Cybersecurity

In today's interconnected world, virtually all companies, their suppliers and their customers are potential targets for cyber attacks. The risks associated with such incidents require a robust cybersecurity program in order to manage this fast-changing risk and remain in compliance.

Our global multidisciplinary team of lawyers and operational consultants advise on all issues surrounding cyber security, from building cyber resilience, through to incident response, and post-incident remediation, providing a holistic and tailored client service.

KEY CONTACTS

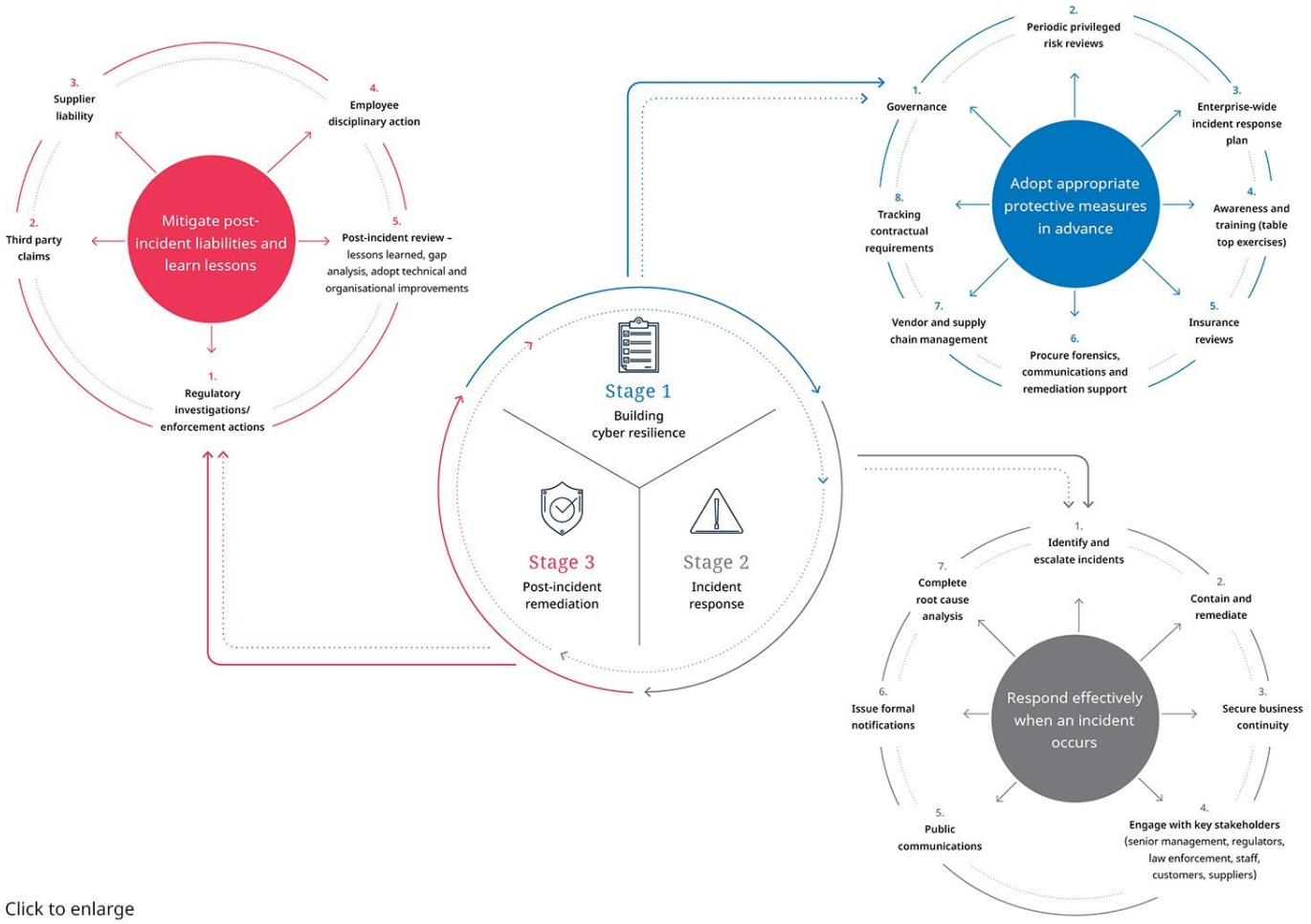
Jean-Pierre Douglas-Henry
Partner
London
T: +44 (0)207 153 7373
JP.DouglasHenry@dlapiper.cc

