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:

Would the Standard of Cybersecurity be Improved by the Introduction of Mandatory Cybersecurity Controls?

Nigel Parker

Alex Shandro

Allen & Overy LLP

> "My medical friends tell me that it is possible to drastically reduce deadly hospital infections if doctors wash their hands for two minutes before operating. And yet only half of them do. These are doctors, they know the facts, real people are dying, and still they don't comply".[1]

These were the words of SWIFT CEO, Gottfried Leibbrandt, when announcing the company's plan to introduce mandatory cybersecurity requirements for users of the SWIFT money transfer platform. He was speaking in the wake of the so-called Bangladesh Bank Heist in February 2016, when attackers issued dozens of fraudulent money requests to the Federal Reserve Bank of New York using SWIFT credentials of Bangladesh Central Bank employees. The attackers were successful in obtaining $81 million, and a further $851 million in money transfer instructions were blocked.

Reports continue to emerge that other banks had also been targeted in the attack. Some of the attacks failed. For example, Leibbrandt revealed that one target: "… had the latest antivirus and had updated the latest security patch on our software, and in that case alerts from the antivirus and from the latest security patch triggered alerts that prevented further fraud happening there as well."

SWIFT itself was not the target of the attack, and nor were SWIFT systems or networks compromised in the attack. Rather, the systems and networks of banks using the SWIFT platform (within the particular bank's ICT environment) were targeted.

SWIFT's response has been to introduce a set of mandatory security controls for SWIFT's customers.[2] These requirements were likened by Leibbrandt to "basic hygiene", based on a combination of technical, logical and physical controls and incident response planning and staff training. By the end of December 2017, all users of the SWIFT platform will be required to have certified (together with supporting data) that they comply with those requirements.

The SWIFT platform is used by banking institutions throughout the world and processes approximately 25 million money transfers each day. It is a critical component of the financial services ecosystem and users of the platform are a prime target for cyber threat actors. SWIFT's decision to impose cybersecurity standards on its customers is borne out of a concern that, notwithstanding the apparent risks, its customers do not have basic cyber hygiene in place.

SWIFT's approach raises broader questions. In the absence of mandatory controls, are organisations sufficiently incentivised to invest in cybersecurity measures? Would the standard of cybersecurity be improved by the introduction of mandatory controls?

In the UK, a recent government survey of the largest public companies by market capitalisation, found that in more than two-thirds of those companies the directors have no training in responding to cyber attacks, and more than 10% have no plan in place to respond to a cyber incident. Together with the regular stream of cyber incidents making the headlines recently, this suggests that many organisations may not have appropriate cybersecurity controls in place.

As demonstrated by this guide, in many jurisdictions the legal framework applicable to cybersecurity is fragmented. Against an ever-growing threat landscape, on the face of it the argument for introducing mandatory regulatory standards (and robust enforcement of those standards) is compelling. Organisations in a wide range of sectors are now increasingly connected and hold increasing amounts of data. The consequences of a cyber attack are severe, from business interruption and other economic losses, to loss of or damage to data and damage to reputation, among others. The value of robust cybersecurity may be more readily apparent to organisations that provide a critical service, that rely on networks and IT systems to carry on their business, or that hold valuable intellectual property and data (or in SWIFT's case, all of the above). Some organisations, however, may be reluctant to invest significant costs in cybersecurity measures, as this does not show any immediate or easily measurable benefit (at least until an attack occurs). The introduction of mandatory security controls would at least set a minimum threshold.

However, as businesses, technology and the threat landscape continue to evolve, it is difficult to see how a meaningful set of umbrella security controls could be applied in practice. Mandatory security controls may result in weaker, rather than stronger, cybersecurity because organisations may decide to invest to meet those standards and no more. As the spate of high-profile attacks this year demonstrates, cybersecurity is not a finite problem that can be solved. It is a constant and evolving challenge for organisations, as cyber threat actors will continue to find cracks in any defences. The consequence of mandatory security controls could be a 'compliance' mindset, which fails to take account of the shifting context of the particular business, systems, vulnerabilities and threats. In the UK, for instance, the Government's focus is not on additional regulation, but on better education and improved information-sharing among businesses and the Government.

The diverse range of cyber threats means that it will never be possible to be completely immune. Equally, it means that regulatory standards alone are unlikely to present a workable risk management solution for organisations facing those threats.

