Four steps to a proactive big data security and privacy strategy

Elevate data security to the boardroom agenda
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>3</td>
</tr>
<tr>
<td>Why a proactive data security approach matters</td>
<td>4</td>
</tr>
<tr>
<td>Becoming proactive: A four-step process</td>
<td>6</td>
</tr>
<tr>
<td>The IBM approach to holistic data security and privacy</td>
<td>7</td>
</tr>
<tr>
<td>It's time to get started</td>
<td>9</td>
</tr>
<tr>
<td>Resources</td>
<td>12</td>
</tr>
</tbody>
</table>
Introduction

You’ve probably heard the saying “Data is the new oil.” Just as raw oil can be turned into fuel to power everything from lawnmowers to jets, analyzing data can generate transformative insights, whether for individualizing marketing campaigns, understanding business risks or creating smarter cities.

And like oil companies on the quest for new wells, leading organizations are looking to develop more and deeper insights by extending their enterprise architectures to accommodate data from new sources. When organizations integrate data from these disparate sources with their existing enterprise data, they get a better view into their customers, business operations and competitors.

However, the power to harness big data comes with the responsibility to safeguard it both externally and internally. Big data contains valuable information—some of it sensitive customer data—that creates a lot of risk. It can be a honeypot for internal and external attackers, but accidental and unforeseen data leaks are just as damaging as deliberate attacks.

As today’s organizations accumulate more data in on-premises and cloud repositories, the risk of a data breach rises accordingly. In fact, the Identity Theft Resource Center recorded 30 percent more breaches in 2013 compared to 2012, and pegged compromised records for 2013 at a whopping 91 million worldwide.¹

This ebook outlines four steps to develop a proactive approach to data security and privacy that will help you keep big data safe, and shows how IBM® InfoSphere® solutions can help protect data while giving your staff the right levels of access to do their jobs efficiently and accurately.
Introduction

Why a proactive data security approach matters

In December 2013, a leading retailer was a victim of a data security breach. Thieves siphoned off massive amounts of payment card information, putting more than 40 million customers at risk of identity theft. Spectacular breaches like this are increasing pressure on governments to develop new legislation that holds enterprises more accountable for data security failures.

Unfortunately for the corporate victims, recent breaches also mark a turning point in consumer tolerance. The failure to protect data has not only resulted in stiff financial penalties levied by governments and trade groups; it also has led to measurable increases in customer churn, shrinking brand equity and even falling share prices.

No time to wait for security

Given the increasing reliance on big data for business insight and competitive advantage—and the risk to revenue and reputation if that data is misused—organizations must take a proactive approach to secure enterprise data and enhance defenses against emerging threats.
As shown in Figure 1, data breaches can happen for a variety of reasons. Whatever the cause and wherever the data resides—whether in a data warehouse or on an Apache Hadoop platform—breaches have an adverse impact on the business. A proactive and holistic approach to data security and privacy helps organizations mitigate risk, demonstrate compliance and prepare for additional regulatory constraints without interrupting critical business processes or daily operations. Such an approach also helps organizations tailor policies and processes for different types of data and the different information needs of internal and external stakeholders without compromising business process efficiency.

Figure 1. Data breach costs and causes vary around the world, but all have damaging effects on reputation and budgets.

Becoming proactive: A four-step process

Four steps can help you achieve a proactive approach to security and privacy:

1. **Discover and classify sensitive data**
   Protecting sensitive data first requires defining what "sensitive data" means for your enterprise. Once that is clear, determine where sensitive data resides and how it is related to other information and systems. Document the various types of sensitive data and their locations to create a heat map for protection efforts.

2. **Harden the environment**
   Once sensitive data is understood and discovered, it’s time to harden the environment. Sensitive data—both structured and unstructured—can be obfuscated through data masking and encryption. First, be sure you have a comprehensive enterprise security strategy in place. Next, confirm that security policies and procedures fit with your strategy and support compliance with regulatory mandates. Finally, evaluate your systems to ensure they enforce the security policies.

3. **Secure and continuously monitor access to the data**
   Enterprise data stores require real-time insight to protect and audit data access. Policy-based controls should rapidly detect unauthorized or suspicious activity and alert key personnel. In addition, databases and file shares need protection against internal threats, accidental leaks and malicious activity and should be continually monitored for weaknesses.

4. **Protect and remain vigilant**
   As data risks rise, regulators expect organizations not only to increase their reporting, but also to enact auditable data management processes. Confirm that your audit reporting and sign-offs facilitate compliance processes while using intelligent workflows, pre-configured reports and other capabilities to keep costs low and minimize technical and business disruptions. As an iterative process, further protection is introduced with the creation and discovery of additional sensitive data and with changes in regulations and internal policies.
The IBM approach to holistic data security and privacy

Progressing through the four steps requires a clear path and solid supporting technology. Based on its years of experience with data security and information governance, IBM has developed a holistic approach to data security and privacy that is anchored by integrated technology and processes designed for the needs of big data (see Figure 2).

Throughout the four-step process, IBM helps organizations to:

- Protect against and prevent data breaches and fraud, from both internal and external sources
- Control access to sensitive information
- Streamline the process for compliance around data protection through automation and centralization

In addition, IBM solutions offer the ability to scale in an efficient and cost-effective manner as your business grows.