Stéphane Lemarchand
Partner
Paris
T: +33 (0)1 40 15 24 46
stephane.lemarchand@dlapip

Andrew Serwin
Partner
San Diego (Golden Triangle)
T: +1 858 677 1418
andrew.serwin@dlapiper.com

RELATED SERVICES

- Data Protection, Privacy and Security
- Litigation, Arbitration and Investigations
- White Collar and Corporate Crime
- International Trade, Regulatory and Government Affairs
- Corporate
- Public Company and Corporate Governance
- Intellectual Property and Technology



Click to enlarge

Risk mitigation - In order to ensure organizations are best placed to respond to an incident we help design and implement corporate governance structures to protect companies and their directors; offer privileged tools to assess risk and comply with evolving regulatory requirements; advise on developing and refining sound corporate policies and strategies to create and maintain a culture of security; and responsible supply-chain and vendor risk management techniques and contract support.

Incident response - We have helped clients through more than 800 security incidents globally. Our team can provide the experienced support you need 24x7 with confidence. We understand the legal and regulatory landscape in depth, having helped to draft almost all of the US data security and state breach notice laws and develop important best practices. We work as a cohesive team bringing a coordinated response to investigations and incidents on a worldwide basis.

Holistic approach - We combine technology, incident response, litigation, insurance and employment, and sector-adapted experience to give in depth support. We use round-the-clock communication protocols and a common methodology for immediate coordination and response. Wherever you may be, we can assemble an integrated team of the world's top cybersecurity technicians and lawyers, helping address your security problem, while cloaking those efforts in privilege (to the extent possible), anywhere in the world, within 24 hours of our first notification.

Global capabilities - Our team works together on a weekly basis and shares the same values and vision of client service. We provide a quick and consistent response to the cyber security needs of any organization. We match geographic and substantive breadth with depth, combining our technical knowledge of data protection, data risk and cyber security, cyber risk insurance policies, data transfer, records management, confidentiality, use of social media for business with practical experience and understanding of business imperatives.

Highly regarded - Our Cyber Security team was recently ranked by BTI Consulting Group among the Top 7 cyber security law firm practices. Many of our lawyers are recognized as leading individuals in their jurisdiction, and our global Data Protection, Privacy and Security practice is consistently recognized and top-ranked among our peers in the US, EU and globally by The Legal 500, Chambers & Partners, and other respected industry directories.

What we offer

We offer clients practical guidance through the cyber lifecycle, including:

Planning, design and preparation - building cyber resilience: our assistance includes ensuring clients have appropriate measures in place to manage cyber risk and respond effectively to a cyber-incident, preserving legal privilege and mitigating potential litigation and reputational risks. This includes bespoke training to relevant tiers of stakeholders, supporting the design of incident response plans and helping to lead "tabletop exercises" so that organizations refine and practice their plan to be able to respond swiftly and efficiently.

Incident response and investigations, including immediate access to forensic experts: our advice includes reporting obligations to the relevant supervisory data authorities and other relevant regulators, both civil and criminal. We regularly assist with strategic advice to contain and remediate adverse impacts on businesses, and protecting impact on a brand. We have pre-existing and trusted global relationships with forensic experts to assist with the response to any incident, ensuring swift and seamless instruction on a legally privileged basis, allowing immediate focus on mitigating the root causes of the incident. With over 180 privacy lawyers operating globally we regularly assist large organizations on multi-national compliance and regulatory obligations, ensuring continuity in response.

Post-incident remediation: we help clients to mitigate the impact of any claims or other liabilities resulting from the incident and to learn from the incident through post incident reviews and gap analyses. Our team includes employment, investigation and seasoned litigation lawyers that advise on a wide spectrum of issues relevant to data incidents, including third party claims and potential class actions; direct and officer liability; product / supplier liability; and, where relevant, employee disciplinary action.

Our insights

Rapid Response - From the moment a company learns about a potential breach of cyber security they should be armed with tools to respond quickly and effectively, while ensuring any action that is taken remains protected by legal privilege. Our 'Rapid Response' global crisis management hotline service provides 24-hour, 365-day access to regulatory legal advice and crisis assistance.

