Linklaters

Cyber security

High profile cyber security incidents are being reported in the press more and more often. Clients benefit from our experience, over many years, of advising on some of the most serious hacking and data breach crises in the last decade.

We have one of the longest-standing privacy and cyber security practices in Europe and have been advising clients since the inception of data protection laws more than 20 years ago. One of our key assets as a team is our global reach. Linklaters' internal privacy network spans 14 jurisdictions across Europe and Asia, while our wider network of independent privacy specialists covers over 100 countries.

We have frequent contact with the UK Treasury, Home Office and other government departments, the European Commission, as well as data protection regulators at EU and national levels. These relationships mean that should an incident occur, we have the relationships in place to support our clients as required. The right legal adviser can be pivotal to effectively managing and containing issues like this and thinking ahead before a crisis hits: this is as much about prevention as cure.

In the event of a potential breach, our team is able to:

> act as the core custodian of the facts (typically under legal privilege)

> ensure the right information is available to decision makers, including valuable cyber threat intelligence before an incident occurs

> ensure an accurate and consistent narrative is provided throughout by PR and communications representatives

> support and assist with any internal investigations

> advise on securing and recovering data including by unorthadox means

> provide necessary legal advice as to the board and management's reporting responsibilities with an eye to collateral impacts (for example in updating markets)

> liaise with relevant regulators and law enforcement officials across multiple jurisdictions

> advise on dealing with potential claims

Our team can also assist with putting in place governance and training to help reduce the impact of cyber incidents:

> advise on effective incident response planning and testing, based on our experience in major incidents

> deliver board level scenario training and wider organisational training

> assist with effective vendor risk management including designing procurement and audit processes

> advise on wider privacy compliance issues (eg GDPR and the NIS Directive, issues arising from Brexit, request under the Freedom of Information Act and Environmental Information Regulations)

"Sources are quick to praise the firm's 'broad network, accurate and up-to-date knowledge."

Chambers Global 2017, Data protection: Global-wide

"A very knowledgeable, commercial and pragmatic team."

Chambers UK 2017, Data protection and information law

"They are very good, very responsive and anticipate the questions that local counsel may have. They also understand how a business needs data flowing through it and what the legal requirements of that are."

Chambers Global 2016, Data protection: Global

Case study

Our team assisted a well-known international hotel chain with advice across 54 jurisdictions in Asia, Europe, Middle East and LATAM following a high profile data incident affecting its point of sale systems.

We provided initial support on privilege coverage for ongoing investigations, compliance issues to consider when planning the client's approach to announcing the incident and making notifications to regulators in around 20 countries.

As the results of investigations developed, we then mobilised our global network of privacy specialists to provide fast, high quality advice on action to take (including engaging with the regulator in Japan on Christmas Day). Once actions plans had been finalised, we:

> assisted the client with structuring and planning communications to guests, commercial third parties and to the media

> resolved issues escalated from guests and commercial third parties

> co-ordinated notifications to regulators in affected jurisdictions

> worked with the client team to ensure that the regulators received all the information they required in a timely manner

The in-depth knowledge of our network of privacy specialists on local regulators and local regulations provided valuable support to the client throughout. To date, no enforcement action has been initiated by any regulator or individual in any of the markets in which we or our team advised.

Linklaters crisis response experience:

We have assisted a number of clients with investigations surrounding the circumstances of a hack or serious cyber incident in which our swift intervention and analysis of the facts meant that there was no need to notify either the regulators of their customers. As a result, these instances remain out of the public domain. We worked closely with the client teams to reach a final resolution that didn't damage their reputation and avoided any form of litigation. Examples of these include advising:

> a supplier to the NHS on one of the largest losses of sensitive personal data in the UK, involving over a million records. As a result of or prompt advice and our client's quick implementation of mitigations, no regulatory action was taken and the client was not obliged to notify any individual data subjects of the data loss

> one of the world's largest outsourcing service providers on a likely government sponsored hack resulting in systemic access to credentials of employees working in a number of sensitive industries including energy infrastructure

> a global IT provider on the unauthorised extraction of personal account details (including log in details, passwords and burglar alarm codes) of tens of thousands individuals by a disgruntled employee with previously undiscovered Islamic extremist sympathies. The details extracted included those of close family members of three heads of state, less than two weeks prior to a major inter-governmental conference. Our support involved close liaison with law enforcement and specialist agencies in three European states and resolution of a significant related commercial dispute

We have also worked with clients where both regulators and customers have had to be notified of a breach or incident. In these cases, we provided full support and advice on who to tell about the breach and when. This ensured that information become public knowledge only when absolutely necessary, in a manner that ensured the story was carefully and consistently messaged. Examples include advising:

> a global hotel chain on all aspects of their recent data loss in 54 jurisdictions outside the U.S.

> an information services company on the loss of millions of sets of personal data due to a hacker attack and preparing the defence before the competent data protection supervisory authorities

> assisting a large multi-national telco with its recent employee data fraud including liaison with the NCA and national press

> a global professional services firm on its engagement strategy with a data protection authority in relation to the theft of employee files relating to tens of thousands of EU based employees

> a number of global, U.S.-based financial institutions on their notification strategies with data protection authorities in relation to the loss of back-up tapes being transported by subcontractors to long-term storage, some involving many millions of UK customer details

> a German bank before the competent data protection supervisory authority regarding an alleged large-scale unauthorised data loss

We also have experience in cases brought to the courts both under inquest and due to damages claims. In conjunction with our leading litigation team we have supported clients on related remediation and regulatory engagement, as well as their media strategy, client approach and mitigating damages claims. Examples include:

> News Corporations Management and Standards Committee, chaired by Lord Grabiner, generally in relation to its handling of the News of the World phone hacking cases (the "Milly Dowler affair"), police payments investigation and all other connected issues across News International including more than 300 separate civil compensation claims for phone hacking and related issues before the UK courts

> SWIFT in relation to its investigation by regulators in Belgium and a number of other EU jurisdictions, and its eventual settlement as a result of access to SWIFT's payment networks by U.S. law enforcement

Key contact

Richard Cumbley
Partner
London
Tel: +44 20 7456 4681
richard.cumbley@linklaters.com

linklaters.com

FT INNOVATIVE LAWYERS 2016 AWARD WINNER

GC9566_F/05.17