The Business Case for Database Security
Managing risk, simplifying compliance, and reducing the cost of securing databases

Introduction

Databases are the most strategic data asset of any organization. They store extraordinarily valuable data, such as personal information, medical records, credit card data, financial data, and more. In recent years, a raft of regulations and privacy acts were enacted to ensure organizations protect this data from theft and abuse. This paper examines the database security and compliance requirements imposed on today’s organizations, including:

• Managing and monitoring user access to sensitive data
• Protecting databases and the data they host from attack and unauthorized access
• Assessing vulnerabilities and mitigating the risk of a data breach
• Keeping a complete audit trail of database activities
• Enforcing corporate configuration policies
• Demonstrating compliance through clear, logical reports

This paper examines the business case for database security solutions and reviews solution requirements. This paper also explores how Imperva SecureSphere Database Security Solutions simplify implementation and provides a cost-effective solution that addresses security and compliance requirements through:

• Automation
• Centralization
• Enforcement of effective controls
• Reporting and analysis capabilities
• Proactive Risk Management
Business Requirement—Compliance

Regulatory Compliance Under the Microscope

Most regulations fall into one of two categories:

- Data Integrity: Regulations designed to prevent fraud and ensure that data changes are appropriately managed.
- Data Confidentiality: Regulations designed to protect personal, medical, and financial data from theft and exposure.

The following table lists seven key regulations and identifies the sections that require implementation of data integrity and data protection controls.

<table>
<thead>
<tr>
<th>REGULATION NAME</th>
<th>INTEGRITY OR SECURITY REQUIREMENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Payment Card Industry Data Security Standard (PCI DSS)</td>
<td>Section 10: Requires that merchants track and monitor all access to cardholder data. Merchants must “implement automated audit trails for all system components” and “secure audit trails so they cannot be altered.” Section 8.5.1: “Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.” Section 8.5.5: “Remove/disable inactive user accounts at least every 90 days.” Section 7: Requires merchants to “limit access to systems and data on a business need-to-know.” Section 6.2: “Establish a process to identify and assign a risk ranking to newly discovered security vulnerabilities.” Section 2.2: “Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.”</td>
</tr>
<tr>
<td>Sarbanes-Oxley Act (SOX)</td>
<td>Section 404: Mandates IT controls to ensure the integrity of financial data, and periodic reports to validate the implementation of IT controls.</td>
</tr>
<tr>
<td>Financial Instruments and Exchange Law in Japan (J-SOX)</td>
<td>J-SOX: Requires management to evaluate and prepare a report on the effectiveness of financial reporting. Companies must also demonstrate that system development and operations, change management, and security processes are in place and followed.</td>
</tr>
</tbody>
</table>
| Health Insurance Portability and Accountability Act (HIPAA) | Title II of HIPAA: Defines the following security safeguards:  
  1. 164.308(a)(1): Mandates risk analysis, risk management, and information system activity review.  
  2. 164.308(a)(6): Enforces security incident response, including mitigating and reporting on security events. |
| California Senate Bill 1386              | Businesses must disclose any breach of their personal information to California residents.                                                                        |
  The Safeguards Rule: Requires financial institutions to design and implement safeguards to protect customer information. |
| EU Privacy Directive                     | Directive 95/46/EC: Protects personal data that is processed or transferred. European companies must have IT controls in place to ensure, and prove, to auditors that data is processed correctly. |
As shown above, government and industry regulations require organizations to protect regulated data from unauthorized access and changes. The required controls include:

- Keeping a complete database activity audit trail
- Limiting access to business need-to-know
- In case of a breach, notifying those individuals whose data has been breached

**The Challenge: Implementation of Cost-Effective Controls**

Many organizations struggle with the implementation of cost-effective database auditing and monitoring controls. Since most IT environments include heterogeneous database platforms, each offering different levels of controls, it is impractical to use native database tools to address regulatory requirements. Additionally, the requirement to monitor privileged activity, which appears in all regulations, cannot be addressed by native database tools because they do not support separation of duties. Database administrators (DBAs) should not be in charge of monitoring their own activities, nor should they be able to change audit policies or the audit trail itself.

