Client Update

Seven Takeaways from the UK Government's Cybersecurity Regulation and Incentives Review

LONDON
Jane Shvets
jshvets@debevoise.com

Robert Maddox
rmaddox@debevoise.com

Ayushi Sharma
asharma@debevoise.com

NEW YORK
Jeremy Feigelson
jfeigelson@debevoise.com

Jim Pastore
jjpastore @debevoise.com

WASHINGTON, D.C.
Luke Dembosky
ldembosky @debevoise.com

Building on the UK Government's recently issued cybersecurity strategy[1], the UK Department for Culture, Media & Sport has published its Cyber Security Regulation and Incentives Review (the "Review").[2]

After considering the need for regulation or incentives to boost cyber risk management in the UK, the Review rejected calls for prescriptive cybersecurity regulation. It instead concluded that, at least for now, cybersecurity regulation is unnecessary beyond the forthcoming EU General Data Protection Regulation ("GDPR") and sector-specific regulation such as that arising from the EU Network and Information Systems Directive.

While non-binding, the Review also highlighted measures that organisations may wish to implement to improve their cybersecurity posture. Businesses may, therefore, consult the Review for guidance on how to bolster their cyber-defences.

THE TAKEAWAYS

First, GDPR-preparedness is inextricably linked to cybersecurity. The Review affirmed that meeting the GDPR's enhanced data protection requirements will be integral to robust cybersecurity. This echoes the Government's five-year

---

1 *See* "UK Government Launches Five Year National Cyber Security Strategy" (November 2016), http://www.debevoise.com/~/media/files/insights/publications/2016/11/20161102_uk_government_launches_five_year_national_cyber_security_strategy.pdf.

2 *See* Department for Culture, Media & Sport, "Cyber Security Regulation and Incentives Review" (December 2016), https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/579442/Cyber_Security_Regulation_and_Incentives_Review.pdf.

cybersecurity strategy which identified the GDPR, which comes into force in May 2018, as a key lever for improving cybersecurity in the UK. Businesses should, therefore, consider integrating GDPR-preparedness with their cybersecurity programme. This may include ensuring that their cybersecurity incident response plan recognises the GDPR's mandatory breach notification requirements.

Second, businesses should pursue pro-active and dynamic cyber risk management. The Review warns that a tick-box compliance culture can become outdated quickly in the fast-moving world of cyber threats. It, therefore, encourages organisations to develop a pro-active approach to cyber risk management. This includes having procedures and tools to monitor and pre-empt cyber threats, as well as implementing an effective incident response plan to resolve issues swiftly when they arise. A key part of this is establishing an organisational structure with clear allocation of roles and responsibilities among internal individuals and teams and external advisers.

Third, businesses with reporting obligations should consider whether their reports should address cybersecurity risk. While the Government is not pursuing mandatory cybersecurity annual reporting, the Review notes that around two-thirds of FTSE companies include information on cybersecurity risks in their annual reports. Investors are also increasingly interested in cybersecurity and organisations should, therefore, be mindful of their reporting obligations.

Fourth, cybersecurity "health checks" can be a valuable cyber risk management tool. While the Review found against implementing mandatory cyber health checks, the Government recognises their benefits. Businesses should, therefore, consider whether a cybersecurity audit of their technical, legal and organisational structures might prove useful when reviewing their cybersecurity systems and controls.

Fifth, there is a strong business case for robust cybersecurity. The Review stresses that it is in organisations' own commercial interests to invest in cybersecurity and ensure that they have appropriate systems and controls in place to deter and deal with breaches. Even businesses which hold limited personal data may be targeted for their IP, trade secrets or other sensitive information. Accordingly, businesses with relatively limited exposure to the increased obligations and penalties under the GDPR should still recognise the importance of mitigating their cybersecurity risk profile.

Sixth, the Government is not mandating specific cybersecurity controls, risk management practices or systems. It understands that each organisation has

unique IT systems and hence different technical requirements. Businesses will, therefore, have the latitude to explore and design their cybersecurity posture in a way that best suits their specific cyber risks and business needs. Nevertheless, businesses may find it useful to keep abreast of the National Cyber Security Centre ("NCSC") and Information Commissioner's Office guidance to adhere to emerging best practices, and learning from recent enforcement actions which indicate regulators' expectations.[3]

Seventh, cybersecurity is a shared responsibility. The Review makes clear that, contrary to the trend in other areas of regulatory enforcement, individuals will not be targeted for enforcement action in cases of cyber breaches. Instead, the Government will focus on organisations as a whole, not pinning responsibility on a single individual, with the hope of encouraging a culture of pro-active responsibility-taking (especially on boards), rather than penalisation. The NCSC will also work with a range of partners to ensure investors and shareholders have the tools to build effective partnerships with company boards to influence behavioural change.

CONCLUSION

The Government remains committed to developing an environment that incentivises improved cybersecurity without unnecessary business burdens. While the Government has decided not to implement prescriptive cybersecurity regulations, businesses should not forget the demands of pre-existing and future data protection obligations, most notably the GDPR, on their cybersecurity programmes. Those operating in the financial services sector should also heed the Financial Conduct Authority's recent statements that it expects all regulated firms to have a pervasive security culture.

Organisations should also recognise the business case for robust cybersecurity beyond simply avoiding regulatory enforcement action and take appropriate steps to safeguard their systems and in turn their wider business interests. Actively engaging with both existing and future Government guidance and information sharing initiatives can help businesses achieve this aim.

* * *

Please do not hesitate to contact us with any questions.

---

[3] *See* "UK Telco Fined for Cyber Breach: Lessons Learned" (October 2016), http://www.debevoise.com/~/media/files/insights/publications/2016/10/20161019_uk_telco_fined_for_cyber_breach_lessons_learned.pdf.