

Cybersecurity

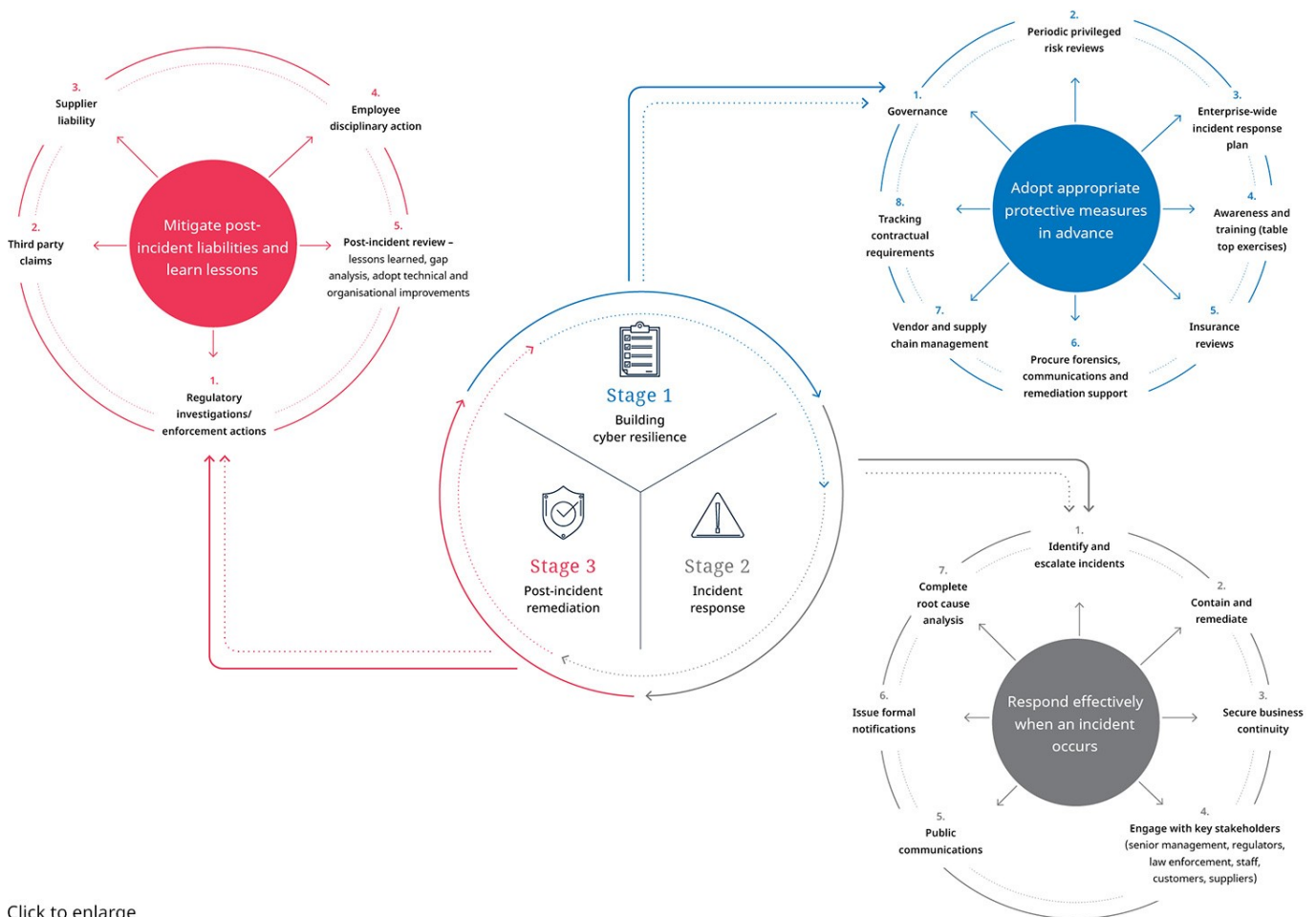
In today's interconnected world, virtually all companies, their suppliers and their customers are potential targets for cyber attacks. The risks associated with such incidents require a robust cybersecurity program in order to manage this fast-changing risk and remain in compliance.

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
 Associé
 London
 T: +44 (0)207 153 7373
 JP.DouglasHenry@dlapiper.com

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

Andrew Serwin
 Associé
 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 creating 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.

CAPABILITIES

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 FCA's 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.

