February 2015

Alert

Cyber Security: The UK/EU Legal Regime and Directors' Liability

By Barry Fishley

2014 saw cyber security attacks providing headlines throughout the year, beginning with the fallout from the Target debacle in the US, and more recently the political and reputational consequences arising from the attack on Sony Pictures. It seems inevitable that the number of attacks is going to grow in 2015. It is also likely that the attacks will be even more destructive. This now means that all companies (and their board of directors), large and small, digital and 'bricks and mortar' should be more alive to cyber security risks than ever before and have in place appropriate and documented measures.

The repercussions from any cyber attack are clear: negative PR, financial losses, governmental and/or regulatory action, and potentially for the director, loss of office and, in some cases personal liability.

Current legislation concerning cyber security attacks in the UK

The UK regime covers cyber security issues in a piecemeal fashion.

- Computer Misuse Act 1990: deals with criminal liability for unauthorised access to computer programs or data. It also covers unauthorised modifications to a computer's content.
- The Data Protection Act 1998 (the "**DPA**")

  The DPA only applies to personal data relating to living individuals and therefore not all types of data.

  Principle 7 of the DPA requires that appropriate technical and organisational measures are taken against the unauthorised processing of personal data and against accidental loss or destruction of, or damage to, such data. Whilst no definitive list of appropriate "measures" exists, a cyber attack which results from a failure to implement appropriate cyber security mechanisms will certainly be caught by the legislation. This was recently demonstrated by a fine of £200,000 which the UK Information Commissioner's Office (the "**ICO**") imposed on the Pregnancy Advice Service for failing to secure a website from which personal data was hacked.

  There is no 'hard' legal obligation on organisations which processes personal data to report breaches of security that result in loss, release or corruption of personal data, except under Regulation 5A of the Privacy and Electronic Communications (EC Directive) Regulations 2003 which requires providers of public electronic communications services (such as internet service providers and telecommunications operators) to notify a breach of data security to the ICO and, in certain circumstances, to the subscriber or user. However, for all other organisations, the ICO has stated that "serious breaches" should be notified to it and in this respect, whether a breach is "serious" should primarily be determined by the potential harm to individuals.

  The DPA also provides in some circumstances for personal liability of directors and officers. A director (or secretary) is personally liable under the DPA for certain offences committed by the company with the consent, connivance or attributable to the negligence of the director (or secretary). Offences include a company's failure to register (or notify) itself with the ICO as being an entity which processes personal data. However the director/ secretary has a defence where all due diligence has been exercised.

- Financial Conduct Authority ("**FCA**")

  Entities regulated by the FCA must comply with the FCA Handbook. The Handbook requires regulated entities to take reasonable care to establish and maintain effective systems and controls for compliance with the regulatory requirements[1] and maintain adequate policies and procedures[2]. Accordingly, cyber security measures form a key part of compliance with the FCA.

  In addition, section 90 of the Financial Services and Markets Act 2000 exposes financial services companies to risk of claims where they publish information which is untrue, misleading or contains omissions when the relevant person within the company knew it was untrue or misleading or was reckless as to its veracity.

- Publicly listed companies ("**PLCs**")

  A PLC may need to disclose a cyber security breach to the market under the Disclosure and Transparency Rules ("**DTR**") if it constitutes "*Inside Information*" (DTR 2.2). For the breach to be categorised as Inside Information, it must be information which concerns the company, is not generally available and would have a significant effect on the company's share price. The FCA has stressed that there is no fixed percentage of share price movement that would trigger this obligation and therefore one must take into account all of the circumstances including the nature of the company's business and the seriousness of the cyber security breach.

  The UK Corporate Governance Code (the "**Code**") "softly" regulates cyber security. PLCs have to comply with the Code's principles, and if failing to do so, must "explain" why in their annual report. Under C.2 of the Code, a PLC must have effective risk management systems in place, and assess the "*principal risks*" the company may face, but as the Code does not specifically identify cyber security as one of the risks that needs to be assessed it is up to the board to determine the relevant risks.

