April 2015

Olswang Cyber Alert

OLSWANG

Introduction and welcome

Welcome to the latest edition of Olswang's Cyber Alert, a regular round up of regulation, best practice and news from our international cyber breach and crisis management team. There is a great deal to report since our last update in October 2014. In February, the Olswang team visited our friends in the US, co-hosting a cyber workshop in Silicon Valley and presenting to the Los Angeles chapter of the IAPP on the latest status of the General Data Protection Regulation. You can read our December 2014 status update on the draft Regulation, which includes an analysis of data breach notification here.

In this edition:

- Melanie Shefford considers whether the UK Government is doing all it can to help tackle the menace of cyber attack.
- Laurence Kalman takes a closer look at the Bank of England's CBEST initiative. Is this a sign of things to come for other industry sectors?
- In our standards and benchmarks section we include the latest round up of UK, EU and Global cyber standards.
- In our regulatory radar section, we report on the latest twists and turns in the negotiations for the Network and Information Security Directive and the General Data Protection Regulation.
- In our threat landscape section, we report on the World Economic Forum's report into global risks which ranks cyber as one of the most likely high-impact threats in the modern world. We also report on the huge Anthem hack in the US and, separately, on the second ever recorded incidence in which a cyber attack caused actual physical damage.

We hope you will find our update useful and we welcome your feedback - but if you'd prefer not to receive future mailings, please use the opt-out link on the email.

Ross McKean
Head of Data Protection
London
+44 20 7067 3378
ross.mckean@olswang.com

Lead article

What is the UK Government doing about cybersecurity?

With headlines frequently reporting large-scale cyber attacks, the UK's cybersecurity measures – and their weaknesses – are under constant scrutiny and criticism. Yet many businesses fail to give sufficient priority to cybersecurity. The City of London Police Commissioner has claimed that businesses will not properly focus on cybersecurity until a cyber attack causes a major global company to cease trading. In the same speech, the Commissioner said that he believed the UK Government is doing "all it can" to address the threat.

Defending against the menace of cyber attack cannot be achieved by any government on its own. The private sector and wider public sector will have to take their share of responsibility to help secure the digital resources of the UK.

Nevertheless, it certainly helps the cause to have strong leadership from government. In this article we consider whether the UK Government really is doing all it can to promote the defence of the UK against the growing menace of cyber attack.

The National Cyber Security Strategy

The Government published the National Cyber Security Strategy in 2011. The vision was to ensure that in 2015 the UK would "*derive huge economic and social value from a vibrant, resilient and secure cyberspace, where our actions, guided by our core values of liberty, fairness, transparency and the rule of law, enhance prosperity, national security and a strong society*". To achieve this, the Government has provided £860 million of funding and committed to the following objectives:

1. to tackle cyber crime and make the UK one of the most secure places in the world to do business online;
2. to make the UK more resilient to cyber-attacks and better protect UK interests in cyber space;
3. to help shape an "open, vibrant and stable cyberspace" which the UK public can use safely and that supports open societies; and
4. to build cybersecurity knowledge, capability and skills in the UK.

What progress has been made so far?

Some key examples of the Government's progress to date which may be of interest to businesses - many of which are documented in a December 2014 Government progress report – include:

Raising awareness and assessing risk

The Government has attempted to increase business awareness of cybersecurity risks and threats in various ways. For example, it has:

- published new guidance for businesses, such as BIS' guidance for the corporate finance sector and Non-Executive Directors (for more commentary, see here) and GCHQ's bring your own device guidance. In January the Government also updated its 10 Steps to Cyber Security guidance;

- carried out annual surveys to help raise awareness of the risks and impact of security breaches, such as the Cyber Governance Health Check (published following a 2014 survey of FTSE350 companies – for more commentary see here) and the Information Security Breaches Survey;

