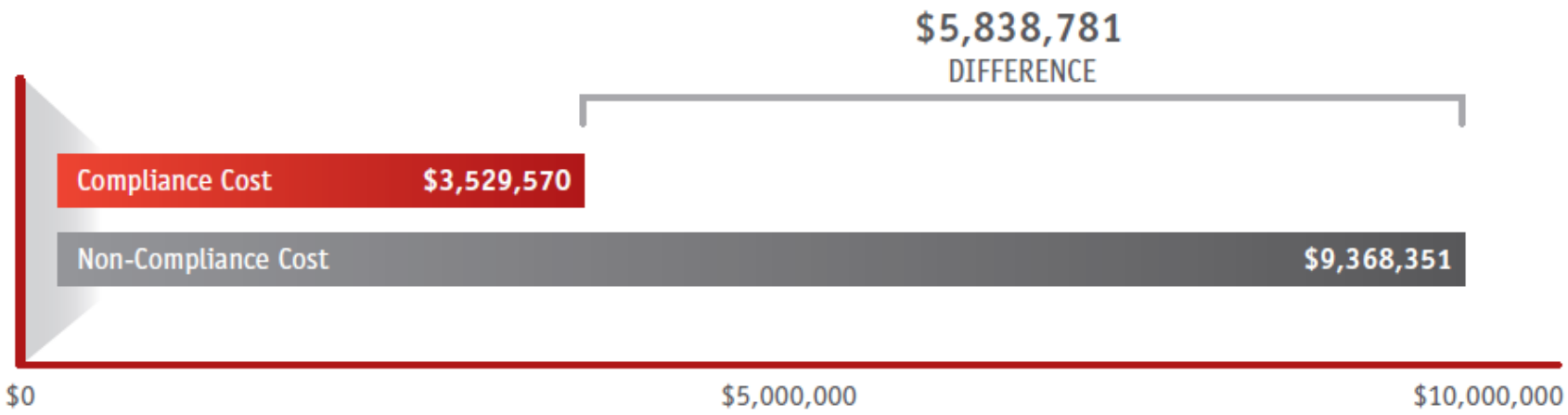
APPLICATION SECURITY, INC.

Database Risk in 2011

Mark Trinidad
Sr. Product Manager
Application Security, Inc.

ISACA
Trust in, and value from, information systems
Tulsa Chapter

Why Bother?



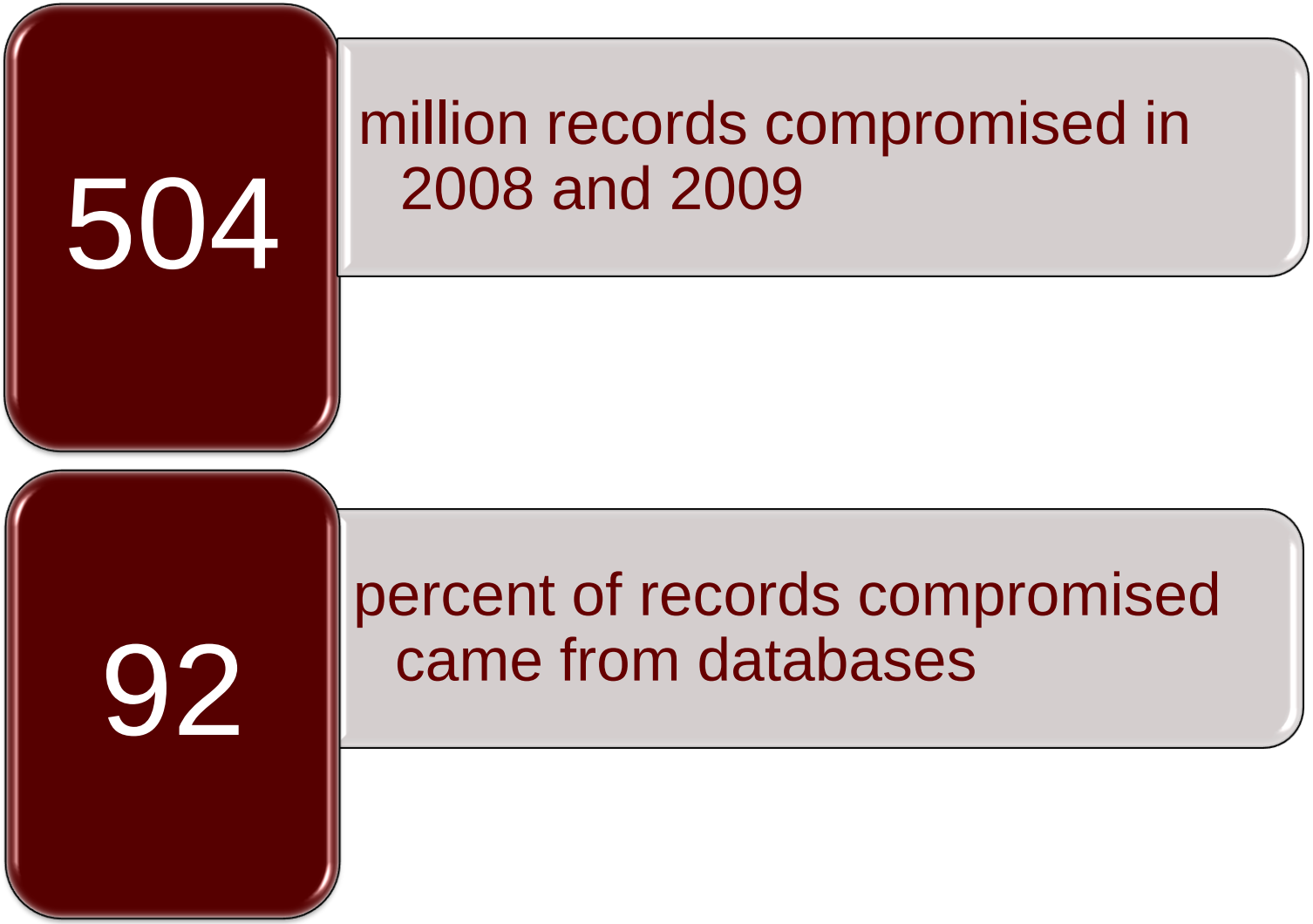
Source: True Cost of Compliance Report, Ponemon Institute, Jan 2011

