Improve Your Data Security and Compliance Strategy

A holistic approach to sensitive data protection

Highlights

- IBM® InfoSphere® Discovery for understanding data
- IBM InfoSphere Guardium® for data security, data encryption and data redaction
- IBM InfoSphere Optim™ to support data masking requirements on demand

News headlines about the increasing frequency of stolen information and identity theft have focused awareness on data security and privacy breaches—and their consequences. In response to this issue, regulations have been enacted around the world. Although the specifics of the regulations may differ, failure to ensure compliance can result in significant financial penalties and even criminal prosecution. Organizations also risk losing customer loyalty and destroying brand equity.

Since data is a critical component of daily business operations, it is essential to ensure privacy and protect data no matter where it resides (databases, file shares, data warehouses or Hadoop-based systems). Different types of information (structured, unstructured, online and offline) have different protection and privacy requirements; therefore organizations must take a holistic approach to safeguarding information:

- **Understand where the data exists:** Organizations can't protect sensitive data unless they know where it resides and how it's related across the enterprise.
- **Safeguard both structured and unstructured sensitive data:** Structured data contained in databases must be protected from unauthorized access. Unstructured data in documents, forms, image files, GPS systems and more requires privacy policies to redact (remove) sensitive information while still allowing needed business data to be shared.
- **Protect nonproduction environments:** Data in non-production (development, training and quality assurance) environments needs to be protected, yet still usable during the application development, testing and training processes.

- **Secure and continuously monitor access to the data:** Enterprise databases, data warehouses, file shares and Hadoop-based systems require real-time monitoring to ensure data access is protected and audited. Policy-based controls based on access patterns are required to rapidly detect unauthorized or suspicious activity and alert key personnel. In addition, data sources and file shares need to be protected against new threats and other malicious activity and continually monitored for weaknesses.
- **Demonstrate compliance to pass audits:** It's not enough to develop a holistic approach to data security and privacy. Organizations must also demonstrate and prove compliance to third-party auditors.

IBM solutions for data security and privacy are designed to support this holistic approach to protect data and incorporate intelligence that enables organizations to proactively address IT threats and enterprise risks while remaining focused on business goals. IBM has developed three simple guiding principles (*Understand and Define*, *Secure and Protect*, and *Monitor and Audit)* to help organizations achieve better security and compliance without impacting production systems or straining already tight budgets.

Understanding the growing focus on data protection

According to the October 2011 report "Databases are More at Risk Than Ever," which surveyed 355 data security professionals, one-fourth of respondents felt that a data breach in 2012 was likely or inevitable. Only 36 percent of organizations have taken steps to ensure their applications are not subject to SQL injection attacks, and over 70 percent take longer than three months to apply critical patch updates, giving attackers the opportunity they are looking for. Most respondents are unable to tell whether there has been an unauthorized access or change to their database. In many cases, a breach would go undetected for months or longer, as only 40 percent of organizations audit their databases on a regular basis. Prevention strategies are almost non-existent at most companies. Only one-fourth of respondents say they are able to stop abuse of privileges by authorized database users, especially highly privileged users such as database administrators, before it happens. Only 30 percent encrypt sensitive and personally identifiable information in all their databases, despite data privacy regulations worldwide requiring encryption for data at rest. Additionally, most admit to having sensitive data in non-production environments that is accessible to developers, testing and even third parties.

Identifying risks associated with insufficient data security and privacy

Corporations and their officers may face fines from USD5,000 to USD1 million per day, and possible criminal prosecution if data is misused. According to the Ponemon Institute "2011: Cost of Data Breach Study" (published March 2012), the average organizational cost of a data breach in 2011 was USD5.5 million. Data breaches in 2011 cost their companies an average of USD194 per compromised record. The number of breached records per incident in 2011 ranged from approximately 4,500 records to more than 98,000 records. In 2011, the average size of breached records was 28,349. As in prior years, data breach costs appear to be directly proportional to the number of records compromised.

Hard penalties are only one example of how organizations can be harmed; other negative impacts include erosion in share price caused by investor concern and negative publicity resulting from a data breach. Irreparable brand damage identifies a company as one that cannot be trusted.

