Privacy and Data Protection Challenges for the Global Enterprise

**Issue**

Businesses and their customers alike collect, store and transmit vast amounts of information electronically, and they want to believe that this information is secure. At the customer level, the concern for data privacy has resulted in a growing number of laws and regulations that address issues including what information can be collected and maintained, how the information should be stored, how and where information can be transmitted, and required actions in the event of a security breach. Notwithstanding the proliferation of requirements, reports of identity theft, inadvertent release of customer and proprietary business information, and successful attempts by hackers to penetrate systems and steal information continue to command headlines in the media.

**Challenges and Opportunities**

More than ever, intangible assets such as customers, systems and information form the foundation on which corporate value is built. In today’s highly competitive business environment, organizations are placing increased emphasis on customer relationship management as a means of gaining market share and differentiating service quality. Customers want choices and ease of access, which requires them to provide personal information and preferences; businesses want to be able to gather, data mine and share this information efficiently.

Certain industries, such as financial services and healthcare, often draw the most attention in the privacy discussion because of the personal information they possess. However, all industries are affected by privacy and data protection requirements.

Protecting sensitive information is, in fact, one objective that governments and businesses share. Many industry associations, such as the Payment Card Industry (PCI), the Healthcare Information Trust Alliance (HITRUST), Telecommunications Service Companies Privacy Regulation (Germany), Information Commissioners Office (United Kingdom), and Privacy and Electronic Communications Regulations (United Kingdom), have issued their own standards to supplement existing laws and regulations.

Given the risks and related requirements, ensuring the privacy of customer information and protecting critical corporate data are “top-of-mind” issues for management teams. Most companies have developed and implemented privacy and data protection programs, yet many of these programs fall short for a variety of reasons, including a lack of understanding the risk landscape (legal, regulatory, etc.) related to information collection and transmission, inadequate organizational policies, insufficient training, and unverified third-party providers, among many others.

**Our Point of View**

Organizations seeking to build and maintain an effective and compliant privacy and data protection program should undertake the following activities:

- Conduct a comprehensive risk assessment that, among other considerations, identifies the nature of information collected, where it is stored, how and where it is transmitted, and the laws, regulations and standards that govern handling of the information. It is important to note that the risk assessment process can be especially challenging for large global organizations that have a multitude of systems and must consider the impact of myriad, and sometimes conflicting, laws and regulations.

- Establish privacy and data protection policies that are monitored and enforced continuously within the organization.

- Ensure there is clear organizational accountability for privacy and data protection, as well as strong coordination among key players—compliance, information technology, security, business lines and internal audit, among other process owners.

- Implement comprehensive training and build employee awareness of risks, particularly what is expected of each employee to protect the organization.
About Protiviti

Protiviti is a global business consulting and internal audit firm composed of experts specializing in risk, advisory and transaction services. The firm helps solve problems in finance and transactions, operations, technology, litigation, governance, risk, and compliance. Protiviti's highly trained, results-oriented professionals provide a unique perspective on a wide range of critical business issues for clients in the Americas, Asia-Pacific, Europe and the Middle East.

Protiviti has more than 60 locations worldwide and is a wholly owned subsidiary of Robert Half International Inc. (NYSE symbol: RHI). Founded in 1948, Robert Half International is a member of the S&P 500 index.

PROVEN DELIVERY

How We Help Companies Succeed

Protiviti’s Global Privacy and Security team understands the inherent risks our clients face and the challenges they encounter in developing and maintaining effective privacy and data protection programs. Drawing on our skills and experience in regulatory compliance, business processes, technology, information security and communications, we assist our clients in building and sustaining privacy and data protection programs that address regulatory requirements and industry best practices.

We have worked with organizations around the world, helping them to:

- Understand the regulatory requirements and applicable industry guidelines.
- Identify and document risks.
- Design customized privacy and data protection programs.
- Develop and execute a plan for optimal implementation of a privacy and data protection program, including initial and ongoing employee training and awareness initiatives.
- Ensure sustainability and effectiveness of the privacy and data protection program through monitoring and testing.

Example

For a leading global IT consulting company with teams deployed on client projects around the world, Protiviti facilitated the implementation of an improved global privacy management framework by assisting with the design and implementation of a repeatable privacy assessment process.

Our privacy impact assessments (PIAs) considered where data was held, transferred and processed; whether existing processes and policies were in line with applicable laws and regulations, including data transfer regulations (e.g., U.K. to U.S. data transfer using the Safe Harbor scheme); and identified gaps between company practice and country regulations. Based on the results of the PIAs, we assisted with the design of an enhanced program.

We tailored our methodology and approach to the firm’s specific business model and risk profile. Coordinated teams in the United Kingdom and United States were used to perform PIAs and leverage knowledge of data privacy regulations in both countries.

Business benefits the client experienced included a consistent and repeatable approach to data privacy management around the world. The client achieved a reduction in data breaches and wider awareness of privacy and data protection issues among client staff.

Contacts

Carol Beaumier  
+1.212.603.8337  
carol.beaumier@protiviti.com

Cal Slemp  
+1.203.905.2926  
cal.slemp@protiviti.com

Ryan Rubin  
+44.207.389.0436  
ryan.rubin@protiviti.co.uk

© 2010 Protiviti Inc. An Equal Opportunity Employer. PRO-0110-107086

Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services.