Managing and Protecting Personal Information

A Microsoft Perspective on Data Governance  
for Privacy and Compliance

footer bar.jpg

Microsoft **TwC**

Trustworthy Computing

The information contained in this document represents the current view of Microsoft Corp. on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This white paper is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording or otherwise), or for any purpose, without the express written permission of Microsoft.

Microsoft may have patents, patent applications, trademarks, copyrights or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights or other intellectual property.

© 2008 Microsoft Corp. All rights reserved.

Microsoft, Active Directory, BitLocker, Forefront, Internet Explorer, OneCare, SharePoint, SQL Server, Visual Studio, Windows, Windows CardSpace, Windows Live, Windows Mobile, Windows Server and Windows Vista are either registered trademarks or trademarks of Microsoft Corp. in the United States and/or other countries. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Microsoft Corp. • One Microsoft Way • Redmond, WA 98052-6399 • USA

Contents

Executive Summary 1

The Landscape 2

A Patchwork of Laws 3

Value Creation Is the True Goal of Secure Data Governance 5

The Data Governance Life Cycle 6

A Technology Framework for Data Governance 8

Identity and Access Control 13

Auditing and Reporting 19

Principle-Based Application of the Technology Framework 20

Conclusion 20

Executive Summary

As the collection and use of personal information become increasingly prevalent, widely publicized security and data breaches and growing concerns about identity theft threaten to erode public confidence in online commerce and government services. They also pose risks for organizations that fail to manage and protect their customers’ personal information. These concerns accentuate the need for a multifaceted approach to data governance that involves a combination of people, processes and technology solutions.

This paper focuses on the important role technology plays in helping organizations responsibly protect and manage personal information, mitigate risk, achieve compliance, and promote trust and accountability. It describes a governance life cycle for private data; the four elements of an effective technology-based framework, including a secure infrastructure, identity and access control, information protection, and auditing and reporting; and a principle-based approach to applying this framework. The paper also includes information about Microsoft technologies that align with this framework and examples of how organizations can use these technologies to manage and protect personal information.

The Landscape

In the past three decades, information and communications technology (ICT) has transformed the global economy—enabling private enterprises, public-sector organizations and hundreds of millions of individual workers to achieve unprecedented benefits. Greater productivity, more efficient internal processes and new ways of collaborating within organizations and with partners and customers are helping companies of all sizes to compete more effectively in fast-paced global markets. And governments are taking advantage of these advances to improve the efficiency of their operations and deliver services more effectively to citizens.

Among the keys to this transformation has been the digitization and flow of personal information over the Internet, which supports rapid information gathering, intelligent analysis, expanded sales and service channels, and more innovative approaches to organizational challenges. But as organizations and individuals have increased their reliance on Web-enabled ICT as an integral part of their business activities, more risks have emerged and the stakes have become higher in the effort to protect privacy and security of information. As organizations handle growing volumes of personal data and use it in more diverse ways to fulfill their goals, they also face a greater responsibility to adequately protect the privacy and integrity of this data.

Consumers, business leaders, government policymakers and privacy advocates are calling for more effective policies, processes and technologies to protect and manage the personal information entrusted to organizations. These organizations must balance the desire to optimize the transparency, flow, utility and value of this information with the responsibility to safeguard it from leaks and misuse.

Meanwhile, widely publicized security and data breaches and rising consumer anxiety about identity theft and the privacy of personal information are eroding public trust in the Internet and threatening to dampen online services and commerce. These real and perceived threats also have the potential to seriously hinder organizations’ competitiveness and damage their reputation.

Another issue of growing concern is data breaches involving the loss, theft or misuse of personal information. From January 2005 through December 2007, more than 211 million records containing sensitive personal information were compromised by security breaches in the United States alone.[[1]](#footnote-2) According to Attrition.org, a nonprofit group that tracks data breach incidents, at least 162 million records containing personal data were compromised worldwide in 2007, compared to 49 million the previous year.[[2]](#footnote-3) And in November 2007, the UK tax agency Her Majesty’s Revenue and Customs disclosed that it had lost computer disks containing the records of 25 million UK residents—about 40 percent of the population—including confidential information such as names, addresses, dates of birth and bank account data. While this was among the more dramatic incidents of compromised data in recent months, such reports are growing increasingly common throughout the world.

In response to these trends, organizational leaders have put higher expectations on their IT departments to safeguard the data that is stored, exchanged and processed by the organization’s technology framework. At the same time, many IT managers are also feeling pressure to reduce costs and staff time associated with these tasks.

Privacy and Data Protection   
at Microsoft

Microsoft’s commitment starts with the people, policies and processes that make privacy and data protection an integral part of the company’s business practices and corporate environment.

**Privacy staffing**. Organizationally, Microsoft implements its privacy goals through three levels of privacy-related staffing. The Microsoft Corporate Privacy Group manages the development and implementation of programs that enhance the privacy of Microsoft products, services, processes and systems. Many of the company’s business units have dedicated full-time privacy staff, and several hundred other employees are responsible for helping ensure that privacy policies, procedures and technologies are applied within the product groups and subsidiaries in which they work.

**Privacy policy.** The foundation of Microsoft’s approach to privacy and data protection is a belief that individuals should be empowered to control the collection, use and distribution of their personal information. Microsoft’s corporate privacy policy incorporates 10 principles that apply to the collection and use of all customer and partner information, including accountability, notice, collection, choice and consent, use and retention, disclosure, quality, access, security and monitoring, and enforcement. This p0licy provides business units and employees with a clear and simple framework to help ensure privacy compliance companywide.

**Privacy guidelines.** Microsoft also has adopted discipline-specific privacy guidelines. For example, the Microsoft Privacy Guidelines for Development establish a framework to help ensure that customer privacy and data protections are systematically incorporated into the development and deployment of Microsoft’s products and services.

