Cybersecurity

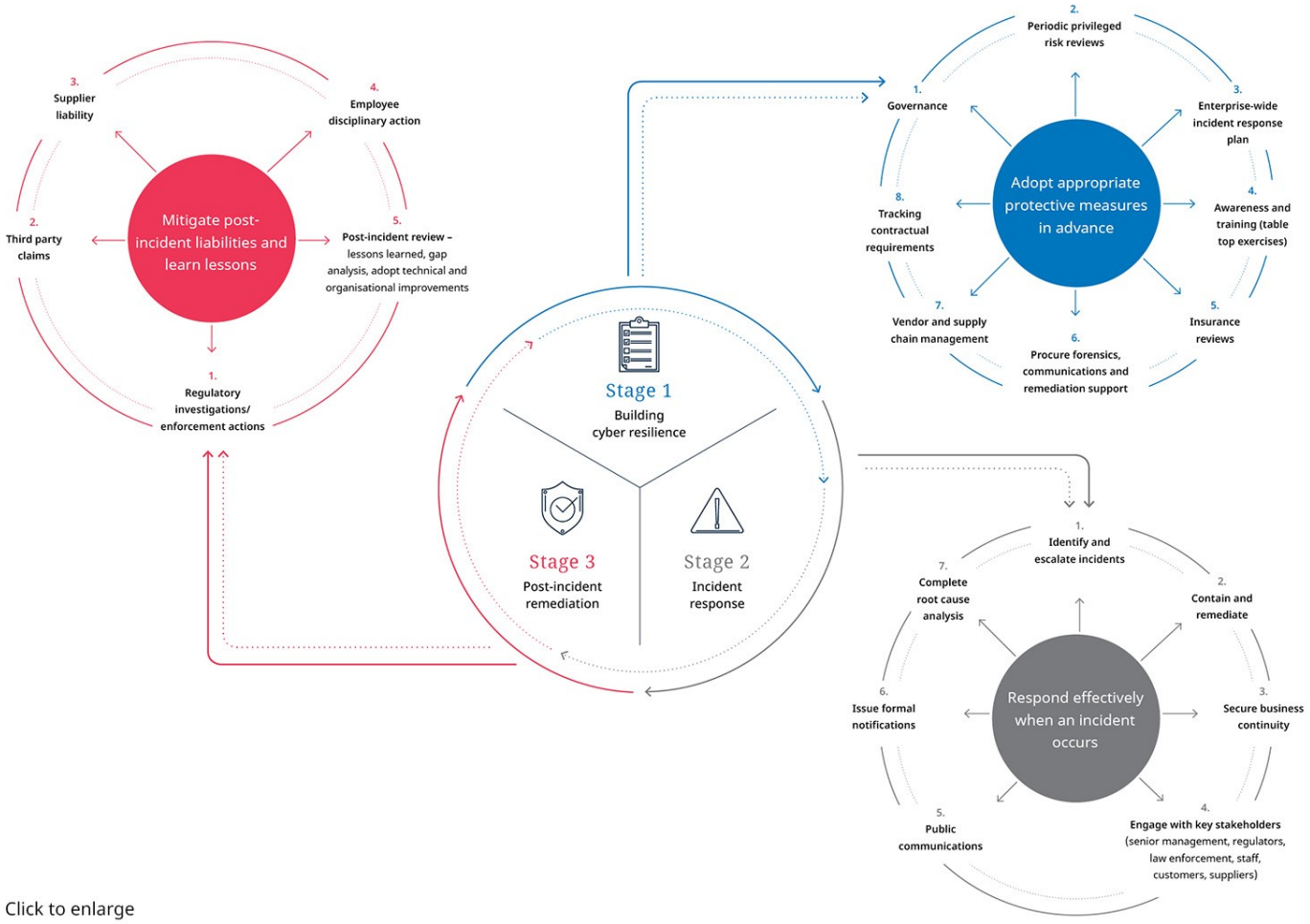
In today's interconnected world, virtually all companies, their suppliers and their customers are potential targets for cyber attacks. The risks associated with such incidents require a robust cybersecurity program in order to manage this fast-changing risk and remain in compliance.

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.

