IMPERVA®

Data Privacy: The High Cost of Unprotected Sensitive Data

6 Step Data Privacy Protection Plan

Introduction to Data Privacy

Today, organizations face a heightened threat landscape with data breaches constantly on the rise. Financial records, medical records, Personally Identifiable Information (PII), and other private business data exist in virtually every enterprise data center. Failing to safeguard the databases that store this information can damage your reputation, impact your operations, and result in regulatory violations, fines, and legal fees.

Data Privacy addresses issues related to gathering and distributing PII, the technology used to store, manage, and protect that data, privacy expectations of individuals, and legal and political issues surrounding PII. Organizations that manage and store data assume great responsibility, especially when entrusted with personal data.

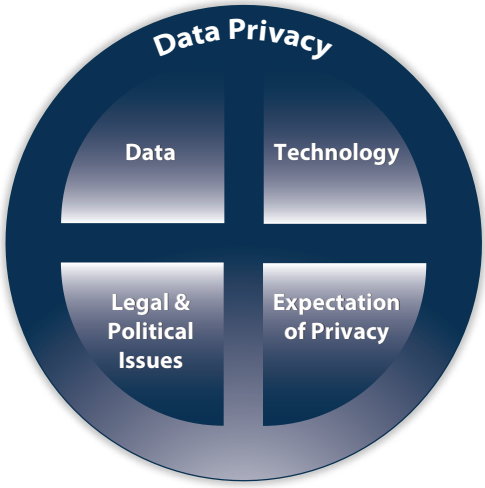

Figure 1. Data Privacy is the relationship between four key areas.

Personally Identifiable Information

"Less than 1% of your employees may be malicious insiders, but 100% of your employees have the potential to be compromised Insiders."

– Ron Arden, Vice President Strategy & Marketing eDocument Sciences, LLC

The "data" in Data Privacy is called Personally Identifiable Information, or PII. PII is any piece of data that can be used to uniquely identify, contact, link, locate, or describe a single person. Common examples of PII include:

- Name
- Address and phone number
- Gender and race
- Health and military records
- National identity number
- Date of birth
- Driver license number

Although the concept of PII is not new, it has become much more important as information technology and the Internet have made it easier to gather PII, leading to a profitable market in legitimately collecting and reselling PII. PII is also valuable to criminals who stalk or steal the identity of individuals, commit fraud, and plan other crimes. As a response to these threats, many privacy laws and regulations exist to specifically address the collection, accessibility, and management of PII.

Business Drivers for Data Privacy

Compliance

58

The number of countries with national data privacy laws that govern the use of PII.

Organizations that work with PII often need to comply with regulations and laws that govern personal information. There are numerous legal structures that affect the collection, use, transfer, or disclosure of PII. In addition to industry regulations, there are nearly 60 countries with national data privacy laws that govern the use of PII, according to DLA Piper.[1] Many national privacy laws restrict trans-border transfers of personal information to countries that do not provide comparable privacy rights and protection. These country-based, cross-border restrictions require extra diligence for multi-national companies with Personally Identifiable Information protected by these laws.

Security

50%

The percentage of data breaches from database servers.

Businesses today process more sensitive data than ever before. The amount of digital data available and the number of people that can access it is growing exponentially. Along with this trend, attacks targeting personal information have increased in sophistication, scale, and frequency. According to the Verizon 2012 Data Breach Investigations Report, nearly 50% of all data breaches were from database servers. The reason for this is quite simple; when hackers and malicious insiders gain access to PII, they can quickly inflict damage, such as drain bank accounts, make purchases with credit cards, and steal identities.

Approaches to Protecting Private Data

Managing and safeguarding Personally Identifiable Information requires organizations to implement processes that identify and secure PII, including understanding how the data is being used, who has rights to access it, and whether they are allowed to do so. To accomplish these tasks, many enterprises turn to "free" tools provided by their database vendors or rely on ad-hoc and manual solutions. These approaches are time consuming, error prone, and can degrade the performance of production databases. The only way to efficiently achieve data privacy is through an automated Database Auditing and Protection (DAP) platform.

The remainder of this guide outlines a six step plan that explains how you can leverage a DAP platform to automate data privacy as well as an introduction to Imperva SecureSphere, a market leading DAP platform.

[1] "Data Protection Laws of the World", ***DLA Piper***, March 2012

6 Step Data Privacy Protection Plan

1. Discover PII and Sensitive Data

Challenge

As organizations accumulate more data they need to ensure that all systems holding sensitive information are included within the scope of any data security/compliance project. Before you can manage, monitor, and safeguard PII, you first need to identify where sensitive data is stored. PII is typically scattered across heterogeneous database systems and often resides in various locations around the globe. Furthermore, the rate at which sensitive data grows can quickly outpace the ability to manage and protect it. While you may know where certain key pockets of PII are located, most organizations simply can't effectively track where all their sensitive data resides. Lack of visibility into the content and location of critical data assets can leave you exposed to significant risk.

Security Tip

Lack of visibility into the content and location of critical data assets can leave you exposed to significant risk.

