Database Auditing Best Practices

INTRODUCTION

Database auditing signifies different things to different people. In the context of the consolidated compliance requirements, one can break down database auditing into two major categories: Activity Auditing and Security Auditing—both of which have components of controls and measure that map directly into the various compliance requirements of Sarbanes Oxley, Graham Leach Bliley, California Senate Bill 1386, etc. as well as best security practices as defined by ISO 17799, FISMA, the Federal Information Systems Management Act or PCI, the consolidated Payment Card Industry Data Security Standard jointly developed through the collaboration of VISA, American Express, Diner's Club, Discover Card, JCB and MasterCard.

This paper approaches the issue of Database Auditing and how to employ best practices from the perspective of a blended view of: Conventional IT Auditing, Best Security Practices and Industry Compliance Requirements. In this paper, two major categories of data access and controls are broken down into five specific activities of best practices that will be explored and then a solution for next steps is provided. The following five activities are as follows:

- **Access and Authentication Auditing**
  Determine who accessed which systems, when, and how.
- **User and Administrator Auditing**
  Determine what activities were performed in the database by both users and administrators.
- **Suspicious Activity Auditing**
  Identify and flag any suspicious, unusual or abnormal access to sensitive data or critical systems.
- **Vulnerability and Threat Auditing**
  Detect vulnerabilities in the database, then monitor for users attempting to exploit them.
- **Change Auditing**
  Establish a baseline policy for database; configuration, schema, users, privileges and structure, then track deviations from that baseline.

DATABASE AUDITING OVERVIEW

Database auditing is more than just tracking and monitoring user activity. It is about dealing with all of the aspects that effect database information controls and counter measures, while also managing all possible means of authorized and un-authorized access to view or modify sensitive data that resides in enterprise databases. It also deals with the monitoring and enforcement of access control policies, configuration standards, and vulnerability management on a regular basis.

Auditing is an important component in a defense-in-depth approach to database security. Privacy, integrity and confidentiality of the data, as well as accountability for changes to that data, are the driving forces behind the need for audit. These are the same forces that drove the creation and enforcement of regulations such as: Sarbanes Oxley, HIPAA, GLBA, SB 1386, and FISMA. Each of these compliance regulations impose similar requirements for the industries they serve. Each one:

- Puts the responsibility and accountability for data privacy and integrity on the corporation or organization that owns and maintains the assets.
- Stipulates control measures that require traceable evidence of security and controls improvement over time.
- Requires the implementation of control measures that must be in place to assess security exposures as well as monitor for unauthorized, malicious and/or abusive behavior by both internal and external threats.
- Mandates that complete records be maintained for all aspects of database information. These records create the audit trails that clearly show who did what, when they did it, and how they did it. Audit trails will also ensure that an organization's data is used only as intended and in appropriate fashion.

To be effective, auditing must be implemented via a methodical and repetitive process. This process needs to be guided by a purpose-built policy driven framework that is simple to implement and comprehensive in scope. Framework standards such as COBIT, COSO, and ISO 17799 are great places to start when setting goals and building an auditing policy and methodology. However, auditing programs that focus on any subset of the five best practice categories defined herein are insufficient and leave the underlying data exposed to the threat of breach, theft and/or deliberate or even inadvertent data corruption.

Moreover, in most of today's enterprise environments, Database auditing requirements are ever evolving and will continue to do so. Periodic review and refinement of the process and underlying policies is critical, particularly as components of the threat environment changes. The implementation must not only be highly repetitive, and in many cases continuous, but it must also be easily adaptable to changes in the threat landscape, user environment as well as adaptable to the ever-changing application infrastructure these critical databases serve.

Access and Authentication Auditing

It is insufficient to merely restrict or grant access to certain users; all database access must be closely controlled and audited in order to maintain a complete record of who accessed what information.

Access auditing allows organizations to determine which users accessed which systems, which data was accessed, when the access occurred, and where the access originated. Inappropriate behavior, such as unnecessary access to sensitive systems, access outside of business hours, or from outside the corporate network, will become evident within the access and authentication audit logs. In the case of a potential breach, this information is critical in determining what, if any, systems were compromised. Both industry and government regulators have noted the importance of this type of auditing. PCI-DSS, COBIT, and ISO 17799 all specify the need to audit for access and authentication.

