

The Rise of the Insider Threat at the Database Level & How to Counter Privileged Users of Sensitive Information

Rob Barnes
Application Security, Inc.



2010 ROCKY MOUNTAIN
**Information
Security
Conference**

**222 million records were
compromised in 2009**

Agenda

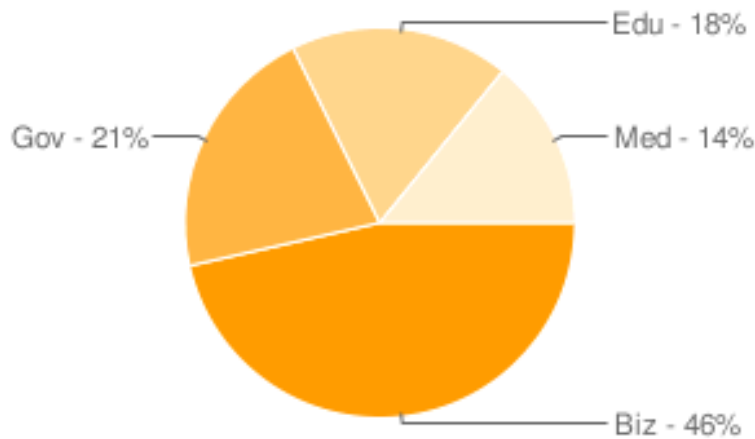
- Threat Background
- Defining the Insider Threat
- Countermeasures/Leading Practices

Database Security Threats Continue to Increase

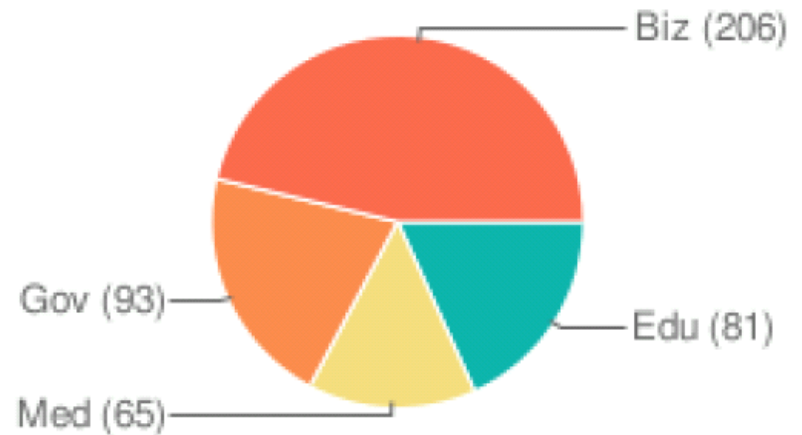
- The database security landscape has changed:
 - Organizations increasingly grant access to a growing number of users: employees, contractors, suppliers, partners and 3rd party vendors, etc.
 - Attackers have gone pro
- Attacks are moving to the database where records can be harvested en mass
- Perimeter security measures are necessary but not sufficient
- Once the perimeter is pierced, organizations often have little-to-no protection at the database application layer
- Data demands of numerous users require access to data—which leaves systems vulnerable
- Poor access control and excess permissions continue to provide attack vectors for hackers, crackers and malicious or careless insiders