"In a Flash!" - A Lesson in Cyber Security - A dramatic film produced by DLA Piper, depicting a fictional corporation dealing with a number of real-world legal and regulatory issues, among them: cyber governance; cyber-risk management; security protocols; incident response plans; the corresponding legal and regulatory environment faced by board members, general counsel and senior business executives; and the delicate balance of managing internal investigations, reporting requirements and stakeholder interests.

Data Privacy Scorebox - Our online "scorebox" is designed to assist with assessing and benchmarking the data privacy maturity level of an organization. The complimentary tool takes the form of a survey which poses a series of questions relating to 12 areas of data privacy, such as storage of data, use of data, and customer rights. It takes no longer than half an hour to complete, with a range of multiple choice answers to select from. Once completed, a report is emailed which includes a visual summary of how the organization scored in relation to key global data protection principles, a practical action point check list, as well as peer benchmarking data.

CAPABILITES

Our cybersecurity team offers:

- **Proactive risk management.** Before a cybersecurity incident occurs, we work with our clients to assess their internal risk management strategy for responding to cyberattacks and assist in the implementation of proactive policies and procedures that enable them to respond effectively, preserving attorney-client privilege and mitigating potential litigation and reputational risks associated with cybersecurity incidents.

- **Field-tested global crisis management coverage.** We can be on the ground, with an integrated team of the world's top cybersecurity technicians and lawyers, helping solve your security problem and cloaking those efforts in privilege, anywhere in the world, within 24 hours of our first notification. We have established round-the-clock protocols for immediate coordination and response.
- **Connections to more than 40 foreign governments.** We know the regulators, the advocates and many of the journalists who focus on data breaches and draw on this experience to guide our clients' response to a breach incident so as to minimize potential reputational damage.
- **Understanding the US and international cyber-regulatory environment.** We have drafted most of the breach notice laws, offer an online tool summarizing breach notice requirements in 72 countries, and have an unsurpassed understanding of the ever-changing US and international cyber-regulatory environment that we apply to both reactive and preemptive solutions. We also offer products that track these developments.
- **Sector-specific focus.** DLA Piper believes that our legal advice should be as pragmatic and solution-oriented as it is technically excellent. We are attuned to the unique requirements of different sectors and staff our teams with lawyers experienced in the client's sector.

EXPERIENCE

- Assisted with drafting the National Association of Corporate Directors (NACD) Cybersecurity Handbook for corporate directors that has been endorsed by the Department of Homeland Security and posted on the Department's website
- Advising the board of directors of a major financial services institution on cybersecurity governance and information security practices to be implemented with respect to key third-party service providers
- Representing a leading global hotel chain in cybersecurity risk assessment and audit of its global operations
- Representing a telecommunications company in cybersecurity legislative and policy issues including monitoring, analysing and conducting strategic outreach on federal cybersecurity legislation and cybersecurity Executive Order implementation by various federal agencies
- Represented a media company's business unit in connection with an FTC security investigation of alleged security issues with one of its mobile apps
- Representing a large nonprofit organization whose members' information was compromised as part of a large national tax-fraud scheme. We are leading its internal and forensic investigation to determine the source and scope of the breach and are providing advice and counsel in connection with legal and contractual obligations to notify individuals and clients that were affected by the breach

INSIGHTS

Publications

Supreme Court dives into circuit split over the Computer Fraud and Abuse Act

28 January 2021
What does it mean to "exceed authorized access" to an Internet-connected device?

Unauthorized financial transaction fraud: Mitigating liability risks

28 January 2021
Prudent financial institutions are seeking to protect themselves against liability for third-party fraud and accountholder carelessness.

When a threat actor strikes: Legal considerations and challenges in a ransomware attack

21 December 2020
Evidence suggests that having employees working remotely significantly increases the risk of a successful ransomware attack.

Cyberfrauds and Cyberattacks: Remote Working Posing Increased Risks and How to Stay Protected

14 December 2020
Cybercriminals are becoming more sophisticated in the ways they facilitate cyberfrauds, with the increasing use of personalised messages on instant messaging platforms such as WeChat or WhatsApp and socially engineered phishing emails to deceive recipients to transfer funds, disclose sensitive information or click on malicious links.

