

Data Masking: Counter-attack to Internal Data Theft

by Stephanie King, B. Comm

Stephanie King is a research analyst with Plato. On behalf of Plato, Ian Turnbull, executive director of the Canadian Privacy Institute, will present RT-1: "Data Masking: Countering Internal Data Theft" at 10:30 a.m. Monday.

In today's technology-driven economy, organizations are collecting, storing and distributing vast amounts of information such as employee, customer, financial and supplier data. One 2007 study highlighted this increase in electronic data capture indicating that 988 exabytes, almost one zettabyte, of digital information will be created by 2010. This projected growth in digital information emphasizes the need to ensure the privacy of personally identifiable information—one of organizations' most valuable assets.

In addition to the growth in electronic data capture, several factors have combined to heighten worldwide awareness on the importance of data privacy. Some of the most significant factors include increases in: data theft, privacy legislation and regulations, individuals' concern for data privacy and the trends towards data sharing and outsourcing.

Data Theft

According to the Privacy Rights Clearinghouse, there have been more than 500 reported data breaches since 2005 that have affected more than 150 million records. Furthermore, one 2006 survey found that nearly 80 to 90 percent of Fortune 500 companies and government agencies have experienced security breaches.

Organizations that have experienced data theft are often subject to a variety of penalties such as legal fines, increased business expenditures and civil litigation. The Ponemon Institute 2006 Annual Study: "Cost of a Data Breach" reported that the cost to recover from a disclosure of sensitive information averaged \$4.7 million, or \$182 per record, with some companies experiencing damages of upwards of \$22 million US. The negative publicity surrounding a

data breach often tarnishes an organization's reputation and brand image, both of which are particularly difficult to overcome.

Legislative Environment

The recent increase in high-profile data breaches has prompted the establishment of new and stringent data privacy legislation and regulations that require organizations to protect sensitive information. The development of new privacy legislation is reinforcing the importance of adopting security measures to ensure the protection of organizational information at all stages of the data management lifecycle. Ernst and Young International's global study in 2006 reported that compliance with the latest international privacy legislation remains the most important factor driving information security practices.

The United States is often considered the leader in the development of privacy legislation and regulations with the establishment of such well-recognized laws including:

- Gramm-Leach-Bliley Act (GLB)
- Health Insurance Portability and Accountability Act (HIPAA)
- PCI Data Security Standard (DSS)
- Sarbanes-Oxley Act (SOX)
- The Privacy Act

In addition, many state laws require organizations to disclose any infringement of personally identifiable information to those individuals affected by the privacy violation. According to the Canadian Internet Policy and Public Interest Clinic, as of December 2006, 34 states had approved security breach notification laws.

The adoption of such privacy legislation is not limited to the United States. Several other countries have established privacy regulations, some of the most notable including:

- Canada Privacy Act
- Canadian Personal Information Protection and Electronic Documents Act (PIPEDA)
- European Union Privacy Act (EUPA)
- European Union Personal Data Protection Directive 1998
- United Kingdom Data Protection Act of 1998
- Australian Privacy Act 1988 (Privacy Amendment Act of 2000)
- Japanese Personal Information Act 2003 (JPIPA)
- Hong Kong Personal Data Ordinance of 1995

Privacy Concerns

As the number of data breaches continues to rise, individuals are becoming more hesitant to provide personal data that is required for organizations to perform their business activities. For example, a study conducted by the Ponemon Institute stated that 58 percent of Americans communicated a decrease in their level of trust and confidence in organizations that experienced data theft. This ongoing concern has forced many organizations to adopt internal security policies and requirements to help mitigate individuals' privacy concerns.

Data Sharing, Outsourcing and Offshoring

Developments in computer and Internet technologies have fueled growth in data sharing. When data is shared, control over sensitive information is often lost, creating a heightened risk of data theft.

Outsourcing and offshoring have also become common practices designed to improve organizational efficiency. According to researchers, the global market for IT outsourcing will exceed \$50 billion by the end of 2007. Not only has the market for offshoring and outsourcing grown, but research indicates that the majority of Americans are apprehensive about organizations sharing their personal information. One 2006 study reported that 83 percent of Americans are concerned with the process of sharing personal information through offshoring and outsourcing activities. As organizations continue to outsource a multitude of activities, the risk for data exposure significantly increases.

Internal Data Protection

Given the significant increase in data privacy awareness, the need for improved data protection is critical. While organizations have been focused primarily on protecting sensitive data from external theft, researchers currently estimate that 70 to 80 percent of all security incidents come from insiders. In fact, one 2006 study stated that 35 percent of IT professionals have abused their computer security and information access privileges in an attempt to access proprietary data.

The focus of many organizations and government agencies has been to secure production data stored and used in IT systems across networks; however they are now realizing the importance of protecting data while it is stored and used outside production environments. Once sensitive data is exposed to individuals in non-production environments for such activities as software development, application testing, quality assurance, training and data mining, etc., the potential for internal data theft greatly increases.

The increase in internal attacks on IT systems has created the need for additional controls beyond the use of firewalls, passwords and encryption. Firewalls and passwords protect the perimeter of the data, however, once inside, data thieves typically have full access to sensitive information. While encryption is useful for protecting data in transmission and for disguising real information, it also renders it unrealistic and unusable for use in non-production environments. Coupled with a heightened awareness in data privacy, worldwide legislation is now forcing organizations to ensure total data protection across the enterprise, whether the data resides in production or non-production databases.

Data Masking Defined

Researchers currently estimate that 45 percent of organizations use live production data in non-production environments for such activities as software development, application testing, quality assurance, training, data mining/research, offshoring and outsourcing. The use of sensitive data for such activities is often strictly prohibited by privacy legislation, as well as by organizations' internal privacy policies. With the increase in internal data theft, organizations must now enforce