February 2013

Data Breach Notification

Key Points

- Data breaches put consumers at risk of fraud and identity theft, and jeopardize the relationship between consumers and historically trusted organizations or government infrastructures.

- Because Microsoft is committed to helping create safer, more trusted computing experiences, it is dedicated to protecting sensitive data and personal information. It recommends a multifaceted approach to data governance that includes policy, people, processes, and technology. Microsoft's approach relies on creating or maintaining more secure infrastructure; identity and access control; protecting information; and auditing and reporting.

- Microsoft supports legislation for notification of data breaches that includes a risk-based trigger of notification when data containing personal information is acquired by an unauthorized person, and when there is a significant risk of fraud or identity theft. Notification should not be required where the potential of harm is nominal. However, the law should require that affected individuals be notified within a reasonable time period unless otherwise directed by a law enforcement agency pursuing an investigation.

BACKGROUND

In recent years, media reports of data breaches at major public and private institutions have captured both headlines and public attention, especially when they jeopardized the sensitive personal or financial information of millions. Data breaches not only put consumers at risk of fraud and identity theft, but also threaten their trust of reputable organizations and governments.

Governments at all levels are examining the need to revise data breach notification laws. Current laws typically require companies or agencies to notify customers when their personal data has been put at risk or compromised, and take one of two forms: an acquisition-based trigger or a risk-based trigger.

Acquisition-based triggers require organizations to notify affected individuals when personal information has, or can reasonably be assumed to have been, acquired by an unauthorized person. In contrast, risk-based triggers require organizations to notify affected individuals when a significant potential risk has been identified.

As policymakers develop new policies governing the notification of data breaches, it is worth noting that in some jurisdictions, organizations are exempt from certain disclosure requirements if their data is encrypted at the time of a security breach. This exemption is a powerful motivator for companies to adopt encryption methods and procedures for protecting sensitive data. In addition, organizations that embrace key concepts of data governance can reduce the risk of data breaches and develop effective plans to address security issues when they do occur.

MICROSOFT APPROACH

Microsoft recommends a multifaceted approach to data governance that includes policy, people, processes, and technology. Its approach relies on:

- Strengthened infrastructure with safeguards that help protect systems from malware, intrusions, and unauthorized access to personal information.
- Identity and access control with systems that help protect personal information from unauthorized access or use, and provide management controls for identity access and provisioning.
- Securing sensitive personal information in structured databases and providing safeguards such as encryption for unstructured documents, messages, and records.
- Auditing and reporting on the integrity of systems and data in compliance with business policies.

POLICY CONSIDERATIONS

- Conflicting laws can complicate compliance across local, state, provincial, or national borders. The wide variance in rules, regulations, and laws threatens to impede economic progress and stifle innovation. In countries such as the United States with multiple state laws, Microsoft supports broad federal preemption as part of any comprehensive privacy legislation. Policymakers, industry, and organizations need to collaborate to develop a mutually agreeable solution that protects both privacy and innovation.
- Microsoft supports data breach notification laws that include:
  - » A risk-based trigger of notification when an unauthorized person acquires data, but only when there is a significant risk of fraud or identity theft.
  - » No requirement of notification when the potential harm to the data subject is nominal, such as where information is encrypted or otherwise unintelligible.
  - » A requirement to notify those affected within a reasonable time period, unless otherwise directed by law enforcement pursuing an investigation.
- While Microsoft supports requirements of mandatory notification when data breaches occur, these requirements should be calibrated to provide timely, meaningful information to consumers. Notification mandates with very short time frames run the risk of giving consumers inaccurate or incomplete information. Broad notification requirements that include all data breaches, even where the risk of harm is negligible, run the risk of flooding consumers with notices that will be ignored.

Helpful Resources

An overview of Microsoft privacy policies and initiatives
www.microsoft.com/privacy