DATA SECURITY PRIVACY GROUP

Edelman

THE COSTS, CAUSES AND CONSEQUENCES OF PRIVACY RISK

Many companies are ignoring mounting consumer and regulatory concerns about data security and privacy.

Companies today are losing their customers, reputation and money because they are failing to properly manage data security and privacy in an environment full of consumer expectations, security threats, critical media and regulatory action. Taken together, now more than ever before, a company's license to operate in the digital age is 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 — and increasingly sensitive information — they are demanding to know how it is managed and protected. Eighty-five percent of consumers around the world feel businesses need to take data security and privacy more seriously, according to Edelman's consumer privacy research. Seventy percent of consumers are more concerned about these issues than they were five years ago likely due to the amount of information that is collected and shared about them online.

Edelman's study also demonstrated that the premium on privacy is more than just a compliance or communications issue — it affects a company's bottom line. Consumers say they would drop services if their personal information is accessed without their permission. Eight out of ten consumers would consider leaving a banking institution that did so, and nearly seven in ten would leave a healthcare provider.

If these mounting consumer concerns were not enough, companies find themselves in increasingly critical regulatory environments. Regulators around the world are cracking down to ensure companies are protecting customer information. In the United States, for example, the Federal Trade Commission is boosting enforcement of privacy and recently leveled a record $22.5 million fine for poor privacy practices. The Securities and Exchange Commission now requires all publically traded companies to disclose data security or privacy incidents in their filings, highlighting the significant damage these incidents can cause. In Europe, regulators are on the verge of passing legislation which will create a single regulatory regime able to levy fines up to two percent of annual turnover for privacy violations.

CONSUMER CONCERN

Three quarters of consumers will stop using an online shop if information was accessed without permission

Less than half of consumers trust healthcare organizations to protect information
-Edelman DSP Group Study

Further, not a week goes by without a company or entire industry in the news for an alleged privacy violation. Every time a breach occurs the media blasts it from the headlines, questioning whether consumers can truly trust corporations to protect their information. The incident typically dominates the company's media coverage for weeks, and

causes many top news outlets to conduct in-depth investigations into the company's business practices. This type of media scrutiny often leads to attention from policymakers, which can spur additional regulatory action or negative headlines.

Despite all of these pressures and demands, companies are struggling to manage the privacy practices that create the most risk. Why?

UNDERSTANDING PRIVACY RISK

"With the level of consumer, media and regulatory attention currently focused on privacy, businesses simply can't afford to gamble with the reputational and financial damage that may result from a security breach or other privacy incident."

-Pete Pedersen,
Global Chair, Technology Practice, Edelman

To better understand how companies are managing privacy, Edelman developed the Edelman Privacy Risk Index℠ (ePRI) in partnership with the Ponemon Institute. This first-of-its-kind study analyzed the leading factors of privacy risk and how 6,400 privacy and security executives in 29 countries across 20 industries manage these issues.

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

CORPORATE PROFILE RISK: WHAT DEFINES YOUR COMPANY

A company's profile contributes strongly to its privacy risk. 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 like Brazil.

The ePRI found that the eleven riskiest markets for data privacy are all in Europe, due to its strong culture of privacy and stringent regulations. Developing nations like 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 means 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 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 if they are at higher risk of an incident so they can change the risk factors they can control.

CORPORATE PRIVACY PRACTICES: HOW YOU OPERATE

"Many of the front line employees who are managing compliance don't believe that they have the necessary practices, protocols and behaviors in place to safeguard against financial or reputational damage."

-Jules Polonetsky,
Director and Co-chair of the Future of Privacy Forum

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 impact 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.

Approximately 2 out of 3 companies do NOT have the expertise and technology to protect personal information

Over half do not have the resources needed to protect the information they collect

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 that made up the ePRI lacked the resources and expertise needed to effectively address privacy concerns. An alarming sixty-two percent say their organization does not have the expertise or technology, and fifty-five percent say they do not have adequate resources to effectively manage the privacy of personal information. This could be partially due to a lack of necessary leadership or buy-in from the top, but more than half (60 percent) of respondents believe their organization does not consider privacy a priority, and fifty-three percent do not believe a data breach would not adversely impact company reputation.

Over half of the organizations surveyed (57%) are not transparent about what they do with personal information collected

And 61% say they are not quick to respond to customer privacy complaints

This lax attitude about privacy does not stop at the top. The day-to-day employees, who often handle sensitive information who are a major cause of incidents, are also not prepared. More than half (57 percent) of companies think 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. More than half (57 percent) of respondents believe their company is not transparent about what it does with employee and customer information, and sixty-one percent are slow to respond to consumer and regulator complaints about privacy.

