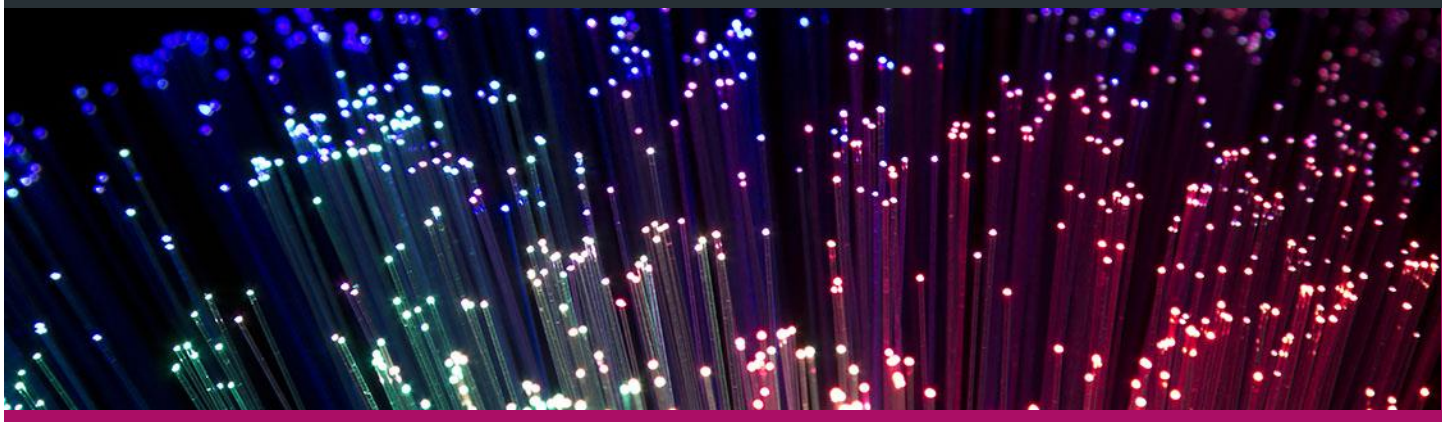

# Breach response

**Cyber-crime remains a huge threat to organisations of all sizes. Reports to the ICO of ransomware incidents have increased by 560% over the past 2 years, with the biggest cyber risk being phishing attacks. However, the biggest single cause of reported data breaches to the ICO involve something as simple as information being sent to an incorrect recipient. People and processes are key.**

These issues require swift action. The first 24 hours following an event are the most crucial. With the ICO having the power to fine up to €20 million, or 4% annual global turnover, an increase in data breach litigation, and the reputational risk to businesses following cyber-crime and data breach incidents, now is the time to ensure you have prepared for, and can respond to, these events.

## How we can help

We understand that the true cost of a data breach and cyber-crime is more than just a number. Penalties from regulators and damage to reputation can lead to business disruption, lost trade and management time and the costs of internal investigations and disciplinary procedures.

We have substantial experience in handling all aspects of cybercrime and data breaches across a number of sectors, with specialist Information Law and Cyber Security teams working together to ensure that clients receive expert advice on preparing for and can responding urgently to these events.

## Prevention

- Advising on strategy to minimise key commercial, financial, regulatory and legal risks.
- Reviewing policies, procedures and information governance to ensure regulatory compliance.
- Working with IT specialists to assess internal safeguards and capabilities.
- Advising on sector specific issues, best practice and formulating effective breach response plans.
- Advising on roll-out of policies, training and internal communications.

## Breach Response

- Working closely with your teams to create or implement breach response plans to protect data and mitigate key business risks.
- Assisting with internal investigations, quickly gathering evidence and conducting in depth investigations when issues come to light.
- Engaging and liaising with forensic IT experts and consultants, PR and Communications teams and legal advisors in other jurisdictions.
- Advising on strategy for and notifications to regulators, individuals and stakeholders.
- Seeking urgent injunctive relief to protect misappropriated money, assets, IP and confidential information from being dissipated or misused.
- Advising on potential losses and options for recovery.
- Providing follow up recommendations together with training.

## Key contacts


**Helen Briant**
Partner, Dispute Resolution and Litigation
+44 (0)121 214 8867
HBriant@trowers.com

**Charlotte Clayson**
Partner, Dispute Resolution and Litigation
+44 (0)20 7423 8087
CClayson@trowers.com