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

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

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



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

Capabilities

Our cybersecurity team offers:

- **Truly global crisis management coverage.** Our team has handled many of the cyber incidents you have read about, and we bring that experience to bear when we handle a cyber incident. Whether an incident involves one or multiple countries, our team members use a common incident response protocol that is adapted to the regulatory and privilege requirements and culture of their countries without creating risk in other parts of the world. We work as a cohesive team bringing a coordinated response to investigations and incidents, regularly working together on a worldwide basis.
- **Proactive risk management.** We draw on deep operational and legal experience to routinely help clients develop, implement and refine proactive strategies for preventing and responding to cyber incidents, while mitigating related enforcement and reputational risks. This includes conducting tabletop exercises as well as creating policies and procedures for companies in all industries. We also utilize common security assessment methodologies that help benchmark security practices.
- **Enforcement and Litigation.** Our team has deep experience in representing clients before government regulators and Data Protection Authorities globally. Our cyber litigators represent clients in the full range of civil disputes – including data breach class action, intellectual property theft, financial fraud, commercial and employment disputes, D&O and securities actions, product liability, and personal injury resulting from cyberattacks.We also represent clients in their role as cybercrime victim in criminal investigations and prosecutions.
- **Thought Leadership.** Members of our team have written many of the definitive privacy and security books, including, *Information Security and Privacy: A Guide to Federal and State Law* and *Compliance and Information Security and Privacy: A Guide to International Law and Compliance* (West 2006-2020), collectively a 6,000-page, three-volume treatise that examines all aspects of privacy and security laws, published by Thomson-West. Our lawyers were instrumental in drafting the widely acclaimed *National Association of Corporate Directors (NACD) Cyber Risk Handbook*, a highly influential roadmap for cybersecurity governance, which has been widely praised by corporate governance experts and the Department of Homeland Security. Our lawyers are currently working on the 3rd edition of the US handbook, helped to draft the UK and German versions of the Handbook, and is currently working on an EU-wide version. We draw on this experience in advising clients on structuring cyber-risk governance and incident response to develop a strong enterprise-wide response.
- **Sector-specific focus.** We believe that our legal advice should be as pragmatic and practical as it is technically excellent. We are attuned to the unique requirements of different sectors and build customized teams that understand a client's business, as well as its cybersecurity needs.
- **Consulting Services.** Our Cybersecurity practice enhances its legal skills with the addition of highly experienced risk and technology consultants in order to support clients as a single Data Protection, Privacy and Security team. This joint legal and consulting approach to data risk, privacy, cyber and security projects is a significant point of differentiation from other large firms that has been recognized by notable rankings entities, including BTI Consulting Group, which recently placed the DLA Piper Cybersecurity practice among the BTI CyberSavvy 16 Law Firms in recognition of standing above all others for cybersecurity prowess. Our team of experienced Consultants are on the front lines of assessing, developing and implementing innovative data risk, privacy and security solutions for some of the world's largest and most geographically diverse companies.
- **Supply Chain Risk Management.** We are well versed in advising companies on how to assess, address, and bolster the cybersecurity practices and posture of its supply chain. Our proactive risk mitigation service involves providing practical, targeted and enforceable strategies throughout a company's supply chain, including: assessments of the risk exposure of cyber incidents in the supply chain; implementing supplier due diligence; and contracting and vendor management strategies to mitigate cybersecurity risks and manage liability, while maintaining compliance with applicable laws and obligations. The DLA Piper team includes former general counsels and chief compliance officers, insurance regulators, and commercial and government contracts attorneys who understand both the regulatory and business requirements of supply chain cybersecurity management.

