Microsoft & Data Breach Notification, Enterprise February 2009

Organizations are increasingly inviting customers to share personal information that can be used for a variety of beneficial purposes, such as improving services and delivering more personalized user experiences. However, as the volume of collected information grows, so does the risk of a breach involving loss or theft of data. Organizations that embrace the concepts of *data governance* can reduce the risk of incurring a data breach and minimize the harm when such incidents occur. Data breaches not only put customers at risk of fraud and identity theft, but also can expose the affected organization to a damaged reputation, financial penalties and loss of market share.

In response to rising concerns among individuals about privacy threats to their personal information, governments at all levels are examining the need for new and evolving laws regarding data breach notification. Some instances of this legislation require organizations to notify their customers whenever a data breach occurs and there is reasonable suspicion that personal information has been acquired by an unauthorized party; others require notification only when there is significant risk that personal information involved in a data breach will be used to harm individuals.

Data Breach Risks and Concerns

Recent, well-publicized instances of data breaches have intensified public concern about the resulting risks such as fraud and identity theft. According to DataLossDB (http://datalossdb.org/), a nonprofit group that tracks data breach incidents using public information, at least 162 million records containing personal information were compromised worldwide in 2007, an increase from 49 million records in the previous year. The actual number could be significantly higher. A 2008 InformationWeek survey of 1,100 IT and business professionals found 66 percent felt that they were as vulnerable, or more vulnerable, to breaches and malicious attacks than the year before.

For consumers, a data breach can result in several potential dangers. If financial information is compromised, the consumer might endure financial loss arising from fraud. Although such losses are often absorbed by financial institutions or retailers while the consumer’s financial account is reimbursed, victims may still face problems with paying their bills, clearing checks and undoing damage to their credit reports. Moreover, losses borne by financial institutions and retailers are eventually passed to consumers in the form of increased fees and surcharges, and higher prices for goods and services.

Guidance for Organizations: Responding to a Data Breach

Microsoft recommends that companies choose and implement data security and privacy policies in the context of a comprehensive Data Governance strategy as part of their overall Governance, Risk and Compliance (GRC) strategy. This strategy will comprise policies, procedures and standards that will enable effective use of the organization’s structured and unstructured data:

* To improve business decision making due to increased data accuracy.
* Reduce data redundancy and related maintenance costs.
* Comply with laws and regulations.
* Reduce exposure of the company’s data to loss or theft.

In addition to the above described preemptive measures, organizations should have a breach notification response plan in place and tested before it is needed. Large organizations that do business in many different locales will likely have to conform to a complicated mixture of breach notification laws. Rather than trying to enact specific notification practices in every locale, organizations may find it simpler to uniformly adhere to the most stringent applicable requirements wherever possible.

Upon detecting a breach, an organization should:

1. **Determine what personal information was compromised.** This is essential to assessing the severity of the data breach and notifying those affected.
2. **Identify mitigating circumstances.** Personal information that is lost or stolen might not actually be compromised if, for example, the data was protected using strong data encryption technologies.
3. **Notify law enforcement.** Investigators may be able to apprehend the culprits before they can use the compromised personal information or commit additional crimes.
4. **Secure affected systems and networks.** Once a data breach has been confirmed, take swift action to prevent further theft or loss of personal information.
5. **Notify affected businesses.** If financial information was breached, organizations should notify banks, credit card issuers and other affected institutions. Once notified, these businesses can take steps to limit potential financial loss to themselves and to retailers.
6. **Notify individuals whose personal information was compromised.** Organizations should notify individuals as soon as possible, but only after law enforcement officials confirm that notification will not compromise their investigation. The notice should clearly describe the following:

* What the organization knows about the data breach and how it occurred.
* What personal information was compromised.
* Steps the organization is taking to help prevent a recurrence.
* How affected customers can minimize risks of financial loss or identity theft.
* How to contact law enforcement to report losses or crimes arising from the breach.

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