A Patchwork of Laws

In addition to being accountable for managing personal information in a manner that complies with internal policies and aligns with customer expectations, organizations must navigate a growing maze of regional, national and local privacy and data security laws that often overlap or even conflict.

In principle, many governments and regional organizations around the world have affirmed their commitment to privacy laws that do not unnecessarily impede international trade and e-commerce. Nonetheless, these divergent approaches to privacy protections continue to create a significant amount of friction in the data flows between—and even within—nations and regions. Activities that may be perfectly legal and commonplace in one part of the world may be prohibited elsewhere, creating confusion for organizations and consumers alike and often adding to the cost of doing business globally.

In the European Union, for example, individual privacy is described as a “fundamental” right.[[3]](#footnote-4) And the European Commission’s Directive on Data Protection imposes limits on the transfer of personal data to nations outside the EU that do not meet their “adequacy” standards for privacy protection.

Many U.S. states have enacted their own privacy laws to govern specific industries, issues or practices, and a growing number also have data breach notification laws in place. In addition, an array of federal laws impose rules for financial institutions, healthcare providers, cable operators and telecommunications carriers; and for children’s online privacy, spam, phishing and telemarketing.

Then there is the proposed Asia-Pacific Economic Cooperation (APEC) Privacy Framework, which starts from the principle that information flows between countries are crucial to trade and economic development. It reflects the region’s commitment to balancing privacy protections with the need to avoid creating unnecessary barriers to the flow of commercial data.

The complexity is even greater in closely regulated industries such as financial services and healthcare, where a company’s best intentions in seeking to establish and follow sound internal business processes may inadvertently conflict with regulations in one or more countries where it operates. Even a beneficial and seemingly harmless activity such as transmitting employees’ performance bonus awards from a company’s European sales office to the U.S. headquarters could run afoul of EU laws that block transfers of personal data beyond EU countries’ borders.

Organizations are left with the daunting and increasingly expensive task of determining which rules apply to their activities, what constitutes a conflict and how to address it. The answers to these questions can be complex: It depends on the type of data involved, the kind of company that collects it, where and how it is collected, and how it might be used.

Consider the challenges facing a consumer goods manufacturer, such as a tire company, that sells products in multiple countries and must collect personally identifiable information (PII) about its customers to administer a warranty program. While storing the information centrally on data servers in India may the most cost-efficient option for this company, doing so could run afoul of EU regulations—particularly if the data is managed by an outsourcing services company whose security and privacy policies cannot be directly controlled and assured by the tire manufacturer. Creating a separate data center in each country can be unwieldy and cost-prohibitive, while conforming to the highest common denominator of privacy and security legislation across all countries can prove to be overly restrictive.

This scenario illustrates some of the intricacies involved in achieving persistent, compliant protection of sensitive information without diminishing its business value for communication, collaboration and commerce.

Value Creation Is the True Goal of Secure Data Governance

As enterprises and governments handle growing volumes of information about individuals, as evolving business models create and rely on greater use of such personal data, and as citizens and policymakers demand more accountability and better protections for individuals, organizations are increasingly looking for ways to manage—or “govern”—data in their possession in such a way that the organization’s goals for protection and value generation are simultaneously achieved. A recent Gartner research survey found that IT professionals who identified security as their highest-priority research topic in 2007 rated risk assessment and management as the most pressing issue overall.[[4]](#footnote-5) Similarly, an April 2007 survey of 30 security and risk managers attending the Forrester Research Security Forum EMEA found that policy and compliance received the highest average rating when respondents were asked to rank their most important responsibilities.[[5]](#footnote-6)

In addition to complying with the regulations increasingly being imposed by the public sector, data governance also involves the management of personal information in a manner that supports an organization’s mission, complies with its own policies and aligns with customer expectations.

However, focusing on compliance and compliance controls is just one of several potential data governance objectives. For many organizations, great opportunities lie in realizing competitive or mission-related advantages other than risk reduction—advantages that can be drawn from governance investments to achieve broader organizational benefits.

Many of the controls necessary to meet compliance requirements may double as operational and financial controls that a savvy manager can employ to improve overall organizational performance. For example, restrictions on the retention of private information that prompt the organization to enact data-aging and purging compliance controls could also lead to reduced storage and maintenance costs—thereby creating higher profits for businesses and opportunities for public-sector organizations to improve services to citizens.[[6]](#footnote-7)

When approached in this way, effective data governance becomes not just a necessary expense but rather a source of organizational value.

The Data Governance Life Cycle

Trustworthy Computing

In 2002, Microsoft Chairman Bill Gates signaled a dramatic shift in the company’s strategy: He made providing a secure, private and reliable computing experience for everyone a top company priority. More than five years later, Trustworthy Computing continues to infuse the company’s efforts to enhance privacy and safety, security and reliability across all of its products.

Microsoft’s commitment to ensuring a trustworthy computing ecosystem has three main areas of focus: technology investments and innovation, leadership and collaboration, and customer guidance and engagement.

**Technology investments and innovation:** Microsoft has changed the way it develops software, incorporating security and privacy checkpoints throughout the product development life cycle. To protect against evolving security threats, the company is building technologies that provide layered defenses against malware, spam, spyware and phishing attacks—to name a few. We’ve also made important strides in providing easy-to-use services and tools that help customers configure their systems correctly and keep them up to date.

**Leadership and collaboration:** Microsoft works with others in industry, business and government to combat privacy threats and promote best practices. These efforts include formal legal actions and support for law enforcement against spammers and phishers, advocacy for comprehensive privacy legislation, and leadership on a variety of industry-driven privacy initiatives.