EXPERIENCE

Experience

- Advising a listed software development company at the outset of a cyberattack and data breach which were reported to be among the worst cyber-espionage incidents ever suffered in the US. We were primarily responsible for responding to the cyberattack, to oversee the forensic investigation, and to respond to resulting litigation.
- Advising a leading retailer as standing counsel for breach response which involved working with several internal investigations into different incidents each involving PCI auditors. As is often the case, we took a coordination role advising on confidentiality rings and privilege in addition to providing advice on notification requirements, the forensic investigation and claims against the supply chain. We also worked closely with the communications team to draft re-active communications and Q&A for contact centers. Insurers were notified.
- Advising the largest financial institution in the US on its cybersecurity program including a risk governance presentation to Board of Directors; participating in a table top exercise with company legal, IT and communications departments; ongoing advice on cybersecurity risk management with regard to security standards, supply chain risk management, incident response program, and governance structures.
- Advising a leading sports car manufacturer on the implementation of its connected car service in multiple APAC jurisdictions and creating and implementing a bespoke data protection and cybersecurity compliance program throughout Greater China.
- Advising as standing counsel for a tier one global bank for cyber security and incident response. As part of this mandate we have advised on specific considerations for ransomware attacks with a particular emphasis on Europe and the US.
- Designing and overseeing a simulated breach response exercise focused on vendor management relationships for a global insurance provider in the commercial space. We worked closely with a small group of company personnel to design an exercise to test the effectiveness of the company's incident response plan and guided them through the program, identifying potential gaps in the program, and, after the program, recommended modifications to the incident response plan.
- Advising Barings on a range of data privacy compliance matters covering their global business, including the implementation of their data privacy framework across APAC and security issues associated with operations in mainland China.
- Advising a global financial services organization on cyber security and incident response, including the deployment of the DLA Piper "Notify" tool and support with incident triage and classification.
- Advising a European life sciences company with a presence in over 40 countries globally in response to a cyberattack deemed a matter of national security by the National Crime Agency (NCA) and the National Cyber Security Centre (NCSC). We advised the client and their cyber insurers on GDPR notifications; US data protection notifications (including notifications pursuant to HIPAA); non-EU/non-US data protection notifications; liaison with international criminal authorities in the US, UK, Germany and Belgium; OFAC regulations in the US and TracFin regulations in France; contractual obligations with customers; engagement of external IT service providers; press releases and engagement with key customers; and insurance.
- Advising a major cyber insurer in responding to a series of ransomware and data ransom attacks over three months across Asia and Latin America by the sophisticated Maze cyber extortionist group. We served as client GC and global cybersecurity lead counsel's right hand to devise and execute on a legally privileged response that included forensic investigation and IT remediation; attacker negotiations; international law enforcement interactions; internal and external global media communications; and business partner, data subject, and regulator notification strategy across the affected regions.
- Advising a global, publicly-traded company in a multi-pronged cyberattack that compromised more than 300 Office 365 accounts in 10 different countries, leading to various phishing campaigns, business email compromises, and payment re-direction schemes around the globe. We led the crisis management and incident response teams, which included management of a legally privileged forensic investigation and IT remediation; internal and external global media communications; and business partner, data subject, and regulator notification strategy across the European Union and Americas.
- Advising a UK based company in the immediate aftermath of a cyber attack which potentially compromised thousands of customers' personal data. We advised the client on the steps to take in order to identify the breach; we advised on the content of the requisite regulatory notifications to be made; we drafted customer communications including the initial notifications as well as Questions & Answers and update communications. In addition we held daily calls with the client for the first three weeks in order to ensure that the breach was dealt with efficiently and effectively.
- Advising a long-standing client in relation to a cyber-incident which may have resulted in loss of sensitive customer data. When the Financial Conduct Authority (FCA) raised queries in relation to the cyber-incident, the client brought in our team to handle the FCA investigation. We assisted the client with responding to multiple FCA information requests and advised on its obligations to notify the FCA (and the extent to which those obligations differed to those under the GDPR) and the FCAs expectations in terms of IT security and cyber-risk mitigation and preparing briefing notes to the Board.
- Engaged to review a financial services company's 2017 data breach and to advise the client on its participation in very high-profile Congressional hearings regarding the breach, including preparing both the former CEO and interim CEO for five separate appearances testifying at congressional hearings and on responses to committees' requests for information.
- Representing a London property insurance market in respect of prospective claims and their liability in connection with a fraudulent cyber phishing hack which resulted in the loss in transit of an electronic claim payment and the need for the insurers to make a replacement payment to their insured client. We provided multi-jurisdictional cross-border advice on merits, strategy and have represented the insurers in mediation and negotiations. There is prospective commercial court litigation in London as well as formal proceedings in the United States.
- Representing various Sony entities in multidistrict litigation arising from one of the world's largest recorded data security breaches. The breach affected more than 77 million users, after which more than 65 class action lawsuits were filed nationwide. Plaintiffs' claims range from violations of consumer protection and data breach notification statutes to common law claims, such as negligence, misrepresentation, breach of contract, breach of warranty, and unjust enrichment.

INSIGHTS

Publications

Commerce Department lays out US path to global leadership on digital assets

4 October 2022
Citing regulatory and technological leadership as the "two key pillars of U.S. competitiveness," the framework proposes four main areas for government action on digital assets.