Proposals for reform

The Cyber Security Directive

The European Commission has moved to address the lack of unified European laws addressing cyber security by means of a draft cyber security Directive which is likely to be passed later this year.[3] The aim of this Directive is to achieve a high common level of network and information security across the EU.

Among other things, it will impose minimum security standards for public bodies and operators of critical industrial infrastructure (such as transport, healthcare, financial services and energy). There will also be an additional obligation for relevant organisations to notify its national or designated competent authority of security incidents which have "significant impact" on the continuity of its core services. Whilst this obligation currently applies to telcos and ISPs in Europe it will also apply to a wider set of organisations.

The Data Protection Regulation

In light of the perceived need to update and clarify the existing data protection legislation, the European Commission has proposed a fundamental shake-up of the European data protection laws by means of a draft data protection Regulation.

Key requirements under the draft Regulation from a cyber security perspective include:

- the scope of the Regulation extending to those who are established outside the EU (e.g US companies) but offer goods or services to individuals in the EU or who monitors their on-line behaviour;
- a requirement to maintain documentation of all processing activities (replacing the annual obligation to register with the national data protection authority);
- the obligatory appointment of a data protection officer including where the company's core activities relate to the processing of "sensitive" personal data (e.g health records) such as an insurance company; and
- an extension of the current data security breach notification procedures to all organisations (as opposed to the current regime, applicable only to public electronic communications services providers) which requires notification of a breach to the regulator and in certain circumstances to the affected individual.

The level of fines for security breaches and other breaches of the Regulation will be fixed by national authorities dependent upon the circumstances and severity of the breach, but can reach up to €100M or 5% of annual worldwide turnover (whichever is the greater), which will no doubt focus minds somewhat! This will mean there is a radical change to the current sanctions which can be imposed, for example, in the UK gives the ICO has power to fine up to £500,000.

Recent US and UK measures

In the US, last year the National Institute of Standards and Technology ("NIST") established a voluntary framework for improving the cyber security measures applying to companies that provide "*critical infrastructure*". The framework itself was created through collaboration between the US government and private sector stakeholders. The framework is not a checklist but a set of industry best practices which apply a risk based approach to cyber attacks. It has proven to be very popular with companies beyond those providing critical infrastructure and in the US is seen as the

de facto benchmark for assessing a company's cyber security compliance.

In the US we also saw the sweep of investment firms by FINRA to assess firms' readiness to cope with cyber security threats.

The Bank of England adopted the "CBEST" framework for testing a firm's resilience to cyber attacks and the European Network and Information Security Agency reviewed 200 organisations for cyber security readiness. The recent announcement by President Obama and Prime Minister Cameron to bolster joint efforts to protect against cyber security attacks means that 2015 will likely see further proactive measures being taken by regulators and governments to assess readiness and promote information sharing on causes and best practice.

In the UK, the government launched a consultation on cyber security organisational standards, resulting in the development of a new voluntary "Cyber Essentials Scheme", which has become the government's preferred standard and focuses on basic cyber hygiene. Launched in June 2014, the Scheme aims to be a "significant improvement" to the standards currently used. It is mandatory for all suppliers bidding for government supply contracts which are assessed as higher risk .Early adopters of the Cyber Essentials scheme include BAE Systems, Barclays, Hewlett-Packard, and Vodafone.

Most recently in the UK the BIS published a tracker report setting out the results of a 2014 cyber security survey of FTSE 350 companies. This will be repeated this year with the aim of providing some benchmarking for governance and general best practices.