**Customer guidance and engagement:** With the understanding that people who use technology also play a vital role in securing the overall computing ecosystem, Microsoft actively engages with customers to help them understand their rights and make educated choices when sharing personal information. For example, Microsoft introduced a “short-layered” privacy notice for many of its online services, providing a clear, concise one-page summary of the company’s online privacy practices.

Examining how information flows throughout an organization over time, and how it is being accessed by multiple applications and people for various purposes, will clarify the various areas where the organization should deploy technologies to protect private information. This cycle comprises four key stages, within which an organization can construct many unique data governance scenarios to address specific considerations.

Collection

Most modern organizations take in sensitive personal data from multiple sources—in person, by mail, online—and must establish appropriate controls that uniformly assure privacy policy compliance regardless of collection method. This involves setting consistent standards and expectations in contracts with external partners that receive or manage the information, as well as addressing consumers’ desire for greater choice and control in how their personal information is collected. It also requires the organization to consider how these policies will be honored throughout the lifespan of the data.

Storage

While protecting data stored only in a database is relatively straightforward, the task is far more complex as personal information scatters within and between organizations in unstructured forms such as e-mail, spreadsheets and text documents. As data in these forms is increasingly being stored on laptops and mobile devices, the risk of data breaches has risen sharply—which in turn may require organizations to implement more aggressive and sophisticated storage controls.

Usage

As information becomes increasingly fluid, it is also subject to access by multiple applications and people—including many that are outside the organization as a byproduct of outsourcing agreements and partnerships. In this environment, ensuring that only the right people can gain access to this data and enforcing strict limits on their ability to take data outside the organization (such as on their laptops) are crucial considerations.

Usage also results in new data describing how the target data was used, when it was accessed, by whom and so on. This data represents a record of data use and is commonly called metadata. Importantly, all of the controls applied to the target data must also be applied to metadata.

Retention and Destruction

Data storage is becoming cheaper every day, to the point where many organizations have found that the time involved in deciding which records to delete from their systems is more costly than simply retaining it all. However, this practice does not account for the liabilities associated with holding onto sensitive personal and confidential information after it has outlived its usefulness. Viewed from the standpoint of minimizing an organization’s exposure to risk from a data breach, the effort involved in setting a finite lifespan for sensitive data and enforcing policies for its automatic deletion or secure archival is a worthwhile investment.

A Technology Framework for Data Governance

A multifaceted approach to data governance involves a combination of policy, people, processes and technology. The risks and problems that may arise when data governance practices aren’t cohesive can be seen in the results of a 2007 research study by Ponemon Institute LLC.[[7]](#footnote-8) The study, conducted in the United States, the UK and Germany, found that:

* **Collaboration is key to reducing the risk of a compromise or breach of personal information.** Seventy-four percent of those organizations indicating that collaboration among their security and privacy professionals was poor reported one or more data breaches in the preceding 24 months, compared to 29 percent of those indicating that their collaboration was adequate to excellent.
* **People who collect and use data don’t often consult with security and privacy professionals.** Although 78 percent of security and privacy professionals believe they are regularly consulted by marketing colleagues on the collection and use of data, only 30 percent of marketers said they actually did so.
* **Individuals responsible for safeguarding data do not share the same views as the people who collect and use data.** Fifty-nine percent of privacy and compliance practitioners and 53 percent of security practitioners believe that the safeguarding of personal information is well coordinated within their organizations. In contrast, only 32 percent of people who collect and use data believe this to be true.
* **Security and privacy professionals believe negligence in data use and sharing is the biggest threat to data protection practices.** Fifty 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.

|  |  |
| --- | --- |
| A Framework for Managing and Protecting Personal Information | |
| Need to do | How to do it |
| More secure infrastructure | Safeguards that protect against malware, intrusions and unauthorized access to personal information and protect systems from evolving threats |
| Identity and access control | Systems that help protect personal information from unauthorized access or use and provide management controls for identity access and provisioning |
| Information protection | Protecting sensitive personal information in structured databases and unstructured documents, messages and records by means such as encryption so that only authorized parties can view or change it throughout its life cycle |
| Auditing and reporting | Monitoring to verify the integrity of systems and data in compliance with business policies |
|  |  |

Technology has a key role in enabling organizations to implement effective data governance processes, policies, and compliance with business practices and regulations.

An effective technology-based framework needs four essential elements to responsibly protect and manage personal information, mitigate risk, achieve compliance, and promote trust and accountability.

Microsoft is committed to delivering technology advances that help organizations protect and manage important personal information. The following sections more closely examine the four elements of this technology framework, describe some of the technologies and capabilities within Microsoft products that support each one, and illustrate how they can be applied in common scenarios. While these scenarios use the example of a fictitious financial services company, Contoso Bank, the underlying privacy requirements and considerations are essentially the same for public-sector organizations.

Secure Infrastructure

The growing importance of information and communications technologies to the way we work and live underscores the need to ensure that the underlying infrastructure is as secure as it can be. Fundamentally, safeguarding and managing sensitive information depends on a secure technology infrastructure that protects against malicious software and hacker intrusions.

To help prevent unauthorized disclosure, organizations should build their IT infrastructure using software that is designed for maximum security, and they should employ tools and services to continually protect against evolving threats.

Scenario**:** Contoso Bank is a midsize consumer bank with an IT infrastructure scattered across dozens of retail branches. It handles large amounts of sensitive customer data ranging from addresses and Social Security numbers to bank account numbers, investment records and employment information. Contoso also is responsible for managing personally identifiable information (PII) about its employees and contractors throughout the region.