Spies among us: State-sponsored actors want to steal your sensitive information

21 September 2022
INTELLECTUAL PROPERTY AND TECHNOLOGY NEWS

The joint statement is an implicit admission by both governments that they can no longer protect private businesses from state-sponsored intellectual property theft.

Biden Executive Order directs a broader national security focus on foreign investments

20 September 2022
This marks the first time since CFIUS was established in 1975 that a president has publicly issued such direction.

Federal agency reports on responsible development of digital assets are due this week

6 September 2022
An array of agency reports are due.

---

eSignature and ePayment News and Trends

6 September 2022
ESIGNATURE AND EPAYMENT NEWS AND TRENDS

Federal agencies' reports on responsible development of digital assets are due to the President this week.

Detoxifying the anonymous internet one troll at a time: Norwich orders

18 August 2022

When people create profiles and interact with one another online, doing so anonymously under an assumed username remains the most common approach. While some major platforms have moved away from this model and have begun requiring users to register with their actual names, the vast majority of platforms continue to operate with anonymity as a key feature. When users layer anonymous accounts upon anonymous accounts it can be nigh impossible for parties who have been wronged online to identify the wrongdoers and hold them to account without the cooperation of platforms and ISPs who are able to connect anonymous usernames with identifying information such as names, email addresses, and IP addresses.

FTC explores sweeping new rules on data privacy and protection

12 August 2022
The FTC is soliciting comment on a wide range of concerns.

Cybercrimes law client update

10 August 2022
Businesses in Hong Kong may soon need to account for cybercrimes laws when establishing their ICT security frameworks.

Cybersecurity litigation for contractors is on the rise – takeaways from recent cases

18 July 2022
Prudent contractors will understand the cybersecurity obligations in their solicitations and contracts and have a plan for demonstrating compliance.

Mehdi Kettani authors Morocco chapter of Data Protection & Cyber Security Comparative Guide

13 July 2022
We are delighted to have recently authored the Morocco chapter of The Legal 500: Data Protection & Cyber Security Comparative Guide.

The rise of global telehealth

30 June 2022
AT THE INTERSECTION OF SCIENCE AND LAW PODCAST SERIES

Partners Kristi Kung and Greg Bodulovic discuss the rise of telehealth amid the COVID-19 pandemic, as well as advancements in technology aiming to address disparate access to healthcare globally.

Data privacy bill in Congress would create federal enforcement over algorithms

29 June 2022
AI OUTLOOK

Policymakers are paying ever more attention to algorithms and the growing role they play in our lives.

Exploring the metaverse: What laws will apply?

22 June 2022
INTELLECTUAL PROPERTY AND TECHNOLOGY NEWS

For those intrigued by the metaverse, and for creators building metaverse projects, here are practical considerations.

DC AG claims Meta CEO Zuckerberg personally accountable for Cambridge Analytica privacy scandal

24 May 2022
The suit is the latest effort by state Attorneys General to take a tougher line against tech companies over misleading privacy practices.

Texas social media law reinstated by Fifth Circuit

20 May 2022
The plaintiffs have appealed directly to the Supreme Court for an emergency stay.

Calling on the code: Civil consequences for cryptocurrency

19 May 2022

Would-be blockchain bandits that still believe cryptocurrency is beyond the reach of the law should think again. In *Cicada 137 LLC v Medjedovic*, the Ontario Superior Court of Justice had no qualms with taking a practical approach to providing relief in respect of digital assets.

Important High Court judgment impacting the viability of data breach and misuse of private information claims - Underwood v Bounty

17 May 2022
On 13 April 2022, the High Court handed down judgment in Underwood & Another v Bounty UK Ltd & Another [2022] EWHC 888 (QB), dismissing claims for misuse of private information ("MPI") and breach of the Data Protection Act 1998("DPA").

Connecticut poised to be fifth state with comprehensive privacy law

2 May 2022
Modeled after the Colorado Privacy Act and the Virginia Consumer Data Protection Act, CT SB6 uses many of the same definitions and provisions in an effort to be interoperable with these laws.

The Crossroads of Biometrics and Privacy – Why It Matters

6 April 2022
CYBER SPOTLIGHT PODCAST SERIES

Kate Lucente and Jennifer Kashatus discuss biometrics trends.

US escalates sanctions targeting Russian evasion networks, tech companies and cyber actors; signals more sanctions are on the way

5 April 2022
GLOBAL SANCTIONS ALERT

These new measures supplement the extensive measures previously announced by the US government.