Meeting data security and privacy challenges

What makes IBM's approach to data protection unique? Expertise. The alignment of people, process, technology and information separates IBM data security and privacy solutions from the competition. The goal of the IBM portfolio is to help organizations meet legal, regulatory and business obligations without adding additional overhead. This helps organizations support compliance initiatives, reduce costs, minimize risk and sustain profitable growth. In addition, IBM has integrated data

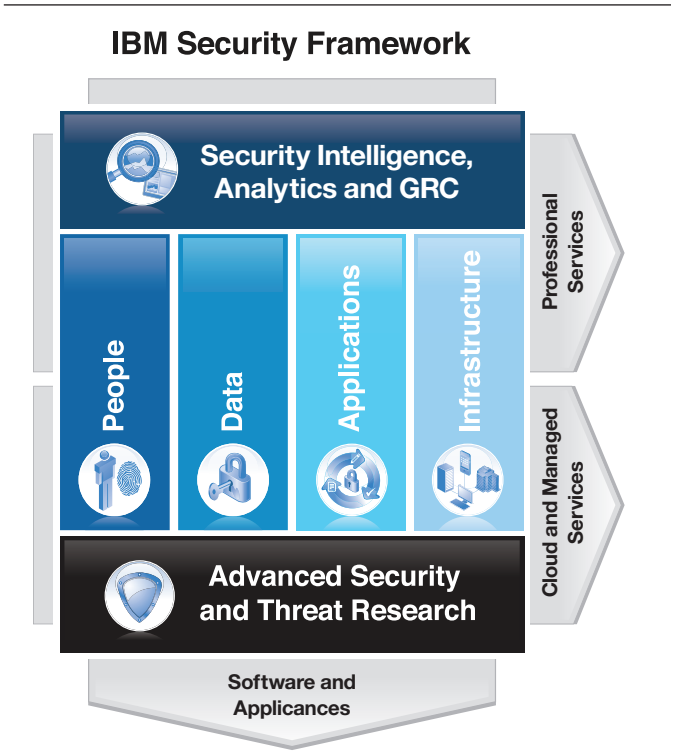

Figure 1: IBM is the only vendor providing security intelligence across people, data, applications and infrastructure

security into a broader security framework. The IBM Security Framework (see Figure 1) and associated best practices provides the expertise, data analysis, and maturity models to give IBM's clients the opportunity to embrace innovation with confidence.

Three guiding principles

The InfoSphere platform provides three guiding principles to ensure holistic data protection:

1. Understand and Define
2. Secure and Protect
3. Monitor and Audit

Understand and Define

Organizations must discover where sensitive data resides, classify and define data types, and determine metrics and policies to ensure protection over time. Data can be distributed over multiple applications, databases and platforms with little documentation. Many organizations rely too heavily on system and application experts for this information. Sometimes, this information is built into application logic, and hidden relationships might be enforced behind the scenes.

IBM InfoSphere Discovery is designed to identify and document what data you have, where it is located and how it's linked across systems by intelligently capturing relationships and determining applied transformations and business rules. It helps automate the identification and definition of data relationships across complex, heterogeneous environments.

Secure and Protect

Data security and privacy solutions should span a heterogeneous enterprise and protect both structured and unstructured data across production and non-production environments. IBM InfoSphere solutions help protect sensitive data in ERP/CRM applications, databases, warehouses, file shares and Hadoop-based systems, and also in unstructured formats such as forms and documents. Key technologies include activity monitoring, data masking, data redaction and data encryption. A holistic data protection approach ensures a 360-degree lockdown of all organizational data.

IBM InfoSphere Guardium Activity Monitor and Vulnerability Solution provides a security solution that addresses the entire database security and compliance life cycle with a unified web console, back-end data store and workflow automation system. It enables you to:

- Assess data center vulnerabilities and configuration flaws
- Ensure configurations are locked down after recommended changes are implemented

- Provide 100-percent visibility and granularity into all data source transactions—across all platforms and protocols—with a secure, tamper-proof audit trail that supports separation of duties
- Monitor and enforce policies for sensitive data access, privileged user actions, change control, application user activities and security exceptions such as failed logins
- Automate the entire compliance auditing process—including report distribution to oversight teams, sign-offs and escalations—with preconfigured reports for the Sarbanes-Oxley Act, PCI DSS and data privacy
- Create a single, centralized audit repository for enterprise-wide compliance reporting, performance optimization, investigations and forensics
- Easily scale from safeguarding a single database to protecting thousands of databases, data warehouses or Hadoop-based systems in distributed data centers around the world

Traditionally, protecting unstructured information in forms, documents and graphics has been performed manually by deleting electronic content and using a black marking pen to hide sensitive information. But this manual process can introduce errors, inadvertently omit information, and leave behind hidden information within files.