- launched the BIS Cyber Essentials accreditation scheme in June 2014 which enables organisations to demonstrate their cyber resilience. The scheme is designed to encourage more organisations to adhere to a basic set of security standards which prevent the most common forms of attack. Accreditation may also help encourage consumer confidence in the businesses which invest time and money in gaining accreditation;

- worked with specific sectors in relation to cybersecurity issues, such as the financial services sector where the Bank of England has developed the CBEST vulnerability testing framework (see our separate article on this, here)

January 2014 also saw the launch of Cyber Streetwise, a campaign intended to improve cybersecurity among the public and SMEs (for example to encourage the use of more secure passwords). This campaign may benefit larger businesses too by (for example) reducing incidences of online fraud.

Promoting the UK cybersecurity industry

The Government has set a target of £2 billion of cyber security exports by 2016 and is working with industry in a joint Cyber Growth Partnership to pursue several initiatives, including the establishment of regional cybersecurity business clusters. The Government has also promoted the UK's cybersecurity expertise overseas. For example, in January David Cameron visited the Obama administration with 12 UK cyber defence firms.

Information sharing

The Cybersecurity Information Sharing Partnership (CiSP) was launched in 2013 and permits organisations to share threat information which is then analysed and provided along with advice to the rest of the CiSP community. In 2014 CERT-UK also launched a scheme to facilitate the exchange of cybersecurity information on a regional basis. In 2015, GHCQ will expand a programme allowing communications service providers to share cyber intelligence so that action can be taken to protect their customers.

Tackling cybercrime

GHCQ is investing £3 billion over the next nine years to develop cyber intelligence. Two new bodies have also been set up to specifically deal with cybersecurity matters: the National Cyber Crime Unit, and the UK's Computer Emergency Response Team (CERT) which supports critical sectors to prepare for cyber-attacks, co-ordinates with other CERTs, and provides alerts and information to CiSP members and the public. Further, dedicated policing units have been established, such as Operation FALCON, a collaboration between the Metropolitan Police's fraud squad and cyber crime unit.

International collaboration

This is a *crucial* building block to cyber defence. Hackers and criminals have no respect for international borders; it is essential that governments build an international governance structure to tackle the international cyber threat. The Government has been working with other countries to crack down on cyber crime, improve cross-border law enforcement, and establish the UK as a technology and policy leader. For example, it was recently announced that the UK and US would work together to stage cyber attack war games – the first one being on the financial sector later this year - and improve their exchange of cyber intelligence.

Education, skills and training initiatives

The UK's poor showing in international education league tables for science, technology, engineering and maths is not just a national embarrassment; it is also a national security issue. The Government recognises this and has implemented various initiatives to ensure that businesses will have access to cyber workers with the necessary skills and expertise, including by:

- funding the development of GCSE and A-level cybersecurity materials;
- working with higher education to develop cybersecurity studies, grant recognised status to research universities, and funding research and training centres. GHCQ has also certified some cybersecurity masters degrees;
- encouraging computer science graduates to develop an interest in cybersecurity;
- organising competitions and other initiatives as part of the Cyber Security Challenge;
- offering professionals a skills certification framework under the CESG Certified Professionals Scheme;
- developing online training courses for lawyers and accountants and SMEs.

Efforts have also been been made to bolster specialist police officers' skills in order to ensure that law enforcement authorities can properly investigate cyber crime.

What else could the Government do to help businesses?

To its credit, the UK Government has made significant progress to date by implementing the National Cyber Security Strategy. However, this is an arms race. The UK's digital economy faces determined criminals and nation states who have the intent and the means to hack UK critical infrastructure and UK business and to exploit UK consumers. There is always more that can be done. For example:

More needs to be done in terms of sensitising organisations to cybersecurity risks.

Many businesses still appear to be in the dark about the true scale of cyber risks based on the results of the 2014 FTSE 350 Cyber Governance Health Check which revealed that only 24% of FTSE 350 companies base their discussions on cyber risk on comprehensive or robust management information. Detection rates of hacks are still

poor. A recent survey found that the median average number of days taken by organisations to detect a hacker on their systems was 229 days, which is a lengthy period of time for hackers to exploit data assets with impunity.