Biden Administration urges American companies to act quickly to improve cybersecurity safeguards

22 March 2022
GLOBAL SANCTIONS ALERT

The White House stresses the importance of taking key steps to thwart nation-state bad actor activities.

CafePress to pay $500,000 for FTC violations

22 March 2022

The FTC's action highlights government expectations that companies maintain robust cybersecurity programs and provide appropriate disclosures and reports regarding security breaches.

SEC proposes sweeping new public company cybersecurity disclosure and governance rules

16 March 2022
This rule proposal follows on the heels of several SEC enforcement actions against public companies related to cybersecurity disclosures.

US Senate unanimously passes the Strengthening American Cybersecurity Act

14 March 2022
Prior versions of this and related legislation failed to win passage in recent years.

Heightened cyber threats in times of crisis - be prepared

3 March 2022
The governments of both Canada and the United States have warned of increased cyberattack risk in light of tension in Eastern Europe and the spike in ransomware and other cyberattacks as a result of an increasing reliance on the internet for work-from-home and online commerce.

SEC addresses cybersecurity risk in proposed rules for the investment management industry

17 February 2022
The proposed rules focus on four key areas: risk management through policies and procedures, incident reporting to the SEC, investor disclosure, and recordkeeping.

US Department of Justice, aided by cryptocurrency exchanges, seizes over US$3.6 billion in stolen Bitcoin

15 February 2022
This landmark seizure highlights law enforcement's growing ability to recover digital assets obtained in cybercrimes, and the importance of the private sector's role in helping to thwart unlawful activities involving cryptocurrencies.

SEC chair signals continuing focus on cybersecurity governance

1 February 2022
Two key points.

Governance Risk: The Seven Core Principles

26 January 2022
CYBER SPOTLIGHT PODCAST SERIES

Andrew Serwin outlines seven core principles for companies to consider, particularly in light of the SEC Chairman's recent remarks regarding the importance of cyber hygiene for companies.

Top 12 privacy and cyber steps to take in January

13 January 2022

Twelve action items to consider for 2022 that can help reduce the impact of a cyber event.

2022 – a busy year for privacy legislation has already started

12 January 2022
Biometric privacy, cybersecurity standards and consumer protection are among the subjects of the bills.

Apache Log4Shell: "greatest vulnerability seen in years"

14 December 2021
Log4Shell allows arbitrary remote code execution on unpatched servers – essentially giving unfettered access to threat actors.

With Civil Cyber-Fraud Initiative, government sharpens focus on cybersecurity obligations for government contractors

13 December 2021
Deploying the False Claims Act to pursue cybersecurity-related fraud.

Google files groundbreaking civil suit to disrupt massive botnet with blockchain backup system

10 December 2021

Civil actions to take down botnets have been around for years, but the blockchain aspect adds a new twist.

Johnson v Eastlight: Another important judgment on de minimis threshold in data protection compensation claims – and other key takeaways

17 November 2021

The High Court in Emma Louise Johnson v Eastlight Community Homes Ltd declined to strike-out a claim for damages for distress following an isolated one-off data incident which was quickly remedied.

Lloyd v Google – Supreme Court Judgment – report and impacts on data protection and mass claims in the UK

10 November 2021
UK Supreme Court allowed Google's appeal against the Court of Appeal decision which had previously granted Mr Lloyd permission to serve his representative claim on Google in the United States. The judgment brings to an end to one of the most significant issues to come before the UK Courts concerning class actions and data protection regimes.

With Civil Cyber-Fraud Initiative, government sharpens focus on cybersecurity obligations for government contractors

1 November 2021
Acting Assistant Attorney General Brian Boynton recently discussed how the Civil Cyber-Fraud Initiative would use the False Claims Act to pursue cybersecurity-related fraud.

ICO's provisional green light of Gambling Commission's Single Customer View raises important issues for gambling operators, their officers, and bettors

26 October 2021

The ICO has provisionally given the green light of Gambling Commission's Single Customer View which would allow data gathered by gambling operators regarding individual player behaviours to be aggregated and shared with other operators. This article discusses the risks associated.

Court awards damages for breach of Data Protection Act where CCTV coverage exceeded lawful basis

21 October 2021
A recent court judgement illustrates the risks associated with the installation of security cameras at property and why it is vital to ensure a lawful basis for capturing and processing such images exists.

