BRIEFING NOTE

DATA PRIVACY, SECURITY AND INFORMATION RIGHTS

Why does it matter and should I care?

Introduction

This note sets out a summary of why businesses and talent should invest in protecting privacy and securing information assets.

Market trends

There is a growing trend (and need) for businesses and individuals to invest more time and resources into managing their information assets and privacy. This has come about as a result of the industrial digital revolution which has brought with it an exponential growth in digital storage capability and an ability to transmit and copy large volumes of data at will.

Whilst this revolution introduces significant opportunities, it also presents substantial risk. This risk presents itself in the potential (accidental or intentional) loss or unauthorised access to sensitive commercial information or personal records. In addition, the popularity of social media and mobile communication has resulted in an increased risk to brands and reputation – employees may post statements for which companies may be vicariously liable; equally, talent may tweet defamatory or untrue statements which may incur liability or cause irreparable harm for a sports team, record label, brand or sponsor.

Added to this, in a desire to cut overheads and capital expenditure, organisations are inclined to outsource technology solutions and business processes; a decentralisation of such systems and processes can threaten and weaken traditional controls over databases, confidential client records and employee data (e.g. outsourcing of a payroll or HR database).

Further, traditional business models which used to rely heavily on sales of physical or digital downloads are increasingly dependent on advertising (or advertiser funded) or subscription revenue. Revenue from the exploitation of data, user profiling and targeting is instead subsidising returns. Accordingly, careful management and protection of such datasets are key to profitability.

Legal developments

Current changes proposed to regulation due to become law in 2015 will see:

- fines for serious data breaches rise from £500,000 to between 2-5% of annual worldwide turnover;
- data processors (i.e. suppliers) become directly liable for breach of statutory regulation (in the same way that data controllers are currently liable);
- suppliers of critical infrastructure and information society services (such as social networks) will be required to notify regulators without undue delay of any material security breaches and imminent threats; and
- financial services and listing rules require companies to disclose material breaches and vulnerabilities to investors and shareholders.

Underpinning these changes, directors should be reminded that they may be personally liable for failing to discharge their duties as directors if such risks are not quantified, assessed and mitigating steps taken accordingly.
BRIEFING NOTE

DATA PRIVACY, SECURITY AND INFORMATION RIGHTS

Why does it matter and should I care?

In short, in the current threat environment, security is business. It is not a nice to have or value-add. It will be essential to survival and to differentiate oneself from the competition.

The pros and cons

The risks threaten revenue streams, customer churn, reputation, contractual liability to suppliers and clients, intellectual property assets (such as source code or content repositories or storage facilities) and merger and acquisitions. Costs for serious breaches can be spine tingling and include:

- Regulatory fines
- Legal costs
- IT forensics and forensic accounting
- PR and reputation management counsel
- Penalties to card issuers
- Claims from consumers and contractual liability to suppliers
- Data breach notification and call centre costs
- Credit monitoring and identity fraud costs
- Impact to share price and potential investor claims
- Director’s personal liability


However, tackling them effectively can improve resilience and customer service, protect share value, maximise ROI on research and development, reduce regulatory burdens, avoid fines, mitigate liability and reduce insurance premiums.

The business case

Sheridans’ Technology and Data Privacy, Security and Information Rights group helps clients devise effective data strategy to:

- identify information assets and vulnerabilities
- maintain brand value and protect reputation
- minimise risk and insurance premiums
BRIEFING NOTE
DATA PRIVACY, SECURITY AND INFORMATION RIGHTS

Why does it matter and should I care?

- maximise return on R&D and information assets
- facilitate due diligence over suppliers in supply chains
- reduce project costs by evaluating privacy and security concerns at concept, rather than prototype stage
- optimise revenue streams and enforcement costs
- achieve compliance and build trust
- develop contingency response plans and providing training

Summary and actions

In summary, information security is now being treated as a core business risk (akin to competition and bribery law).

Clients are advised to prioritise this risk and allocate responsibility to a board member (preferably not an IT director who is often conflicted from making objective assessments of technical and organisational security) to undertake an on-going security programme.

When reviewing budgets, allowances should be made for investing in information security as a core business and reputational risk (this may ease pressure on legal budgets and allow contributions and cost sharing from marketing and corporate governance/risk budgets).

Firms should also review existing insurance cover and consider taking out stand-alone, specific cyber insurance cover (traditional policies often include exclusions which do not cover cyber loss) - see http://www.cnbc.com/id/101804150 for latest trends on insurance purchasing.

We would welcome an opportunity to discuss how we may be able to help in managing these risks and realising the opportunities of unlocking the available returns from digitisation (and, in so doing, managing returns in a secure, resilient ecosystem).

For further information, please contact Philip James or a member of Sheridans’ Technology or Data Privacy, Security & Information Rights teams. Please see:

http://www.sheridans.co.uk/practice-areas/data-privacy.aspx
http://www.sheridans.co.uk/sectors/cyber-risk.aspx

for further details.

PHILIP JAMES, Partner

+44(0)20 7079 0177
pjames@sheridans.co.uk

© Sheridans, August 2014.

This note is only intended to be a general briefing note. Specific guidance and legal advice should be sought in relation to particular circumstances and should not be relied upon.