The bank understands that the protection of personal information begins with a secure technology infrastructure. For basic security, it relies on the Microsoft® Windows® platform, including Windows Server® 2008, Windows Vista™ and Windows Mobile® 6.0. When initially building out its IT infrastructure, Contoso used the Microsoft Baseline Security Analyzer (MBSA) to determine its current level of security and identify areas that needed improvement. The company plans to deploy Microsoft Forefront™ across its IT infrastructure to help its small IT staff better manage a growing network of PCs, servers, laptops and mobile devices.

End-user security is of particular concern because many Contoso employees use company computers and mobile devices for personal business while away from home—potentially exposing the organization’s Windows-based PCs to malware from malicious Web sites. The company relies on the firewall in Windows Vista and the increased security capabilities of Microsoft Internet Explorer® and Windows Mobile 6.0 to protect against these threats. Contoso also takes advantage of User Account Control in Windows Vista to improve system stability and further protect against malicious attacks.

In addition, Contoso has built a number of custom applications to facilitate better customer service. Its developers apply the principles of the Microsoft Security Development Lifecycle (SDL) and companion Microsoft Privacy Standard for Development (MPSD) to ensure greater security in those applications for protecting the information that they handle.

Creating a more secure infrastructure starts with building products and services from the ground up with security in mind. Starting in 2003, Microsoft established a set of strong internal security design and development practices known as the Security Development Lifecycle (SDL). The SDL implements a rigorous process of secure design, coding, testing, review and response for all Microsoft products that are deployed in an enterprise setting, handle sensitive or personal information, or regularly communicate via the Internet. The SDL helps remove security vulnerabilities and minimize the “surface area” for malicious attacks. It also improves system and application integrity and helps organizations more securely manage their networks.

Microsoft also provides detailed guidance on the SDL for independent software developers and the worldwide security community to support their efforts to improve the security of their applications and services. In addition, Microsoft’s Visual Studio® development environment includes tools that help developers create more secure applications by checking for common code flaws and potential vulnerabilities. More information on the SDL is available at [*http://msdn2.microsoft.com/en-us/library/ms995349.aspx*](http://msdn2.microsoft.com/en-us/library/ms995349.aspx)*.*

In conjunction with the SDL, Microsoft has also implemented the Microsoft Privacy Standard for Development (MPSD). It offers guidance for creating notice and consent experiences, providing sufficient data security, maintaining data integrity, facilitating user access, and supplying controls when developing software products and Web sites. In October 2006, Microsoft published a version of the MPSD known as the Privacy Guidelines for Developing Solftware Products and Services at [*http://go.microsoft.com/fwlink/?LinkID=75045*](http://go.microsoft.com/fwlink/?LinkID=75045)*.*

Windows Vista is the first client operating system to be developed from start to finish using the SDL, and it advances all of the security enhancements delivered in Windows XP SP2. Windows Firewall is turned on by default, and Automatic Updates help ensure protection against new and evolving security threats. Security enhancements in Internet Explorer 7 include a pop-up blocker and improved notification and control over potentially harmful content. Windows Vista also provides a number of security enhancements to help end users protect their sensitive information, and it offers new ways for IT administrators to make their organizations’ networks more resistant to attack while preserving data confidentiality, integrity and availability. These include the following:

* Windows Vista User Account Control reduces security risks by limiting the privileges granted to standard users and granting administrative access only when needed (such as when installing new software or changing the system configuration). It gives typical users most of the capabilities they need for day-to-day work, while helping protect systems and networks from unauthorized tampering.
* Internet Explorer 7 in Windows Vista improves security for end users and reduces the risk of malicious attacks that could compromise sensitive data on corporate networks. For instance, Internet Explorer 7 can run in Protected Mode with reduced permissions, to help prevent user or system files or settings from changing without the user’s explicit permission. And the Internet Explorer 7 Phishing Filter and support for High Assurance SSL Certificates help reduce the risk of phishing attacks through its stronger identification of secure and reputable sites.
* Windows Service Hardening in Windows Vista restricts the capabilities and privileges of background system services to those necessary for them to function, reducing the chances that a malicious attack could compromise those services and damage or disclose sensitive data.
* Windows Vista also features security improvements for 64-bit systems. It helps prevent malicious software from making unauthorized modifications to the Windows “kernel,” reducing the risk of so-called “rootkit” attacks, and it improves security and system stability by requiring that all kernel-mode drivers be digitally signed.

More information is available in the Windows Vista Security Guide at [*http://technet.microsoft.com/en-us/bb629420.aspx*](http://technet.microsoft.com/en-us/bb629420.aspx)*.*

Small and midsize organizations can use the MBSA to determine their level of security in relation to Microsoft’s recommendations. This easy-to-use tool helps organizations reduce the complexity of their IT infrastructure by detecting common security misconfigurations and missing security updates, and by offering specific remediation guidance.

Security threats are constantly evolving, so software must also evolve to help keep users, their systems and their data secure. Microsoft, other companies and governments are constantly monitoring for new threats; Microsoft and the IT industry then fix vulnerabilities and get updates out to customers quickly. End users and small and midsize organizations can use Microsoft Update to keep their systems up to date, helping to ensure that malicious software cannot exploit unpatched or out-of-date machines, and that new threats can be more effectively countered.

Windows Server 2008 is the most secure version of this product ever released by Microsoft. Its hardened operating system and security innovations—including Network Access Protection, Federated Rights Management, and Read-Only Domain Controller—are designed to provide unprecedented levels of protection for organizational networks, data and business operations.

