Disputes 2018: Cybersecurity - risks when outsourcing, partnering and using professional advisors

Organisations are, largely, aware of their own responsibilities when holding data, but may be less aware of the risks posed when third parties hold data or have access to data.

Submitted	15 January 2018
Applicable Law	UK (England & Wales)
Topic	Dispute Resolution - Commercial Dispute Resolution - Financial Markets
Contact	Paul Baker, Robert Allen

In brief

- The volume of data being captured and managed by businesses is increasing year on year. Data is frequently shared by businesses with third party service providers or suppliers, thereby increasing the cybersecurity risk.
- The global regulatory landscape is developing to compel businesses to protect data against cyber attacks, including when it is held by third parties. The data protection obligations of businesses, and the sanctions for serious breach, will substantially increase with the introduction of the GDPR in May 2018.
- In the event of a data breach by a third party, the data controller may find themselves facing enforcement action by either (or both) of the ICO and the FCA, as well as civil litigation. We anticipate an increase both in cyber-related civil claims and enforcement activity by regulators.

The risks posed by data sharing and outsourcing

Data may frequently be shared with third party professional service providers, such as law firms and accountants, who will often have access to extremely sensitive data. Many organisations outsource key elements of their business (eg insurers and their claims departments), and increasingly, businesses rely on third parties for their IT infrastructure, and many outsource data retention to cloud data suppliers.

Managed Service providers (MSPs) are an obvious target for malicious cyber attacks; activity in this regard prompted the National Cybersecurity Centre (NCC) to publish a report in April 2017 highlighting the risks and advising on how those risks should be managed. The NCC recommends that any MSP procurement process should include ensuring that all service providers manage their security to a level broadly equivalent to that of the procuring company.

Do you know what security measures your business' third party suppliers and service providers have in place to protect data, and whether they are as strong as your own? Surveys have shown that only a small minority of businesses in the UK require their suppliers to adhere to specific cybersecurity standards or practices.

An organisation’s cyber security is only as strong as that of its weakest third party service provider.

Current and future regulatory landscape

Businesses which are "data controllers", as defined under the Data Protection Act 1998 (DPA) and firms which are regulated by the Financial Conduct Authority (FCA) should be familiar with their primary obligations, but may be less aware of their obligations to protect data which is outsourced or shared.

DPA

Of the DPA’s eight data protection principles, the seventh requires “appropriate technical and organisational measures…against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data”. Breach of this principle, where it is deliberate or reckless and likely to cause substantial damage or distress, may lead to ICO fines of up to £500,000. Any processing by a data processor (i.e. those whose activities are limited to data storage, retrieval, organisation, disclosure or erasure) must be carried out pursuant to a written contract. The responsibility stays with the data controller, who must ensure that any third party data processors provide guarantees with respect to their security measures and must take reasonable steps to ensure compliance. (DPA Sch.1, Part 2, para.11).

General Data Protection Regulation (GDPR, in force from May 2018)

When the GDPR comes into force, businesses across the EU will be subject to increased data protection obligations, and will face greater sanctions for any breach. Businesses which provide data, including personal data, to third parties will have an obligation only to use data processors which provide sufficient guarantees to implement appropriate technical and organisational measures for compliance (GDPR Art 28(1)). Data processors’ activities must be governed by a binding contract, and both data processors and data controllers will be obliged to implement appropriate measures. Breaches must be notified to the ICO. Our article Crime, fraud and investigations 2018: Cyber security looks at cyber risk more generally, with particular focus on changes to the data protection regime when the GDPR comes into force. Our GDPR microsite can be found here.

Network and Information Systems Directive (NIS Directive, due to be implemented May 2018)

Operators of key essential services (including banks and other credit institutions) and key digital service providers (including cloud computing services and online marketplaces) will be subjected to additional risk management and reporting requirements.

FCA-Regulated firms

Financial services providers regulated by the FCA are subject to additional cybersecurity obligations. Principle 3 (PRIN 2.1.1, FCA Handbook) requires firms to take “reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems”. SYSC 6.1.1 (Senior Management Arrangements, Systems and Controls Rules) refers to financial crime and is wide-ranging: “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, with its obligations under the regulatory system and for countering the risk that the firm might be used for further financial crime”.

Liability for breaches

If the security of personal data is compromised as a result of a cyberattack on a third party service provider, the

business which outsourced the information may face enforcement action by the ICO, which can issue fines pursuant to its powers under the DPA. The ICO fined a private health company £200,000 in February 2017 for failure to keep patients' data secure. A transcription service had routinely been sent unencrypted audio recordings of patient interviews to transcribe, without a DPA compliant contract or any guarantees as to storage or destruction of the data.

The GDPR will allow far greater sanctions, including administrative fines of up to 4% of annual worldwide turnover or £20m, whichever is the greater.

The FCA will also take enforcement action when it identifies weak controls of third party service providers in the financial services industry. Poor cybersecurity control of third party service providers has led to significant fines. Two Aviva entities were fined a total of £8,246,800 in late 2016 for failures in their oversight of outsourced providers who were managing client assets, and Zurich Insurance plc was fined £2,275,000 following the loss by another Zurich group entity's sub-contractor of an unencrypted back up tape containing customer data.

Civil claims for breaches of the DPA (in the case of individuals), or based on either the tort of misuse of private information or breach of confidence, may well follow a data breach. Group litigation orders can enable multiple individuals jointly to bring claims under the DPA against data controllers following a breach. Contractual claims may also be brought, particularly where an organisation has made representations to customers or contractual counterparties about the strength of its own cybersecurity systems. The delegation of data processing to third parties will not provide a shield to litigation. Our article about the class action brought by employees of Morrisons supermarkets following a data breach "Vicarious liability and deliberate data breaches by employees" can be found here.

What it means for you

Businesses can take various practical steps to minimise the threat, in particular:

- assessing the risk, including reviewing who has access to data and why, and conducting due diligence on, and a security assessment of, each third party
- reviewing contracts and ensuring that they comply with relevant standards, and that, for example, they impose obligations as to secure use, storage and deletion of data
- putting in place systems for appropriate oversight and monitoring - for example, ensure regular reports from and audits of third parties, and
- ensuring that procedures and obligations are in place with third parties to enable proper incident reporting and response.

elexica Limited, CityPoint, One Ropemaker Street, London EC2Y 9SS