The Government could consider more proactive measures such as requiring certain businesses deemed to be particularly high risk (e.g. critical infrastructure providers) to undergo *mandatory* cyber accreditation.

More needs to be done to share and encourage the sharing of threat information.

The Government could take a more pro-active role in terms of sharing detailed threat information and making it easier for businesses to share knowledge with each other. As the Commissioner himself said: *"The answer is not more policing […] But better collaboration between law enforcement and industry, with the role of police increasingly about helping industry to protect itself."* Some businesses are already partnering to share information with each other, but the reach of individual businesses is necessarily more limited than the Government's. The UK could learn here from the US experience where the flow of information between business and law enforcement (notably the FBI) is much more of a two-way street.

Policing and law enforcement needs to improve.

Despite the National Crime Agency's estimate that cyber crime costs several billion pounds a year, a recent report into policing found that more work is required to close the widening gap between cyber threats and police capability. In particular, the report refers to a serious underreporting issue when it comes to cyber crime, arguably due to lack of confidence in the police – according to a 2013 Home Office report, businesses report *less than 2%* of online incidents to police. Further, whilst the UK has specialist officers with expertise in cyber crime, the report states that every police officer should receive cyber training, understand cyber crime and be able to deal with it.

The Government needs to ensure businesses have access to skilled workers.

Lastly, the Government could do more to ensure that in the long term, people with the right skills are available to support businesses. The Government's initiatives so far are a step in the right direction, but have focussed on secondary and further education only. Many in the industry think that the national curriculum for all children – not just those above 11 years old - should include computer science skills so that children learn how computers work, as well as how to use them. This would encourage more people to eventually get into the more complicated field of cybersecurity. Fortunately, the Government appears to be taking initial steps to remedy this, having announced that tech businesses are supporting a £3.6m initiative to deliver computing training in primary schools.

Conclusion

Cyber defence costs money and in the current climate it is unlikely that we will see any further significant investment in cyber defence by the UK Government, whoever wins the May election. With competing demands for public funding and further significant cuts likely to be imposed by the next administration, cyber defence will have to make do with a limited budget. As such it is all the more important for the UK Government to use that limited resource wisely and encourage the private sector and wider public sector to step up and share the burden of cyber defence.

CBEST security testing in the financial services sector: a new line of defence?

In May 2014 the Bank of England launched "CBEST", the first framework for testing the cybersecurity vulnerabilities of the UK's financial institutions. The exercise aimed to shift financial firms' focus from preventing attacks to improving resilience and the ability to bounce back after suffering an attack. In our article "CBEST: a new line of defence?", we examine how CBEST differs from standard penetration testing, whether the programme will be expanded beyond the UK's core financial system and whether it may be a sign of things to come for other industry sectors.

Read the full article on our Datonomy blog here.

Standards and benchmarks

UK standards and benchmarks

- **Cybersecurity guidance for non-executive directors: 25 key questions to ask:** Reflecting just how far cybersecurity has now risen up the business agenda, in December 2014, the Department for Business, Innovation and Skills (BIS) issued "Cyber Security: balancing risk and reward with confidence (Guidance for Non-Executive Directors)".Read our summary of the key issues here.

- **Latest FTSE 350 Cyber governance Health Check shows that cyber threat continue to rise up the risk agenda:** In January BIS released its second annual review of FTSE 350 companies' preparedness for potential cyber attacks. The BIS report, entitled "FTSE 350 Cyber Governance Health Check Tracker Report", revealed a number of interesting trends. Read our summary of the key issues here.

