ICLG

The International Comparative Legal Guide to:

Cybersecurity 2018

1st Edition

A practical cross-border insight into cybersecurity work

Published by Global Legal Group, with contributions from:

Allen & Overy
Angara Abello Concepcion Regala & Cruz Law Offices
Baker McKenzie
Boga & Associates
BTG Legal
Christopher & Lee Ong
Creel, García-Cuéllar, Aiza y Enríquez, S.C.
ENSafrica
Erkelens Law
Eversheds Sutherland
Holland & Hart LLP
JIPYONG
Josh and Mak International
King & Wood Mallesons
Lee, Tsai & Partners Attorneys-at-Law
Maples and Calder
MinterEllison
Mori Hamada & Matsumoto
Niederer Kraft & Frey Ltd.
R&T Asia (Thailand) Limited
Rajah & Tann Singapore LLP
Shibolet & Co.
Simmons & Simmons LLP
Udo Udoma & Belo-Osagie

glg
global legal group

global legal group

Contributing Editors
Nigel Parker & Alex Shandro, Allen & Overy LLP

Sales Director
Florjan Osmani

Account Director
Oliver Smith

Sales Support Manager
Toni Hayward

Sub Editor
Oliver Chang

Senior Editors
Suzie Levy, Rachel Williams

Chief Operating Officer
Dror Levy

Group Consulting Editor
Alan Falach

Publisher
Rory Smith

Published by
Global Legal Group Ltd.
59 Tanner Street
London SE1 3PL, UK
Tel: +44 20 7367 0720
Fax: +44 20 7407 5255
Email: info@glgroup.co.uk
URL: www.glgroup.co.uk

GLG Cover Design
F&F Studio Design

GLG Cover Image Source
iStockphoto

Printed by
Ashford Colour Press Ltd.
October 2017

ISBN 978-1-911367-77-2
ISSN 2515-4206

Strategic Partners

General Chapters:

Country Question and Answer Chapters:

Enemy at the Gates? The Cybersecurity Threat Posed by Outsourcing, Partnering and Professional Advisors

Robert Allen

Paul Baker

Simmons & Simmons LLP

The cybersecurity threat posed by outsourcing, partnering and professional advisors – companies are well-informed of the need to buttress their own cybersecurity defences, but what about third parties that hold their data or with whom they share access to systems?

1 Introduction

In 2017, no business can plead ignorance of the cybersecurity risks inherent in a digitally connected global marketplace. The headlines expose and denounce the corporate victims of cyberattacks[1] and reel off the latest statistics about the rise of cybercrime.[2] Businesses are, accordingly, well-informed that they must buttress their cybersecurity defences or become one of the statistics.[3] Yet, it is often at this level of awareness that the conversation about cybersecurity ends. And, to the extent that businesses are focused on cybersecurity, that focus is concentrated only on the business's own defences.

That focus is naïve. No business operates in isolation. Each contract with suppliers seeks advice or services from professional services firms, and outsources to (for example) payment services, complaints handlers and data custodians. This network of third parties holds the business's data and may share access to the business's systems (often across numerous jurisdictions), forming a crucial part of the first line of defence against cybersecurity breaches. As recently as August 2017, TalkTalk Telecom Group was fined £100,000 by the Information Commissioner in the UK, when customers' personal data were compromised via one of its providers of network coverage solutions and complaints resolution.[4] The questions therefore for each business must be: what does it know about these third parties and their security (if anything); and what steps does it take to ensure that such security is maintained to the appropriate standard?

The magnitude of the risk posed by third parties is often overlooked in a business's assessment of cybersecurity. In the UK, for example, only 13% of businesses require their suppliers to adhere to specific cybersecurity standards or good practice.[5] In this article, we examine the scope of the threat arising out of third-party relationships, the degree to which third-party security risk is currently regulated, the potential enforcement and litigation consequences of a cybersecurity breach at a third party, and some practical guidance to help to identify and assess the risks they create and (if necessary) remediate the harm caused by a breach.