Figure 2. IBM capabilities support the four steps to achieve holistic data security and privacy with the tools and technologies to help keep data protected yet accessible.
Why IBM InfoSphere for data security and privacy?

Data security and privacy are key elements of the IBM InfoSphere Information Integration and Governance (IIG) portfolio, which helps organizations build confidence in big data. InfoSphere solutions deliver an enterprise-class foundation for information-intensive projects, providing the performance, scalability, reliability and acceleration needed to simplify big data challenges and deliver trusted information in a timely fashion.

IBM solutions are open and modular and support all aspects of data security and privacy for all types of data—including structured, semi-structured and unstructured data—no matter where it resides. This broad scope helps organizations proactively protect data and support compliance initiatives while reducing total cost of operations and minimizing risk.

With unique breadth and depth in both data governance and other data security and privacy capabilities across industries and geographies, IBM can help you align your people, processes, technology and information to create a cohesive, coordinated approach to data security.

IBM data security: Backed by world-class R&D

IBM operates one of the world’s broadest organizations for data security research, development and delivery, comprising 9 security operations centers, 9 research centers, 11 software security development labs and an Institute for Advanced Security with chapters in the United States, Europe and Asia-Pacific.

InfoSphere users can leverage built-in automation capabilities to simplify the process of adapting to changes in audit requirements and the data environment. Audit information from multiple data sources and collectors is automatically normalized and aggregated into a single, secure, centralized audit repository with advanced reporting and analytics. In addition, there is extensive application programming interface (API) support for script-based automation and automated information sharing between functions. These capabilities enhance ROI and enable IT to effectively implement data security even amid shrinking teams and budgets.
It’s time to get started

The direct and indirect costs associated with data breaches will only continue to escalate. The time to secure enterprise data is now, before big data, analytics and business intelligence initiatives progress to production stages without compliance controls.

While many organizations start data security initiatives with compliance in mind, forward-thinking organizations shift to a risk-based model, incorporating data security as a cornerstone for all their business initiatives. This approach positions these organizations to easily adapt to regulatory mandates as they are enacted and enforced.

Forward-thinking companies also elevate the importance of data security by making it a part of the boardroom agenda and standard business processes. Data security and privacy are best practices in all of their big data, analytics and business intelligence initiatives.

Target data protection with IBM big data and governance solutions

Unlike piecemeal approaches, a best practices-based, holistic approach to data protection aligns people, processes and technologies to help organizations secure data throughout its lifecycle. Data security solutions from IBM support big data environments that include Hadoop, NoSQL and in-memory database platforms. Built-in automation capabilities help reduce the inefficiencies associated with manual tasks and enable the organization to protect data and comply without any adverse impact on the day-to-day business processes.
Two InfoSphere solutions provide valuable data security and privacy control (see Figure 3):

- Continuously monitor data access, protect repositories from data breaches and support compliance with IBM InfoSphere Guardium®.
- Ensure that sensitive data is masked and protected with InfoSphere Optim™ data lifecycle management solutions.

To learn more about these data security and privacy solutions, visit: ibm.com/software/data/guardium and ibm.com/software/data/optim

Figure 3. Implement end-to-end data security and privacy with IBM InfoSphere solutions.
As a core component of IBM Watson™ Foundations, the IBM big data and analytics platform, InfoSphere solutions offer comprehensive capabilities for information integration and governance that build an infrastructure for data security (see Figure 4).

In addition to information security and privacy solutions, InfoSphere provides other critical information governance capabilities, including:

- Metadata, business glossary and policy management
- Data integration, including batch data transformation and movement, real-time replication and data federation
- Data quality
- Master data management (MDM)
- Data lifecycle management

Figure 4. IBM Watson Foundations supports an integrated approach to big data and analytics.
Introduction

Why a proactive data security approach matters

Becoming proactive: A four-step process

The IBM approach to holistic data security and privacy

It's time to get started

Resources

To learn more about the IBM approach to information integration and governance for data security and privacy initiatives, please contact your IBM representative or IBM Business Partner, or check out these resources:

- Comprehensive data protection for physical, virtual and cloud infrastructures
- Top Three Myths about Big Data Security
- Top tips for securing big data environments
- Webcast: Forrester Research. Inc. - Why big data doesn’t have to mean big security challenges

Additionally, IBM Global Financing can help you acquire the software capabilities that your business needs in the most cost-effective and strategic way possible. We’ll partner with credit-qualified clients to customize a financing solution to suit your business and development goals, enable effective cash management, and improve your total cost of ownership. Fund your critical IT investment and propel your business forward with IBM Global Financing. For more information, visit: ibm.com/financing
© Copyright IBM Corporation 2014

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
June 2014

IBM, the IBM logo, ibm.com, Guardium, IBM Watson, InfoSphere, and Optim are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at "Copyright and trademark information" at ibm.com/legal/copytrade.shtml

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation.

---


2 Target.com: Data breach FAQ. https://corporate.target.com/about/shopping-experience/payment-card-issue-FAQ