Questions to Ask

Every board should raise (and document the answers to) the following questions:

1. What IT-based information/intellectual property/data is most critical to the business and what value is at stake in the event of a cyber security breach? Need to prioritise measures based on level of risk.
2. Is customer health and/or financial information stored on IT systems? Heightens potential reputational consequences of a breach.
3. Does the company have enough people working full time protecting systems?
4. Is the company spending adequately on IT protection?
5. Is the company taking any non-standard risks?
6. Which stakeholders have responsibility for cyber security matters?
7. Are the company's employees educated on prudent safety measures, if so how often?
8. Does the company have appropriate IT policies in place?
9. Have there been any security breaches, if so what lessons were learned, what measures have been implemented to mitigate against further risk?
10. Does the company perform regular penetration tests and what are the results?
11. Does the company have comprehensive IT monitoring in place?
12. Does the company have a fully document cyber attack response plan ready in case of a breach?
13. Does the company's Audit Committee receive reports on cybersecurity on a regular basis?
14. What data is handed to, or accessible by, third parties such as through an outsourcing, cloud computing or other arrangements?
15. Is cybersecurity a regular component of counterparty diligence for transactions, such as outsourcing?
16. Review and consider updating insurance cover to specifically govern cyber attacks and consequences such as product recall, customer notifications, system changes etc.

Takeaways

- In general, all companies should have firm, written policies and procedures with respect to all aspects of "best practices" in cybersecurity. These policies should be frequently updated.
- Adoption of some "standard" relating to cyber security e.g.– NIST or ISO 27001– consider adoption of Cyber Essentials Scheme. Evidence of adoption/ discussions related to adoption may evidence "due care" or "best practices" or "appropriate measures" and may affect company's ability to obtain cyber insurance or the price of premiums payable!
- Document the company's efforts to train employees on information security, phishing, password creating/protection and network/access.
- Document due diligence exercises covering counterparties such as the security policies and measures undertaken by 3rd party providers (e.g. cloud).
- Document the company's actions taken to detect, log and respond to unauthorised cyber-related activity (intrusion event histories, digital signature recognition efforts, etc.).
- Have in place a fully documented IT security policy which, among other things should cover actions with former employees who leave the company with passwords/network privileges.
- Document cyber-security incident response plan in case a data breach/other cyber attack takes place including:

- team members and their responsibilities: who is the owner of the plan, both in UK and overseas locations?
- 3rd party providers and consultants on retainer;.
- how the company would deal with customers, clients, shareholders, investors and law enforcement authorities.
- plans to "stop the bleeding" (i.e. diagnosis, containment, remediation and eradication efforts).

- Consider increased collaboration/ information sharing with peers
- Speak to insurance brokers/ providers to better understand nature of available policies and coverage.

1. Senior Management Arrangements, Systems and Controls 3.2.6R: *"A firm must take reasonable care to establish and maintain effective systems and controls for compliance with applicable requirements and standards under the regulatory system and for countering the risk that the firm might be used to further financial crime".*
2. Senior Management Arrangements, Systems and Controls 6.1.1R: *"A firm must establish, implement and maintain adequate policies and procedures sufficient to ensure compliance of the firm including its managers, employees and appointed representatives (or where applicable, tied agents) with its obligations under the regulatory system and for countering the risk that the firm might be used to further financial crime".*
3. 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 (2013/0027(COD)

Barry Fishley

Expertise

Barry Fishley is a partner in the London office and has had wide ranging experience in data protection, technology, intellectual property, e-commerce and general commercial matters.

He advises financial institutions, major international companies and private equity funds on a range of transactions and issues including data protection, technology and intellectual property aspects of M&A and banking transactions, complex international licensing arrangements, outsourcing, strategic alliances, manufacturing supply and other international commercial transactions.

In the areas of data protection and privacy, Barry has extensive experience of advising on the consequences of a security breach, international transfers of data, privacy audits and general compliance.

Barry regularly speaks and writes on various topics. His most recent work was a series of presentations on cyber security including cyber security implications for M&A.

Barry is recommended in *Legal 500 UK 2014* for his media & entertainment expertise.

Contact Details

Barry Fishley
Partner
barry.fishley@weil.com
110 Fetter Lane
London, EC4A 1AY
Tel. +44 20 7903 1410

If you would like more information about the topics raised in this briefing, please speak to your regular contact at Weil or to any member of the Technology & IP Transactions Group:

Barry Fishley barry.fishley@weil.com +44 20 7903 1410