Access and authentication auditing ensures that critical systems and data are accessed by only known authorized users, and that all of their actions can be traced. Key controls in this area include monitoring who is logging in, what time they login, which hosts they connected from, and which applications they used to access the database. Failed attempts to login to the database should also be monitored, as this information can be indicative of attempts to gain unauthorized access.

User and Administrator Auditing

Auditing administrator and authorized user access is critical to the success and reliability of any audit system. Tamper resistance in the audit system, secure storage of audit data, and separation of duties between the watcher and the watched are all critical in order for audit logs to be meaningful and trustworthy.

Auditing actions performed in the database gives an organization a granular view of access and modification to data, changes to configuration and structure, and modification of security-related controls and settings. Inappropriate modifications to sensitive data, unapproved changes to configuration or security settings, and potentially disruptive changes to database structure all become evident within the user and administrator audit logs. In the case of a potential breach, these logs identify

what data was accessed or what configuration changes were made. Providing this type of evidence could mean the difference between fully disclosing an incident where private data MAY have been leaked, and keeping private a close call where an intruder got in, but where data was not leaked.

User and administrator auditing provides a very detailed view into exactly what users are doing in the database, and how they are doing it. Here, the exact database queries are captured and stored, along with information about the user, application and the host who executed them. Auditing should include all DDL and DML statements issued by ad-hoc query tools, along with any modifications to database configurations such as privileges, user accounts, or authentication settings.

Suspicious Activity Auditing

Suspicious activity auditing involves analyzing the data collected during access/authentication auditing and user/administrator auditing to look for patterns that indicate misuse. This information is critical, as it boils down a large amount of data into normal and suspicious categories, allowing administrators to quickly put a halt to misuse. Traditional or network Intrusion Detection Systems do not have the capability to detect the subtle differences between normal and suspicious access; however, specialized auditing systems do. Detecting abnormal access can often stop attackers in the early information-gathering phase, long before any real damage is done. Putting measures in place to detect and stop misuse of sensitive data (financial data, customer data, etc…) are what regulations such as SOX, GLBA, HIPAA and PCI-DSS are all about.

Suspicious activity auditing examines behavior by looking for access events that do not fit into an established baseline. Simple examples of these events include detecting a connection to an Oracle database from TOAD when that database is normally only accessed by SAP, or detecting access to a critical internal database from a host that is outside the trusted corporate network. Detecting suspicious and abnormal access is a powerful tool to protect sensitive data and ensure regulatory compliance.

Vulnerability and Threat Auditing

Vulnerability and threats can easily occur at anytime and often come from unexpected sources. Vulnerability and threat auditing involves detecting vulnerabilities in the database, then monitoring for users attempting to exploit them.

Vulnerability and threat auditing occurs in two phases: detection and monitoring. First, the vulnerabilities or security weaknesses present in the database must be identified. The most common issues here are: default or weak passwords; un-patched buffer overflow or denial of service vulnerabilities; improper configurations; and, excessive privileges granted to users. Once these vulnerabilities have been identified, monitoring should be deployed immediately to detect anyone that may attempt to exploit the vulnerabilities in an effort to compromise a database or the data within.

Vulnerability and threat auditing allows an organization to determine their level of risk of database compromise, and then take significant steps to mitigate that risk by continuously monitoring for known attacks in the database. This type of auditing is also important from a regulatory perspective. While some regulations are specific about the need for scanning and monitoring (such as PCI-DSS), others are more vague. Vague regulations tend to allow organizations to justify the efforts they have (or have not) taken to protect sensitive data. Vulnerability scanning and threat monitoring are widely accepted methods of securing systems and the data within. Building a case for a data security program that does not include scanning databases for vulnerabilities is quickly becoming difficult or impossible to justify to organizations such as the SEC or FTC.

With vulnerability and threat auditing, scanning for proper password strengths, up-to-date patch levels, proper configurations, and access controls is a critical first step, as it provides an organization with a better view into the business risks associated with their database security stature. This information also allows organizations to create targeted policies that monitor only for the vulnerabilities that exist in a system. A best of breed approach includes vulnerability scanning on a monthly basis that is integrated with a 24/7 monitoring system that provides real-time alerting on attacks and misuse. Integrating this approach allows organizations to reduce the risk of a database breach to well within the comfort zone.