There is a Diverse Range of Cyber Threats

As our lives become increasingly connected, the range of threats increases and it becomes harder to protect against them. According

to the National Cyber Security Centre (NCSC), the UK authority with responsibility for protecting critical services from cyber attacks and managing major cyber incidents, critical services in the UK were hit by 188 "high-level" attacks and "countless lower ones" in the last three months of 2016 alone.[3] Cyber incidents are caused by a wide range of threats and threat actors, from highly sophisticated criminals deploying bespoke malware to high-volume and more opportunistic attacks using 'off the shelf' malware.

Recent high-profile attacks, such as the Bangladesh Bank Heist, the attacks on the US Democratic National Party and the hack on Ukraine's power grid (the first confirmed hack to take down a power grid) were carried out by highly skilled threat actors according to carefully planned assaults. So too was the global Wannacry ransomware attack in May 2017, which Europol considers to be unprecedented in scale. The attackers exploited a vulnerability in the Microsoft Windows operating system to encrypt a computer's data and demand payment of Bitcoin ransom payments. The infection spread to computers on the same network and to random computers on the Internet, resulting in overall economic losses estimated to be in the hundreds of millions. In another example of the complexities of the cyber risk landscape, it has since been revealed that the US National Security Agency knew of the vulnerability but did not inform Microsoft, preferring to use the knowledge for its own cyber warfare offensive purposes.

Alongside the attacks that hit the headlines are hundreds of thousands of lower-level attacks, which are arguably of more concern to organisations from a risk management perspective, as little or no technical expertise is necessary. Malicious software can be downloaded from the Internet for free by almost anyone, and then used to launch an attack and wreak havoc on ICT-depending infrastructure. These so-called 'commodity threats' are increasingly used by organised criminals as a relatively risk free method to steal information and exhort money.

Although external cyber attacks may receive the majority of the media publicity, a recent IBM survey found that most cyber incidents originate from within an organisation.[4] Disgruntled employees may steal information and disclose it to competitors, or may leave a 'back door' open in a system that can be exploited by others. Indeed, a US Government audit report in August 2017 on the Office of Personnel Management identified a high turnover of staff in key positions as a key cause of cybersecurity weaknesses in the US Government.[5]

The proliferation of connected devices – the Internet of Things – has also contributed to the growing threat. Connected consumer devices (from home appliances to cars) are being produced rapidly on a mass-market scale and are typically poorly secured. Any network of connected devices is vulnerable to attack through any of the devices in the network, and each device is a potential entry point for cyber attackers. For instance, 'Mirai' malware turns devices running Linux software (such as cameras and home routers) into 'bots' that are capable of being remotely controlled. In September and October 2016, Mirai was used to carry out denial-of-service attacks on several high-profile websites, including Twitter, Reddit and Airbnb. The malware exploited the typically weak password protection requirements of connected devices, and successfully logged into hundreds of thousands of devices by applying the most common factory default passwords. Those devices were effectively conscripted into a botnet and used to flood the targeted websites with traffic, thereby disrupting services. The US Government, among others, is now considering legislation mandating specific security requirements for Internet of Things devices procured by the US Government.[6]

To mitigate (albeit not eliminate) the risks of such a wide array of threats and threat actors – both internal and external – cybersecurity measures must accordingly be multi-faceted, spanning technical security measures, staff training, management reporting, technology procurement processes and more. These measures would require organisations to incur significant costs. Where the risks are hypothetical (albeit potentially severe, as explored further below), mandatory regulatory standards (plus enforcement of those standards) may well serve to incentivise that investment. However, it is difficult to envisage a set of security controls covering each of these areas in a meaningful and effective way for organisations of different sizes, business models and industries.

The Risks of a Cyber Incident are Equally Diverse

A cyber incident may result in economic losses, including business interruption, internal costs (i.e. time involved to identify, remedy and manage the fall-out of the incident), out-of-pocket expenses (e.g. legal advice and forensic investigators), regulatory fines, damages awards in civil actions, and damage to market reputation and goodwill. An incident may also result in the theft or deletion of data and intellectual property. Threat actors may also tamper with the integrity of an organisation's data. This is particularly dangerous because the victim may not be aware that its data has been compromised. For instance, at the end of 2016, the cybersecurity consultants Security Research Labs demonstrated how security vulnerabilities in travel booking systems used by major airlines could enable attackers to tamper with passenger records used to store reservations and thereby steal flights, divert air miles, or use the passenger information in more targeted phishing attacks.