- **Revised Cybersecurity Guidance for Businesses:** In January the UK government revised and augmented its cybersecurity guidance (originally published in 2012). The revised suite of documents, published jointly by The Cabinet Office, CESG, Centre for the Protection of National Infrastructure and BIS, now comprises: the 10 Steps Guidance, 10 Steps: Board Level Responsibility, 10 Steps Executive Companion, a guide to Reducing Risk in 10 Critical Areas, a new paper entitled "Common Cyber Attacks: Reducing The Impact" and various accompanying infographics.

- **Revised guidance from the ICO:** The UK Information Commissioner's Office has revised its high-level guide to data protection. The section on Information Security (Principle 7) provides a non-exhaustive list of the kinds of technical and organisational measures which may be appropriate, and provides links to the ICO's various detailed guidance documents on security-related compliance including its IT security top tips, and guidance on asset disposal, encryption, BYOD and the use of cloud-based storage.

- **Updates to the Cyber Essentials Scheme:** BIS launched its Cyber Essentials Scheme in June 2014. This sets out 12 technical requirements that organisations must meet to achieve certification. Since October, Cyber Essentials certification has become a requirement for suppliers bidding for certain government contracts involving sensitive and/or personal information. In January BIS published an updated version of its Assurance Framework.

- **CESG Information Risk Management Guidance:** CESG has published (in November 2014) and updated (March 2015) its guidance for public sector organisations "*to support people making decisions in technology projects which have a security impact*". It comprises: a detailed guide to Managing information risk, Principles of effective risk management, a detailed Analysis of risk management methodologies and three case studies. It also includes a set of principles for effective risk management, and some case studies based on procurement by The Cabinet Office, CERT UK and CESG.

- **Guidance for cyber exports:** TechUK (the technology trade association), in association with the Institute of Human Rights and Business, has published government-backed guidelines entitled "Assessing Cyber Security Export Risks" for UK cybersecurity companies. The guidance aims to maximise profits from such exports, whilst protecting companies from reputational damage, protecting national security and ensuring the products

are not used in human rights abuses. Culture Minister Ed Vaizey has described the guide as a *"valuable and accessible tool which will help British companies respond with confidence to opportunities in the global cybersecurity market*".

EU standards and benchmarks

ENISA, the European Network and Information Security Agency, has published the following new reports and guidance:

- The Secure ICT Procurement in Electronic Communications report, which highlights the growing dependency of providers on ICT products and outsourced services and the Security Guide for ICT Procurement, which maps security risks to the full framework of security requirements which can be used as a tool during procurement.

- A "Good Practice Guide on Training Methodologies", to provide guidance to organisations on how to create, organise and conduct training for information security and CERT professionals. This new guidance is intended to be coupled with the ENISA CERT training material.

- "Privacy and Data Protection by Design – from policy to engineering", detailing leading privacy design strategies. The report aims to marry the EU's existing legal framework with expected technological implementation measures in the field. Targeted at data protection authorities, policy makers, regulators, engineers and researchers, the report suggests producing further incentives for adopting privacy by design measures and new standards for electronic communication.

- "Cloud Certification Schemes Metaframework" (CCSM). The CCSM is an online tool for businesses to ensure security when purchasing cloud storage services. By requiring 27 security objectives in order to become a certified cloud scheme provider, Udo Helmbrecht, the Executive Director of ENISA, hopes that procurement of cloud services can be greatly simplified.

Global standards

ISO 27018 Code of practice for protection of PII in public clouds; where are we now? Since its release in August 2014, ISO 27018 is becoming well established as the "go to" standard to help cloud customers to comply with their privacy obligations when using public cloud services. Privacy regulators recognise and refer to the new standard. Cloud customers are using it in their RFP requirements. This post on Olswang's telecoms blog looks at how the new ISO is gaining recognition from privacy regulators and cloud customers around the world.

Regulatory radar

Draft Network and Information Security Directive: entering final negotiation phase?

