Microsoft & Data Governance February 2009

Personal information shared over the Internet fuels a wealth of business activities, from processing credit card transactions on Web sites, to all kinds of services for individuals and individual-based communities. However, as organizations handle growing volumes of personal data and use it in more diverse ways, they also must contend with greater risks of data leakage, theft and misuse.

Fortunately, research suggests that even relatively simple steps like improving communication between data handlers can substantially cut the risk of data breaches—the accidental exposure or outright theft of personal information. For example, a 2007 Ponemon Research study found that 74 percent of organizations with poor collaboration reported one or more data breaches in the preceding 24 months, but that number fell to 29 percent among those with adequate to excellent cooperation.

Data governance is the application of policies and processes designed to extract the maximum value from data held within an organization while also managing risks, enhancing privacy protection and ensuring that compliance requirements are met. Microsoft has developed a set of practices and a technology framework for data governance that are designed to be easy to adopt and implement by organizations of all sizes and types.

Background: The Threat Environment

As the collection and use of personal information become increasingly prevalent, widely publicized data breaches and growing public concerns about identity theft threaten to curtail the growth of online commerce and services. Organizations that fail to manage and protect personal information face considerable risks—including reputational damage, penalties and sanctions, lost market share and needless expense. The growing maze of privacy and data security laws—many of which overlap or even conflict—adds to these challenges.

In the 2007 Ponemon study, 50 percent of privacy and compliance professionals and 35 percent of information security professionals cited negligence and mistakes in data use and sharing as the top risks in their organization. At the same time, many IT managers are feeling pressure to reduce related costs and time spent by staff. With an effective data governance program, organizations can reduce risk and costs.

Guidance for Organizations

Examining how information flows through the organization, and how it is accessed by applications and users, can help organizations implement data governance. The phases of the information life cycle are:

* **Collect:** Asorganizations collect sensitive personal data, they must set appropriate privacy and compliance controls; adopt consistent standards and expectations with external partners; and give consumers choice and control in how their personal information is collected.
* **Data Storage:** The risk of data breaches increases when information is stored and exchanged, including on laptops and mobile devices. More aggressive and sophisticated storage controls are necessary.
* **Update:** Organizations shouldensure that only current, accurate data is maintained.
* **Process:** Tight control over who can access data, and for what purpose, is essential.
* **Delete:** The lifespan for sensitive data should be finite and policies for its automatic deletion or secure archival should be enforced.
* **Transfer:** Data used to run reports, transferred to third parties for processing, or exported for long-term backup or retention, need the same privacy and integrity as the original dataset.

Technology Framework for Managing and Protecting Personal Information

An effective technology-based framework for data governance can help organizations protect and manage personal information, mitigate risk, achieve compliance, and promote trust and accountability. Key elements of this framework include the following:

* **Secure Infrastructure.** Microsoft builds products and services from the ground up with security and privacy in mind, and which can be updated to continually protect against evolving threats.
* **Identity and Access Control.** Microsoft offers authentication and authorization technologies that help prevent unauthorized access to information while seamlessly facilitating its availability to legitimate users.
* **Information Protection.** Microsoft products include data encryption and rights management technologies that help safeguard information against data breaches resulting from loss or theft.
* **Auditing and Reporting.** Microsoft provides a set of products that can be used to verify that systems and controls are operating effectively and identify suspicious or noncompliant activity.

Strengthening compliance and compliance controls is one possible objective for an enterprise’s data governance strategy. By leveraging the elements above described, organizations can also reduce storage and maintenance costs, and leverage the knowledge of the company’s data use, data flows and data lifecycle that they acquire to attain goals related to data quality, Data Warehouse implementation and Business Intelligence. Thus, data governance can also become a catalyst for increased profits.

*For more information on Microsoft’s work in computer security, privacy, and online safety, please visit: www.microsoft.com/mscorp/twc*