**Other challenges organizations are facing include:**

- **Defining the scope of the audit**
  - How do you ensure that you are defining the correct scope in dynamic environments that continuously grow and change?
- **Measuring compliance with configuration standards**
  - How do you ensure that all systems continuously meet configuration standards?
- **Assessing database vulnerabilities**
  - How do you assess vulnerabilities across heterogeneous platforms when there are new vulnerabilities discovered almost every day?
  - How do you manage mitigation efforts?
- **Managing user rights and periodic user rights reviews**
  - How do you implement a repeatable, cost-effective process for reviewing user rights?
  - How do you verify that user rights are limited to business need-to-know?
- **Implementing database activity audit requirements**
  - How do you audit database activity 24x7?
  - Do you need to audit all activities?
  - How do you manage the audit trail and ensure its integrity?
- **Demonstrating compliance through reports**
  - Which reports should you produce to satisfy the auditors?
  - How do you demonstrate risk mitigation controls to satisfy multiple compliance requirements?

To meet multiple compliance requirements and implement controls across heterogeneous platforms, Imperva SecureSphere Database Security Solutions provide a cost-effective method to enable consolidation of compliance efforts and implementation of repeatable, automated processes. SecureSphere reduces the operational expenses related to compliance by eliminating manual processes and replacing them with more effective, automated processes. SecureSphere enables organizations to manage their database compliance audits and assessments from a single solution and provides out-of-the-box, customizable policies and reports necessary for demonstrating compliance with various regulations.
Business Requirement—Security

The Impact of a Data Breach

Corporate databases perform a vital role in enabling daily operations and business processes. These databases contain organizations’ most strategically valuable assets, including financial data and intellectual property as well as personal information about employees, patients, and customers.

The impact of a data breach can be financially devastating. Direct costs include notification and legal defense costs, while indirect costs include lost customer business resulting from abnormal churn. Today's consumers care about loss or theft of their personal information and hold organizations accountable for safeguarding the plethora of personal information entrusted to them. To quantify the impact, the Ponemon Institute estimated that in 2010 the total average cost of a data breach in the U.S. was $7.2 million USD per breach, or $214 per compromised record.1

According to the Ponemon Institute, decreased confidence and trust in the company is the most significant cost impact. Due to a malicious attack, insider abuse, or an inadvertent leak, a large-scale, data breach can be devastating on an organization’s bottom-line, both in the short term and the long term.

Database Security Threats

Database security threats include external hacking threats, such as Advanced Persistent Threats (APT), SQL injection attacks, and worms. Internal attacks, or “insider threats,” also pose significant risk to database security.

External Threats:

- **Advanced Persistent Threats (APT):** The term APT refers to a long-term pattern of targeted, sophisticated hacking attacks aimed at political targets or companies. APTs are typically made up of a series of attacks that use different techniques to bypass corporate defenses and gain access to internal resources.

- **SQL Injection Attacks:** These attacks exploit vulnerabilities in Web applications. The attacker takes advantage of input validation vulnerabilities in Web applications to pass unauthorized SQL queries to a back-end database. Using this technique, a hacker can gain unrestricted access to the contents of an entire database.

- **Worms and Malware:** Vulnerabilities enable the spread of malware exposing databases to hackers. Worms have also been used to exploit known database vulnerabilities. The SQL Slammer worm, for example, first surfaced in January 2003. It exploited a known buffer overflow vulnerability in SQL Server 2000. Microsoft released a patch to remove this vulnerability in the summer of 2002. However, unpatched database servers enabled the rapid spread of this attack and this worm was still active in 2010.
Insider Threats:
Malicious users have numerous opportunities to steal or alter the data hosted in databases. Whether abusing the trust bestowed on the user or exploiting a well known database weakness, malicious users are often able to access sensitive data. The following examples illustrate common database attack techniques that can lead to a costly database breach.