The severity and range of risks of a cyber incident were well demonstrated in an attack on UK telecoms firm TalkTalk in October 2015 that resulted in the theft of the data of more than 157,000 customers, including bank account details. The day after the attack, the value of TalkTalk shares fell by 10%, and a further 20% the week after the attack. TalkTalk revealed recently that its costs have since run to over £45 million and that it had lost an estimated 101,000 subscribers in the wake of the attack. In October 2016, TalkTalk was fined £400,000 by the UK data protection regulator, the Information Commissioner's Office (ICO), for failing to take the basic security steps that, according to the ICO, would have prevented the attack. Echoing the words of SWIFT CEO Leibbrandt, the Information Commissioner, Elizabeth Denham, said: "TalkTalk's failure to implement the most basic cyber security measures allowed hackers to penetrate TalkTalk's systems with ease." The attack targeted database software holding customer data inherited from a 2009 takeover of a rival firm, Tiscali, and the software had not been updated since. The ICO found that TalkTalk was unaware of the problem, which could have been solved easily, despite being victim of two cyber attacks earlier in the same year that should have alerted TalkTalk to the issue.

In some cases the potential risk is not economic but physical. In 2016, a pair of white hat hackers demonstrated an exploit that allowed them to control the air conditioning, audio system, windshield wipers and brakes of a Jeep, causing the vehicle to stop on the road. Had the exploit been in the hands of malicious threat actors, there would have been potential for considerable physical harm. Separately, Johnson & Johnson revealed in October 2016 that one of its insulin pumps for diabetics was vulnerable to being hacked, thereby causing an overdose.

Surgical robots are already being used in hospitals to carry out keyhole surgery and other procedures. As robotics (operated by artificial intelligence technology) become increasingly prevalent in the health and many other industries, the risks become much greater, especially

if the robot is not secure (for instance, if a robo-surgeon is hacked while in the operating theatre). Cyber consultancy firm IOActive predict that robots may be turned against their employers by criminals or competitors, being used to spy or disrupt production lines.[7]

The Legal Framework for Dealing with Cyber Risks is Dispersed and High Level

Set against the scale and diversity of the threats, and the potential severity of the risks, is a relatively fragmented legal landscape. In the US, for instance, various federal and state laws and regulations govern cybersecurity incidents, with the applicability of each dependent on the sector and geographic operations of the relevant organisation.

In fining TalkTalk in October 2016, the Information Commissioner, Elizabeth Denham, concluded that: "Companies must be diligent and vigilant. They must do this not only because they have a duty under law, but because they have a duty to their customers." This reference to legal duties was notable, because in the UK, as in the vast majority of other jurisdictions surveyed in this guide (including Australia, Belgium, Canada, Switzerland, the US and Taiwan, among others), there are few laws mandating cybersecurity measures and those that do exist are based on high-level principles or otherwise apply in limited cases (e.g. to specific sectors or in a government procurement context).

The UK legal framework applicable to cybersecurity is dispersed across statutes, common law doctrines and sector-specific regulatory guidance, as summarised in the England & Wales chapter of this guide. Among them are high-level security requirements with which certain organisations must comply. For instance, UK data protection legislation requires all organisations that control personal data to implement technical and organisational measures to safeguard that personal data, which may involve implementing cybersecurity controls.

From 25 May 2018, the EU General Data Protection Regulation (the **GDPR**) will take effect and will bolster the security requirements with which controllers of personal data must comply (albeit still within a principles-based approach). Among other things, the GDPR requires controllers of personal data to carry out privacy impact assessments in relation to certain 'high risk processing', to employ data protection officers and to notify data breaches to regulatory authorities and data subjects within prescribed time periods. These requirements are accompanied by a much tougher sanctions regime, including potential fines of up to 4% of annual worldwide turnover for certain breaches.

The UK Government regards implementation of the GDPR as an opportunity to improve cybersecurity risk management and has stated that they "…will ensure that cyber security is at the centre of the way we promote and implement the GDPR".[8] This statement was made in a UK Government cybersecurity review in December 2016 which concluded that, beyond the GDPR, additional cybersecurity regulatory standards were not justified, for the reasons explored further below.

For its part, the EU has indicated its support for harmonised cybersecurity standards. The Cyber Security Strategy of the European Union, issued in 2013, states that: "There need to be appropriate cyber security performance requirements implemented across the whole value chain for ICT products used in Europe."