Solution

- **Discover Database Servers:** Leverage discovery tools that scan enterprise networks and identify active database services. Look for solutions that can reduce scan duration by filtering on IP addresses and ranges and by specific database services (e.g. Oracle, Microsoft SQL, IBM DB2, etc.).
- **Identify and Classify PII:** Scan the objects, rows, and columns of databases for PII to pinpoint sensitive data. The results should include the IP address and host name of the asset and indicate the existence of PII on that server. Automatically identifying PII helps narrow the scope of security and compliance efforts.
- **Analyze Discovery Results:** Review discovery and classification results to determine which databases contain PII and need to be monitored.

2. Find and Remediate Database Vulnerabilities

Challenge

Data risk management requires knowledge of vulnerabilities that, if exploited by a hacker or insider, can lead to a data breach. Any database platform, software, or configuration weakness will put your PII at risk for data theft or misuse. The dynamic nature of businesses and changes to IT infrastructure and application growth make the identification of database vulnerabilities an ongoing challenge.

Security Tip

Any database platform, software, or configuration weakness will put your PII at risk for data theft or misuse.

Solution

- **Scan for Vulnerabilities:** Use database vulnerability assessment tools to identify security vulnerabilities, mis-configurations, and missing vendor patches. Assessments should use industry best practices, such as DISA STIG and CIS benchmarks. Vulnerability assessments help document weaknesses that put databases at risk and configurations that deviate from defined standards.
- **Calculate Risk Scores:** Score risks based on the severity of vulnerabilities and the sensitivity of the data. Severity values should be based on known systems, such as the Common Vulnerability Scoring System (CVSS). Risk scores help prioritize risk, manage, and research vulnerabilities.
- **Analyze Risk and Prioritize Remediation Efforts:** Generate reports to efficiently manage and mitigate discovered vulnerabilities. Use solutions that provide an overview of open vulnerabilities, trends, and mitigation status to facilitate better decision making.
- **Mitigate Vulnerabilities:** Use database "virtual patching" to protect systems from attempts to exploit known vulnerabilities. Virtual patches enable risk mitigation without requiring actual patches or changes to the current configuration of the server.

3. Understand Who Has Access to Private Information

Challenge

With sensitive data scattered across multiple databases, the process for untangling the web of user rights and privileges can be a monumentally complex task. Database access rights reviews and the identification of excessive rights are not only required by various industry regulations but are an established best practice for securing PII. Failure to understand database access rights prevents you from identifying users with excessive or unused privileges and puts your PII at risk.

Security Tip

Failure to understand database access rights prevents you from identifying users with excessive or unused privileges and puts your PII at risk.

Solution

- **Aggregate Access Rights:** Scan databases for granted user rights and aggregate details, such as who granted them, who received rights, and objects to which rights have been granted. Aggregating user rights into a single repository helps streamline the reporting and analysis of user access to sensitive data.
- **Enrich Access Rights Information with User Details and Data Sensitivity:** Collect contextual information to user rights, including user name, department, sensitivity of database objects accessed, and last time accessed. This allows you to focus on analyzing access rights that represent the highest business risk.
- **Remove Excessive Rights and Dormant Users:** Identify users that have too many privileges and those that don't use them. This helps determine if user access rights are appropriately defined and if there are any issues with separation of duties as well as removes excessive rights that are not required for users to do their job.
- **Review and Approve/Reject Individual User Rights:** Perform an organized review of user rights to determine if they are appropriate. Approve or reject the granting of these rights, or assign them to another for review, and then report on this process. Conducting rights reviews meets regulatory requirements and reduces risk by ensuring that user privileges are granted on a need-to-know basis.

4. Protect Data from Unauthorized Access

Challenge

Preventing data theft is essential to any effective data security strategy. Attacks on data are on the rise and databases containing PII and sensitive data are a top target for hackers and malicious insiders. Attackers are proficient at exploiting vulnerabilities in applications that access PII and the databases that store sensitive information. Insiders can take advantage of their privileges to view and make changes to sensitive information or worse, steal it.

Security Tip

Databases containing PII and sensitive data are a top target for hackers and malicious insiders.

Solution

- **Real-time Blocking:** Monitor all database access activity and usage patterns in real time to detect data leakage, unauthorized SQL transactions, and protocol and system attacks. Terminate the session and block users when attempts to access unauthorized data occur.
- **Encrypt Databases:** Encrypt database files storing PII and monitor access by system users. The encryption process should provide support for heterogeneous database environments with minimal performance and management overhead. Encrypting critical data stores can reduce the risk of data theft and meet some regulatory requirements.
- **Mask Sensitive Data:** Obscure or replace sensitive data elements before they are accessed. Look for solutions that mask sensitive data elements on-the-fly without touching applications or physical production databases, or can permanently mask sensitive data elements in non-production environments. Data masking protects organizations by ensuring that PII accessed from application screens, reports, development and DBA tools is replaced with credible but not real data.

5. Alert on Unusual Access Activity

Security Tip

Unusual or anomalous database access attempts to PII may indicate suspicious activity.

Challenge

Unusual or anomalous database access attempts to PII can often indicate suspicious activity. Understanding a user's "normal" activity patterns and deviations from that is complicated because it requires continuous monitoring of access activity as well as a policy framework for analyzing and responding to significant activity changes.