When we published our last Cyber Alert in late October 2014, the first trilogue negotiation between the three EU institutions had just taken pace, a second took place in November and the third and final meeting was scheduled for 9 December. The outgoing Italian Council Presidency published a statement that it was "*confident the EP and the Council…will reach a deal before the end of the year*". However, progress updates then went quiet. It was not until 11 March that the (now Latvian) Council Presidency announced that the Council's negotiating mandate had been agreed at the Permanent Representatives Committee. This means that negotiations with the Commission and Parliament can resume, and this third trilogue is scheduled for late April.

It appears that one of the main sticking points within the Council has been the scope of the "market operators" who will be caught by the new obligations to report cyber attacks. The Commission's original proposal sought to catch not only classic critical infrastructure providers, but also online platforms. In contrast, last year the European Parliament voted to exclude online platforms from scope. It is reported that within the Council, Member States are split 50/50 over whether the new rules should apply to ecommerce and social media or not. This 126 page leaked Council draft comparing the relative positions of the Commission, the Parliament and the Council's proposed negotiating stance seems to indicate that the Council favours a middle position, extending the new rules to certain providers of "*essential services in the fields of Internet infrastructure and digital service platforms*" which meet a set of strict criteria (which also apply to more conventional critical infrastructures such as energy, transport, banking, health and drinking water).

There has been intense lobbying activity by ecommerce and software providers to stay out of scope of the NISD – see for example this open letter sent by the CCIA (Computer and Communications Industry Association) late last year. It remains to be seen where the perimeters of the "market operator" definition will be drawn. We will provide a full analysis of the "what, who and when" of the new cyber security and reporting rules once the text is agreed. Member States will then have between 18 and 24 months to transpose it into national law – so, even if it agreed in April it is unlikely to take effect until late 2016 at the very earliest, or more likely 2017.

Draft GDPR: latest predictions – agreement at Council level by Summer?

Meanwhile, the draft General Data Protection Regulation is inching forward. In our October update we reported that the Council had recently formulated its position on the data security and breach notification provisions. However, the Council has still only reached a "partial general approach" on a few of the text's eleven chapters (although the frequency with which new documents are being posted on the Council's Consilium website indicates that there is no shortage of activity and discussion among the Member States. On 13 March the Council announced it had reached a partial general approach on two further (and important) aspects of the draft Regulation. These are the provisions on the One Stop Shop approach to enforcement as set out in Chapters 6 and 7 and the principles for processing personal data in Chapter 2.

Until the Council has formulated its negotiating stance on all aspects of the draft Regulation it cannot enter into trilogue negotiations with the Commission and Parliament. The latest official statements on the timetable for adoption of the draft Regulation include a statement in January by Digital Single Market Vice President Ansip that the Council could agree its common position by June 2015.

Our best guess of the likely timescale is that the Council will agree the text this summer with at least 6 months of trilogue negotiations to follow after that. Once there is an agreed text it will then need to be translated which, for a regulation of this complexity, could take a further three months. Adding those steps together, we do not expect to see the Regulation published until the end of June 2016. There is likely to be a two year transposition with the Regulation coming into force in 2018.

Germany

We report on the latest progress of the draft IT Security Act here.

Belgium

Belgium has recently established its Center for Cyber Security and its Center of Excellence for Training, Research and Education. Read more on our Datonomy blog here.

Asia

The Cybersecurity Agency (CSA) of Singapore is due to go live on 1 April 2015. Read more from Olswang's blogging team in Asia here.

United States

We report on the latest US moves to promote a culture of cyber attack information sharing between the private and public sectors here.

The threat landscape and other recent news

Threat landscape

Trends and vulnerabilities reported in Q1 2015 include the following:

- The World Economic Forum's 2015 report into global risks listed cyber attacks as one of the most likely high-impact threats in the modern world (only behind water crises, interstate conflict and failure of climate-change adaptation).

- The European Network and Information Security Agency (ENISA) recently published:

    - The third annual "Threat Landscape" document analysing the top cyber threats currently facing the world. Among the major changes noted in 2014: increased complexity of attacks, successful attacks on vital security functions of the internet, and successful international coordination of operations involving law enforcement and security vendors.