Windows Server 2008 helps protect against failure and unauthorized connections to an organization’s servers, networks, data and user accounts. Network Access Protection allows IT managers to isolate computers that don't comply with the organization's security policies, and it enables network restriction, remediation and ongoing compliance checking. Federated Rights Management Services provides persistent protection for sensitive data, helps reduce risks and support compliance, and provides a platform for comprehensive information protection. Its Read-Only Domain Controller and BitLocker™ Drive Encryption let the organization more securely deploy Active Directory® Domain Services while restricting replication of the full Active Directory database, to better protect against server theft, corruption or compromise of the system. Server and Domain Isolation (SDI), another new feature in Windows Server 2008, creates a logical separation of network devices based on policy. SDI limits access to network resources to trusted, managed PCs, thereby reducing the risk of network-borne security threats and safeguarding sensitive data.

For more information on Windows Server 2008 and its security capabilities, visit [*http://www.microsoft.com/windowsserver2008/default.mspx*](http://www.microsoft.com/windowsserver2008/default.mspx).

To help organizations maintain and enhance the security of their IT infrastructure, Microsoft has combined a number of security technologies into Microsoft Forefront. This comprehensive group of business security products provides greater protection and control through simplified deployment, management and analysis. It includes the following:

* **Forefront Client Security.** This product provides unified malware protection for business desktops, laptops and server operating systems. Built on the anti-virus and spam-filtering engines already in use by millions of people worldwide in products such as Microsoft Windows Live™ OneCare™, Microsoft Windows Defender, and Microsoft Windows Live Safety Center, it helps guard against traditional threats such as viruses, worms and Trojan horses, as well as emerging threats such as spyware and rootkits. It integrates with existing IT infrastructure, including Active Directory, and offers simpler administration through centralized management.
* **Forefront Security for Exchange Server.** Formerly called Microsoft Antigen for Exchange, this server-based anti-virus solution performs real-time scanning of inbound and outbound e-mail to provide comprehensive protection across Exchange Server 2003 and Exchange Server 2000 environments. It can be deployed on front-end or back-end Exchange servers, protecting against threats from outside the network as well as containing threats originated internally.
* **Forefront Security for SharePoint®.** Formerly called Antigen for SharePoint, this product helps organizations protect their SharePoint Portal Server and Windows SharePoint Services deployments against viruses, worms and inappropriate content. Using multiple anti-virus engines, it scans all documents as they are uploaded or retrieved from SharePoint document libraries. It also offers content-filtering capabilities that help prevent inadvertent or intentional posting of documents containing offensive language or other inappropriate content, as well as file types that potentially expose organizations to legal risk, such as MP3 audio files.
* **Antigen for Instant Messaging.** Antigen for Instant Messaging protects against viruses, malware and inappropriate content on Microsoft Office Live Communications Server. Using the same anti-virus engines as other Forefront products, it scans instant messages and file transfers for viruses and malware, as well as inappropriate content or unwanted file types, both within Live Communications Server and between it and public instant messaging (IM) clients.
* **Microsoft ISA Server 2006.** Internet Security and Acceleration Server (ISA Server) 2006 is an integrated edge security gateway designed to help organizations protect against Internet-based threats while giving users secure access to Microsoft applications and data. ISA Server 2006 helps secure an organization’s application infrastructure, streamline its networks and safeguard its IT environment with a packet- and application-layer firewall, virtual private networking, filtering for harmful content and a Web-caching solution.
* **Forefront code name “Stirling.”** This product combines unified security management and reporting capabilities with coordinated protection across clients, server applications and the network edge. Through its deep integration with the existing infrastructure, such as Active Directory and Microsoft System Center, “Stirling” enables customers to achieve a more secure and well-managed infrastructure with less complexity.

To facilitate private, secure transmission of sensitive information, Windows Server 2008, Windows XP, Windows 2000 and Windows Vista all include support for Internet Protocol security (IPsec). IPsec is also integrated with Active Directory, so its policies can be assigned through Group Policy settings at the domain, site or organizational unit level.

Identity and Access Control

All types of organizations must increasingly handle large amounts of confidential data, ranging from customers’ and citizens’ PII to extremely sensitive business documents. This data must be protected for competitive reasons, to defend personal privacy and to comply with an expanding range of laws, regulations and policies.

To reduce the risk of a deliberate or accidental data breach, and to help organizations comply with regulatory requirements, Microsoft offers identity and access control technologies that protect personal information from unauthorized access while seamlessly facilitating its availability to legitimate users. These include authentication mechanisms that verify a user’s identity to help ensure that only valid users can connect to an organization’s system; access controls that determine what resources and data each user is allowed to access; and provisioning systems and management technologies that help organizations manage user accounts across multiple systems and with partners they trust.

Scenario: Contoso Bank stores a vast amount of information about its customers, all of which must be handled in accordance with a number of privacy laws and Securities and Exchange Commission regulations. As a publicly traded corporation, the bank must also follow data retention, governance and disclosure policies in compliance with the Sarbanes-Oxley Act.

Contoso routinely hires college students as front-line customer service representatives and tellers who handle basic account services and inquiries. Employee turnover in this department is high, so Contoso uses Active Directory and Microsoft Identity Integration Server (MIIS) to quickly set up accounts for new employees and immediately revoke access for those who leave. The bank also uses Windows Rights Management Services (RMS) and Authorization Manager in Windows Server 2008 to enforce role-based access to data. Tellers and customer service representatives can view only the basic account data they need, while senior bank branch personnel have access to more complete account records.

Under Sarbanes-Oxley, the company is required to work with outside auditors to certify the controls and processes used to generate financial results. This involves giving auditors access to a number of internal software tools and exchanging a large amount of sensitive data across company borders. Contoso uses Active Directory Federation Services (ADFS) to connect its identity system with that of its auditors, providing them with ready access to the resources they need.

Active Directory is a central component of the Windows platform that provides the means to manage the identities and relationships that make up network environments. Using Active Directory Rights Management Services (ADRMS), IT administrators can link together privileges for user accounts, e-mail inboxes, network access and access to specific applications. This enables single sign-on access to resources by end users as well as simplified management and security for administrators. It also helps ensure that employees can obtain the resources they need, while restricting access to sensitive data and applications that they don’t need.

