SLAUGHTER AND MAY/

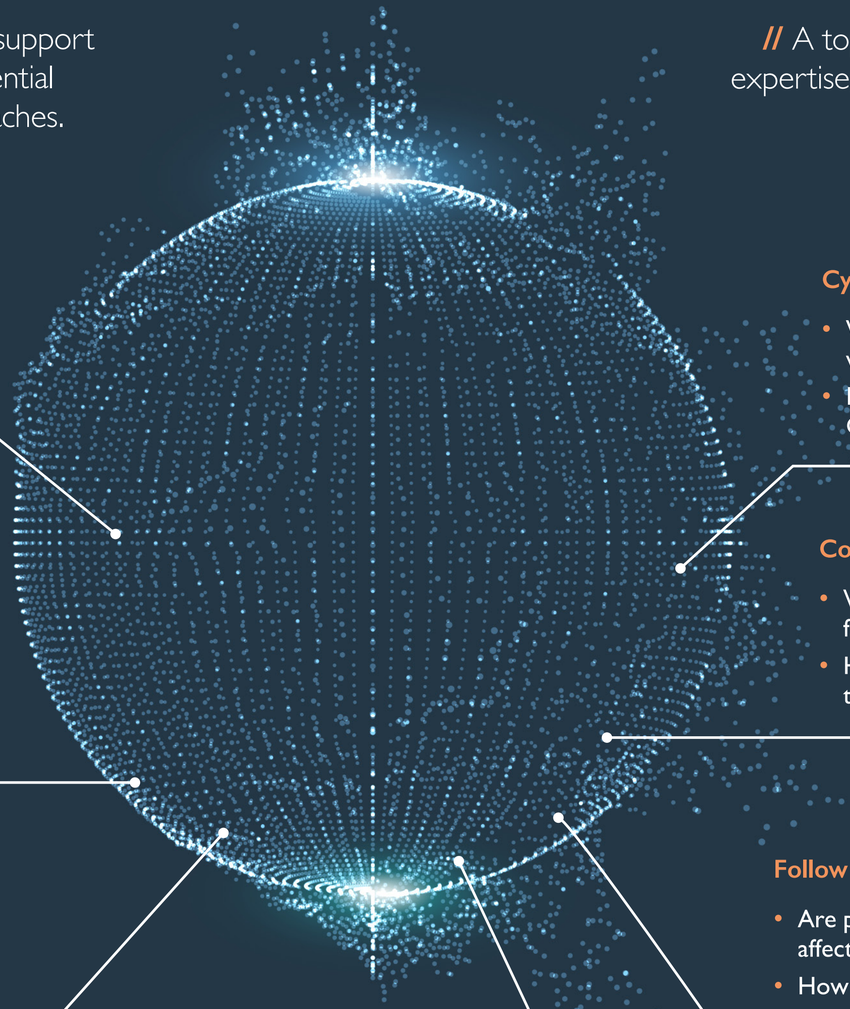
MANAGING YOUR CYBER RISKS

2021

Our specialist Cyber team provides global and multi-disciplinary support to clients across all sectors to both manage and prepare for potential cyber threats as well as to respond to specific incidents and breaches.

// A top notch team in terms of technical ability and market expertise, as well as commercially aware and client-orientated. //

CHAMBERS UK



Cyber risk assessment and preparation

- Have you identified your most "at risk" assets and platforms?
- What impact would a cyber incident have on your ability to perform day-to-day operations or on your longer term reputation and share price?

Directors Duties

- Is the board asking the right questions?
- Who is responsible for challenging the CISO?
- How often is your cyber risk assessment tested and challenged?
- Are shareholders re-assured by cyber threat policies and procedures and is there a process to keep them informed of any cyber incidents?

Regulatory responsibilities and investigations

- How will you communicate efficiently with all appropriate global regulatory bodies?
- Is there a plan to mitigate potential fines and pay outs?
- Are you fully aware of your cyber responsibilities to the ICO / FCA / PRA etc.?

Insurance

- What degree of insurance do you have in the event of a cyber incident?
- Are your trusted advisors named on your policy?

Cyber breach – crisis management

- Who is ultimately responsible for managing any incident response? Is a wider team in place that is primed and aware of their responsibilities?
- Is there a clear hierarchy of roles for directors, senior execs, IT, legal, CISO, DPO, PR team and client relationship management?

Corporate transactions, M&A due diligence

- Who is responsible for assessing the security of potential future assets (e.g. Marriott's experience)?
- Have all technological / data management assets been tested and appropriately monitored?