Navigating China Episode 14: New draft national, harmonised data protection law for Mainland China

23 October 2020
NAVIGATING CHINA: THE DIGITAL JOURNEY
A first national level personal information protection law for Mainland China has been published, reinforcing and heightening existing data protection compliance obligations for organisations doing business in China.

China signs off on PRC Biosecurity Law: What this means for industry players in China

21 October 2020
The Biosecurity Law establishes a comprehensive framework replacing the current somewhat piecemeal legislation.

Singapore: Imminent Changes to the Personal Data Protection Act 2012 (PDPA)

16 October 2020
On 5 October 2020, the Singapore Personal Data Protection (Amendment) Bill (Bill) was tabled in Parliament for the first reading. It is expected that the Bill will be passed before the end of the year if not sooner.

Philadelphia grows privacy capabilities with a new arrival

30 September 2020
Ronald Plesco, an internationally known information security and privacy lawyer, has joined our Philadelphia office.

***Schrems II:* Now what? New FAQs from EU data protection supervisors provide guidance on data transfers**

28 July 2020

Organizations relying on Privacy Shield for transfers to the US of personal data subject to GDPR must immediately implement an alternative mechanism or cease transfers.

Navigating China Episode 13: (More) Important Developments in China's Privacy and Cyber Laws

10 June 2020
NAVIGATING CHINA: THE DIGITAL JOURNEY
China's privacy and cyber authorities have been busy in the last month enacting substantial enhancements and clarifications to data protection compliance obligations; and even more changes are expected before the end of 2020.

New Chinese Civil Code Introduces Greater Protection of Privacy Rights and Personal Information

9 June 2020
China's top legislature, the National People's Congress, recently enacted the PRC Civil Code (the Civil Code), which will come into force on 1 January 2021. This first ever "codified" legislation covers a wide spectrum of rights and issues such as property rights, contracts, matrimonial and family law and tort liability.

Facial recognition technology: Supporting a sustainable lockdown exit strategy?

8 May 2020
Technology has played a dominant role during the lockdown and will be a key aspect of ensuring the transition back to normality is successful. This article discusses recent trends, particularly in Ireland, Denmark and China, regarding the adoption of facial recognition technology (FRT) as a result of the COVID-19 pandemic.

Top of Mind: COVID-19 technology sector insights

28 April 2020
In this time of growing uncertainty, we recognize that many tech businesses are facing significant disruptions and unprecedented challenges arising from the coronavirus disease 2019 (COVID-19) pandemic.

FINRA publishes COVID-19 information notice providing suggested measures to strengthen cybersecurity controls

10 April 2020

FINRA provides numerous suggested measures for strengthening cybersecurity controls regarding increased risks associated with employees working remotely.

Episode 12: More obligations on Chinese mobile app operators to comply with

9 April 2020
NAVIGATING CHINA: THE DIGITAL JOURNEY

Following the crackdown by Chinese authorities against non-compliant mobile apps in late 2019 (please see Episode 8 in this series), the authorities have issued a series of app compliance guidelines (including the Guide to Self-Assess Illegal Collection and Use of Personal Information by Apps, Methods for Identifying Unlawful Acts of Apps to Collect and Use Personal Information, and Draft Specification for Collecting Personal Information in Mobile Applications). These guidelines imposed detailed obligations and practical actions to urge mobile app operators to conduct self-assessments and to rectify any non-compliant data processing practices. Organisations may have noted that some of these guidelines contain conflicting requirements.

Important updates for British Columbia Public Bodies amidst COVID-19 (Canada)

1 APR 2020
In light of the current and developing COVID-19 circumstances, the following alerts have been released for British Columbia Public Bodies, subject to the Freedom of Information Legislation. One order permits public bodies to use and disclose personal information using tools and cloud services outside of Canada in certain circumstances. Another extends the time for freedom of information responses. Last, organizations are asked to remain vigilant for cyber crime.

Coronavirus: Cybersecurity considerations for your newly remote workforce (United States)

31 March 2020

Cyber risk management involves balancing the productivity of a workforce with ensuring confidentiality, integrity and availability of the company's own systems and data, as well as that of their supply chain.

