Cyber Security: UK Government Initiatives and Proposed EU Laws

Additional obligations to report incidents and data breaches are on the cards.
By **Mark Young.**

News stories about cyber attacks and security breaches have become all too familiar. The scale of the problem is daunting. GCHQ recently suggested that eight in every ten of the biggest British companies have suffered a serious cyber attack. The average cost of a security breach to organisations in the UK has gone up significantly in the past year, particularly for small businesses. The government's response has been to launch several initiatives to raise awareness and improve security measures and practices within companies.

In this environment, debate continues about minimum security measures that companies should put in place and whether they should be required to share information about attacks and to report incidents to regulators. The UK government has so far tended to encourage voluntary information sharing arrangements, but certain mandatory security and reporting requirements exist and more have been proposed at EU level [PL&B UK November 14, p. 10-11].

This article summarises current UK initiatives and legal requirements as well as proposed new EU laws. While highlighting the recent good work of the UK government, this also reveals the growing maze of obligations that companies have to navigate as a result of legislative and policy responses to cyber threats.

UK Government Initiatives

The UK government has launched several cyber security related initiatives in recent years. In its National Cyber Security Strategy of 2011, the government set out the following objectives:

- to make the UK one of the most secure places in the world to do business in cyberspace
- to make the UK more resilient to cyber attack and better able to protect its interests in cyberspace
- to help shape an open, vibrant and stable cyberspace that supports open societies; and
- to build the UK's cyber security knowledge, skills and capability.

The government identified in its strategy document several actions to help deliver these objectives. In a report at the end of 2014, the government highlighted key initiatives, including providing cyber security advice to businesses, such as the "10 Steps to Cyber Security"; creating a Cyber Security Information Sharing Partnership (CiSP) with businesses to allow the government and industry to exchange information on cyber threats in a trusted environment; rolling out a tool that assesses and reports levels of cyber security awareness and preparedness in FTSE 350 companies; and publishing sector specific guidance. Other important developments have included establishing the UK's national Computer Emergency Response Team, CERT-UK, which in addition to hosting CiSP, leads on national impact cyber incidents and acts as the UK central contact point for international counterparts in this field. The government also has launched public awareness-raising campaigns such as "Cyber Streetwise", and the "Cyber Essentials" accreditation scheme to incentivise widespread adoption of basic security controls. Further, the government is investing in tackling cybercrime (e.g. setting up the National Cyber Crime Unit), and is taking steps to promote the UK cyber security industry (e.g., via the Cyber Growth Partnership (CGP) with techUK, and UK Trade & Investment's Cyber Exports Strategy).

The government has received plaudits for all of these efforts and for allocating significant funds towards them (£860 million until 2016) despite the environment of austerity. That said, important work remains to be done, especially in relation to educating and supporting SMEs, increasing the flow of actionable threat information from government to industry, and continuing to improve the competence and resources of law enforcement in this area.

> The government is investing in tackling cybercrime, and is taking steps to promote the UK cyber security industry.

Existing UK Security and Reporting Requirements

Compared to this flurry of initiatives, the number of "cyber" specific laws on the books looks sparse. Instead, the seventh principle of the Data Protection Act 1998 establishes high-level requirements to protect personal data, and company legislation sets out broad requirements in relation to corporate governance and directors' general duties. In addition, sector-specific regulations – perhaps most notably in the financial services and public sectors – establish specific security requirements.

Existing EU Security and Reporting Requirements

Similar to the UK, there is no single overarching EU-wide cyber security law that applies to all companies in all sectors across all Member States. Instead, different EU laws require

companies in certain sectors or that provide specific services to secure data and infrastructure and to report data breaches to regulators.

For example, telecommunications providers are subject to overlapping requirements to report:

- security breaches or losses of integrity that significantly impact networks and services to regulators; and
- breaches involving personal data to regulators within 24 hours, where feasible, and to notify affected individuals "without undue delay" when the breach is "likely to adversely affect [their] personal data or privacy".

The European Network and Information Security Agency (ENISA) and EU data protection authorities have published guidance on these obligations, including what it means for a breach to "adversely affect" an individual's privacy. A key takeaway for telecommunications providers is that implementing effective security measures such as encryption and rendering data unintelligible to intruders may trigger exceptions to the requirement to notify individuals.