FTC's Policy Statement on breach notifications in mobile health apps: a new, broad approach that may face legal challenge

27 September 2021
The Policy Statement highlights the FTC's intention to step up enforcement consistent with these broad new interpretations.

Cybersecurity obligations for government contractors – focus on them before the government focuses on you

22 September 2021
Liability under the False Claims Act can be financially debilitating, particularly for small and mid-size contractors.

Protecting your company from supply chain cyber attacks

September 2021
Today, virtually all companies rely on third-party technical solutions to manage their business. The downside is that incorporating new third-party technology into business operations creates new vectors for cyberattacks.

Cybersecurity considerations for executives and boards of directors: How recent cyberattack trends and developments inform strategies for reducing cyber-risk

23 August 2021
We review recent trends and costs associated with cyberattacks and analyze how organizations can implement strategies for reducing cyber-risk.

***Lloyd v Google LLC* - data protection class action claims**

12 July 2021
The judgement in *Lloyd v Google LLC* will become the leading authority on damages for breaches of data protection law of any size and scope, and on the ability for representative actions to proceed in England and Wales. This article outlines the key issues heard so far.

Mexico: IFT issues guidelines on net neutrality

7 July 2021
These Guidelines implement the "Net Neutrality" chapter included in the Federal Law of Telecommunications and Broadcasting.

Ransomware preparedness: NYDFS announces additional expectations of regulated entities' cybersecurity programs

7 July 2021
As regulatees address their vulnerabilities to ransomware, NYDFS raises its expectations.

Fending off phishing attacks: Some simple steps using trademark law

June 2021
We often think about how to respond once a breach has occurred, but rarely do we consider how to prevent a breach or scam entirely.

What the Biden Cybersecurity Executive Order means for technology vendors and service providers in the federal ecosystem

June 2021
Steps technology vendors should consider as they prepare.

European Commission's standard contractual clauses: extensive new requirements coming for US businesses receiving EU personal data subject to GDPR

8 June 2021
Adopting and complying with the New SCCs may require considerable effort for importers, particularly those that are not otherwise directly subject to GDPR.

Episode 18: Increased scrutiny over connected car and automobile industry data from Chinese regulators, including push towards data localisation

4 June 2021
NAVIGATING CHINA: THE DIGITAL JOURNEY

The Chinese cybersecurity authorities have published new draft rules clarifying data and cyber compliance obligations for the automobile industry, including a push towards most personal information and important data being kept in China.

Supreme Court significantly limits the scope of the Computer Fraud and Abuse Act

4 June 2021
The decision will largely gut the CFAA as a tool for addressing insider data theft.

What does the cybersecurity executive order mean for federal government contractors and their supply chains?

19 May 2021
Key sections of the EO that are likely to impact federal contractors and the practical effects of those requirements.

President Biden issues broad-ranging Executive Order on cybersecurity

13 May 2021
The EO sets forth new requirements for federal agencies and government service providers.

The UKJT Digital Dispute Resolution Rules – Keeping Pace with Change

10 May 2021
The new Digital Dispute Resolution Rules are designed to enable rapid, innovative and cost-effective resolution of legal disputes concerning novel digital technology, such as cryptoassets, cryptocurrency, smart contracts, distributed ledger technology, and fintech applications.

Navigating China Episode 17: China's Draft Privacy and Security Laws

4 May 2021
NAVIGATING CHINA: THE DIGITAL JOURNEY

The Draft Personal Information Protection Law (Draft PIPL) will – once passed – become the first comprehensive personal data protection law in China.

Second Circuit sets standing threshold for data-breach class actions

30 April 2021
The court ruled there are limits to the "increased-risk" theory of standing.

Georgia's HB 156, requiring state notice for utility cybersecurity incidents, is now in effect

21 April 2021
The law creates specific notice requirements for state agencies and utilities that experience cybersecurity attacks and requires swift notice to the state director of emergency management in Georgia.

Latest regulatory changes reduce burden for software and technology companies under US export controls

6 April 2021
Revisions to the US Export Administration Regulations implement changes to Export Controls for Conventional Arms and Dual-Use Goods and Technologies.

Episode 15: Comprehensive New E-Commerce Rules Introduced

23 March 2021
NAVIGATING CHINA: THE DIGITAL JOURNEY

Operators of e-commerce platforms, websites and apps in China, and those using third party e-commerce, social media or livestreaming platforms to sell their products and services in China, must update their operations, services and systems in advance of wide-ranging new rules.