Our aim in this article is to highlight to businesses (and their advisers) that their trusted suppliers, custodians and advisors may in fact be unwitting 'enemies at the gate' when it comes to cybersecurity.

2 Scope of the 'Third Party Threat'

Year on year, the aggregate of data created and captured grows exponentially. In 2025, the IDC forecasts that the global 'datasphere' will grow to 163 zettabytes, 10 times the data generated in 2016.[6] As data capture increases – fuelled by embedded systems, data analytics, technological advances and even regulation[7] – businesses are forecast to manage even more data (from 30% in 2015 to nearly 60% in 2025);[8] data which, in many instances, they are obliged to protect.

However, notwithstanding the commercial value and regulatory importance of data, businesses increasingly do not hold their own. Data growth has driven – and continues to drive – heightened reliance on third parties for IT infrastructure (often collectively described as Managed Service Providers or MSPs). For instance, data retention is routinely outsourced by firms to cloud service providers to lessen the burden of data storage. MSPs present particularly desirable targets for malicious cyberattacks, in light of their disproportionate access to valuable information held by multiple businesses. Recently, the detection of ongoing targeted attacks against global MSPs by a hostile actor has prompted the UK's National Cybersecurity Centre to publish advice for enterprises regarding their security assessments and monitoring of MSPs.[9]

Moreover, data may be frequently shared by a business with other third-party professional services firms such as law firms, accountants and management consultants for analysis, audit and advice. These firms, given the nature of their work, are likely to be repositories of a business's most sensitive and valuable data – and therefore a prime target for cyber attackers. The recent compromise of DLA Piper's systems provides an obvious example. In June 2017, the international 'Petya' ransomware attack rapidly infected the entire DLA Piper network, requiring employees globally to turn off their computers and to avoid use of any element of the firm's IT infrastructure. While DLA Piper has not seen any evidence of theft of client data,[10] some IT systems were still inoperable up to two weeks later.

Therefore, while support from MSPs and professional firms may be critical for reasons of cost, efficiency or specialism, it must be recognised internally by businesses that the outsourcing and/or sharing of data to a network of third parties displaces and indeed magnifies the cybersecurity risk. This should raise particular alarm bells where third parties operate in jurisdictions that offer a lower cost base but present a heightened cybersecurity risk, whether as a result of weaker regulation, corruption risks, or higher rates of cybercrime.

Stakeholders, regulators and the public generally do not take kindly to a business seeking to pass blame to a third party which it selected and the business's reputation is intrinsically linked to the outsourced providers it engages. A business is, therefore, as vulnerable to attack and damage to reputation as its weakest third-party service provider.

3 Regulation

In light of the pernicious and expanding threat to cybersecurity posed by third parties, it is unsurprising that the global regulatory landscape has developed to compel businesses to protect their data against cybersecurity attacks on vulnerable third-party defences. From a UK perspective, the businesses that are most heavily regulated are data controllers as defined under the Data Protection Act 1998 (DPA), and firms regulated by the Financial Conduct Authority (FCA). However, current data protection obligations, and the associated sanctions for breach, will be appreciably bolstered with the introduction of the General Data Protection Regulation (GDPR) in May 2018 (to be implemented into UK law notwithstanding Brexit).[11] Below we consider the current and prospective legislative impetus to protect oneself against the 'third party threat'.

Data Protection Act 1998

In the UK, the DPA[12] requires data controllers to comply with eight data protection principles[13] with respect to personal data; a broad concept that encompasses any information which can be used to identify an individual.[14] Relevantly, the seventh data protection principle requires the following security obligations:[15]

> "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."

The DPA envisages that data controllers will provide access to personal data to third parties for a multitude of reasons. Indeed, the data controller is under a mandatory duty to notify the Information Commissioner's Office (ICO) of its disclosure to third parties and is prohibited from doing so without such registration.[16] These third parties may be data processors (entities whose activities are limited to data storage, retrieval, organisation, disclosure or erasure) or themselves data controllers.