Episode 11: Important clarifications and changes to China's data privacy standards

27 March 2020
NAVIGATING CHINA: THE DIGITAL JOURNEY

Important updates to China's de facto data privacy regulations will come into force on 1 October 2020. The amendments to the Personal Information Security Specification (PIS Specification) comprise important clarifications rather than substantial changes to the existing regulations.

Blockchain and Digital Assets News and Trends

25 March 2020
BLOCKCHAIN AND DIGITAL ASSETS NEWS AND TRENDS

The age of viral outbreaks – key contract considerations in a post-COVID-19 world, plus latest legal, regulatory and case law developments around blockchain and digital transformation.

Coronavirus: Cyber hygiene practices

25 March 2020
While the world is responding to the coronavirus disease 2019 (COVID-19), and individuals are increasingly focused on personal hygiene and social distancing, augmenting cyber hygiene efforts at home and at work are increasing in importance too.

Episode 10: Stricter data localisation and security rules for financial and insurance data in China

06 Mar 2020
NAVIGATING CHINA: THE DIGITAL JOURNEY

The People's Bank of China has released new guidelines on the collection and processing of personal financial information (PFI Guidelines), which provide much-needed clarity on how personal financial information in China should be processed, secured, and transferred. While the PFI Guidelines do not impose an outright ban on personal financial information leaving China, mandatory compliance steps (including consent and impact assessments) must be taken.

Opportunities arising from Asia's data protection frameworks (AsiaPac)

14 February 2020
The media controversy surrounding China's coronavirus COVID-19 detection app, the "close contact detector," has highlighted a common misapprehension about how data protection law is universally applied around the world.

EU MDCG issues new guidance on Cybersecurity for medical devices

27 January 2020
On 7 January 2020, the EU Medical Device Coordination Group published new guidance to help manufacturers fulfil all relevant cybersecurity requirements in Annex I to the new Medical Device Regulations (Regulations 2017/745 on medical devices and 2017/746 on in vitro diagnostic medical devices).

DLA Piper GDPR Data Breach Survey 2020

20 January 2020

According to DLA Piper's latest GDPR Data Breach Survey, data protection regulators have imposed EUR114 million (approximately USD126 million / GBP97 million) in fines under the GDPR regime for a wide range of GDPR infringements, not just for data breaches.

France, Germany and Austria top the rankings for the total value of GDPR fines imposed with just over EUR51 million, EUR24.5 million and EUR18 million respectively. The Netherlands, Germany and the UK topped the table for the number of data breaches notified to regulators with 40,647, 37,636 and 22,181 notifications each.

Episode 9: 2020 - Privacy, Security and Content Regulation to Increase in China

10 January 2020
NAVIGATING CHINA: THE DIGITAL JOURNEY

China's authorities have published a much-anticipated brand new directive on internet content regulation and governance, which will come into force on 1 March 2020. This law will require organizations which host websites in China to make fundamental changes to their website governance frameworks.

Congressional hearing to focus on facial recognition and national security

12 December 2019
AI OUTLOOK

Technologies controlled by foreign governments and their implications for privacy and national security are expected to be a major topic.

Corporations need to remain vigilant amidst the rise of cyberattacks and cyberfrauds

2 December 2019
Recent figures show that Hong Kong and China remain the top destinations of fraudulent funds, most of which are the result of cyberfrauds. Read our article which gives helpful tips on how to avoid falling victim to these attacks.

Episode 7: New China encryption law passed

6 November 2019
NAVIGATING CHINA: THE DIGITAL JOURNEY

The new PRC Encryption Law will come into force on 1 January 2020. It will bring fundamental changes to the sale, import and use of encryption technologies in China by foreign and domestic organizations.

Episode 6: Further developments in PRC data privacy regulations

1 November 2019
NAVIGATING CHINA: THE DIGITAL JOURNEY

An updated draft of China's Amended Personal Information Security Specification (Amended PIS Specification) and proposed new amendments to the privacy specification for mobile apps (App Privacy Specification) were published this week, alongside brand new draft regulations for the banking sector.

The government in your cloud

24 July 2019

As companies shift more data to the cloud, the US government's ability to access that content should not be overlooked.

Episode 3: Yet more regulators join the party in enforcing cybersecurity

4 June 2019
NAVIGATING CHINA: THE DIGITAL JOURNEY

Licensed telcos and internet businesses in China face a new wave of investigations by the Ministry of Industry and Information Technology (MIIT) as they announce a new enforcement campaign aimed at ensuring network security compliance.