To Make Matters Worse - Threats Are Very Real

Incidents by Business Type - Last Year



Incidents By Sector

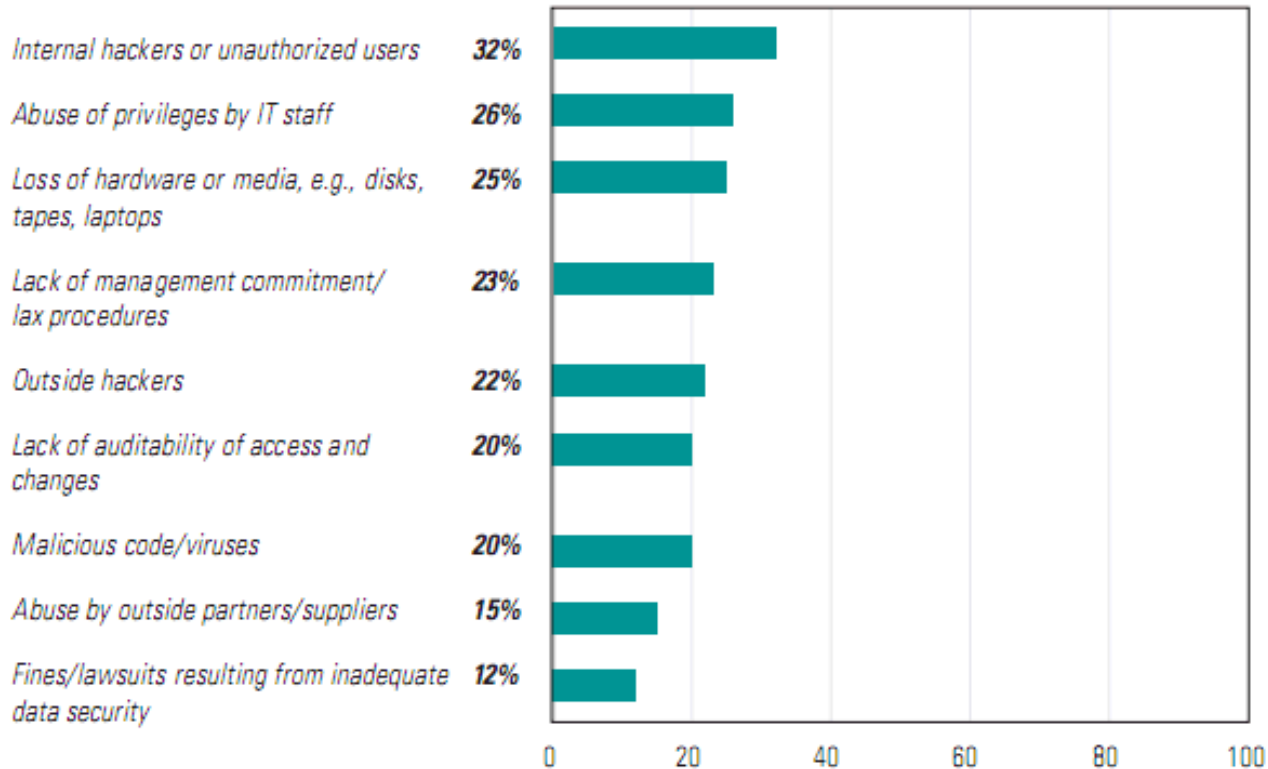


Dataloss Database Website

The Insider Threat Remains the Top Concern

Figure 10: Greatest Risks and Threats to Enterprise Data

(Respondents ranking "4" or "5" in severity on a scale of 1 to 5)



Source: 2009 Independent Oracle Users Group (IOUG) Data Security Report

Overview: Database Breaches

- Who is behind data breaches?
 - 74% external sources
 - 32% business partners
 - 39% multiple parties
 - **20% insiders**



Source: Verizon 2009 Data Breach Investigation Report

Defining The Insider Threat



According to CERT, Definition of a Malicious Insider

Current or former employee, contractor, or business partner who

- o has or had authorized access to an organization's network, system or data and
- o intentionally exceeded or misused that access in a manner that
- o negatively affected the confidentiality, integrity, or availability of the organization's information or information systems.

The Database “Insider Threat”

Who are Insiders?

The **CISO** of one of the largest banks in the world says...

“I define insiders in three categories

1. Authorized and intelligent
 - use IT resources appropriately
2. Authorized and “stupid”
 - make mistakes that may appear as malicious or fraudulent
3. Unauthorized and Malicious
 - mask either their identity or their behavior or both!

The first two categories I can identify and track with identity management systems

– the latter, I can not!!”



Understanding the Insider Risk

Anyone with knowledge of the database or systems is a potential threat...

Authorized Users

- Employees - Clerks, accountants, finance, salespeople, purchasing, etc.