    - A report aimed at internet infrastructure owners and operators highlighting the threat landscape and best practice. Specific threats to connectivity include routing threats, DNS threats and denial of service threats.

    - The "Threat Landscape and Good Practice Guide for Smart Home and Converged Media" report. Read the full report here.

- ENISA also concluded its year-long simulated cyber crisis, Cyber Europe 2014, including 23 European Union countries. The simulated exercise aimed to review cyber crisis management mechanisms throughout the continent. Early indications suggested that Europe has a strong and maturing community of cyber crisis managers, however, the report is not due to be published until May 2015. Plans are already underway for Cyber Europe 2016.

- Cisco's 2015 Annual Security Report suggested that government agencies, in general, appear to be better able to cope with data breaches and have stronger cybersecurity than the private sector. About 43% of the public sector fell into the "highly sophisticated" category while financial services and pharmaceutical companies registered 39% and 32% respectively.

- PwC's latest Global Economic Crime Report concluded that, having surveyed 5,128 companies from 99 different countries, one in four companies experienced cyber crime and of those, 11% have suffered losses greater than $1 million.

- According to various sources including this report on Reuters, Russian cybersecurity company, Kaspersky, publically stated that a hacker group called Carbanak stole up to $1 billion from financial institutions around the world in the last two years. The conclusion was the result of Kaspersky's collaboration with Interpol and Europol, in which it was found that the group used carefully crafted emails to trick particular employees into using invasive software (a technique called "spear phishing"). Once the software had been opened, the

hackers supposedly gained access to video surveillance and began mimicking the activity of bank tellers when transferring money between accounts and then ordering cash machines to dispense money at predetermined times. Read more broadsheet coverage here and here.

- The Guardian reported that NATO fights a daily cyber war against malware, hacktivists, organised criminals and state-sponsored attacks with a 200-strong team covering operations for about 100,000 people at 34 NATO sites. The unit dealt with over 3,600 abnormal activity or instruction attempts last year, of which there were about five confirmed cyber attacks per week.

- In November 2014, the Information Commissioner's Office (ICO) warned organisations that they must do more to protect their websites against one of the most common forms of online attack, known as SQL injection. The warning came after Worldview Limited, a hotel booking website, was fined £7,500 following a serious data breach stemming from the company's website's vulnerability.

- The global hotel chain, Marriott, was warned about the vulnerability of its customers' data by software developer Randy Westergren when he found problems with the company's Android app. Westergren discovered a security issue that made available customers' full names, postal and email addresses and credit card information. Westergren and Marriott security have now moved swiftly to address the issue.

- The US and UK made a serious pledge to collaborate on cybersecurity in January 2015. The first collaboration was the planned "war games" to test each other's preparedness for a cyber attack. The drill simulated attacks on the City of London and Wall Street in order to test the resilience of financial institutions. In order to plan further joint war games, Cameron and Obama spoke of setting up cyber cells either side of the Atlantic in which GCHQ and the NSA can share information and review strategies.

Recent attacks

Some recently reported attacks which illustrate a range of public and private sector targets - and a range of consequences – include:

- US health insurance company, Anthem, reported that hackers stole personal information relating to up to 80 million people. The hackers obtained names, birthdays, social security numbers, street addresses, email addresses and employment information, including income data. Anthem had to alert the FBI and hire cybersecurity firm FireEye to investigate. This led to security experts warning that healthcare and insurance companies could become the next big targets of cyber crime. As healthcare and insurance companies tend to hold masses of personal (and often very private) data about large numbers of individuals, the tech press picked up on expert predictions that hackers are moving away from financial organisations towards the less secure health sector. In the UK, the ICO also made similar predictions about the NHS.

- The hack of an unnamed steel mill in Germany in January 2015 was reported to be the second ever recorded incidence in which a cybersecurity breach caused actual physical damage. The hackers managed to manipulate the control systems to the steel mill's blast furnace causing destruction of equipment.