Episode 2: New stringent cyber security rules announced in China, what will your business need to do?

29 May 2019
NAVIGATING CHINA: THE DIGITAL JOURNEY

Organisations with operations in China must prepare now for new comprehensive cybersecurity rules. The Chinese authorities have announced MLPS "version 2.0", which will come into force on 1 December 2019, and have potential significant impact to businesses' infrastructure and operations in China.

CCPA vs. GDPR: the same, only different

11 APR 2019
Businesses that have undertaken GDPR compliance will have an advantage in addressing CCPA, but those efforts alone won't suffice.

EU: new obligations for digital services providers and operators of essential services

28 JUN 2016
In line with the EU's broader Cyber Security Strategy, the NIS Directive is a significant step towards a more secure cross-border cyberspace with a high shared level of network and information system security.

Plan now to use off-band communications during an incident response: key points

27 OCT 2015
A robust IR plan should include communications techniques that operate outside regular company communication methods.

***The Cybersecurity Framework:* Administration, Congress move to incentivize private-sector cooperation, strengthen federal acquisition process**

12 SEP 2013

Cybersecurity and US federal public procurements: what contractors need to know

11 MAR 2013
Practical considerations for US federal contractors

EU releases cybersecurity strategy

15 FEB 2013

Events

Previous

Mitigating cross-border cyber risk in the age of LGPD

19 November 2020 | 9:00 - 10:00 EST
Webinar

Cybersecurity for a 2020 workforce

28 May 2020 | 1:30 - 2:30 ET
Webinar

COVID-19: Important Issues for Israeli Companies to Consider

6 April 2020
Webinar

NEWS

DLA Piper's Luxembourg team enters World Trademark Review ranking

25 February 2021
Our Luxembourg office is pleased to announce that we have been ranked as a recommended law firm in the World Trademark Review.

Ana Teresa Barreto joins DLA Piper as head of Industrial and Intellectual Property practice in Peru

30 September 2020
DLA Piper announced today that Ana Teresa Barreto has joined the firm as of counsel and head of the Industrial and Intellectual Property practice in Peru.

DLA Piper announces partnership promotions for 2020

30 April 2020

DLA Piper is proud to announce that 67 lawyers have been promoted to its partnership. The promotions are effective as of April 1, 2020 in the United States and May 1, 2020 for EMEA and Asia Pacific. The promotions have been made across many of the firm's practice areas in 35 different offices throughout 13 countries.

Across the firm's practices globally, Corporate saw the largest intake of new partners with 19 promotions, followed by Litigation and Regulatory with 15. Intellectual Property and Technology and Finance and Projects had ten and eight promotions respectively, while there were six in Real Estate. Tax and Employment both had four, and there was one in Restructuring.

DLA Piper lawyers named Acritas Stars

10 March 2020

Acritas has named over 200 DLA Piper lawyers as 2020 Acritas Stars. Now in its fourth year, Acritas Stars highlights the stand-out lawyers in private practice as nominated by clients around the world. More than 3,000 senior in-house counsel feed into the nomination process to give a comprehensive view of highly recommended lawyers across the globe.

DLA Piper to advise ITW Global Leaders' Forum on blockchain-based telecoms platform

2 July 2019
DLA Piper has been appointed to advise the ITW (International Telecoms Week) Global Leaders' Forum (GLF) on the launch of a special purpose vehicle that will develop a live, blockchain-based platform.

DLA Piper announces launch of Artificial Intelligence practice

14 MAY 2019

DLA Piper announced today the launch of its Artificial Intelligence practice, which will focus on assisting companies as they navigate the legal landscape of emerging and disruptive technologies, while helping them understand the legal and compliance risks arising from the creation and deployment of AI systems.

DLA Piper announces partnership promotions for 2019

1 APR 2019

DLA Piper is proud to announce that 77 lawyers have been promoted to its partnership. The promotions are effective as of April 1, 2019 in the United States and May 1, 2019 for EMEA and Asia Pacific. The promotions were made across many of the firm's practice areas in 43 different offices throughout 20 countries.

DLA Piper hosts leading business and diplomacy conference

14 MAR 2019
DLA Piper's London office has hosted the Annual Conference of the International Diplomatic and Business Exchange (IBDE).