STEPHENSON HARWOOD

*Cyber*

# CAPABILITIES AND CREDENTIALS

# EXPERTISE
# CYBERSECURITY

## PREPARATION AND PREVENTION

**Cyber advisory:** We help GCs, in-house legal teams and company boards to manage cyber risks and enhance their organisational legal response capabilitywith defined cyber and data security legal projects.

**Corporate transactions:** Given the rapid rise of cyber risk on the corporate agenda, cyber increasingly plays an important role in M&A transactions. We advise buyers, investors, targets and sellers on the range of cyber issues as they relate to a transaction, as well as providing proactive audit services in the context of preparing for a transaction. We partner with technical providers where a holistic technical and organisational approach is sought.

**Audits and investigations support:** In a world of heightened national tensions and cyber threats, governments and regulatory bodies are turning to auditing and investigatory powers to routinely test and assess organisations, especially those deemed important to the national interest. Our lawyers have experience of supporting clients in their engagement with such processes, advocating for their practical and commercial needs while seeking to work cooperatively with national stakeholders.

**Incident response planning:** In the event of a business-critical incident, the early hours are key, and a lack of before-the-event planning can make a bad situation worse. On the other hand, a defined and practiced pre-incident plan allows stakeholders to react quickly, decisively, and in accordance with agreed policy positions to take control of the situation and mitigate ongoing damage. Well thought-out plans provide comfort to investors and other key stakeholders as to the cyber-readiness of an organisation. We ensure that legal response plans dovetail with other organisational and technical plans.

## CONTAINMENT, ERADICATION AND RECOVERY

**Cyber incidents:** Our team members have experience of working across a wide range of cyber events, both domestic and international, from catastrophic ransomware incidents, nation-state espionage and business-email compromise fraud through to insider attacks and "bad leaver" security incidents, and we regularly partner with external forensic, PR and other providers to provide a seamless incident response service.

**Crisis management:** We provide business-critical crisis support to clients suffering business-critical incidents, working in tandem with in-house teams and external specialists to keep any financial and reputational damage to a minimum.

## POST-INCIDENT ACTIVITY

**Investigations (regulatory and internal):** We support clients through regulatory enquiries, investigations and enforcement activity connected to cyber incidents, as well as providing support in the context of internal organisation investigations, e.g. where an incident relates to the actions of a current or former employee.

**Cyber litigation:** We regularly act on disputes relating to a wide range of data privacy and cyber related claims, including follow-on litigation resulting from a data breach (both from a data subject perspective and at a B2B level), stalking horse claims, class actions and cases involving the obtaining of injunctions.

**Post incident analysis:** We regularly work with clients in the aftermath of a breach to advise on measures to prevent a breach from recurring and to conduct a ‘lessons learned’ analysis.

**We engage with:** Regulators, data subjects, customers and suppliers and other impacted stakeholders to ensure our clients comply with their legal obligations while managing their legal exposure appropriately and strategically.

# RECENT EXPERIENCE
# CYBERSECURITY

## INCIDENT RESPONSE

**Pharma company:** Advised a pharma company in respect of a cyber incident affecting the health data of data subjects located in the UK and overseas, and supported with the consequential reporting and notification obligations.

**International charity:** Advised an international charity in respect of a data breach arising from a ransomware attack (affecting the personal data of over 500,000 children globally), which raised a number of challenges regarding appropriate data subject notification efforts.

**Fund:** Advised a fund on a data breach resulting from a cyber-attack made against the client's outsourced HR and payroll provider, by ensuring that they were in compliance with their notification obligations under the UK GDPR, and coordinating with an independent technical expert to formulate a robust response to the breach and ensure that the risk to our clients' systems was limited.

**Lised financial services provider:** Advised in relation to a data breach of a payment platform operated by the client, where hackers had gained unauthorised access to the personal data of customers of over 5,000 merchants. This included advising on all aspects of incident response and potential disputes with third parties.

**Telecoms company:** Advised a telecoms company on its reporting and notification obligations following a ransomware attack in which the data of a number of its subscribers were affected. Also acted on the resultant follow-on litigation.