The DPA requires a data controller to ensure that any third-party data processors provide guarantees with respect to their security measures and to take reasonable steps to ensure compliance by third parties with those security measures.[17] More specifically, the DPA mandates that any processing by a data processor must be carried out pursuant to a contract made or evidenced in writing and that the data processor may act only on the data controller's instructions and in doing so comply with equivalent security obligations to the data controller.[18] No action can be taken against a data processor itself so these measures place responsibility squarely on the data controller to mitigate against vulnerable security standards in data processing.[19]

In circumstances of serious breach of this principle by the data controller, of a kind likely to cause substantial damage or distress and where the breach was deliberate or reckless, the ICO may impose a fine of up to £500,000.[20]

General Data Protection Regulation

The data protection obligations on businesses and the sanctions for serious breach will substantially increase with the introduction of the GDPR in May 2018, in the UK and across EU Member States. Materially, for businesses that provide information including personal data to third parties, they will have an obligation only to use those data processors that provide sufficient guarantees to implement appropriate technical and organisational measures to ensure processing meets the requirements of the GDPR.[21] Data processor activities must be governed by a binding contract between controller and processor,[22] which must make specific provision for (among other things) instructions, sub-processing (which is prohibited without the authorisation of the controller[23]), compliance and confidentiality.

In terms of security, processors *and* controllers will be obliged to implement measures that are appropriate, taking into account factors such as the type of data, the nature and purpose of processing, the risks to individual rights associated with any security breach and the costs of implementation.[24] Regular testing and evaluation of the effectiveness of any security measures is also required if appropriate.[25] From the perspective of businesses outsourcing data retention and organisation, additional comfort can soon be taken from these new security obligations and additional requirements on processors to maintain records of personal data processing activities.[26]

The GDPR also substantially increases the enforcement and litigation risk profile in the event of a security breach involving personal data.[27] Such breaches must be notified by data processors to data controllers, and by data controllers to the relevant supervisory authority (in the UK, the ICO) without undue delay.[28] At present, such reporting only represents good practice,[29] and the compulsion of such reporting may lead to more frequent enforcement by the ICO (and, as a consequence, civil lawsuits, which are discussed further below). Second, where enforcement is pursued, the possible sanction – fines of up to 4% of global annual turnover[30] – is severe.

NIS Directive

In addition to the GDPR, it should not be forgotten that the Network and Information Systems (NIS) Directive is also due to be implemented by EU Member States in May 2018, which will subject operators of key essential services (including banks and other credit institutions) and key digital service providers (including cloud computing services and online marketplaces) to additional risk management and reporting requirements. This Directive can be expected to raise security standards on digital service providers, which will be especially important for businesses reliant on cloud computing. However, like the GDPR, it may increase the likelihood of enforcement or litigation when data breaches occur and are required to be reported.

Principles for Business and SYSC Rules

In addition to ICO enforcement, financial services providers regulated by the FCA are subject to additional security obligations that encompass cybersecurity risks. The FCA handbook provides a number of rules where failure to properly engage with and understand the issue of cybersecurity would constitute a breach. Principle 3 (PRIN 2.1.1, FCA Handbook) is the most obvious, and was invoked by the FCA in its censure of Royal Bank of Scotland Plc, National Westminster Bank Plc and Ulster Bank Ltd following their major IT systems failure in June 2012. This Principle requires a firm to "take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems".

The Senior Management Arrangements, Systems and Controls rules (SYSC) are also relevant. Two of the SYSC rules specifically reference financial crime, which is inextricably linked with cyberattacks. SYSC 6.1.1 is particularly 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 to further financial crime."

In July 2016, the FCA produced guidance for regulated firms when outsourcing to the cloud and other third-party IT services in the context of the existing UK and EU framework.[31] This guidance is designed to assist regulated firms to discharge their oversight obligations and avoid enforcement action pursuant to the SYSC rules or otherwise for poor risk management (examples of which are provided further below).

4 Liability

In the event of a data breach at a third party, whether an accountant, website builder or cloud service provider, it will be essential to assess and understand where liability for such breaches may lie.