The new e-ID and Trust Services Regulation 910/2014 creates similar security and breach notification requirements for providers of trust services, such as electronic signatures, electronic seals and website authentication. The law was adopted last year and these requirements will apply directly in all Member States from 1 July 2016.

Potential new requirements for several sectors

In recent years, questions have been asked why security and reporting obligations do not apply more broadly. In February 2013, the European Commission responded by publishing its proposal for a Network and Information Security ("NIS") Directive, elements of which mirror existing telecommunications regulations.

The NIS Directive targets private companies in the energy, transport, financial services and health sectors. Software developers and hardware manufacturers are excluded from scope (see recital 24 of the original Commission proposal). Legislators have been considering making cloud computing service providers, social networks and search engines (referred to as "enablers of key internet services" and equally strained and unclear phrases during the legislative process) subject to the new requirements; this has proven controversial, but the latest information at the time of writing suggests that cloud providers will be in scope one way or another.

The proposed new law would require companies that are in scope (i) to implement new security measures and (ii) to notify competent national authorities of any security incident that has a significant impact on the continuity of core services they provide. Competent national authorities may require that the public be informed. To be clear, this notification requirement is separate from and potentially wider than breaches involving personal data.

> The NIS Directive targets private companies in the energy, transport, financial services and health sectors.

The incident reporting obligations may be the biggest cause for concern for private sector companies. Not everybody is convinced that there is a clear benefit to extending an obligation to report incidents so broadly, arguably beyond providers of truly critical services. Several stakeholders have asked whether national authorities will have the capability to react to reports and take appropriate mitigating measures. Some have expressed concern that this requirement could become an administrative burden for companies and an exercise in collecting statistics that does nothing to improve security. The Commission has suggested that harmonising implementing measures for the NIS Directive will ensure that companies don't end up dealing with 28 systems for reporting breaches, but many companies that operate across the Union remain unconvinced, and worry that by creating what the Commission describes as "a common minimum level" the Directive could result in Member States adopting diverging security and reporting requirements. Unclear rules on when national regulators have jurisdiction to regulate such companies would complicate matters further.

The Commission hoped that the proposal would become law by the end of 2014, but, despite some progress being made, most notably in the Parliament, the original timeframe has been missed. The issue of scope – i.e. which companies would be subject to the proposed requirements – remains the trickiest to resolve. This challenge is now in the hands of the Latvian Presidency of the Council, working with negotiators from the Commission and the Parliament. The Latvian Presidency hopes that the NIS Directive will be adopted this summer. Member States would have 18 months to enact implementing national legislation, meaning that the new requirements could apply in all Member States by early 2017.

Potential new DP requirements for all companies

In addition to sector specific requirements under the NIS Directive, broad data breach requirements have been proposed as part of the General Data Protection Regulation ("GDPR"). Current European data protection legislation (the Data Protection Directive (95/46/EC)) does not impose mandatory reporting of personal data breaches (although some Member States have created national requirements). But under the proposed Regulation, all companies that process personal data – regardless of sector – may be required to notify regulators of data breaches "without undue delay" and to notify adversely affected individuals (the timing of notifications and precise triggers are still being debated).

The Commission proposed the GDPR over three years ago. Despite repeated appeals to conclude the long

running negotiations and create a more certain legislative framework for companies, progress remains slow and the timeframe for adoption is unclear. New obligations would take effect two years after the GDPR is adopted, meaning that companies will have time to adjust to new rules before they take effect.

Concerns

Questions have been raised about aspects of these EU-level proposals and how they will work in practice, including:

- Will new obligations overlap with existing sector specific and/or national requirements and/or each other?
- Which national regulators will be designated the competent authorities for the purpose of the NIS Directive and how will they work with other national sector-specific authorities?
- Is there a risk that a legal requirement to report incidents may undermine voluntary arrangements and efforts to build trust among stakeholders, such as CiSP?
- What will additional obligations to report incidents and data breaches actually achieve? Will such obligations incentivise better security within companies? Unless incident response teams receive actionable information – e.g. information that is relevant, timely, accurate and complete – it is questionable whether reporting obligations lead to better security.
- Will regulators, which often are underfunded, have adequate resources to fulfil new functions?

European legislators must ensure that they create a workable system that is clear to regulated companies and regulators, and helps achieve the aim of enhancing network security. Attention will soon turn to agencies such as ENISA and national regulators who will be responsible for issuing guidance and standards on these topics and for interpreting and enforcing the new requirements.