**Global payments fintech:** Advised a global payments fintech on incident response and management in relation to a personal data breach.

**Financial institution:** Advised a financial institution in Hong Kong on a data breach incident allegedly caused by the negligence of a third-party service provider.

## ADVISORY AND COMPLIANCE

**International companies:** Advised numerous clients in relation to their cybersecurity obligations and the applicability (or otherwise) of various legislative developments in the UK and the EU, including NIS2, DORA, the Cyber Resilience Act, and the Product Security and Telecommunications Infrastructure Act.

**Investment management firm:** Advised an investment management firm on the data privacy issues of remote working cyber security penetration testing in the DIFC.

## LITIGATION AND INVESTIGATIONS

**Corporate clients:** Represented numerous corporate clients defending civil claims brought by data subjects alleging breaches of the UK GDPR and/or the UK's Data Protection Act, including the defence of stalking horse claims seeking damages in resect of alleged data breaches and cyber incidents.

**Global social media platform:** Advised in a large international cyber, data and privacy investigation undertaken by a global social media platform relating to issues such as the safety of minors, content moderation, age verification, algorithm optimisation, rabbit-holing and data collection.

**Global technology company:** Advised a global technology company with a large cross-jurisdictional internal investigation in relation to an anticipated regulatory investigation arising from a defective product with associated cyber and data issues.

**IT/software companies:** Advised on a number of matters relating to the misappropriation of data and/or source code by former employees of IT/software companies, involving the obtaining of injunction and the civil recovery of digital assets.

# CLIENT TRAINING MODULES: EXAMPLES
# CYBER


**JOANNE ELIELI**
*Partner, Cyber lead*
+44 20 7809 2594
+44 7386 688 752
joanne.elieli
@stephensonharwood.com



**KATIE HEWSON**
*Head of Data Protection*
+44 20 7809 2374
+44 7702 141 048
katie.hewson
@stephensonharwood.com



**SARAH O'BRIEN**
*Managing associate*
+44 20 7809 2481
+44 7766 828548
sarah.o'brien
@stephensonharwood.com



**MONICA MYLORDOU**
*Associate*
+44 2078 092 242
+44 7350 453 268
monica.mylordou
@stephensonharwood.com


## BREACH RESPONSE

**Target audience: all key stakeholders, including C-suite, Legal, Compliance, IT and cyber teams:**

Regular training is a critical element of any technical and organisational resilience strategy. Recent studies have found that that approx. 90% of all breaches arise from some form of human error or targeted phishing attack.

**The training we offer is focussed on:**

+ helping in-house legal teams and business stakeholders understand the legal risks associated with cyber events; and
+ developing and implementing measures to restrict, prevent and respond to cyber events as they occur.

We offer a variety of sessions, focused on prevention (e.g. identifying and avoiding phishing or payment redirection attacks), legal team coordination and response planning, and legal issues arising during incidents. We also work with technical providers, where requested, to provide combined technical and legal training scenarios. Topics are regularly revisited as the threat landscape evolves.

## DATA BREACH LITIGATION

**Target audience: Legal, compliance, IT and cyber teams**

We will examine the data breach landscape and the types of litigation that often follow a breach, including a discussion on potential damages and risk mitigation.

**The session will cover:**

+ liability: breach incidents and regulatory fines;
+ regulatory breaches under the UK GDPR and the DPA 2018;
+ tortious claims: misuse of private information, breach of confidence and negligence;
+ contractual claims, including breach of warranties, application of indemnities and liability caps;
+ damages: likely quantum associated with data breach claims;
+ privacy class action landscape: representative actions, group actions and stalking horse claims; and
+ mitigation of litigation risk and dispute avoidance strategies.

## EXAMPLES OF THE MOST REQUESTED CLIENT TRAINING SESSIONS INCLUDE:

+ **Overview sessions:** Lifecycle of a data incident and overview of cyber threats and legal risks.
+ **Tabletop training / war gaming:** Ransomware, data extortion, BEC fraud and Nation State espionage scenarios.
+ **Trends and advisory:** Regulatory trends in the UK and EU, cyber trends in contracting and cyber liability and litigation