- **Database Privilege Abuse:** When users are granted database access privileges that exceed the requirements of their job function, they may abuse these privileges to access data for malicious purposes, e.g., data theft.
- **Database Privilege Elevation:** A malicious “insider” may take advantage of database platform vulnerabilities to convert ordinary access privileges into administrator privileges. Vulnerabilities may be found in stored procedures, built-in functions, protocol implementations, and even SQL statements.
- **Weak Audit Controls:** Weak audit controls enable malicious insiders to evade the audit process or delete any evidence of their misdoing in the audit trail. As a result, the breach may not be detected in a timely manner and investigators will struggle to understand the cause and effect of the breach.

Database Security Requirements
Since databases contain the organization’s most valuable and sensitive information, it is imperative to protect databases against data compromise. To safeguard databases, organizations must implement a comprehensive database security strategy consisting of the following measures:

- **Discovery and Classification of Sensitive Data:** To implement effective security controls, organizations need to know where to focus their efforts. Too often organizations forget, or do not know, about the existence of old databases or rogue database instances that are not properly managed. Businesses should have an accurate and complete understanding of all database instances on the network. Furthermore, they must know which databases contain sensitive data such as credit card and Social Security numbers. Identifying all sensitive data will help organizations prioritize risk and improve spending efficiency.
- **Vulnerability Assessment:** Organizations should assess their databases for misconfigurations and vulnerabilities that could increase the risk of a data breach. Assessment tests should identify and present discovered vulnerabilities, their severity level, and vulnerability mitigation steps in clear, comprehensible assessment reports.
- **User Rights Management:** Organizations should limit user rights to data to ‘business need-to-know’. This helps reduce and better control the risk of a data breach. Dormant accounts should be disabled.

---

1. Ponemon Institute, *2010 Annual Study: U.S. Cost of a Data Breach*
• **Database and Application Attack Prevention**: To protect database data, organizations should identify, and optionally block, attacks in real time. Due to the unique nature of database attacks, a security solution must recognize known database exploits as well as abnormal database activity. All database activity should be inspected since an attack can originate via an application attack, e.g. SQL injection, as well as from an Insider user account. Additionally, when it comes to SQL injection protection, it is also recommend to use an intelligent Web application firewall to provide the first line of defense against database attacks.

• **Database Activity Monitoring and Auditing for Forensics**: If unauthorized activity does occur, organizations must be able to track the source of the data leak. Comprehensive database auditing enables organizations to reconstruct past events and determine the extent of a compromise. An auditing solution helps reduce the scope of a data breach and limit liability by identifying the individual records that may be exposed, rather than the entire database.
Beyond Database Security and Compliance

Deployment and Operational Considerations

When looking into database security and compliance solutions, organizations also need to consider the deployment and operational aspects of such solutions.

• **Will the solution have any impact on database and application availability?** Database availability is paramount for many organizations. Downtime has an immediate negative impact on revenue, productivity, and user satisfaction.

• **What kind of impact will the solution have on database performance?** As the only way to capture privileged activity performed directly on database servers, database activity monitoring solutions utilize agents, or rely on native auditing functionality. These components consume database resources and could have significant impact on database performance. However, not all solutions work the same way and the impact varies. When the expected impact is high, additional capital costs might be needed to compensate for the performance impact.

• **Can the solution be transparently deployed?** Some solutions may require changes to monitored databases or applications. These changes are not easily done and can lengthen the deployment process. Most organizations prefer transparent deployments that do not require database or application changes.

• **Can the solution be centrally managed?** Database infrastructure is often distributed across the globe. Organizations must be able to administer the database security solution through a single, unified management interface which enables security and compliance professionals to manage policies, monitor status, and report on audit data from multiple locations without being required to manage each server separately.

• **Does the solution enforce separation of duties?** Since all regulations require monitoring of privileged users and their activities, privileged users should not have the ability to modify or audit security policies, or the audit trail itself.