ICO enforcement

If the security of personal data is compromised as a result of a cyberattack on a third-party service provider, the business which outsourced such services may face enforcement action by the ICO. Pursuant to its powers under the DPA, the ICO can and has often issued fines to data controllers for breaches of the seventh data protection principle (often in connection with other principles) in situations where their third-party data processor has lost or left unsecure the personal data in its possession.

For example, in February 2017, the ICO fined private health company HCA International Ltd (HCA) £200,000 for failing to keep fertility patients' confidential personal information secure. The ICO found that HCA had, since 2009, routinely sent unencrypted audio recordings of interviews with fertility patients by email to a company in India for transcribing services. HCA had no guarantee that the company would use a secure FTP server to store the recordings or erase them after transcription, failed to monitor the company in relation to any security measures and did not have a DPA compliant contact with the company in relation to the processing. The contraventions came to light only in 2015 when a patient informed HCA that transcripts could be found online via a search engine.

On 4 November 2015, the Crown Prosecution Service (CPS) was fined £200,000 after three laptops containing videos of police interviews were stolen from the owner of a private film studio in a burglary. The CPS had engaged the owner in 2002 to edit the interviews for use in criminal proceedings. The ICO found the CPS in contravention of the seventh data protection principle, observing that it had no guarantees from the owner in relation to storage, return or secure destruction at the end of the case; that it failed to monitor the owner in relation to any security measures taken by him; and that it did not have a DPA-compliant contract in relation to the processing.

While some deterrent for lax monitoring of third parties, these penalties pale in comparison to the sanctions soon to be available under the GDPR and, indeed, the regulatory settlements entered for data breach in the United States. In May 2017, Target paid $18,500,000 to settle state enforcement action arising out of its 2013 data breach, which involved attackers stealing credentials from a heating and air conditioning subcontractor to access Target's gateway server and steal customer details.

FCA enforcement

In the financial services industry, weak cybersecurity controls of third-party service providers (whether or not the subject of a cyberattack) also routinely capture the attention of FCA enforcement. While the greatest financial penalty imposed for inadequate IT systems and controls remains the £42,000,000 fine on Royal Bank of Scotland Plc, National Westminster Bank Plc and Ulster Bank Ltd (arising from software failings in the updating of systems), significant fines have also been levied on financial institutions in respect of the poor cybersecurity controls of their third-party service providers.

In October 2016, Aviva Pension Trustees UK Limited and Aviva Wrap UK Limited (together Aviva) were fined £8,246,800 for failings in oversight of outsourced providers in relation to the protection of client assets between 2013 and 2015. In this period, Aviva did not have in place appropriate controls over Third Party Administrators (TPAs) to which they had outsourced the administration of client money and external reconciliations in relation to custody assets, in breach of Principle 3.[32] While client money was at risk in this instance, there was no actual cybersecurity breach by the TPAs.

Similarly, Zurich Insurance plc paid a penalty of £2,275,000 following a data loss incident in which the subcontractor of another Zurich Group entity, Zurich Insurance Company South Africa Limited (ZICSA), lost an unencrypted back-up tape with data relating to 46,000 customers. As a result, the FSA found that Zurich Insurance plc had failed to take reasonable care with respect to its management of risks associated with securing customer information in breach of Principle 3, SYSC 3.1.1R and SYSC 3.2.6R.

Civil litigation

Civil claims may be brought against businesses as a result of a cyberattack against one of its third-party service providers, regardless of whether there has been any regulatory enforcement action.

In the UK, section 13 of the DPA provides a route for individuals to claim, where they can demonstrate that the data controller has breached the DPA (which includes failure to ensure compliance with the DPA by third parties) and has suffered damage as a result. Whilst pecuniary loss was previously a prerequisite for 'damage', the Court of Appeal in *Vidal-Hall et al v Google*[33] confirmed that 'damage' could include emotional distress only.

Alternatively, under English law, claims may be brought against business on the basis of:

(A) the tort for misuse of private information; and/or

(B) an action for breach of confidence.