Privileged Users

- DBA's, DB/App developers, application QA, contractors, consultants

Knowledgeable Users

- IT Op's, Network Op's, security personnel, audit personnel

Outsiders or Malicious User with Insider Access and/or vulnerability knowledge

- The sophisticated "white collar" criminal

Insider Attacks

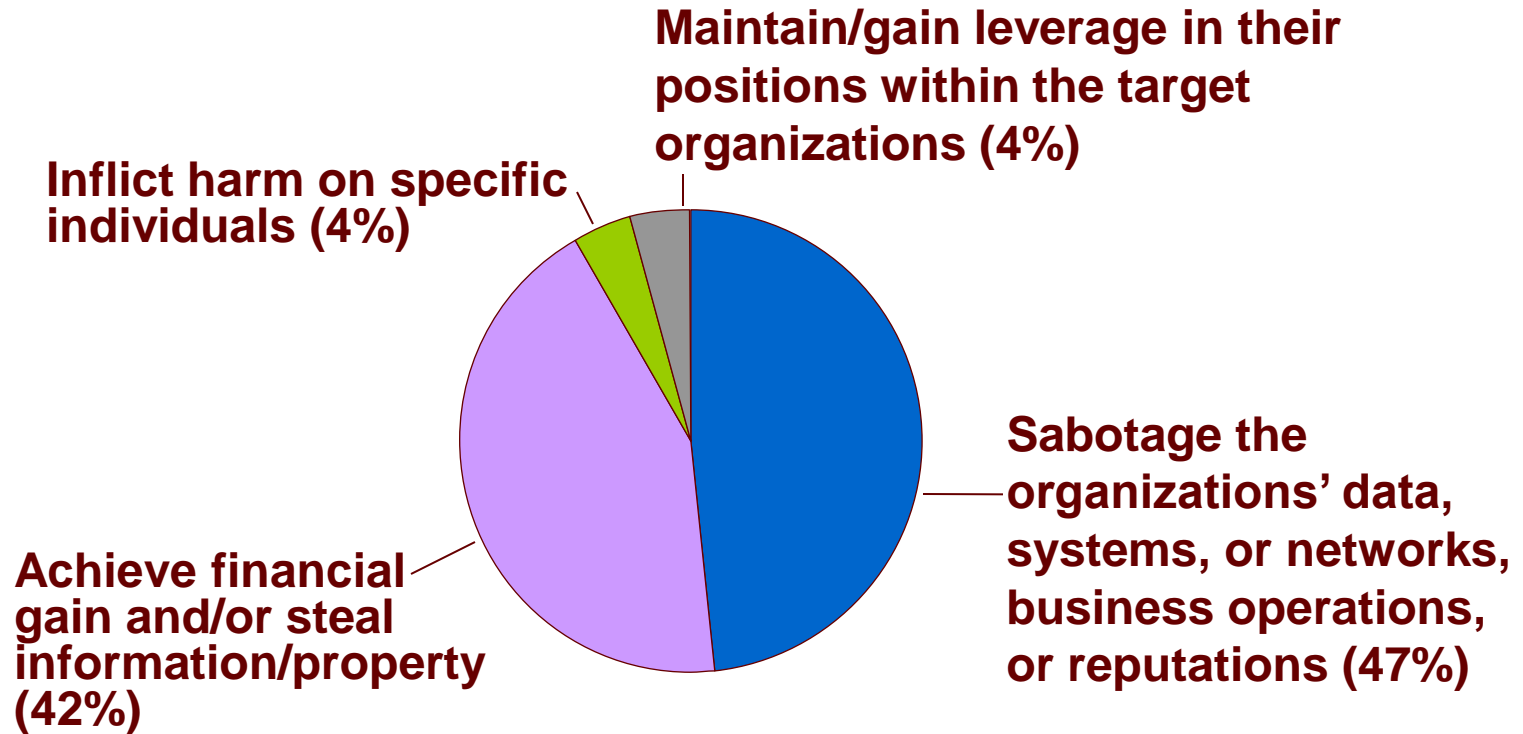
DBA steals data from their own database

Employee leaves a door open to let a criminal in

IT Admin sells a network diagram and vulnerabilities list

User abuses network access to hack database systems

The Insider Threat is Motivated and Capable



Key Findings: Insider Threat Study

- Over half of the insiders used relatively sophisticated tools or methods for their illicit activities, including scripts or programs, autonomous agents, toolkits, probing, scanning, flooding, spoofing, compromising computer accounts, or creating unauthorized backdoor accounts
- Only half of the insiders had authorized access to the system/network at the time of the incidents; the others gained access in other ways
- Most activities were planned in advance but the attacks themselves were often triggered by a work-related event
- The majority of insiders took steps to conceal what they did

Source: U.S. Secret Service and CERT/SEI 2008 Insider Threat Study

Key Findings: The Insiders

Characteristics

- Current and former employees carried out illicit insider activities in nearly equal numbers.
- Most insiders were either previously or currently employed full-time in a technical position within the organization
- Insiders represented a wide range of ages, from 17 to 58 year, and a variety of racial and ethnic backgrounds

Key Findings: The Insiders (cont.)

Motives

- Multiple motives were reported for the majority of insiders. Revenge was reported as the main motive in just over half the cases.
- The most frequently reported goals of insider attacks were financial gain, theft of information/property, and sabotage to the organization.
- Seventy-six percent of the insiders developed plans in advance to harm the organizations.

Implications

- An Inside threat can come from anywhere within the organization. It's impossible to predict where the threat will come from



Understanding the Threats

Emerging Database Threats

- Sophisticated attacks that exploit un-patched vulnerabilities
 - Double or triple encrypted SQL-injection attacks that render web-application firewalls virtually useless
 - Insider attacks
 - Insider mistakes
-  **The Insider Threat**
- Advanced identity theft via database rootkits
 - Increasingly sophisticated social engineering leading to full-blown database disclosures
 - Weak or non-existent audit controls
 - Powerful self-propagating attacks distributed via “infection kits” on legitimate websites and other creative means

How Are Databases Hacked

Exploiting known/unknown vulnerabilities:

This is one of the easiest and preferred methods that criminals use to steal sensitive information.