• **Does the solution provide a tamper-proof audit repository?** Can it ensure the integrity of audited data? Database audit solutions that do not provide these capabilities require the user to build their own tamper-proof audit repository. If an organization selects a solution that uses an RDBMS as an audit repository, users face a few problems:
  - **Performance Issues:** Trying to write all the activity monitored on multiple RDBMS into a single RDBMS is a challenge, especially since RDBMSs are optimized for read activity and not write activity.
  - **Database Vulnerabilities:** Inevitably, databases have vulnerabilities. These vulnerabilities can expose the audit trail and allow users to change audit records. Therefore, the database needs to be patched and monitored, just like other databases.
  - **Separation of Duties:** As explained above, privileged users should not have access to the audit database.
• **Can the solution provide real-time alerts or block attacks?** Real-time alerts require quick analysis of database events and the ability to notify security professionals about attacks and unauthorized access. The faster you receive an alert, the faster you can respond. Solutions that can block attacks can provide effective real-time protection.

• **Does the solution require enablement of native tools?** Native tools, provided by database vendors, vary in their audit capabilities. Some provide only basic audit data that is not enough to satisfy audit requirements. Due to the considerations mentioned above, the usage of native tools can be very problematic for the following reasons:
  - Lack of visibility, which is dependent on the tool’s audit capabilities.
  - No separation of duties since native tools are available to DBAs.
  - No centralized management because native auditing needs to be enabled, and policies need to be defined, on each and every server.
  - No real-time alerts that allow users to receive notifications about important events. Instead, users search audit data manually.
  - High performance impact on monitored servers: in some cases, native audit tools can consume up to 50% of the CPU resources.
  - Native database logging tools require a high investment in time and expertise since they are manually operated. As a result, U.S. businesses spent over $2.5 billion USD on head count costs for SOX compliance in 2007. These compliance expenses escalate disproportionately every time a new regulation is introduced.
SecureSphere—The Trusted Choice for Database Security

SecureSphere Database Security Solutions offer organizations cost-effective, practical products that lower auditing expenses while bolstering database security.

What Are SecureSphere Database Security Solutions?
SecureSphere Database Security Solutions are a family of products that audit and protect databases.

- SecureSphere Database Activity Monitoring (DAM) supports database discovery, vulnerability and configuration assessment, database activity monitoring, auditing, real-time alerts, and compliance reporting.
- SecureSphere Database Firewall (DBF) adds the ability to block database attacks and unauthorized access in real time. The firewall also provides virtual patching capabilities by blocking attempts to exploit known vulnerabilities. DBF includes all the functionality available in the DAM solution.
- SecureSphere User Rights Management for Databases (URMD) enables automatic aggregation and review of 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.
- SecureSphere Discovery and Assessment Server (DAS) provide vulnerability assessment and configuration audits that allow users to measure compliance using 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 organizations prioritize and better manage risk mitigation efforts.

The SecureSphere Platform: Superior Performance, Scalability, and Flexibility for Every Network
These SecureSphere Database Security Solutions are available on purpose-built appliances that deliver unmatched performance, scalability, and flexibility to meet the needs of the most demanding network environments.

Virtual appliances meet the needs of customers who want to leverage existing hardware, maximize the utilization of their servers and network infrastructure, and cut power, cooling, and support costs.

SecureSphere Database Security Solutions also utilize light-weight host-based agents to monitor and audit database activity, and manage privileged user access to sensitive data.

2 AMR Research, "With GRC Spending at an All-Time High, What Happens to SOX?", 2008
SecureSphere provides a flexible architecture that allows organizations to deploy an optimized mix of agent-based and network-based activity monitoring to meet their needs. Architecture components are transparently deployed, without requiring any database, application, or network topography changes.

The SecureSphere MX Management Server provides a single point for managing, monitoring, and reporting on multiple SecureSphere gateways. By centralizing administrative tasks, SecureSphere provides a global view of data security across all database platforms.