Solution

- **Detect Unusual Access Activity:** Establish a comprehensive profile of individual user activity. These user baselines provide the basis for detecting anomalous activity by providing a point of comparison. When variances are detected, generate alerts or block users. Creating activity-based user profiles increases the likelihood of detecting inappropriate access to PII.

6. Monitor Privileged User Activity

Security Tip

Abuse of privileged user accounts can lead to compromised PII, data leakage, or fraudulent activity.

Challenge

Privileged users, including DBAs and System Administrators, are required to manage and maintain databases. However, their broad database privileges pose a risk. Since these users often need to access databases directly and perform highly sensitive operations on database configurations and content, they are often provided with unlimited access to PII and sensitive content. Abuse of these privileges by malware or other malicious users can compromise your PII and enable data leakage and fraudulent activity.

Solution

- **Track Privileged Access:** Install an activity monitoring "agent" on the database server to inspect and analyze traffic to all local system access. Generate alerts and block access when unusual or unauthorized access events are detected.

Summary

The collection and use of Personally Identifiable Information is exploding. With this expansion there is increasing pressure from individuals, industry regulators, and lawmakers for organizations to protect sensitive data from hacker attacks and insider abuse or theft. The six steps outlined in this paper illustrate the challenges around the protection of sensitive data and how a Database Auditing and Protection solution, like Imperva SecureSphere, can be used to safeguard PII and comply with industry regulations and data privacy laws.

SecureSphere Database Security Products: Automate and Protect

Imperva's SecureSphere Database Security solutions help organizations automate the management, monitoring, and security of private data. The table below shows how the six recommendations outlined in this paper map to Imperva SecureSphere functionality.

6 Step Data Privacy Protection Plan	Database Activity Monitoring	Database Firewall	Discovery & Assessment Server	User Rights Management for Databases
Step 1: Discover sensitive information. Automate the discovery and classification of databases storing sensitive information.	√	√	√	
Step 2: Find and remediate database vulnerabilities. Scan databases for security vulnerabilities, configuration flaws, and missing vendor patches.	√	√	√	
Step 3: Understand who has access to private information. Identify database users with excessive or unused privileges.				√
Step 4: Protect data from unauthorized access. Block hackers and insiders from unauthorized access to private data.		√		
Step 5: Alert on unusual access activity. Generate alerts when anomalous database activity is observed.	√	√		
Step 6: Monitor privileged user activity. Supervise the usage of your most highly-privileged users; your Database and System Administrators.	√	√		

Database Activity Monitoring (DAM)

Delivers automated, scalable activity monitoring, auditing, and reporting for heterogeneous database environments. SecureSphere helps organizations demonstrate regulatory compliance through automated processes, analysis, and reporting. SecureSphere accelerates incident response and forensic investigation with centralized management and advanced analytics.

Database Firewall (DBF)

Provides real-time database protection against internal and external threats by alerting or blocking attacks and abnormal access requests. SecureSphere provides 'virtual patching' for database software vulnerabilities reducing the window of exposure and impact of long patch cycles. DBF includes the auditing and analytics capabilities offered by DAM.

Discovery and Assessment Server (DAS)

Delivers vulnerability assessment and configuration audits allowing users to measure compliance with industry standards and best practices. Data discovery and classification enables organizations to accurately scope security and compliance projects. With a combined analysis of sensitive data and vulnerabilities, SecureSphere helps prioritize and better manage risk mitigation efforts. DAS is bundled with DAM and DBF.

Video [2:33]

VIP Data Privacy Case Study

A Database Administrator (DBA) at a financial news and information services company is asked to create a report with executive salary and personal information. The DBA accidently distributes this report to the entire company. Using SecureSphere, the company is now enforcing data privacy policies with visibility into user rights and database activity, along with triggering alerts when access activity doesn't align with business policy.

View Video

User Rights Management for Databases (URMD)

Enables automatic aggregation and review of database user access rights. SecureSphere helps identify excessive rights and dormant users based on organizational context and actual data usage. Using URMD, organizations can demonstrate compliance with regulations, such as SOX, PCI 7, and PCI 8.5, and reduce the risk of a data breach.

ADC Insights

ADC Insights provide pre-packaged application awareness of leading enterprise applications that streamlines compliance and security projects for key regulations, such as SOX, PCI DSS, HIPAA, and others. Insights packages are available for SAP, Oracle EBS (E-Business Suite), and PeopleSoft.

About Imperva

Imperva, pioneering the third pillar of enterprise security, fills the gaps in endpoint and network security by directly protecting high-value applications and data assets in physical and virtual data centers. With an integrated security platform built specifically for modern threats, Imperva data center security provides the visibility and control needed to neutralize attack, theft, and fraud from inside and outside the organization, mitigate risk, and streamline

IMPERVA®

www.imperva.com

© Copyright 2014, Imperva
All rights reserved. Imperva and SecureSphere are registered trademarks of Imperva.
All other brand or product names are trademarks or registered trademarks of their respective holders. WP-6STEPS-DATA-PRIVACY-0314.1d