Contracts may also provide a basis for further liability in the event that the third party's cybersecurity systems are compromised. A business may well expect to terminate or pursue an action in contract damages against the third party pursuant to data protection clauses that have been breached. But the business itself should anticipate contractual claims being made against it if it has made representations about the robustness of its cybersecurity systems to customers or other third parties. Such statements may appear, for example, in response to RFPs, or in prospectuses or marketing materials, and could result in misrepresentation claims by investors, shareholders, suppliers or customers.

In short, the delegation of data processing to third parties provides no shield against litigation following a cyberattack. Indeed, in the

UK, group litigation orders enable the joint management of claims which give rise to common or related issues of fact or law and expand the spectre of corporate liability irrespective of the nature of the claim. These orders have proved particularly useful for individuals to pursue claims arising out of data breaches, including over 5,000 employees of Morrisons whose bank, salary and national insurance details were leaked online by a rogue employee of the supermarket chain.[34]

5 Practicalities

As well as the framework of legislation and rules, and mechanisms by which a business may seek compensation after the event of a cyberattack, there are various practical steps that can be considered. To conclude, we set out below a check list outlining suggested steps to mitigate the third party threat, divided into four categories: risk assessment; contract; oversight; and incident management.

It is worth focussing briefly on the contract category in particular because, if well-drafted, relevant agreements will provide a clear picture of the parties' rights and obligations when it comes to cybersecurity, and help clarify the risks specific to the third-party relationship. In contemplating the contractual obligations concerning cybersecurity the following should be considered:

(A) Basic security provisions; for example: physical security requirements of the third-party premises; any vetting requirements for third-party staff members (and their third-party contractors); and the use of agreed, manufacturer-supported, password-protected operating systems.

(B) Specific data security provisions that set out requirements about the use and storage of data; for example: how will data be given to the third party? Should it be encrypted? Should it be backed up and by whom? For how long should it be stored? How and under what circumstances should it be destroyed or returned?

(C) Cooperation provisions, for example: information requirements to allow businesses to obtain all necessary information to ensure compliance with data protection provisions; cooperation provisions to ensure data security audits are effective; review and security testing requirements; and staff training provisions.

(D) Breach provisions; for example: notification requirements in the event of a breach; further cooperation provisions to ensure breaches are investigated and managed effectively; and business continuity provisions.

(E) Indemnity and limitation of liability clauses: as the GDPR provides for higher fines than under current domestic legislation, it may be prudent to modify these clauses accordingly.

Checklist: The Third Party Threat

Risk Assessment	Have you mapped out who holds or has access to your data?
	Have you considered the business rationale for and appropriateness of providing data to each third party service provider?
	Have you conducted recent and reliable due diligence on each third party?
	Have you conducted (and documented) a security assessment of your risks specific to each third party?
Contract	Does your contract require the third party to comply with international standards?
	Does your contract make specific provisions for the security of data throughout transfer, use, storage and deletion?
	Does your contract also provide for security with respect to physical premises and people?
	Does your contract preclude the use of sub-contractors without authorisation?
Oversight	Do your third parties provide regular reports to you regarding security testing, risks and status updates?
	Do you regularly audit third party service providers for security risk?
	Do you have effective access to the data held by the third party?
	Do you have records of the data processing activities conducted by third parties?
Incident Response	Are your third party service providers contractually or otherwise obliged to report data breach and/or loss to you?
	Does your cyber incident response plan consider data breach at a third party?
	Can you cooperate with regulators' requests for information and/or access to data?
	Do you have and can you enforce indemnity clauses for data breach in the jurisdictions in which you operate?