MANAGING DATA PRIVACY

"Senior business leaders need to assess their company privacy risk and avoid becoming a high profile example of the damage that results from high profile misuse or loss of consumer data."

-Jules Polonetsky,
Director and Co-chair of the Future of Privacy Forum

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 behaviors 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 twelve 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.

12 PRIVACY PRACTICE IMPERATIVES

COMMUNICATIONS & ENGAGEMENT

- My organization is transparent about what it does with employee and customer information.
- My organization is quick to respond to privacy complaints or questions from customers and regulators.
- My organization makes a substantial effort to educate employees about privacy and data security.
- Employees in my organization understand the importance of privacy and how to protect personal and/or sensitive information.

BUSINESS OPERATIONS

- My organization considers privacy and the protection of personal information a corporate priority.
- A high-level executive leads my organization's privacy program and is empowered to make decisions.
- My organization understands global privacy cultural differences.
- My organization strictly enforces all levels of non-compliance with laws and regulations.

DATA PROTECTION

- My organization believes a data breach would adversely affect our reputation and financial position.
- My organization has ample resources to protect employee and customer information.
- My organization is able to prevent and quickly detect the theft or misuse of personal information.
- My organization has the expertise and technology to protect personal information.

Executing against these twelve imperatives requires managing privacy as more than a compliance or technology issues. Effective privacy management requires collaboration across an organization that includes communications, legal, business, human resources and technology leaders addressing their respective areas of privacy risk.

COMMUNICATIONS must ensure privacy is managed as a core corporate reputation issue and consider how privacy can help enable business. Privacy communications programs 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.

BUSINESS OPERATIONS must ensure the company is properly governing the collection, the use and storage of information, as well as ensuring that consumers are notified. Further, for companies designing new technologies and services, it is essential that privacy be incorporated into the design process.

LEGAL departments must ensure a company understands, and is in compliance with, the various local data protection laws in all of the geographies where the business operates. Further, they must have the resources and understanding to properly respond to a data breach or the potential litigation due to a privacy incident.

TECHNOLOGY departments must ensure the proper security safeguards are in place to prevent and quickly recover from an incident. This includes technologies that limit the people and ways in which sensitive information can be accessed within an organization.

To help businesses improve their stance on data security and privacy, Edelman developed an online benchmarking tool to accompany the Privacy Risk Index. The tool enables businesses to quickly benchmark their own privacy risk against the 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 companies that see the risks, understand them and work to change will be the leaders of the next century. They will establish consumer trust, avoid monetary losses and be ahead of regulations, which will give them to license to lead in the data economy. Building greater trust as a company that respects privacy can allow it to better leverage the data they collect without raising concerns with their stakeholders, as well as help inoculate companies from reputation loss if an incident occurs.

ABOUT THE EDELMAN DATA SECURITY AND PRIVACY GROUP

Edelman's Data Security & Privacy (DSP) Group helps companies navigate the increasingly complex environment surrounding the collection, use and protection of corporate and personal data. Edelman DSP Group helps companies enhance trust and advance brand, reputation and competitiveness through communications and stakeholder engagement.

ABOUT THE PONEMON INSTITUTE

The Ponemon Institute is dedicated to advancing responsible information and privacy management practices in business and government. To achieve this objective, the Institute conducts independent research, educates leaders from the private and public sectors and verifies the privacy and data protection practices of organizations in a variety of industries.

ABOUT EDELMAN

Edelman is the world's largest public relations firm, with 66 offices and more than 4,500 employees worldwide, as well as affiliates in more than 30 cities. Edelman was named Advertising Age's top-ranked PR firm of the decade in 2009 and one of its "A-List Agencies" in both 2010 and 2011; Adweek's "2011 PR Agency of the Year;" PRWeek's "2011 Large PR Agency of the Year;" and The Holmes Report's "2011 Global Agency of the Year" and its 2011 "North American Large Agency of the Year." Edelman was named one of the "Best Places to Work" by Advertising Age in 2010 and 2012 and among Glassdoor's top five "2011 Best Places to Work." Edelman owns specialty firms Edelman Berland (research), Blue (advertising), A&R Edelman (technology), BioScience Communications (medical communications), and agencies Edelman Significa (Brazil), and Pegasus (China).

WEB:
Datasecurity.edelman.com
Edelman.com/expertise/practices/data security & privacy

TWITTER:
@EdelmanDSP

CONTACT:
Pete Pedersen, *Global Chair, Technology*
Pete.Pedersen@edelman.com

Ben Boyd, *Global Chair, Corporate*
Ben.Boyd@edelman.com

DATA SECURITY & PRIVACY GROUP

Edelman