Edelman is the world's largest public relations firm (www.edelman.com). Edelman's Data Security and Privacy (DSP) Group (<http://datasecurity.edelman.com/>) helps companies navigate the increasingly complex environment surrounding the collection, use and protection of corporate and personal data. Please send any queries regarding this column to Jonathan Hargreaves (jonathan.hargreaves@edelman.com)

Consumer demands for protection growing

Legal and Regulatory Update

Preparing to manage privacy risks

Jonathan Hargreaves

Journal of Direct, Data and Digital Marketing Practice

(2013) **14**, 257–261. doi:10.1057/dddmp.2013.7

Topic: Edelman Privacy Risk Index (ePRI)

Who: Edelman, Ponemon Institute

Where: Global

When: 2012

What happened

This paper looks at the key findings of the Edelman Privacy Risk Index (ePRI) created in partnership with the Ponemon Institute. The research assesses the readiness of businesses to meet the changing risk and reputational demand that legislative, technological and consumer changes are bringing to the management of personal data.

It reports on key findings that 57 per cent of respondents think their organization does not consider privacy and the protection of personal information to be a corporate priority, and 61 per cent companies do not strictly enforce all levels of compliance with laws and regulations. Further, 62 per cent of respondents say that their organization does not have the expertise or technology, and 55 per cent say that they do not have the adequate resources to adequately protect personal information. In addition, 57 per cent of respondents believe that their company is not transparent about what it does with employee and customer information, and 61 per cent are slow to respond to consumer and regulator complaints about privacy.

The results and associated ePRI calculator enable businesses to assess their own readiness and make informed decisions about reducing risk and making strategic reputational decisions.

Creating the Edelman Privacy Risk Index (ePRI)

Companies today are losing their customers, reputation and money because they are failing to manage data security and privacy properly in an environment full of consumer expectations, security threats, critical media and regulatory action. Taken together, a company's licence to operate in the digital age is now largely dependent on how it manages privacy and security.

Consumers care more than ever about the security and privacy of their personal data. As they are increasingly asked to share more, increasingly sensitive information, they are demanding to know how it is managed and protected. To understand better how companies are

Figure 1: Privacy risk profiles

managing privacy, Edelman developed the ePRI (<http://www.edelman.com/insights/intellectual-property/privacy-risk-index/>) in partnership with the Ponemon Institute. This first-of-its-kind study analysed the leading factors of privacy risk and how 6,400 privacy and security executives in 29 countries and regions across 20 industries manage these issues.

Corporate profile risk: What defines a company

The ePRI found that corporate profile (factors such as industry and geographic footprint) and a company's privacy practices were the best indicators of a company's risk for reputation or financial damage because of a privacy incident. It also found that companies in high-risk industries and markets are failing effectively to implement strong privacy practices and make the protection of consumer information a corporate priority.

A company's profile contributes strongly to its privacy risk (see Figure 1). Companies find themselves in very different starting points based on the industry they are in, the markets where they operate, the size of their organization and the type of information they collect.

The ePRI found that companies operating in high-risk markets, information-intensive industries or in more than one country are particularly vulnerable to privacy incidents — much more so than their counterparts operating in low-data industries, such as agriculture, and in markets less focused on privacy, such as Brazil.

The ePRI found that the 11 riskiest markets for data privacy are all in Europe, because of its strong culture of privacy and stringent regulations. Developing nations such as Brazil and India, on the other hand, pose significantly less concern. The ePRI also found that companies with a greater global footprint tend to face higher levels of privacy risk, since more markets mean increased regulatory issues and cultural expectations. Therefore, even if a global company is based in a low-risk market, it could also have to manage privacy risks in a high-risk market where it has operations.

The ePRI also shows that highly regulated, consumer-facing industries such as financial services, health and pharmaceuticals, and

Starting from different places on privacy

Companies vulnerable to privacy risks

Figure 2: Preparedness to manage privacy risks

communications present the highest levels of privacy risk. These industries face more regulation and have a greater potential for losing sensitive information, as they collect so much more of it. While companies are not able to fundamentally change the risks caused by their business operations, it is essential for them to understand whether they are at a higher risk of an incident so that they can change the risk factors they can control.