Many organizations need to be able to share resources and data with trusted partners and customers, but ensuring secure access across these boundaries has been a challenge for IT administrators. Windows Server 2008 ADFS capabilities help administrators to securely share user identity information in a privacy-friendly way across organizational boundaries. ADFS federates a company’s identity system with those of its partners and customers, helping ensure that security and privacy policies are enforced consistently. Organizational credentials can be exchanged through secure token servers to help ensure that only the minimum information required to complete a transaction is shared across organizational policy boundaries.

Windows Server 2008 features a unified infrastructure for identity and access through Active Directory that simplifies deployment, provides a consistent policy and access control model, and delivers a common management experience. This new Active Directory helps IT teams build a better, organizationwide identity system by bringing together the identity and access services of Windows Server 2008 and new services for building and managing connected systems. All of these services are aligned around a unified architecture, policy model, development model and management experience.

MIIS is a centralized service that stores and integrates identity information for organizations that use multiple directories to store this data. It can provide organizations with a policy-driven, unified view of all known identity information about users, applications and network resources. It enables IT administrators to synchronize this information across a wide variety of different systems, so it can be updated across disparate platforms while maintaining the integrity and ownership of the data. It also helps them easily provision and deprovision user accounts across the entire network. They can quickly give new employees the access they need, and they can immediately revoke access for those who leave the company. In addition, MIIS enables centralized password synchronization and management, which can reduce help desk workloads and make password management simpler for users.

RMS is an information protection technology that helps safeguard digital information from unauthorized use—whether online or offline, and both inside and outside the firewall. Combining features in Windows Server 2008 with developer tools and industry security technologies, including encryption, certificates based on Extensible Rights Markup Language (XrML), and Active Directory authentication, Windows RMS augments any organization’s security strategy by applying persistent usage policies that remain with the information, no matter where it goes. Information Rights Management technology extends the capabilities of RMS into the Microsoft Office system and Internet Explorer.

To help application developers apply more granular access control to software that handles sensitive data, Windows Server 2008 includes a flexible framework for integrating role-based access control that enables administrators to provide access to sensitive applications through assigned user roles that relate to job functions.

The Identity Metasystem

One of the challenges facing organizations that operate in a networked world is that the Internet was not designed with a secure identity system in mind. As a result, there are different identity systems in use today, each with its own strengths and weaknesses, and no single system meets the needs of every digital identity scenario.

Because universal adoption of a single identity product is unlikely, Microsoft and the technology industry are working toward an “identity metasystem” that facilitates interoperability between different identity systems and ensures a consistent and straightforward user experience.

The concept of the identity metasystem is built on the “laws of identity,” a set of seven principles that govern any universally adopted, sustainable identity architecture. These principles state that the identity metasystem should:

* Reveal information identifying a user only with that user’s consent
* Disclose only the minimum amount of information necessary to facilitate identification
* Be designed so the disclosure of identifying information is limited to parties with a necessary and justifiable place in the identity relationship
* Support both “omnidirectional” identifiers for use by public entities and “unidirectional” identifiers for private entities
* Use and interoperate with multiple identity technologies and providers
* Feature an unambiguous user interface with mechanisms to protect against identity attacks
* Guarantee users a simple, consistent experience

One important step in helping software developers begin building an identity metasystem is Windows Cardspace™, a Microsoft .NET Framework 3.0 component that simplifies and improves the safety of accessing resources and sharing personal information on the Internet by putting end users in control of how they store their identity information. Built on open industry-standard WS-\* Web services protocols, Windows CardSpace facilitates interoperability between systems used to manage online identities. It helps users manage multiple digital identities, similar to how they use wallets or purses to hold physical identity cards. It helps users know when to use which of their digital identities, like the sticker on a shop window indicating which credit cards are accepted for payment. And it helps assure users that the parties asking for digital identities are who they say they are. For more information about the Identity Metasystem and the 7 Laws of Identity, please visit Kim Cameron’s Identity Weblog at [*http://www.identityblog.com*](http://www.identityblog.com)*.*

Information Protection

Legal and regulatory requirements and client expectations regarding management and retention of personal, financial and other business information are greater than ever. As sensitive data is increasingly shared within organizations and across organizational boundaries, it requires persistent protection from interception and viewing by unauthorized parties. In addition, organizations must ensure that their document management systems and practices can safeguard personal information contained in documents throughout their life cycle.

Protecting Information Through Encryption

Supported by strong identity and access controls, data encryption can help safeguard customer and employee information stored in databases and on mobile devices, laptops and desktop computers, and transferred via e-mail and across the Internet. Use of encryption as part of storing, transmitting and disposing of sensitive information greatly reduces the risk of a harmful data breach resulting from an intruder break-in or from a lost or stolen computer.

Scenario: The sales staff at Contoso Bank travels often to meet clients, and they store meeting notes and other confidential data on company-issued laptops and centralized file servers. They also discuss potential investments with customers over e-mail and IM, and they use a custom-built lead-tracking solution to keep track of new customer opportunities.

Contoso uses the Encrypting File System (EFS) and smart card–based authentication to protect sensitive data on client machines. The bank also has deployed Windows Vista and Windows Mobile 6.0 for mobile workers to take advantage of the improved EFS capabilities in both products. Windows BitLocker Drive Encryption and the remote-wipe functions in Windows Vista provide added layers of protection for mobile devices or laptops that could be lost or stolen.