Change Auditing

Change auditing involves detecting changes in key areas of the databases structure and configuration. By providing a complete picture of before and after values, administrators are able to measure and compare any differences, allowing them to determine not only which changes are acceptable and should be added to the baseline, but also which changes are unacceptable and must be rolled back. Change auditing allows organizations to detect changes made by software updates, patches, automatic batch processes, and ad-hoc changes by users or administrators. This data can be used to measure the health of a database, quickly detect changes in permissions or roles, and to check for configuration compliance of a database before

leaving QA for production. The ability to detect these changes in the database is a critical component in maintaining the security controls mandated by both industry and government regulations.

THE SOLUTION: APPSECINC

Application Security, Inc. (AppSecInc) provides a complete database security solution, addressing all aspects of database auditing. Recognized as "the most complete database security suite" by Forrester Research, AppSecInc products protect databases at many of the world's largest enterprises. Through the AppSecInc Console™, organizations get a centralized management and reporting system that covers all databases within an enterprise. Combining the capabilities of AppDetective™, the industry standard for database vulnerability assessment, with real-time monitoring of database activity via AppRadar™, the AppSecInc Console provides a holistic view of an enterprise's overall database security posture. With a big picture overview, CISOs can create a far more accurate assessment of business risk and regulatory non-compliance.

A role-based access control system that integrates seamlessly into an active directory infrastructure ensures that only authorized individuals have access to the system that provides complete coverage of Microsoft SQL Server, Oracle, Sybase and IBM DB2 databases. A centralized reporting system with an executive dashboard ensures the proper level of detail is available for any type of user, from a database administrator to the corporate CIO. The AppSecInc Console is designed to assist organizations in implementing a comprehensive vulnerability management lifecycle approach to database security. The system will discover applications, establish a baseline of vulnerabilities, prioritize based on risk, provide guidance to take corrective actions and eliminate root causes, and continuously monitor the environment for threats and changes.

Much of the core functionality of the AppSecInc Console is provided by AppDetective and AppRadar. AppRadar is a real-time database monitoring system designed to carefully analyze every database transaction in order to implement several key auditing controls. Access and authentication auditing, user and administrator auditing, suspicious activity auditing, and threat monitoring are handled all at once by AppRadar. AppDetective is an award-winning database vulnerability scanner with the capability to discover any database running on the network, perform in-depth scans of databases for vulnerabilities, and provide details on fix information, including customized remediation scripts. Complete with a Security Change Auditing module that systematically detects and highlights any schema, user, or configuration change in the database, AppDetective fulfills the requirements of both vulnerability and change auditing.

CONCLUSION

A business is only as good as its data. Protecting and regularly auditing the database should never be left to chance or patchwork solutions. A complete all-inclusive auditing solution must be implemented that can easily accomplish each of the following key areas:

- Access and Authentication Auditing
- User and Administrator Auditing
- Suspicious Activity Auditing
- Vulnerability and Threat Auditing
- Change Auditing

Without an all-encompassing auditing solution, organizations put their precious data at risk. Corrupt, inaccurate, or compromised data equals lost money, lost time, and compromised customer and employee relationships.

ABOUT APPLICATION SECURITY, INC. (APPSECINC)

AppSecInc is the leading provider of application security solutions for the enterprise. AppSecInc's products—the industry's only complete vulnerability management solution for the application tier—proactively secure enterprise applications at more than 350 organizations around the world. By securing data at its source, we enable organizations to more confidently extend their business with customers, partners and suppliers while meeting regulatory compliance requirements. Our security experts, combined with our strong support team, deliver up-to-date application safeguards that minimize risk and eliminate its impact on business. Please contact us at 1-866-927-7732 to learn more, or visit us on the web at www.appsecinc.com.

APPLICATION SECURITY, INC.

www.appsecinc.com

575 8th Avenue, Suite 1220, New York, NY 10018 TOLL FREE 866 9APPSEC MAIN +1 212 912 4100 FAX +1 212 947 8788