**Achieving Cost-Effective Security and Compliance with SecureSphere Database Solutions**

SecureSphere Database Security Solutions are designed from the ground up to meet the audit, assessment, and security requirements of mission critical databases. These solutions include several features and capabilities that reduce the costs and resource investment of implementing and maintaining database security and compliance.

**Reducing Cost through Consolidation and Centralization**

By consolidating audit efforts across heterogeneous platforms, SecureSphere eliminates the need to deploy and manage multiple specialized tools. From the centralized user interface, security and compliance professionals can easily manage audit and security policies, assess vulnerabilities, manage risk mitigation efforts, and produce reports to demonstrate compliance with various regulations.

**Reducing Cost through the Automation of Manual Processes**

Manual reporting processes are expensive. They require the same investment of time and resources every time a report is needed. Manual reporting processes are also error prone. Individuals who are tasked with daunting manual processes tend to burn out quickly, which leads to high turnover and related recruitment and training costs.

Automation enables reliable, repeatable processes and frees up resources. It is also a regulatory requirement.

**Return on Security Investment**

SecureSphere provides immense benefits by safeguarding database assets. SecureSphere delivers the most comprehensive and accurate protection available; detecting database attacks, SQL protocol violations, and unauthorized behavior. This protection can save companies millions of dollars when compared to the economic impact of a data breach.

**Enabling Effective, Proactive Risk Management**

In addition to real-time security, SecureSphere helps organizations focus and prioritize their IT security spending. SecureSphere can discover database servers in the organization, and classify sensitive data in these databases. Combining this information with the results of vulnerability and configuration scans, SecureSphere provides a risk navigation dashboard that highlights areas of risk to data.

User rights management enables automatic aggregation and review of user rights, focused analysis of rights to sensitive data, and the identification of excessive rights and dormant users based on organizational context and actual usage.
Reducing the Impact of a Data Breach

SecureSphere provides real-time alerts on database breach attempts, enabling security professionals to take immediate action. Organizations can also choose to automatically block events that violate data access policies.

SecureSphere’s comprehensive audit trail boosts forensics efforts. By recording detailed information about every query, SecureSphere provides information about the who, what, when, where, and how, including the business context of the event. This enables investigators to have full visibility into suspicious transactions, accurately assess the scope of a security incident, and limit overall liability.

Reducing the Cost of Maintaining Up-to-Date Solutions

SecureSphere Database Security Solutions provide additional benefits out-of-the-box that speed up the implementation of security and compliance controls. This includes audit and security policies and pre-defined, customizable reports. Automated feeds from the security and compliance experts at the Imperva Application Defense Center (ADC), ensure that SecureSphere is always armed with the latest defenses against new threats and the most recent regulatory compliance best practices.

Summary

As compliance regulations become more stringent and database threats escalate, the need for database security has become imperative. At the center of this perfect storm are a host of regulations that mandate database protection and enforce incident response. Initiatives such as the PCI Data Security Standard set forth database security and monitoring requirements to protect private information, like card holder information. Other regulations, like SOX, require that businesses implement controls to ensure the integrity of their financial data. SecureSphere Database Security Solutions not only satisfy these compliance requirements, but also lower the recurring costs associated with manual audit and reporting.

SecureSphere Database Security Solutions also safeguard database assets from attack, and reduce the risk of a data breach which can lead to brand damage, lawsuits, and fines. SecureSphere ensures that organizations, most sensitive and strategic information is safe.

With its indisputable value, it is not surprising that SecureSphere has become the market leader in application and data security. Trusted by hundreds of leading organizations around the world, SecureSphere is the most practical, cost-effective solution for database security and compliance.

About Imperva

More organizations trust Imperva to protect their business applications and databases than any other vendor. Only Imperva delivers innovative technology to give full audit accountability and separation of duties to meet regulatory compliance. The award-winning Imperva SecureSphere is the only solution that delivers full activity monitoring from the database to the accountable application user.