# WILLIAM FRY

# Breach Management and Incident Response Service

Businesses must prepare in advance how they will deal with a data breach or similar incident in order to minimise and manage reputational damage and regulatory risk. With vast experience in dealing with complex data breaches, our specialist team provides breach management and incident response services to affected organisations.

We provide a co-ordinated, multi-disciplinary and strategic approach to ensure the most effective, efficient and customer- focused response plan is implemented to suit business needs.

**Our Incident Response Service**

- Regulatory liaison service
- Cyber insurance cover implications
- Incident management reporting
- Analysis of notification obligations
- Breach containment & preservation of evidence
- Communications & PR strategy
- IT forensics
- Post-breach remediation
- Legal advice & representation
- Strategic risk management

Contact us at: **cybersecurity@williamfry.com**

**David Cullen**
Partner

T +353 1 639 5202
David.cullen@williamfry.com

**Leo Moore**
Partner

T +353 1 639 5152
leo.moore@williamfry.com

**John Magee**
Partner

T +353 1 489 6532
john.magee@williamfry.com

**John O'Connor**
Partner

T +353 1 639 5183
john.oconnor@williamfry.com

# WILLIAM FRY

## How to respond to a cyber attack

- Quickly assess the scale of the cyber attack and the information at risk

- Seek legal advice to co-ordinate the response while maintaining legal privilege

- Direct your IT department to backup and maintain all audit trails

- Monitor banking activity on organisation accounts and inform your bank of a breach

- Preserve evidence and record all actions taken

- Check your organisation's insurance policy and coverage

- Determine if the cyber attack requires notifications outside your organisation (for example, the Data Protection Commissioner, affected individuals, the Gardaí etc.)

- Alert public relations team and decide on a communications strategy

## Key items for securing your organisation

- Put cybersecurity on your board agenda

- Ensure your organisation has mechanisms in place to detect cyber threats

- Implement an appropriate information security policy

- Create an incident response plan and delegate responsibility for co-ordination of the response

- Make staff at all levels aware of the implications of a cyber attack

- Audit the effectiveness of existing processes, procedures and security controls

- Ensure all critical data are backed up securely

- Put in place appropriate access management controls for remote and mobile devices

Contact us at: **cybersecurity@williamfry.com**