- The Obama administration was given a stark reminder of the threat posed by hackers after the US military's Central Command twitter account was allegedly hacked by ISIS in January 2015. The terrorist group posted

the message, “American soldiers, we are coming, watch your back. ISIS” on the account and provided a link to a statement that claimed the terror cell were already inside all the military’s computers.

- The Australian government became concerned about the rising threat of cyber espionage after reports that Chinese spies had stolen the designs of its new F-35 Joint Strike Fighter jet.

- Games developer, Money Horse, were forced to abandon the development of its game “Glorious Leader!” after hackers penetrated the game’s data files and shut down production completely. The game allowed players to assume the role of the North Korean leader, Kim Jong-un, as he bids to take on the US Army.

- Malaysia Airlines were hacked in January 2015 by the hacking group, Lizard Squad. The airline’s website went down for almost a full day as Lizard Squad left the message, “404 – Plane Not Found” (a reference to the the missing plane MH370). Worryingly, the message also said that the site had been hacked by the “Cyber Caliphate” raising suspicions that Lizard Squad, who previously only attacked gaming sites, may now be allied with the Islamic State.

M&A and investment

Recently reported investment and M&A activity in the cyber security sector includes:

- Venture capital funding in new cybersecurity companies increased by more than a third in 2014 according to research company Privco, as reported by the *FT*. Over $2.3 billion was invested last year as high-profile hacks fuelled early stage investment in online security companies.

- In 2014, ESG, a leading provider of testing, inspection and compliance services, published its IT spending intentions survey revealing that “security/IT risk management initiatives” is the most popular initiative driving IT spending at large organisations. This marked the first year that security has topped the list.

- The latest Cybersecurity 500 (containing the cybersecurity companies to watch in 2015) featured only 11 UK companies, as reported by *TechWorld*.

- London will be launching a cybersecurity technology business incubator in April 2015. The incubator, named CyberLondon (or CyLon), will grant £5,000 each to ten teams who will then house themselves within the incubator for 13 weeks. The incubator has been founded by Alex van Someren of Amadeus Capital Partners, however, the incubator is not-for-profit and will not take equity stakes in any of the businesses.

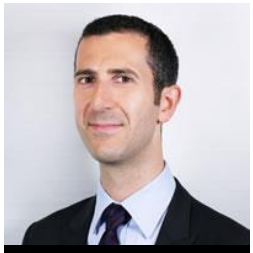
Key contacts

Katharine Alexander
Trainee Solicitor
London
+44 20 7067 3560

Blanca Escribano
Partner
Madrid
+34 91 187 1924

Matthew Hunter
Associate
Singapore
+65 9827 8711

Ashley Hurst
Partner
London
+44 20 7067 3486



Laurence Kalman
Senior Associate
London
+44 20 7067 3078

Carsten Kociok
Senior Associate
Berlin
+49 30 700 171-119

Christian Leuthner
Rechtsanwalt/Associate
Munich
+49 89 206 028-414

Ross McKean
Partner
London
+44 20 7067 3378

Tom Pritchard
Paralegal
London
+44 20 7067 3635

Sylvie Rousseau
Partner
Brussels
+32 2 641 1272

Melanie Shefford
Associate
London
+44 20 7067 3258

Thibault Soyer
Avocat à la Cour
Paris
+33 1 70 91 87 75

Dr Andreas Splittgerber
Partner
Munich
+49 89 206028-404

Elle Todd
Partner
London
+44 20 7067 3105

Claire Walker
PSL
London
+44 20 7067 3174

Berlin
+49 30 700 171 100

Brussels
+32 2 647 4772

London
+44 20 7067 3000

Madrid
+34 91 187 1920

Munich
+49 89 206 028 400

Paris
+33 1 70 91 87 20

Singapore
+65 6720 8278

Thames Valley
+44 20 7071 7300

OLSWANG

Olswang:
Changing Business

www.olswang.com