Singapore: More Stringent Requirements under the MAS Technology Risk Management Guidelines

22 February 2021
Regulated financial and insurances businesses in Singapore (FIs) must take additional compliance steps when managing their IT infrastructure and vendors, under the updated Technology Risk Management Guidelines recently introduced by the Monetary Authority of Singapore (MAS).

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.

Landmark artificial intelligence legislation advances toward becoming law

16 December 2020
AI OUTLOOK

An overview of the key AI initiatives and funding set out in the defense bill.

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.

FDA seeks feedback on industry best practices for medical device cybersecurity communications

9 December 2020
The agency emphasizes the evolving responsibility of medical device manufacturers to promptly, clearly communicate cybersecurity issues to patients and healthcare providers.

Navigating Asia-Pacific data breach notification requirements

2 December 2020

Data breach notification obligations throughout Asia-Pacific are in a state of flux, with several jurisdictions either introducing new requirements or updating their existing regimes in late 2020 and 2021. Our interactive map contains the current state of data breach notification requirements in key jurisdictions throughout the Asia-Pacific region.

Japan's Telecommunications Business Act to be Amended: What to Know

23 October 2020
Significant changes will be made to Japan's Telecommunications Business Act, which means that Foreign Operators offering telecommunications services in Japan will now be treated identically to Domestic Operators under Japan's telecommunications laws. This will remove uncertainties but increase compliance obligations.

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.

New OFAC guidance for ransomware payments

16 October 2020
On October 1, 2020, the OFAC issued an advisory to companies providing services to victims of ransomware attacks, informing them of the potential "sanctions risks" for facilitating ransomware payments.

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.

Unpacking the DOJ's cryptocurrency guidance: Enforcement priorities and industry implications

15 October 2020
A warning to offshore cryptocurrency exchanges and other money services businesses operating outside of the reach of US authorities.

Women in IP Law: panel examines divided infringement, cyber-risk

20 DEC 2016

High points from a CLE panel discussion about cutting-edge issues in the IPT space.

Is your cybersecurity upgrade FDA reportable?

28 SEP 2016

Draft guidance lends insight into the way the FDA may apply existing postmarket regulatory requirements to evolving cybersecurity-related technological issues.

Cybersecurity: past is prologue

29 MAR 2016

During 2016, we will likely see another increase in cyberattacks, and we will see cybersecurity being taken more seriously by its potential victims.

NYDFS announces final cybersecurity rules for financial services sector: key takeaways

22 FEB 2017

The Final Rule's reach is very broad and presents operational challenges. It may prompt other states to enact their own rules.

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.

The blockchain revolution, smart contracts and financial transactions

26 APR 2016
Blockchain-based smart contracts have enormous potential to streamline financial transactions and reduce counterparty risks.

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

Data Protection & Cyber - Hot Topics

29 September 2022
Edinburgh

Navigating China's new cross-border data transfer rules and responding to cyber and data incidents

14 September 2022
Webinar

Data Protection and Cyber Security – what you need to know

5 July 2022
Manchester

Cyber Law Roundtable Series

28 January 2022
Webinar

Data protection compensation claims – Review of 2021 and looking ahead to 2022

26 January 2022
Webinar

New cybersecurity requirements for Department of Defense (DoD) contractors

13 December 2021 | 2:00 pm - 3:00 pm EST
Webinar

Security Event: "Can I Pay the Ransom?"

23 June 2021 | 12:30 – 1:30 EDT
Webinar

Mitigating cross-border cyber risk in the age of LGPD

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

Planning for an Uncertain World

16 November 2020

TechLaw Event Series
Webinar

A practical guide to privilege in cyber investigations

15 October 2020
Webinar

NEWS

DLA Piper advises Critical Start in US$215 Million Strategic Investment

13 April 2022

DLA Piper advised Critical Start, a leading provider of Managed Detection and Response (MDR) cybersecurity solutions, in its over $215 million strategic growth investment from Vista Equity Partners, a leading global investment firm focused exclusively on enterprise software, data and technology-enabled businesses.

DLA Piper announces collaboration with The Providence Group

1 March 2022
DLA Piper is pleased to announce a collaboration with The Providence Group to deliver trusted cyber, privacy and data use risk governance insights through wargames, table-top exercises, and other scenario-based services to clients to prepare them to mitigate business and mission interruptions, as well as regulatory and reputational risk.