EFS is a powerful tool for encrypting files and folders on client computers in order to automatically protect data from unauthorized access. In Windows Vista and Windows Server 2008, EFS includes new security, performance and manageability features. It offers broader support for smart card integration, enabling users to use their smart card for encryption and authentication. IT administrators can also store recovery keys on smart cards, set policies that require smart cards for EFS, enforce encryption of key system files, enforce minimum encryption key lengths and require the user’s Documents folder to be encrypted. In addition, EFS enables ”on-the-wire” encryption to servers running Windows Server 2008 so sensitive data can be more safely stored on remote servers. Windows Mobile 6.0 also provides new support for encryption of data stored in external removable storage cards as well as the ability to remotely wipe the device and send/receive rights-managed messages and documents.

Another Microsoft offering, Crypto Next Generation, provides a flexible cryptographic development platform that allows IT professionals to create, update and use custom cryptography algorithms in applications such as Active Directory Certificate Services, SSL and IPsec.

Each year, hundreds of thousands of computers are lost, stolen or insecurely decommissioned. Data on these machines can often be viewed by installing a different operating system, moving the disk drive to a new machine or using any number of other “offline” attack methods. BitLocker Drive Encryption is a data-protection feature that addresses these attack methods. It is available in Windows Vista Enterprise and Ultimate editions for client computers and in Windows Server 2008.

BitLocker provides mobile and office workers with enhanced data protection in case their systems are lost or stolen, and secure data deletion when it is time to decommission those assets. It protects data by preventing unauthorized users from breaking Windows file and system protection on these computers. With BitLocker, all user and system files are encrypted, including the swap and hibernation files.

Government regulations and industry standards offer further reasons for organizations to increase the security of e-mail communications. However, many existing solutions—including server-to-server encryption, public key infrastructure (PKI) and password-protected files—can be difficult to integrate and deploy, especially for communication across organizational boundaries. To address the need for secure e-mail communications, Microsoft offers Exchange Hosted Encryption, a convenient e-mail encryption service that enables users to send and receive encrypted e-mail directly from their desktops as easily as regular e-mail. Users can encrypt their business communications without having to purchase, configure and maintain complex hardware and software. Exchange Hosted Encryption is deployed over the Internet, which helps minimize upfront capital investment, free up IT resources and mitigate risks before messages reach the corporate network.

The Data Encryption Toolkit for Mobile PCs, which Microsoft is releasing in stages, provides tested guidance and powerful tools to help protect an organization’s most vulnerable data. The toolkit is available at [*http://www.microsoft.com/technet/security/guidance/clientsecurity/dataencryption/default.mspx*](http://www.microsoft.com/technet/security/guidance/clientsecurity/dataencryption/default.mspx)*.*

Protecting Data Throughout the Information Life Cycle

Rights management technologies can be applied to desktop productivity, e-mail and line-of-business applications to help safeguard sensitive information and control how the information is used, through “persistent protection” that extends throughout its life cycle. These technologies can help ensure that sensitive data such as financial reports, product specifications, customer data and confidential e-mail messages do not intentionally or accidentally get into the wrong hands. For example, access to internal documents can be restricted to specific employees within an organization, preventing users from printing them, forwarding them outside the organization, or copying and pasting the text. Users can also apply document retention policies that cause certain content to “expire” after a set amount of time and thereafter be accessible only to the document’s creator.

Scenario: Contoso Bank uses RMS extensively in its client information protection efforts. Access to all documents related to a particular client is limited to the client team and senior managers. Teams use RMS and ADFS to more securely share client financial plans with their in-house and vendor analysts. Client documents are exported from the company’s relationship management and portfolio management software into the XML Paper Specification (XPS) format. By enabling rights-managed documents to be shared with analysts in this secure fashion, Contoso can more effectively manage clients’ investment portfolios against specific risk and return targets. Client documents are kept in rights-protected SharePoint libraries accessible only to the project team.

Notably, the bank uses SharePoint Portal Server to apply more granular document protection, including ensuring that the rights granted to users persist with the document even when it is removed from the document library. Contoso also uses the enhanced RMS capabilities of Exchange Server 2007 to enforce encryption and rights protection on every e-mail message exchanged with clients.

Information rights management technology extends the capabilities of RMS into the Microsoft Office system and Internet Explorer. The 2007 Microsoft Office system provides even broader RMS capabilities through new developments in Microsoft SharePoint. Administrators can set access policies for SharePoint document libraries on a per-user basis. For example, users who have “view-only” access to documents in a library—but cannot print, copy or paste—will have those policies enforced by RMS, even when the document has been removed from the SharePoint site.

Previous versions of Windows required the installation of additional components to enable rights management functionality. To make RMS simpler to deploy and use, Windows Vista includes an integrated RMS client. In addition, Windows Server 2008 integrates ADRMS with ADFS to support protected collaboration across organizations. By connecting identity and authentication mechanisms across organizations, the integration of ADFS and ADRMS helps organizations share sensitive information among themselves and with business partners while being protected by the same mechanisms they use today to protect their internal information.

In addition, RMS is now integrated with the .NET Framework 3.0 APIs for developers and with the new XPS format—an open, cross-platform document format that helps customers create, share, print, archive and protect rich digital documents. Using a new print driver that outputs documents in the XPS format, any application can produce documents that can be protected with RMS, significantly broadening the range of information that can be protected by this technology.

Exchange Server 2007 includes enhancements that further protect sensitive data and make working with protected information simpler and more efficient. First, it includes RMS licenses within rights-protected documents, reducing the need to contact the server to obtain and verify permissions. Second, it can help organizations comply with data governance regulations by automatically applying information rights management principles at the gateway level. Exchange Server 2007 can detect whether certain types of sensitive information (such as a Social Security number) are in an outgoing e-mail message, reject that message and offer the user guidance on how to transmit such data properly.