- Attackers can exploit **buffer overflows**, **SQL Injection**, etc. in order to own the database server.
- Via this method, firewalls are completely bypassed and databases can be hacked from the Internet.

Exploiting misconfigurations:

Misconfigurations can leave databases vulnerable with excess functionality or security holes.

Password guessing/brute-forcing:

If passwords are blank or not strong they can be easily guessed/brute-forced. After a valid user account is found its easy to compromise the database.

How Are Databases Hacked (cont.)

Installing a rootkit/backdoor:

Actions and database objects can be hidden so administrators won't notice someone has hacked the database.

- The hacker continues to have access.
- A database backdoor can be used, designed to steal and transmit data and/or to give the attacker stealth unrestricted access at any given time.

How Are Databases Hacked (cont.)

Delivering a Trojan:

Not a common database server attack, but this is a frequent choice of Insiders.

- Delivered by email, p2p, IM, CD, DVD, pen drive, etc.
- Once it is executed, it will stealthily and automatically obtain information using ODBC, OLEDB, JDBC configured connections, sniffing, etc.
- When enough information is collected, the trojan can connect to database and begin stealing data.
- Can also run zero-day attacks to elevate privileges to own the database server, install rootkits to hide its actions, send the stolen data (encrypted) to the “**Evil Lair**” by email, HTTP, etc.

Native Logs Are Incomplete - SQL Server Example

Events Captured by the SQL Server Error Logs and Windows Application Logs:

- Failed or successful login attempts
- Backup and restore information
- Extended stored procedures Dynamic Link Library (DLL) loading
- Server options being disabled/enabled (sp_configure)
- Database options being changed (sp_dboption)
- Some Database Consistency Checker (DBCC) commands
- Error messages

Types of events you will not find in the error logs:

- Extended stored procedures execution
- SELECT statements
- Some DBCC commands execution
- Data Definition Language (DDL) statements (structure)
- Data Manipulation Language (DML) statements (manipulation)

To identify data that was accessed or changes that were made to the data or structure of the database, one has to look elsewhere

Countermeasures: Database Security Best Practices



Leading Practices: Stopping the Attack

Key Findings

- Half of the insiders had authorized access to the systems/networks at the time of the incidents.
- Over half of the insiders used relatively sophisticated tools or methods for their illicit activities.
- Over half of the insiders exploited systemic vulnerabilities in applications, processes, and/or procedures.



Leading Practices: Stopping the Attack

Implications

- Apply the principle of “least privilege” giving users only the access they need to do their jobs – separation of duties
- Eliminate weak or default passwords on systems
- Maintain role-based access controls and disable access after an employee changes positions within a company
- Formal policies and procedures for disabling access upon an employee’s termination or resignation should be established and followed
- Procedural and technical controls should be established for system administrator functions
- Periodic account audits should be conducted to check for unneeded or unauthorized accounts, including: Remote access accounts, login accounts, DBA accounts, application, customer, and company accounts

Database Security Leading Practices

Assess Security Posture

- Assess database security risks
- Determine processes, applications and systems affected
- Prioritize risk and establish work plan



Address Risk

- Document risks and controls
- Align business and IT goals
- Develop business case for investment in security



Implement Monitoring

- Implement the program
- Monitor risks and controls
- Distribute BI and Analytics reports to provide perspective to executive teams
- Test and remediate
- Audit and attest
- Measure and monitor readiness



Establish Controls

- Set responsibilities and accountability
- Establish mechanisms for reporting and assessment
- Apply the principle of least privilege and role based access controls
- Implement policies and procedures to minimize exposure

Addressing Database Vulnerabilities

- Start with a Secure Configuration
- Stay Patched
 - Stay on top of all the security alerts and bulletins
- Defense in Depth / Multiple Levels of Security
 - Regularly scan your databases for vulnerabilities
 - Fix the problems reported!
 - Implement database activity monitoring...
 - ...and database intrusion detection
 - Especially if you can't stay patched!
 - Encryption of data-in-motion / data-at-rest



Summary

- Don't forget the database.
- Who are your insiders, and what are they doing?
- Understand the threats...all insiders are capable of hurting your business... whether they know it or not.
- You can limit your exposure to the Insider Threat... it's actually pretty easy to do.**



** If your boss gives you money, resources, trusts and empowers you, etc... 😊

Do You Know What You're Up Against?

**APPLICATION
SECURITY, INC.**

appsecinc.com

