Microsoft & Data Breach Notification November 2008



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 citizens 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

Organizations that respond quickly to a data breach can help protect their customers from the most severe consequences. Upon detecting a breach, an organization should respond in a timely and careful fashion.

1. **Determine what personal information was compromised,** in order to assess the severity of the data breach and notify those affected.
2. **Identify mitigating circumstances,** such as whether the lost or stolenpersonal information might have been protected using strong data encryption technologies, or whether a laptop computer thief might have chosen to wipe the hard drive clean.
3. **Secure affected systems and networks** to prevent further theft or loss of personal information.
4. **Notify law enforcement** to give investigators a better chance of catching the suspects before they use the compromised personal information to commit additional crimes.
5. **Notify affected businesses** such as banks and credit card issuers so they can cancel and reopen accounts, increase monitoring for signs of fraud, and limit potential financial losses.
6. **Notify affected individuals** as soon as possible after law enforcement officials confirm that notification will not compromise their investigation. The notice should clearly describe how the data breach occurred, what personal information was compromised,steps the organization is taking to help prevent a recurrence, how affected customers can minimize their risks of financial loss or identity theft, andhow to contact law enforcement to report losses or crimes arising from the breach.

Guidance for Governments: Data Breach Legislation

Data breach notification laws usually take one of two forms: acquisition-based trigger legislation and risk-based trigger legislation.

Acquisition-based trigger legislation requires an organization to notify affected individuals whenever personal information has—or can reasonably be assumed to have been—acquired by an unauthorized person. By contrast, risk-based trigger legislation requires an organization to notify affected individuals only when a significant potential risk is identified.

With acquisition-based trigger legislation, a potential unintended consequence is that consumers receive notices that their personal information may be at risk, even when an organization has no clear evidence of such a risk. While consumers may initially respond with appropriate diligence, over time they may begin to ignore such notices and potentially be exposed to significant harm.

With risk-based trigger legislation, the criteria for risk assessment vary. In some cases, risk is determined by the number of individual records involved in the data breach; in others, it is determined by how many different pieces of personal information were involved. As a result, some consumers at risk of fraud or identity theft may never receive a notice.

Governments can balance the interests of consumers with the needs of organizations, and avoid excessive notification of data breaches, by introducing legislation at the federal level that includes:

* An acquisition-based trigger of notification when data containing personal information is acquired by an unauthorized person and a significant risk of fraud or identity theft can reasonably be inferred
* A requirement to notify affected individuals within a reasonable time period, unless directed otherwise by a law enforcement agency while it is pursuing an investigation
* A timeframe of at least 45 days in which organizations can investigate the scope of a data breach, and take steps to prevent a recurrence by securing their systems and networks, before the organization is required to notify consumers.

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