of these figures are still relatively low).

More action needed

However, the report also gives a strong sense that more action is still needed to ensure this awareness results in the right behaviours and practical tools to embed cyber resilience into an organisation. The following table sets out some:

- issues identified in the report; and
- actions, and good practice tips, we have drawn from the report and our experience of advising on cyber incidents and risk management.

ISSUE IDENTIFIED BY REPORT	SUGGESTED ACTION
Cyber strategy: while most businesses have a cyber strategy, only two thirds have one that is aligned with their business objectives (suggesting a third still see cyber as a predominantly operational issue) and less than half have a dedicated budget for it.	Understand what cyber risk means to your business (operationally, reputation, regulation etc.). Ensure your cyber strategy aligns to business objectives (so "business' goals and KPIs disseminate to employee performance metrics and…cyber security is embedded throughout the organisation") and allocates sufficient resource. Also, understand and document your risk appetite (through qualitative statements and associated quantitative metrics) and manage, rather than merely monitor, cyber risk through your risk register.
Incident response plan: many businesses have an incident response plan, but are not testing it on a regular basis. Even fewer are using external audits to check their incident plans are fit for purpose or are running cyber crisis simulation exercises with their boards.	11% of respondents experienced a major cyber incident which disrupted their business in the last 12 months, and a good incident response plan can help you quickly respond to threats and limit long-term damage. However, cyber threats evolve over time and regular testing is important to ensure your plan stays relevant, and that everyone in your organisation knows their responsibilities in case of an incident. Internal and external audits, penetration testing, vulnerability testing, regular crisis simulation, benchmarking and discussions with consultants and staff were all cited by organisations who responded to the survey as ways they test their plans.
Supply chain risk: supply chain risk is increasing. While the risk is recognised, the majority of boards do not understand risks further down their supply chains (second tier/ fourth party and beyond) leaving them vulnerable.	In today's complex supply chain landscape, ensure you understand how your supply chain works beyond those organisations you contract with directly. Do your DD and use contractual flow down requirements to secure minimum security standards (and adoption of schemes such as Cyber Essentials if these are used in your business) in contracts with suppliers. NCSC guidance on supply chains may help organisations understand this risk and establish effective oversight of their supply chain. Also consider non-BAU activities involving third parties which could create a similar cyber risk (for example M&A activity).
Board awareness and expertise: general awareness has increased, but there is still room for improvement. For example, only: • 12% of respondents rated board understanding of the business's information, data and systems as fully comprehensive; • 16% stated that their boards have a comprehensive	Ensure your board has the right expertise (e.g. engage NEDs with a technology background and consider nominating a board member to take lead responsibility) and is given the right information. The CISO or an appropriate staff member should clearly communicate information to the board on a regular basis in a way that aligns with business objectives. The board and GC should review and challenge information provided to it. Having a CISO which reports directly to the board may also help. Where this happens boards are more likely to consider that the information they receive is comprehensive. However, the report recognises that it cannot conclude from the data received whether that

understanding of all types of impact tested (i.e. threats on customers, share price and reputation); and • 15% rated board understanding of their personal, legal and fiduciary responsibilities as comprehensive (although half did still score their boards highly on this).	information is more comprehensive, or if boards with a more comprehensive understanding of cyber are more likely to request that the CISO reports directly to them. The Government have said this is something they will explore further in future Health Checks. The report also highlights that the Financial Reporting Council has recently updated its Corporate Governance Code which underpins the board's fiduciary duties. The Risk Management and Internal Control section may be a useful source for board members, although it does not contain specific information about cyber risk.
Keep up-to-date with Government guidance and new regulations: the GDPR, for example, appears to have increased board engagement with cyber and resulted in increased security measures.	The majority of boards are responding to Government advice and over half have specifically stated that they have used the Government's 10 Steps to Cyber Security. The report refers to a number of NCSC guidance notes, including its board toolkit and the NCSC/ICO GDPR Security Outcomes guidance. Also, while the GDPR does seem to have played a role in increasing board discussions on cyber, cyber risk and regulation is much broader than data/personal data. In our experience it is also best managed when it is seen as a business risk requiring top levels of corporate governance, not just a 'personal data' risk.

At Slaughter and May we recognise that cyber risk is a key concern for boards. We have developed a range of materials and training sessions that we would be happy to share with you and your boards, including our cyber breach response checklist. For more information on how we can help you with any Cyber related matter, please contact Rob, Victoria, Richard, Natalie or your usual Slaughter and May contact

Rob Sumroy
T +44 (0)20 7090 4032
E rob.sumroy@slaughterandmay.com

Natalie Donovan
T +44 (0)20 7090 4058
E natalie.donovan@slaughterandmay.com

Richard Jeens
T +44 (0)20 7090 5281
E richard.jeens@slaughterandmay.com

Victoria MacDuff
T +44 (0)20 7090 3104
E victoria.macduff@slaughterandmay.com