Auditing and Reporting

Compliance with internal policies, government regulations and consumer demands for better control over personal information requires the use of monitoring technologies to assist organizations with audit and reporting related to data, systems and applications. Technologies for systems management, monitoring and automation of compliance controls can be used to verify that system and data access controls are operating effectively, and to identify suspicious or noncompliant activity.

Scenario: Contoso Bank has experienced rapid growth as a result of client trust and an abundance of referrals. The combination of a growing IT infrastructure and increased regulatory requirements has further emphasized the need to keep track of a large number of technology assets and keep control over a wider range of sensitive documents. Using Microsoft System Center products including Configuration Manager 2007, Data Protection Manager 2007 and Operations Manager 2007, Contoso can more quickly and easily deploy technology in newly opened offices and ensure that it stays up to date. The bank also has applied a third-party add-on for Operations Manager 2007 to make sure that these assets are monitored and audited in line with new regulatory obligations. In addition, Contoso uses RMS to keep better track of access to financial data, logging whenever users obtain access to these records and keeping track of when they are accessed and used.

Microsoft System Center is a family of systems management products focused on giving IT administrators the tools and knowledge to help ease operations, reduce troubleshooting time and improve planning capabilities as they manage their technology infrastructure.

Through integration with Network Access Protection capabilities in Windows Server 2008, Microsoft System Center Configuration Manager 2007 helps IT administrators ensure that computers connecting to or communicating on their network have the required updates to meet administrator-defined requirements for system health. It can deliver critical business productivity applications reliably and easily to users; manage software assets and ensure license compliance by monitoring how installed applications are used; and improve the security of the Windows environment through reliable delivery of software updates across servers, desktops and laptops.

Data Protection Manager 2007 provides continuous protection for Windows application and file servers, rapid and reliable data recovery, and advanced technology for enterprises of all sizes. It protects a broad ecosystem of files and applications—including Microsoft SQL Server®, Exchange Server and SharePoint Portal Server— under a common framework.

Using Operations Manager 2007, organizations can reduce IT complexity and keep costs under control by simplifying the identification of reliability or integrity problems on the network, determining the root cause of those problems and facilitating quick resolution to restore service and prevent further issues.

Microsoft has worked with industry partners to develop add-on packs for Operations Manager 2007 that address specific regulatory concerns. For example, System Controls Management Pack provides comprehensive auditing and reporting services for Windows Server security events in order to support regulatory auditing requirements for Sarbanes-Oxley, the Federal Information Security Management Act of 2002, the Gramm-Leach-Bliley Act and others.

RMS creates a log entry for every server action, such as users obtaining RMS credentials or consuming newly protected content, to help organizations better monitor and report on the use of sensitive data. SharePoint administrators can also set auditing policies to log such activities as deletion and modification of documents, and monitor those policies through reports. They can also implement document-retention policies, such as “expiring” unneeded content after a certain amount of time.

Principle-Based Application of the Technology Framework

Having assessed the four elements of Microsoft’s technology framework for managing and protecting personal information, another important consideration remains: how to approach the task of applying these technologies in a way that addresses the organization’s core objectives.

This is essentially a matter of considering data governance from an architectural perspective, which flows from conceptual principles or value statements down to specific applications of the technologies. Following a set of clearly defined principles for technology design and deployment will help ensure successful protection of both individual and organizational privacy.

Suggested principles include the following:

* **Honor policies throughout the private data lifespan.** Software applications that collect, use and store private data should be controllable through policies and rules.
* **Minimize risk of data misuse.** Implement applications and systems that guard against unauthorized use of sensitive data.
* **Minimize impact of data loss.** Safeguard data to ensure that it is not usable when outside of an organization’s direct control.
* **Demonstrate the effectiveness of data privacy controls.** Look for data privacy technologies that enable quick response to emerging threats through controls and logs that help uncover problems and determine their source.

Conclusion

A major data spillage, security breach or failure to comply with government regulations can have significant long-term implications for an organization’s bottom line and for its brand. Managing and protecting sensitive personal information is not only the right thing to do for customers, it’s also the right thing to do from a business perspective.

In combination with the right policies, people and processes, technology can help lay a strong foundation for a successful data governance strategy. With its depth of experience and breadth of technologies that range from servers and desktop and laptop PCs to mobile devices, Microsoft offers the most comprehensive technology solution and guidance to address these challenging issues.

1. Source: “A Chronology of Data Breaches,” Privacy Rights Clearinghouse/UCAN. [*http://www.privacyrights.org/ar/ChronDataBreaches.htm*](http://www.privacyrights.org/ar/ChronDataBreaches.htm)*.* [↑](#footnote-ref-2)
2. Source: Attrition.org, [*http://attrition.org/dataloss/dldos.html*](http://attrition.org/dataloss/dldos.html)*.* [↑](#footnote-ref-3)
3. Source: “Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.” Journal of the European Communities of 23 November 1995 No L. 281, p. 31. [↑](#footnote-ref-4)
4. Source: Gartner Inc., “Researching the Research Agenda Survey, 2007: Key Implications for Security, Privacy and Risk Professionals.” May 3, 2007. [↑](#footnote-ref-5)
5. Source: Forrester Research, “What’s Top of Mind for European Security Managers?” May 5, 2007 [↑](#footnote-ref-6)
6. Source: Prentice, Robert A., "Sarbanes-Oxley: The Evidence Regarding the Impact of Section 404." Cardozo Law Review, forthcoming at SSRN: [*http://ssrn.com/abstract=991295*](http://ssrn.com/abstract=991295). [↑](#footnote-ref-7)
7. Source: “Microsoft Study on Data Protection and Role Collaboration Within Organizations,” independently conducted by Ponemon Institute LLC, October 2007. [↑](#footnote-ref-8)