Andrew Serwin named a 2022 Top Cyber Lawyer by the *Daily Journal*

20 January 2022

DLA Piper is pleased to announce that Andrew Serwin, US chair and global co-chair of the firm's Cybersecurity and Data Protection, Privacy and Security practices, has been named to the *Daily Journal*'s 2022 Top Cyber Lawyers list recognizing top-tier cybersecurity lawyers practicing in California.

DLA Piper recognized as a top litigation firm, named a Powerhouse firm for class action and cybersecurity litigation by BTI Consulting Group

7 October 2021
DLA Piper is pleased to announce that it was recognized as a "most feared" law firm in litigation in BTI Consulting Group's *BTI Litigation Outlook 2022: Post-Pandemic and Beyond* report and was named a "Powerhouse" – the highest rating in the report, representing the top 1 percent of all law firms – for class action and cybersecurity litigation.

Cyber attorney Justine Phillips joins DLA Piper's Regulatory and Government Affairs practice in San Diego

5 October 2021
DLA Piper announced today that cyber attorney Justine Phillips has joined the firm's Regulatory and Government Affairs practice as a partner in San Diego.

DLA Piper announces beta launch of Artificial Intelligence Scorebox tool

5 October 2021
DLA Piper is pleased to announce the beta launch of its Artificial Intelligence Scorebox, a digital tool aimed at helping organizations and businesses assess AI adoption readiness based on a series of questions and criteria.

Antonio Tovo joins Campos Mello Advogados as a partner in the Corporate Criminal Law, Compliance and Cybersecurity practices

10 August 2021
DLA Piper announced today that Antonio Tovo has joined Campos Mello Advogados (CMA) as a partner in the Corporate Criminal Law, Compliance and Cybersecurity practices.

DLA Piper lawyers and practices ranked in latest edition of *The Legal 500*

17 June 2021
DLA Piper announced today that the firm received 42 individual lawyer rankings and 49 firm rankings in *The Legal 500 United States* 2021 guide.

DLA Piper partners and firm COO named to *Law360* 2021 Editorial Advisory Boards

10 May 2021
DLA Piper is pleased to announce that 11 of its lawyers, as well as firm COO Bob Bratt, have been named to *Law360*'s 2021 Editorial Advisory Boards.

DLA Piper boosts technology practice with partner hire in Australia

20 April 2021
DLA Piper announces that Anthony Lloyd joined the firm as partner in its Australian Intellectual Property and Technology practice on 19 April 2021. Anthony, who will be based in DLA Piper's Sydney office, joins with extensive experience advising on major technology, media and communications projects across Asia, the US and Europe.

DLA Piper GDPR fines and data breach survey: January 2021

19 January 2021
According to DLA Piper's latest annual General Data Protection Regulation (GDPR) Fines and Data Breach Survey, Ireland reported 6,615 data breaches in the past twelve months to the Irish Data Protection Commission. Ireland recorded the sixth highest level of breach notifications across Europe and third highest on a per capita basis.

Nederland tweede van Europa in aantal gemelde datalekken sinds invoering AVG

19 January 2021
Ruim 65.000 gemelde datalekken sinds mei 2018 in Nederland, alleen Duitsland had er meer. Totale boetebedrag in Europa afgelopen jaar met 39% gestegen. Het aantal meldingen van datalekken groeide afgelopen jaar met 19%

Nine DLA Piper lawyers recognized by BTI Consulting Group for superior client service

10 December 2020
DLA Piper is pleased to announce that BTI Consulting Group has recognized nine of its lawyers for providing superior service to clients.

DLA Piper appoints Natalia Kirichenko as head of IPT in Ukraine

25 November 2020
DLA Piper today announces the appointment of Natalia Kirichenko as Head of the Intellectual Property and Technology practice in its Kyiv office, starting with immediate effect. The appointment follows the departure of Natalia Pakhomovska, who led the team and has decided to leave the firm to explore new opportunities in other areas.

Andrew Serwin named a 2020 Leader in Law by the *San Diego Business Journal*

20 November 2020
DLA Piper is pleased to announce that Andrew Serwin, US chair and global co-chair of the firm's Cybersecurity and Data Protection, Privacy and Security practices, has been named a winner of the *San Diego Business Journal*'s 2020 Leaders in Law awards.