Corporate privacy practices: How businesses operate

A company's profile is just the start. What are more important — and more easily altered — are a company's privacy practices. A business with a high-risk profile can significantly affect its overall privacy risk based on privacy practice management. Best practices include:

- Becoming more transparent about what a business does with employee and consumer information;
- Prioritizing the privacy and the protection of personal information; and
- Understanding that a data breach would adversely affect its reputation and financial position — and then putting forth ample resources to ensure it does not happen.

Yet the ePRI found that companies are not taking the steps necessary to meet the privacy demands they face. More than half of the organizations surveyed for the ePRI are not transparent about what they do with the personal information they collect.

Privacy departments at the organizations surveyed for the ePRI lacked the resources and expertise needed to effectively address privacy concerns (see Figure 2). An alarming 62 per cent say that their organization does not have the expertise or technology, and 55 per cent say that they do not have adequate resources to manage the privacy of personal information effectively. This could be partially due to a lack of necessary leadership or buy-in from the top; however, 60 per cent of respondents believe that their organization does not consider privacy a

Reducing risk through better practice

Lack of expertise and resources

Figure 3: Transparency about data usage

priority, and 53 per cent do not believe that a data breach would not adversely impact on company reputation.

This lax attitude about privacy does not stop at the top. The day-to-day employees who often handle sensitive information and are a major cause of incidents are also not prepared. More than half of the companies (57 per cent) think that their employees do not understand the importance of security and privacy, while two-thirds do not proactively educate employees on privacy issues.

Despite calls from regulators and consumers for companies to be more accountable for the information they collect and use, there is a major lack of transparency in many organizations (see Figure 3). More than half of respondents (57 per cent) believe that their company is not transparent about what it does with employee and customer information, and 61 per cent are slow to respond to consumer and regulator complaints about privacy.

Actions in the light of the Edelman Privacy Risk Index

Opportunities in privacy risk

Businesses can no longer shove data security and privacy management to the side. Consumers, media and regulators simply won't allow it, and the reputational and financial risks are simply too high.

In the burden of these risks, there is opportunity. There is a true competitive advantage to prioritizing privacy, and the businesses that choose to adjust their cultures and behaviours to reflect privacy will give customers what they are looking for most — a brand they can trust.

Getting there is not an impossible feat. The ePRI identified 12 privacy practices that most contribute to a company's ability to manage privacy risk. Taking action to improve these areas can significantly reduce the risk to an organization.

Communications must ensure that privacy is managed as a core corporate reputation issue and consider how privacy can help enable business. Privacy communications programmes should include employee engagement and education to mitigate the potential misuse or loss of information, data breach response preparedness, as well as

stakeholder engagement and public affairs, to manage communications with policymakers and advocates.

The companies that see the risks, understand them and work to change will be the leaders of this century. They will establish consumer trust, avoid monetary losses and be ahead of regulations, which will give them the licence to lead in the data economy. Building greater trust as a company that respects privacy can allow it to leverage better the data they collect without raising concerns with their stakeholders, as well as help inoculate companies from reputation loss if an incident occurs.

Online benchmarking tool

The ePRI calculator

To help businesses improve their stance on data security and privacy, Edelman developed an online benchmarking tool to accompany the ePRI — The ePRI calculator (<http://www.edelman.com/privacy-risks/>). The tool enables businesses to quickly benchmark their own privacy risk against the survey data and provides a Privacy Risk Index score, with a high score indicating a company is more likely to suffer reputational damage or economic losses from a privacy-related incident.

The ePRI calculator benchmarks privacy risk against organizations of similar size, geographic footprint and industry sector. This propriety assessment method rates an organization's ability to prevent and quickly recover from loss, theft or misuse of personal information.

Jonathan Hargreaves, Head of technology, EMEA, Edelman
E-mail: jonathan.hargreaves@edelman.com

Osborne Clarke is one of Europe's most respected law firms and a UK leader in advising marketers on the legal issues affecting them. The firm's Marketing Law.co.uk website has provided marketers with authoritative legal insights for over 10 years. Please send any queries regarding this column to Stephen Groom (stephen.groom@osborneclarke.com)

What happened

Did assignment of rights 'arising from the performance of the services' work?

Stephen Groom

Journal of Direct, Data and Digital Marketing Practice (2013) 14, 261–263.
doi:10.1057/dddmp.2013.8

Topic: Intellectual property

Who: Susan Wilkinson vs London Strategic Health Authority

Where: Patents County Court

When: November 2012

Law stated as at: 5 December 2012

Susan Wilkinson sued her former client London Strategic Health Authority ('LSHA') for copyright infringement.