AUTHOR

Mark Young is Special Counsel at Covington LLP, London.
Email: myoung@cov.com

REFERENCES

1 FT, "GCHQ warns of cyber crime cost to UK economy," 16 January 2015.
2 The average cost of the worst security breach of the year recently was estimated at £600k - £1.15m for large organisations and £65k-£115k for small organisations, see Department for Business, Innovation & Skills (BIS), "2014 Information Security Breaches Survey - Executive Summary", available at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/307297/bis-14-766-information-security-breaches-survey-2014-executive-summary-revision1.pdf.
3 Cabinet Office, "The UK Cyber Security Strategy - Protecting and promoting the UK in a digital world", November 2011, available at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf.
4 The Office of Cyber Security and Information Assurance (OCSIA) in the Cabinet Office coordinates the work carried out under the National Cyber Security Programme across government departments and agencies.
5 Cabinet Office, "The UK Cyber Security Strategy - Report on Progress and Forward Plans", December 2014, available at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/386093/The_UK_Cyber_Security_Strategy_Report_on_Progress_and_Forward_Plans_-_De___.pdf
6 Materials available at https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility. See also, GCHQ, "Re-launch of '10 Steps to Cyber Security'", 16 January 2015, available at http://www.gchq.gov.uk/press_and_media/news_and_features/Pages/Relaunch-10-Steps-to-Cyber-Security.aspx.
7 By December 2014, more than 750 companies had joined CiSP since its creation in March 2013. For more information, see https://www.cert.gov.uk/cisp
8 See the most recent tracker report (published in January 2015) and related materials at https://www.gov.uk/government/publications/cyber-governance-health-check-2014.
9 For example, last year the Department for Business, Innovation & Skills (BIS) published cyber security guidance for the corporate finance sector in partnership with the Institute for Chartered Accountants in England & Wales (ICAEW), see http://www.icaew.com/en/technical/corporate-finance/corporate-finance-faculty/corporate-finance-news/cyber-security-in-corporate-finance.
10 See the Cyber Streetwise campaign at https://www.cyberstreetwise.com/, and "Cyber Essentials scheme: overview" at https://www.gov.uk/government/publications/cyber-essentials-scheme-overview
11 Relevant regulations in the financial services sector include various parts of the UK Financial Conduct Authority's Handbook of Rules and Guidance, such as the Principles for Businesses, Senior Management Arrangements, the Systems and Controls Sourcebook (SYSC), the appropriate Conduct of Business Sourcebooks, and the Financial Crime Guide. The Payment Services Regulations 2009 and the Payment Card Industry Data Security Standard (PCI DSS) contain additional rules.
12 Article 13a of the Telecommunications Framework Directive 2002/21/EC (as amended).
13 Article 4 of the e-Privacy Directive 2002/58/EC (as amended) and associated Regulation 611/2013.
14 Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union - COM(2013) 48 final - 7/2/2013 - EN. See summary at InsidePrivacy, "EU Adopts CyberSecurity Strategy and Proposes Network and Information Security Directive", 7 February 2013, available at http://www.insideprivacy.com/data-security/cybersecurity/the-european-commission-together-with/.
15 The Commission provided examples of the types of companies that it had in mind, and named specific companies as examples in official documents accompanying the legislative proposal, see the Annex to European Commission Memo IP/13/94, "Proposed Directive on Network and Information Security – frequently asked questions", 7 February 2013, available at http://europa.eu/rapid/press-release_MEMO-13-71_en.htm.
16 See European Commission Memo IP/13/94, id.
17 Id. The Commission acknowledged that "[t]hose Member States and businesses that want to be frontrunners in terms of NIS by going beyond the minimum requirements are free to do so".
18 InsidePrivacy, "European Parliament Votes to Ensure that the Proposed Network and Information Security Directive Focuses on Protecting Critical Infrastructure", 15 March 2014, available at http://www.insideprivacy.com/data-security/cybersecurity/european-parliament-votes-to-ensure-that-the-proposed-network-and-information-security-directive-foc/.
19 See ENISA report of November 2014 on "Actionable Information for Security Incident Response", 19 January 2015, available at http://www.enisa.europa.eu/activities/cert/support/actionable-information/actionable-information-for-security.