Follow on claims / litigation

- Are processes in place for the correct initial contact with clients and others affected by the breach?
- How do you plan to mitigate claims and pay outs?
- Have you assessed all the potential sources of claims and litigation you might face? Have these been prepared for and mitigated wherever possible?

Our cyber hub

Cyber is a key, and growing, risk for our clients. We acknowledge the range of challenges it presents to them. We recognise cyber primarily as a corporate governance risk, and so our cyber response team is led by lawyers who know the client, and will be trusted by its senior stakeholders. It is important that we have your trust to guide you through tough times.

We also know cyber response needs the full spectrum of legal support, and our cross-stream Cyber Hub comprises legal experts from our corporate, financial services, technology, data privacy, investigations and dispute resolution teams. This enables us to advise on the full spectrum of cyber issues, most importantly helping our clients to understand and mitigate cyber risks and to respond to cyber incidents. For example, we can help you:

- develop a global cyber risk management framework, enabling you to assess your compliance with laws, regulation and best practice
- manage cyber risk within your general corporate governance framework, working effectively with your senior stakeholders to set appropriate risk parameters and to offer them training, scenario testing and breach response support
- provide co-ordination to your global cyber response – key to our model is co-ordinating the advice of leading cyber lawyers from around the world. We provide quality, consistency and efficiency through our one-stop shop approach
- manage ransomware attacks, liaising with specialist advisors and law enforcement agencies where appropriate
- prepare for a range of cyber breaches, helping you design tailored cyber response plans
- manage the initial stages of a breach response, helping prioritise work streams and providing a measured response in a high pressure environment
- ensure co-ordination with internal and external technical advisors – our flexible approach to co-ordinating a 'one team' response means we can manage the co-ordination where appropriate, or support others in that role. We will work closely with your CTO/CISO, insurers and cyber specialists, and have deep working relationships with a range of cyber consultants (PWC, Kroll, Deloitte, Stroz Friedberg etc.) and PR advisors
- consider the longer term impacts of an incident, coordinating breach investigations, liaising with regulators and third parties and managing any legal or regulatory actions (including fines and mass claims)
- manage cyber risks when engaging in M&A activity or other corporate / commercial transactions which create specific cyber risks.

Relevant key experience:

- A UK-based bank in respect of a DDOS attack and the associated ransom demand to prevent further attacks
- A global bank on the production of a register of Cyber and Information Security legal and regulatory obligations including market practice around compliance in 8 core territories and 51 secondary jurisdictions
- A publicly-listed telecommunications provider on its response to a system-wide ransom hack, including its strategies for notification to the UK data regulator and customers, assessment of its corporate governance and reporting obligations, and its compliance with related regulatory requirements
- An international services and construction company on all aspects of a major cyber-attack, including in relation to law enforcement and regulator interaction, reporting obligations and subsequent data regulator investigations
- A global insurance group suffering a significant global data breach affecting 500,000 customers in 60 jurisdictions, and involving regulatory enforcement action
- A multinational transport conglomerate on the successful resolution of the data regulator's investigation into the unauthorised disposal of IT assets and potential loss of associated personal data (including advising on its broader communication and notification strategy)
- A multinational technology company in relation to a multi-million pound email spoofing scheme in which we obtained a freezing injunction to prevent fraudsters (who intercepted the payment of a legitimate invoice that was payable by our client) accessing funds in a non-UK jurisdiction
- A major multinational utilities company on its cyber risk management framework which it uses to assess its compliance with the laws, regulations, guidance and best practice relating to cyber risk
- A UK government department on a potentially significant data loss incident, including steps to mitigate the risk of subsequent litigation and challenge from counterparties.

Clients call on us and trust us to support them because of:

1.

Our depth of knowledge of our clients and their markets.

2.

Our approach to advising on risk management and embedding cyber risk in an effective risk management framework.

3.

The strategic and technical expertise we have developed and can source globally and promptly when the need arises.

Key partner contacts

Rebecca Cousin
Co-Head of Data Privacy
T +44 (0)20 7090 3049
E rebecca.cousin@slaughterandmay.com

Rob Sumroy
Co-Head of Data Privacy and
Global Head of Cyber Hub
T +44 (0)20 7090 4032
E rob.sumroy@slaughterandmay.com

Nick Bonsall
Partner
T +44 (0)20 7090 4276
E nick.bonsall@slaughterandmay.com

Richard Jeens
Partner
T +44 (0)20 7090 5281
E richard.jeens@slaughterandmay.com

Victoria MacDuff
Partner
T +44 (0)20 7090 3104
E victoria.macduff@slaughterandmay.com