

EVERSHEDS

Clicking into place
Protecting your business
from evolving global risk



90% of large organisations report that they have suffered an information security breach – an increase of 9% since 2014.*

Clicking into place

Protecting your business from evolving global risk

Information Security

Helping your business prepare and respond to the evolving global risk

Information security breaches for big brand names continue to grab the headlines, but these tell only part of the story. The UK Government's 2015 Information Security Breaches Survey highlights the increasing prevalence, scale and cost to businesses large and small throughout the UK. The average cost (to surveyed companies) caused by a breach, including business disruption, regulatory fines and compensation, has increased to as much as £311,000 for small businesses and £3.47m for large organisations. The damage to their reputation and trust, as well as loss of confidential information, intellectual property and trade secrets, can be far more significant and impossible to repair.

Information security breaches can come from inside the organisation, for example from disgruntled employees or those who are leaving to set up in competition, as well as the more widely reported theft or loss of electronic devices or malicious cyber attacks.

Information security is a continuing and critical challenge, to which the response cannot be regarded as simply technical. The way an organisation prepares can both reduce the likelihood of a breach incident occurring and improve the outcome should an incident occur.



*UK Government's 2015 Information Security Breaches Survey.

How we help our clients

Our wealth of experience has given us an understanding not just of the law in this area, but also of the way in which to approach its application practically both before and after information security breaches, helping you to prepare, prevent and respond when the worst occurs. Using our international reach, we help our clients to develop these solutions in a way that make sense for their businesses globally.

1

Help you to review and develop your policies and procedures, including on data protection, information security and employee conduct, and help you to embed those policies through focused training.

2

Tailor your contracts to ensure that you have the best protection as regards your customers, suppliers of critical IT systems and employees (e.g. through restrictive covenants) and in your corporate acquisitions.

3

Provide guidance on dealing with "threats from within" through lawful communication monitoring programmes.

4

Advise you on the impact of information security risk on corporate governance and your directors' duties.

5

Assist with legal compliance in support of applications for ISO7799 certification.

6

Advise you on your cyber insurance policy coverage.

7

Assist with optimising your incident response planning, including communication strategies, investigation and strategy formation.

8

When breaches occur, take quick and decisive action across multiple jurisdictions, helping you with legal action (injunctions) to contain damage, notifying and liaising with regulators and reputation management in the traditional and online media.

9

Conduct effective investigations, interface with regulators and provide guidance on any criminal liability flowing from information security breaches.

10

Assess liabilities and rights, as well as pursue claims on your behalf against third party IT suppliers (in cases of external data breaches) and employees (in cases of internal data breaches) and handle customer complaints and claims against your organisation arising from a loss of customer data.

With representatives on the committee of the British Computer Society – Information Security Specialist Group, and government backed IT security initiatives, we speak and write regularly on international security and cyber law.

Clicking into place

Protecting your business from evolving global risk

Examples of our work

Acting for a client that suffered a serious hack, resulting in the theft of data for hundreds of thousands of customers. We supported the client from the initial incident to a successful resolution. In particular:

- we helped our client make an informed decision about notifying the ICO and its customers and prepare the necessary documentation to submit a full notification
- we advised our client on sensitive and crucial communications with its customers and reputation management issues
- we advised the client in relation to claims for compensation from a number of affected customers, as well claims that our client itself may have against its IT providers.

Advising a national retailer in relation to cyber insurance cover after it suffered an attack from one of its own employees. The employee hacked into the client's employee database and extracted other employees' personal data, which they published online. Our client incurred significant costs in addressing the consequences of this breach, including engaging external consultants, setting up a helpline and compensating affected individuals. Eversheds' Insurance team worked closely with the client on selecting appropriate cyber insurance cover to protect its business against such losses in the future.

Helping a client develop a cross-function data security response team with a toolkit to assist recognition and management of data security breaches, conduct impact assessments and aid decision making on reporting to the ICO and affected individuals.

Helping a developer of data loss prevention tools to review potential barriers to adoption arising from the application of data protection, communications and employment laws across several countries and ways of mitigating those barriers.

Advising a TMT client on reporting requirements across the EU when their B2B customer database was the subject of a Phishing penetration.

Acting for an international advanced alloys manufacturer concerning the misuse of confidential information and trade secrets by certain employees in their alleged attempt to set up a competing business with a Chinese corporation. At very short notice we assembled a multi-disciplinary team and guided our client through urgent injunctive springboard relief, e-disclosure, search and seizure, disciplinary proceedings and an expedited trial in what were hard fought Court proceedings.

Key contacts



Paula Barrett

Partner, Head of Privacy & Information Law
International Data Privacy
Tel: +44 207 919 4634
paulabarrett@eversheds.com



James Hyde

Partner, Head of TMT Disputes
Litigation & Dispute Management
Tel: +44 113 200 4066
jameshyde@eversheds.com



Fiona Bolton

Partner
Employment
Tel: +44 207 919 4560
fionabolton@eversheds.com



Simon Brooks

Partner, Head of Insurance & Reinsurance
Insurance & Reinsurance
Tel: +44 207 919 4583
simonbrooks@eversheds.com



Andrew Terry

Partner
Reputation Management & Brand Protection
Tel: +44 207 919 4828
andrewterry@eversheds.com

eversheds.com

©Eversheds LLP 2015 © Eversheds International 2015.

All rights are reserved to their respective owners.

Eversheds International is an international legal practice,
the members of which are separate and distinct legal entities.

DT05158_09/15