A key pillar of this strategy is the Network and Information Systems Directive (the **NIS Directive**), which is required to be implemented into national legislation by EU Member States by 9 May 2018. Among other things, it requires 'operators of essential services' and 'digital service providers' to put in place reliable security measures for its network and information systems, so as to prevent and minimise the impact of cyber incidents. As with the GDPR, this is principles-based. There are no standards set out in the NIS Directive, and the text contemplates that the EU Agency for Network and Information Security (ENISA) will work with Member States to develop more detailed guidance on specific technical areas. On 14 September 2017, the European Commission issued draft guidance on security measures to be taken into account by digital service providers. These include technical security measures, incident handling procedures, business continuity management, auditing and ongoing monitoring measures. The Commission intends to release equivalent guidance for operators of essential services later in 2017. The NIS Directive's effectiveness will therefore depend on how the requirements are passed into national law of Member States and subsequently enforced by national regulators. The terms 'operator of essential services' and 'digital service providers' are not specifically defined in the NIS Directive, with Member States being tasked with identifying the entities falling under these categories. With much of the detailed application of the NIS Directive left to the national implementing laws of Member States, there is a risk of fragmentation. Entities caught by the NIS Directive may have to comply with different standards in different Member States.

Where cybersecurity requirements are principles-based, organisations will have to determine the steps that are required to comply. Some may elect to take a view on existing (and perhaps inadequate) cyber measures if it enables them to save significant costs. After all, the risks of a cyber incident are hypothetical until one occurs. However, it is questionable whether more prescriptive security standards are the solution. If an organisation is prepared to take a view on existing (and perhaps inadequate) cyber measures today, it is possible that they will continue to do so in a world with more granular mandatory security controls. Rather, the issue would appear to lie in the underlying perception that cyber risks are not worth investing in.

Cyber Law Must Remain Flexible and Encourage a Culture of Cyber Hygiene

Businesses and technology are constantly evolving, whether through M&A activity, adoption of new technology or deployment of new devices. As businesses and technology evolve, so too does the nature of the cyber threat. It would seem to follow that cyber law must remain sufficiently flexible. There is unlikely to be a 'one size fits all' regulatory standard that could be applied.

This was at the crux of the UK Government's cybersecurity review in December 2016, which concluded that no additional cybersecurity regulation was needed beyond the principles set out in the GDPR and NIS Directive.[9] This review concluded that additional cybersecurity regulation could lead to a mere tick box exercise and "encourage a 'compliance' culture rather than proactive cyber risk management".[10]

The UK Government considers that the GDPR will provide the necessary incentive to improve cyber risk management, particularly when coupled with the implementation of the NIS Directive for those organisations that operate essential services. This conclusion was based on a belief that the principles applying to personal data in the GDPR would help to protect other categories of data held by organisations, with the overall result that security awareness would increase across the business. If this belief is borne out in practice, the same may apply in other EU Member States and non-EU jurisdictions with principles-based data privacy legislation (including Australia, Canada, Israel and Switzerland, among others).

It remains to be seen whether the UK Government is relying too heavily on the data privacy principles in the GDPR. The requirement to notify data breaches, and the resultant negative publicity, may well act as an incentive to improve cyber hygiene within an organisation. However, in the longer term, if data breach notifications become more commonplace, it is possible that the amount of publicity (and corresponding incentive to comply) will wane, albeit that the potential for significant fines will remain.

Rather, the UK Government's ambitious strategy to make the UK the safest place in the world to go online is intended to be delivered through non-binding best practice guidance that underlines the importance of the culture of cyber hygiene, together with government initiatives to ensure that organisations in the UK are kept aware of the latest cybersecurity threats (and therefore where they can best focus their security efforts).

In the absence of specific legal requirements, many organisations currently seek to comply with best practice industry standards (such as ISO / IEC 27001 or PAS 555), as they provide a helpful reference point for good security and are useful to demonstrate to regulators that steps have been taken to protect information. To this end, the NCSC has issued multiple layers of cybersecurity controls, from a set of basic controls designed to show organisations how to protect themselves against low-level threats (the 'Cyber Essentials' scheme) to more sophisticated controls (the '10 Steps to Cyber Security'). These are presented not as prescriptive controls, but as categories of steps that should be kept under constant review in the specific business context. The UK Government has confirmed that it does not recommend mandatory compliance with these standards,[11] although all suppliers bidding for certain Government contracts are required to comply with the 'Cyber Essentials' controls.

Encouraging the Right Strategy Appears Key

The UK Government's approach recognises that an organisation can never be completely immune from a cyber incident, and good cybersecurity is instead a question of risk management spanning the organisation's technology, people and processes. In principle, this appears to be a pragmatic approach to the ever-evolving threat landscape.