IBM InfoSphere Guardium Data Redaction protects sensitive information buried in unstructured documents and forms from unintentional disclosure. This automated solution lends efficiency to the redaction process by detecting sensitive information and automatically removing it from the version of the documents made available to unprivileged readers. Based on industry-leading software redaction techniques, InfoSphere Guardium Data Redaction also offers the flexibility of human review and oversight if required.

IBM InfoSphere Optim Data Masking Solution provides a comprehensive set of data masking techniques that can support your data privacy compliance requirements on demand, including:

- **Application-aware masking capabilities** designed to help ensure that masked data, like names and street addresses, resembles the look and feel of the original information
- **Context-aware, prepackaged data-masking routines** that make it easy to de-identify elements such as payment card numbers, Social Security numbers, street addresses and email addresses
- **Persistent masking capabilities** that propagate masked replacement values consistently across applications, databases, operating systems and hardware platforms
- **Static and dynamic capabilities** to mask data in applications or in databases

IBM InfoSphere Guardium Data Encryption provides a single, manageable and scalable solution to encrypt enterprise data without sacrificing application performance or creating key management complexity. Unlike invasive approaches such as column-level database encryption, PKI-based file encryption or native point encryption, InfoSphere Guardium Data Encryption offers a single, transparent solution that is also easy to manage.

IBM Tivoli® Key Lifecycle Manager helps IT organizations better manage the encryption key life cycle by enabling them to centralize and strengthen key management processes. It can manage encryption keys for IBM self-encrypting storage devices as well as non-IBM encryption solutions that use the Key Management Interoperability Protocol (KMIP). IBM Tivoli Key Lifecycle Manager provides the following data security benefits:

- Centralizes and automates the encryption key management process
- Enhances data security while dramatically reducing the number of encryption keys to be managed
- Simplifies encryption key management with an intuitive user interface for configuration and management
- Minimizes the risk of loss or breach of sensitive information
- Extends key management capabilities to both IBM and non-IBM products
- Leverages open standards to help enable flexibility and facilitate vendor interoperability

Monitor and Audit

After data has been located and locked down, organizations must prove compliance, be prepared to respond to new internal and external risks, and monitor systems on an ongoing basis. Monitoring user activity, object creation, configurations, and entitlements helps IT professionals and auditors trace users between applications and databases. These teams can set fine-grained policies for appropriate behavior and receive alerts if these policies are violated.

Organizations also need to quickly show compliance and empower auditors to verify compliance status. Audit reporting and sign-offs should help facilitate the compliance process while keeping costs low and minimizing technical and business disruptions. Organizations need to create continuous, fine-grained audit trails of all database activities, including the "who, what, when, where and how" of each transaction.

IBM InfoSphere Guardium Activity Monitor provides granular database management system (DBMS)-independent auditing with minimal impact on performance. InfoSphere Guardium is also designed to help organizations reduce operational costs via automation, centralized cross-DBMS policies and audit repositories, and filtering and compression.

Building protection with scalable, modular IBM software

Protecting data security and privacy is a detailed, continuous responsibility that should be part of every best practice. IBM provides an integrated data security and privacy approach delivered through the three guiding principles: Understand and Define, Secure and Protect, and Monitor and Audit. Protecting data requires a 360-degree holistic approach. With deep, broad expertise in the security and privacy space, IBM can help your organization define and implement such an approach.

About IBM InfoSphere

IBM InfoSphere software is an integrated platform for defining, integrating, protecting and managing trusted information across your systems. It provides the foundational building blocks of trusted information, including data integration, data warehousing, master data management and information governance, all integrated around a core of shared metadata and models. The portfolio is modular, allowing you to start anywhere and mix and match InfoSphere software building blocks with components from other vendors, or choose to deploy multiple building blocks together for increased acceleration and value. The InfoSphere platform delivers an enterprise-class foundation for information-intensive projects, providing the performance, scalability, reliability and acceleration needed to simplify difficult challenges and deliver trusted information to your business faster.

About IBM Security

IBM's security portfolio provides the security intelligence to help organizations holistically protect their people, infrastructure, data and applications. IBM offers solutions for identity and access management, database security, application development, risk management, endpoint management, network security and more. IBM operates the world's broadest security research and development and delivery organization. This consists of nine security operations centers, nine IBM Research centers, 11 software security development labs and an Institute for Advanced Security with chapters in the United States, Europe and Asia Pacific. IBM monitors 13 billion security events per day in more than 130 countries and holds more than 3,000 security patents.

For more information

To learn more about IBM InfoSphere solutions for protecting data security and privacy, please contact your IBM sales representative or visit: ibm.com/guardium

IBM Corporation
Software Group
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America
October 2012

Please Recycle

IMS14383-USEN-02