Endnotes

1. For example, see: *"DLA Piper hack could cost 'millions', brokers say"*, Legal Week (7 July 2017); *"Tesco Bank suspends 'all transactions' as 20,000 customers lose money after hack attack"*, Independent (7 November 2016); and *"TalkTalk hit with record fine over cyber attack"*, Financial Times (5 October 2016).
2. *"Cybercrime costs the global economy $450 billion"* according to CNBC (7 February 2017) available at https://www.cnbc.com/2017/02/07/cybercrime-costs-the-global-economy-450-billion-ceo.html. In the UK, the BBC has reported on the "estimated 3.6 million cases of fraud and two million computer misuse offences in a year" in *"Cyber Crime and fraud scale revealed in annual figures"* (19 January 2017), available at http://www.bbc.co.uk/news/uk-38675683.
3. In the UK, three-quarters (74%) of businesses say that cybersecurity is a high priority for their senior management. Dr Rebecca Klahr *et al.*, *"Cybersecurity breaches survey 2017 Main report"* (April 2017) at 1.
4. ICO Press Release, *"Personal data belonging to up to 21,000 TalkTalk customers could have been used for scams and fraud"* (10 August 2017), available at https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/08/personal-data-belonging-to-up-to-21-000-talktalk-customers-could-have-been-used-for-scams-and-fraud/.
5. This percentage is higher in the finance and insurance sectors (30%) and among education, health or social care firms (22%). Dr Rebecca Klahr *et al.*, *"Cybersecurity breaches survey 2017 Main report"* (April 2017) at 35.
6. David Reinsel, John Gantz and John Rydning, *"Data Age 2025: The Evolution of Data to Life-Critical"* (April 2017) at 3, available at http://www.seagate.com/www-content/our-story/trends/files/Seagate-WP-DataAge2025-March-2017.pdf.
7. By way of example, MiFID 2, which comes into force on 3 January 2018, significantly expands the transaction record keeping obligations for investment firms within EU Member States, including the introduction of extensive rules on phone taping and electronic communications.
8. David Reinsel, John Gantz and John Rydning, *"Data Age 2025: The Evolution of Data to Life-Critical"* (April 2017) at 21.
9. National Cybersecurity Centre, *"Global targeting of enterprises via managed service providers"* (3 April 2017), available at https://www.ncsc.gov.uk/information/global-targeting-enterprises-managed-service-providers.
10. DLA Piper, *"Malware Attack Update"* (10 July 2017), available at www.dlapiper.com/en/sweden/focus/dla-piper-malware-attack-update/.
11. The UK Minister of State for Digital and Culture, Matt Hancock MP, has confirmed that the UK will implement the GDPR in full.
12. Which implements the *Data Protection Directive* (*95/46/EC*) into UK law.
13. DPA, section 4(4).
14. DPA, section 1(1).
15. DPA, Schedule 1, Part 1, paragraph 7.
16. DPA, section 17.
17. DPA, Schedule 1, Part 2, paragraph 11.
18. DPA, Schedule 1, Part 2, paragraph 12.
19. See further Information Commissioner's Office *"Data controllers and data processors: what the difference is and what the governance implications are"*, available at https://ico.org.uk/media/for-organisations/documents/1546/data-controllers-and-data-processors-dp-guidance.pdf. This guidance notes that the ICO "may decide not to take enforcement action against a controller if it believes it has done all it can to protect the personal data it is responsible for and to ensure the reliability of its processor, for example through a written contract".
20. DPA, section 55A; Data Protection (Monetary Penalties) (Maximum Penalty and Notices) Regulations 2010.
21. GDPR, Article 28(1).
22. GDPR, Article 28(3).
23. GDPR, Article 28(2).
24. GDPR, Article 32(1).
25. GDPR, Article 32(1)(d).
26. GDPR, Article 30(2).
27. Article 4 GDPR defines a personal data breach as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed".
28. GDPR, Article 33.
29. Currently, in the UK there is no legal obligation under the DPA to report personal data breaches to anyone. However, the ICO guidance recommends that serious breaches should be brought to its attention.
30. For some breaches of the Regulation (including failing to comply with the conditions for processing) data controllers can receive a fine of up to the greater of 4% of global annual turnover for the preceding year (for undertakings) or €20,000,000. For other breaches (e.g. failing to keep records or complying with security obligations), the fine can be up to the greater of 2% of global annual turnover (for undertakings) or €10,000,000.
31. FCA, *"FG 16/5 – Guidance for firms outsourcing to the 'cloud' and other third-party IT services"* (July 2016), available at https://www.fca.org.uk/publication/finalised-guidance/fg16-5.pdf.
32. Principle 3 (Management and Control) states that a firm must take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems.
33. [2015] EWCA Civ 311.
34. Dataiq, *"5,000 join action against Morrisons over data leak"* (3 March 2016), available at http://www.dataiq.co.uk/news/5000-join-action-against-morrisons-over-data-leak.