Does Database Risk Factor into IT GRC?

YES

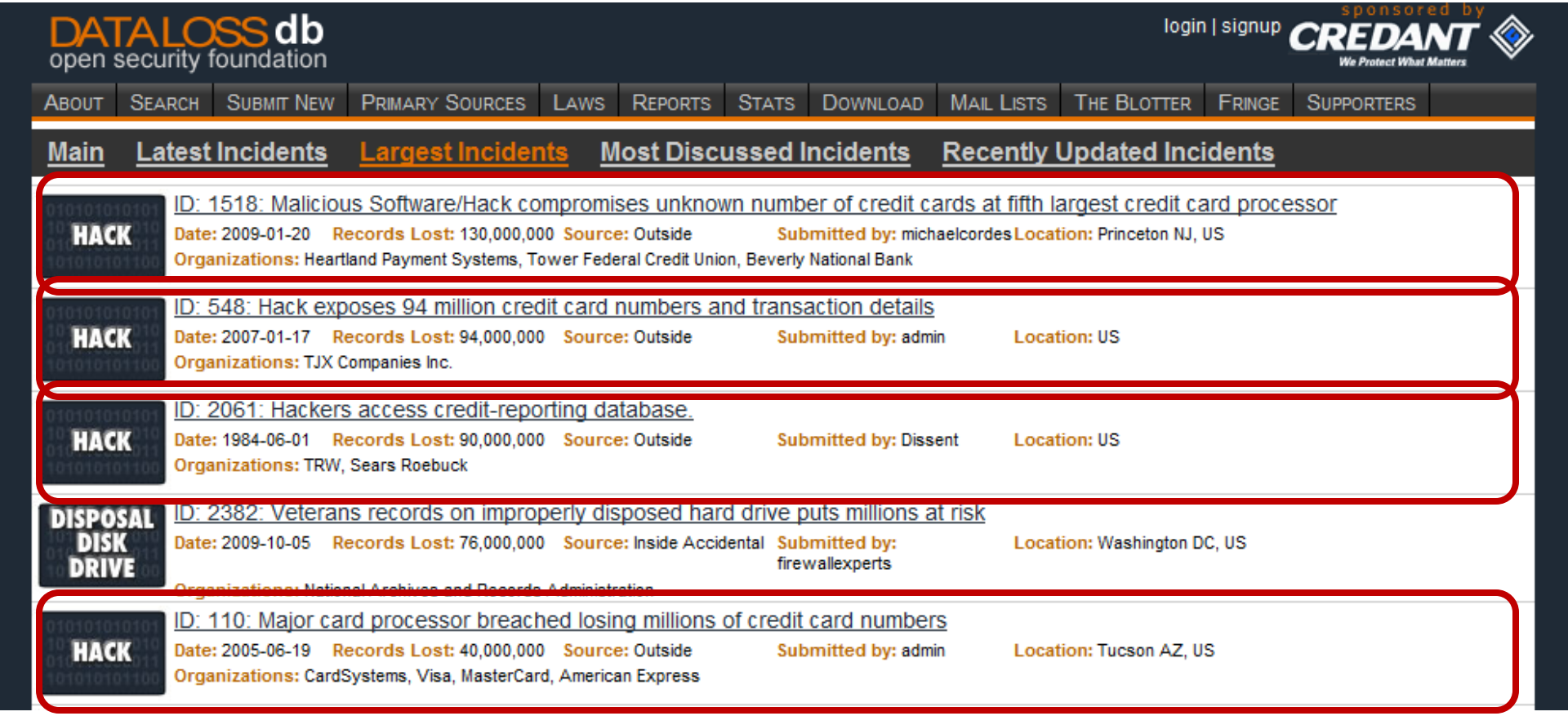
It has to….somehow….

