# Is regulation keeping pace with cyber's evolving threat?

May 2017

**The Government has stated it is committed to making the UK the safest place in the world to go online - a worthy, and ambitious, intention. But are they doing enough to help businesses in this area?**

In December the Department for Culture, Media and Sport published the results of its Cyber Security Regulation and Incentives review, which looked at whether there was a need for additional regulation or incentives to boost cyber risk management across the wider economy (i.e. outside the area of critical national infrastructure). The headline conclusion is that no additional regulation is required, beyond that planned for personal data - and the report stresses in a number of areas how the Government will use the implementation of the new General Data Protection Regulation (GDPR) next May to further its cyber agenda. However, in reaching that conclusion, it provides some useful insight into its current thinking on the evolving cyber threat, plans for the NIS Directive and how good cyber risk management could be better embedded into corporate governance processes. It also looks at a number of incentives the Government plans to take, including advice and guidance which will be delivered by the new National Cyber Security Centre (NCSC), in support of the Government's existing business engagement strategy.

### The Government's approach….

"Providing the right regulatory environment for cyber security - which incentivises better security but avoids unnecessary business burdens - should be a competitive advantage for the UK as we seek to harness the opportunities presented by leaving the EU"

(Cyber Security Regulation and Incentives Review 2016)

**The Cyber Security Context**

The review was commissioned due to a concern at Government level that the pace of change across the wider economy has not been sufficient to deal with an increasing cyber threat - a theme also expressed in its recent National Cyber Security Strategy. The strategy sets out a number of areas in which the Government is working to improve businesses' understanding of the threat and how to respond (for example, by providing advice and tools such as the Cyber Essentials Scheme). However both the strategy, and this review, stress that addressing cyber issues is a joint endeavour, and businesses must ultimately accept responsibility for putting in place the appropriate controls and systems to deter breaches, and manage them if they do occur. Evidence suggests that at present this is not the case - despite potentially significant financial consequences, just over half of all businesses (51%) have actually taken recommended action to identify cyber risks, and only 10% have a formal

incident management plan. This is in part due market failures, such as a lack of information about threats and uncertainty about which 'cyber-experts' they can trust. Government therefore sees a clear role for it to help combat these failures. It is hoped the new NCSC will help improve guidance and information, and it is also looking at the possibility of certifying trusted organisations to deliver cyber risk management.

**The role of the GDPR**

In the Government's view "[t]here is a strong justification for regulation to secure personal data because it may not be in organisations' commercial interests to implement protection to a level that is in the public interest." In particular, while they may protect their own sensitive data (including IP) they may not be as concerned with mitigating against the wider external costs that could occur from a successful breach (e.g. the impact on customers or other businesses). Implementation of the GDPR therefore gives the Government an ideal opportunity to incentivise 'significant improvements in cyber risk management.' It not only codifies current best practice (for example around privacy impact assessments), but also introduces significant new obligations (particularly around breach notification and fines). Cyber security will therefore be at the centre of the way it promotes and implements the GDPR. The data regulator, the Information Commissioner's Office, will also work in close partnership with the NCSC to:

- agree clear information security principles to 'underpin guidance for organisations and enforcement'. The NCSC will also engage the business community in designing and testing the guidance it develops;

- use breach reporting data (which will become more readily available post GDPR) to increase understanding of the threat, and will share this with businesses, insurers, and regulators - including as part of a regulators forum, where appropriate.

The Government also believes that raising the bar for personal data security will also lead to an associated general uplift in security awareness and action.

**NIS Directive**

While the report focussed on cyber security in the wider economy and therefore was not looking at issues associated with critical national infrastructure, it did seem to clarify that the UK would implement the NIS Directive (which relates to cyber security in essential service operators such as banks and energy companies as well as certain digital service providers) next May. November's National Cyber Security Strategy made no mention of the NIS Directive. However, the review states that the "Government is separately considering additional regulation might be necessary in the context of the NIS Directive due to be implemented in 2018 as well as wider national infrastructure considerations." We therefore await the detailed scope and security requirements for NIS implementation that the government has confirmed it will set out this year.

**Corporate Governance**

Corporate governance was a particular interest for the Review, focussing on how good cyber risk management could be better embedded into the corporate governance process. There were a number of suggestions for regulation in this area - for example around the inclusion of cyber security in annual reports or the statutory audit process. However, the Review concluded that adopting a more positive business engagement stance would be more beneficial than instituting a culture of compliance (which can lead to a tick boxing exercise which fails to deliver the necessary change in behaviours).

The NCSC will therefore work with a range of organisations, such as the Financial Reporting Council, to 'send messages to Boards about the importance of understanding cyber risk and what

they can do to improve their risk management in this area.' Board engagement has long been seen as key to truly addressing cyber risk in business. However, the Government goes on to state that it also hopes to educate the investment community about cyber risk, working with the Investment Association and key investors to give them "tools to challenge boards, building on partnerships with legal, accountancy and audit professions." This is seen as a key part of the strategy, given the significant influence investors and shareholders can have in influencing corporate policies and behaviours.

**Comment**

While the National Cyber Security Strategy seemed an ambitious, sometimes aspirational, policy setting document, this Review provides a more practical look at what the Government is doing, and can do, to help the UK combat an increasing cyber threat.

Businesses will be glad to see that it is not looking to increase the regulatory burden around cyber beyond that already planned (with the GDPR and NIS Directive). However, it will be interesting to see if there may be an over-reliance on the effectiveness of the GDPR. Mandatory breach notification will undoubtedly bring more breaches to the public's attention initially. But will this remain an effective deterrent over the longer term, or could it instead lead to 'breach fatigue' amongst the press (and public), leaving large fines the main concern?

The Review also does not look at new risks from emerging technology such as the Internet of Things (which was beyond its scope). It does, however, recognise concerns in this area, and confirms that the Government will consider the need for incentives to ensure internet connected products and services are secure by default as a 'growing priority'.

And perhaps most interestingly, despite stating its aim is to make the UK the safest place in the world to go online, the Review seems satisfied that the Government's focus on data protection and critical infrastructures is consistent with the vast majority of countries comparable with the UK. While 'consistency' may not lead to 'world-leading', it is important for companies trading internationally, and will again be welcomed by a business community uncertain of its post Brexit regulatory environment.

*This article was written by Duncan Blaikie and Natalie Donovan from Slaughter and May's Cyber Group. It first appeared in Cyber Security Practitioner, March 2017.*

**Duncan Blaikie**
**T +44 (0)20 7090 4275**
**E duncan.blaikie@slaughterandmay.com**

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