However, the August 2017 survey of the FTSE 350 companies (which, among other issues, revealed that more than half of the UK's largest public companies have not taken recommended action to identify cyber risks) suggests that there is still significant progress to be made. Absent government intervention, organisations need to be sufficiently incentivised to adopt appropriate cyber risk management measures. Board engagement appears to be essential to this process. In the UK, for instance, the NCSC intends to work with organisations such as the Financial Reporting Council and Investment Association to educate boards and investors about cyber risk and the risk management steps that boards should be taking.[12]

It then becomes not only a question of cost, but how those costs are invested. No matter how strong an organisation's cybersecurity may be, motivated hackers will find cracks. It follows that good cybersecurity should be based on developing the right processes to identify, mitigate and respond to vulnerabilities. For example, a high-profile hacking attack of an organisation may prompt CEOs to increase investment on their ICT infrastructure to ward off external threats. However, in doing so, they may be diverting resources away from internal threats (e.g. employees falling victim to phishing attacks) that, as noted by the IBM report referred to above, may be just as damaging.

It is a complex picture, and one that seems unlikely to be improved by the introduction of additional regulatory standards alone. In practice, greater awareness of the threats, risks and best practice security controls is essential. This could be achieved by ensuring that cyber incidents are well-publicised and any breaches of existing laws and standards are enforced robustly. In addition, steps could be taken to improve information-sharing and cooperation among businesses and regulatory bodies. In the wake of the Wannacry incident, for instance, a bipartisan bill was put forward to the US Congress, seeking to limit the ability of US intelligence agencies to horde vulnerabilities and, in certain circumstances, require notification of the vulnerability to the manufacturer. As laws such as the GDPR come into force, more information on data breaches will become available to regulators, and that information could be shared with other regulators around the world with a view to ensuring greater awareness of threat information and developing consistent good practice. This in turn should improve the ability of organisations to manage their cyber risks and develop informed investment strategies.

Endnotes

1. https://www.sibos.com/media/news/united-fight-against-cyber-attacks.
2. https://www.swift.com/myswift/customer-security-programme-csp/security-controls.
3. https://www.ncsc.gov.uk/content/files/protected_files/news_files/The%20Cyber%20Threat%20to%20UK%20Business%20%28b%29.pdf.
4. 2017 IBM X-Force Threat Intelligence Index, https://www.ibm.com/security/data-breach/threat-intelligence-index.html.
5. www.gao.gov/assets/690/686400.pdf.
6. Internet of Things Cybersecurity Improvement Act 2017.
7. www.ioactive.com/pdfs/hacking-robots-before-skynet.pdf.
8. HM Government, 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.
9. HM Government, 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.
10. *Ibid.*, p. 3.
11. *Ibid.*, para. 5.7.
12. *Ibid.*, para. 5.6.

Nigel Parker
Allen & Overy LLP
One Bishops Square
London E1 6AD
United Kingdom

Tel: *+44 203 088 3136*
Email: *nigel.parker@allenovery.com*
URL: *www.allenovery.com*

Nigel is a partner specialising in intellectual property, data protection and privacy, commercial contracts and IT law. He is a member of the firm's Cyber Security Group and has advised clients on strategies for managing legal risk in relation to cybersecurity, including the deployment of a variety of risk management tools, on the response to attacks and dealing with regulatory authorities, and on taking pro-active steps in response to attacks.

Chambers 2015 cites Nigel as an expert in the fields of data privacy and outsourcing, describing him as "technically faultless" as well as "very practical and very good at finding solutions".

Alex Shandro
Allen & Overy LLP
One Bishops Square
London E1 6AD
United Kingdom

Tel: *+44 203 088 4594*
Email: *alex.shandro@allenovery.com*
URL: *www.allenovery.com*

Alex is a senior associate specialising in commercial contracts, intellectual property, cybersecurity and data protection law. Alex advises clients in technology and data-rich sectors on their most complex commercial arrangements, including outsourcings, licensing, collaborations and IP / data exploitation. A member of the firm's Cyber Security Group, Alex has advised regularly on risk management strategies in relation to cybersecurity, including contractual arrangements with vendors.

ALLEN & OVERY

Allen & Overy is a full-service global elite law firm headquartered in London. Our commitment to help our clients deliver their global strategies has seen us build a truly global network now spanning 44 offices in 31 countries. We have also developed strong ties with relationship law firms in more than 100 countries where we do not have a presence.

We have a strong cybersecurity practice comprising a core team of 15 partners with diverse backgrounds in data protection, bank regulation, antitrust, securities laws, technology, IT, litigation, employment, IP and corporate. This spread is crucial because cybersecurity incidents frequently span a wide range of traditional legal practice areas. There is an important legal component to cybersecurity and our integrated team of diverse practitioners reflects this requirement. As a full-service global elite law firm, we are able to advise clients on all legal issues concerning cybersecurity.

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