Robert Allen
Simmons & Simmons LLP
CityPoint
One Ropemaker Street
London EC2Y 9SS
United Kingdom

Tel: *+44 20 7825 4852*
Email: *robert.allen@simmons-simmons.com*
URL: *www.simmons-simmons.com*

Robert is a partner in the Financial Markets Litigation group in Simmons & Simmons LLP's London office. He specialises in retail and consumer finance litigation, including cybersecurity issues, investigations, general banking disputes and contentious regulatory matters. Robert is a member of the firm's Cybersecurity group and advice to clients in this field includes defending a major financial institution against threatened claims by a client of the bank following a cyber-attack on the client's account. Robert also advises clients on data protection considerations, particularly in relation to litigation and other contentious situations. He is a member of the firm's Data Protection and Privacy group. Robert was named in *Legal Week*'s 2016 list of Rising Litigation Stars in London.

Paul Baker
Simmons & Simmons LLP
CityPoint
One Ropemaker Street
London EC2Y 9SS
United Kingdom

Tel: *+44 20 7825 4580*
Email: *paul.baker@simmons-simmons.com*
URL: *www.simmons-simmons.com*

Paul is a partner in the Financial Markets Litigation group in Simmons & Simmons LLP's London office, specialising in complex financial disputes and investigations, with a particular focus on contentious asset management work. Paul is a member of the firm's Cybersecurity group and leads the firm's reputation management practice. Paul has advised clients on various aspects regarding cybersecurity, including incident response planning, the investigation of breaches and reputational issues arising from such breaches. Paul is a regular presenter on cybersecurity topics and was highlighted by Legal Business in its 2015 Disputes Yearbook as of one the next generation of leading disputes partners.

Simmons & Simmons

Simmons & Simmons LLP is a leading international law firm with fully integrated teams working through 21 locations in Europe, the Middle East and Asia, and have 1,500 staff worldwide, including more than 240 partners and a total legal staff of over 1,000. The firm's strategy is designed to ensure it provides its clients with high-quality advice and delivers value through new and innovative ways of working. Their current client base includes a significant number of the current FTSE 100 and Fortune Global 500 companies.

A key commercial advantage is their focus on specific sectors, which include Asset Management & Investment Funds, Financial Institutions, Life Sciences and Telecoms, Media & Technology (TMT). Simmons & Simmons LLP acts regularly on the most innovative cases, deals and transactions in its chosen areas of specialism and receives recognition for the quality of its work from clients and others within these industry sectors.

Current titles in the ICLG series include:

- Alternative Investment Funds
- Anti-Money Laundering
- Aviation Law
- Business Crime
- Cartels & Leniency
- Class & Group Actions
- Competition Litigation
- Construction & Engineering Law
- Copyright
- Corporate Governance
- Corporate Immigration
- Corporate Investigations
- Corporate Recovery & Insolvency
- Corporate Tax
- Cybersecurity
- Data Protection
- Employment & Labour Law
- Enforcement of Foreign Judgments
- Environment & Climate Change Law
- Family Law
- Fintech
- Franchise
- Gambling
- Insurance & Reinsurance
- International Arbitration
- Lending & Secured Finance
- Litigation & Dispute Resolution
- Merger Control
- Mergers & Acquisitions
- Mining Law
- Oil & Gas Regulation
- Outsourcing
- Patents
- Pharmaceutical Advertising
- Private Client
- Private Equity
- Product Liability
- Project Finance
- Public Investment Funds
- Public Procurement
- Real Estate
- Securitisation
- Shipping Law
- Telecoms, Media & Internet
- Trade Marks
- Vertical Agreements and Dominant Firms

glg global legal group

59 Tanner Street, London SE1 3PL, United Kingdom
Tel: +44 20 7367 0720 / Fax: +44 20 7407 5255
Email: info@glgroup.co.uk

www.iclg.com