Understanding Database Risks: The Facts



Source: Verizon 2010 Data Breach Investigations Report

Understanding Database Risks: The Facts

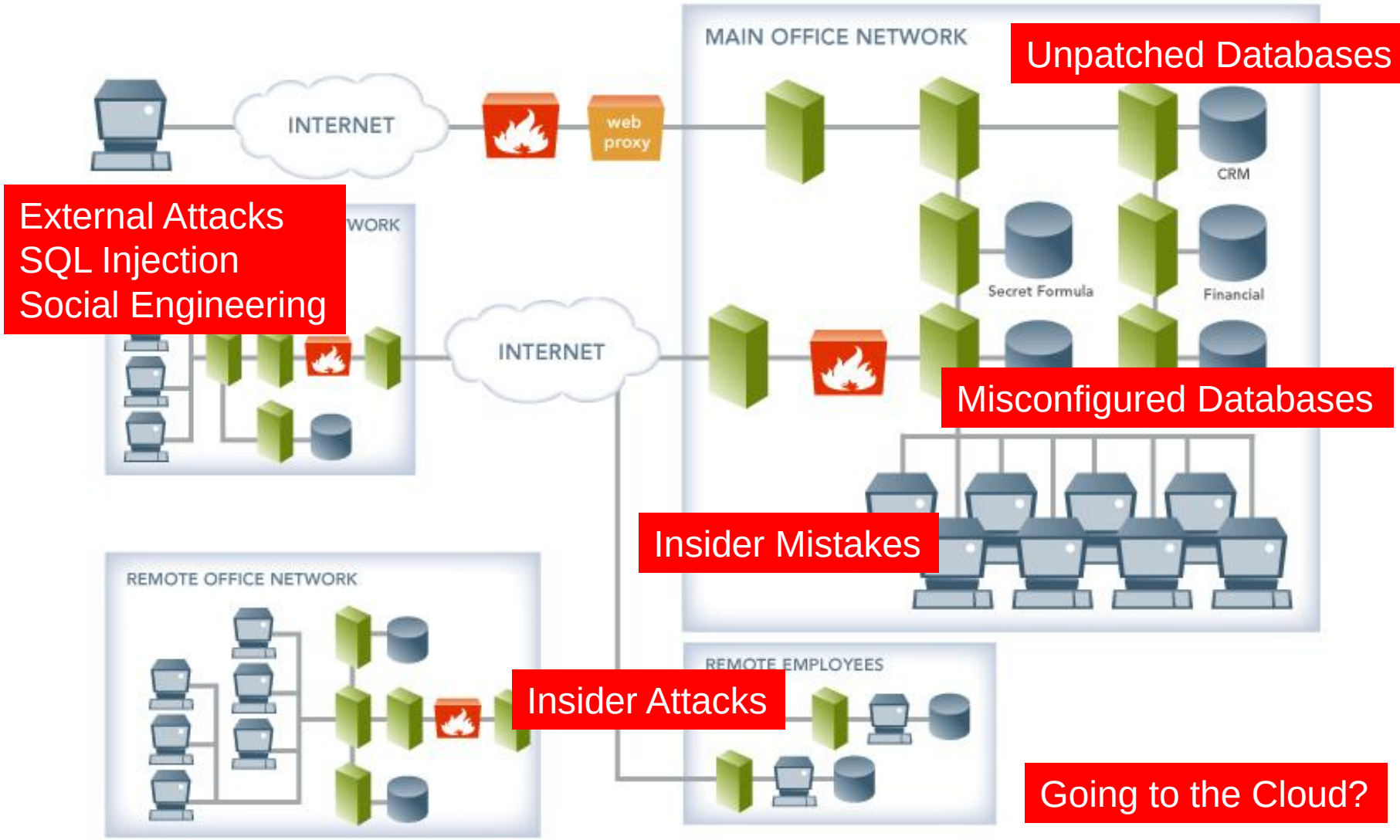


Source: www.datalossdb.org

Understanding Database Risks: The Facts

1. Databases Are the Target
2. Security and Audit Programs Don't Always Do A Good Job at the Database
3. Database Risk Is Not Properly Factored into IT GRC

Database Risks for 2011



Database Risks for 2011

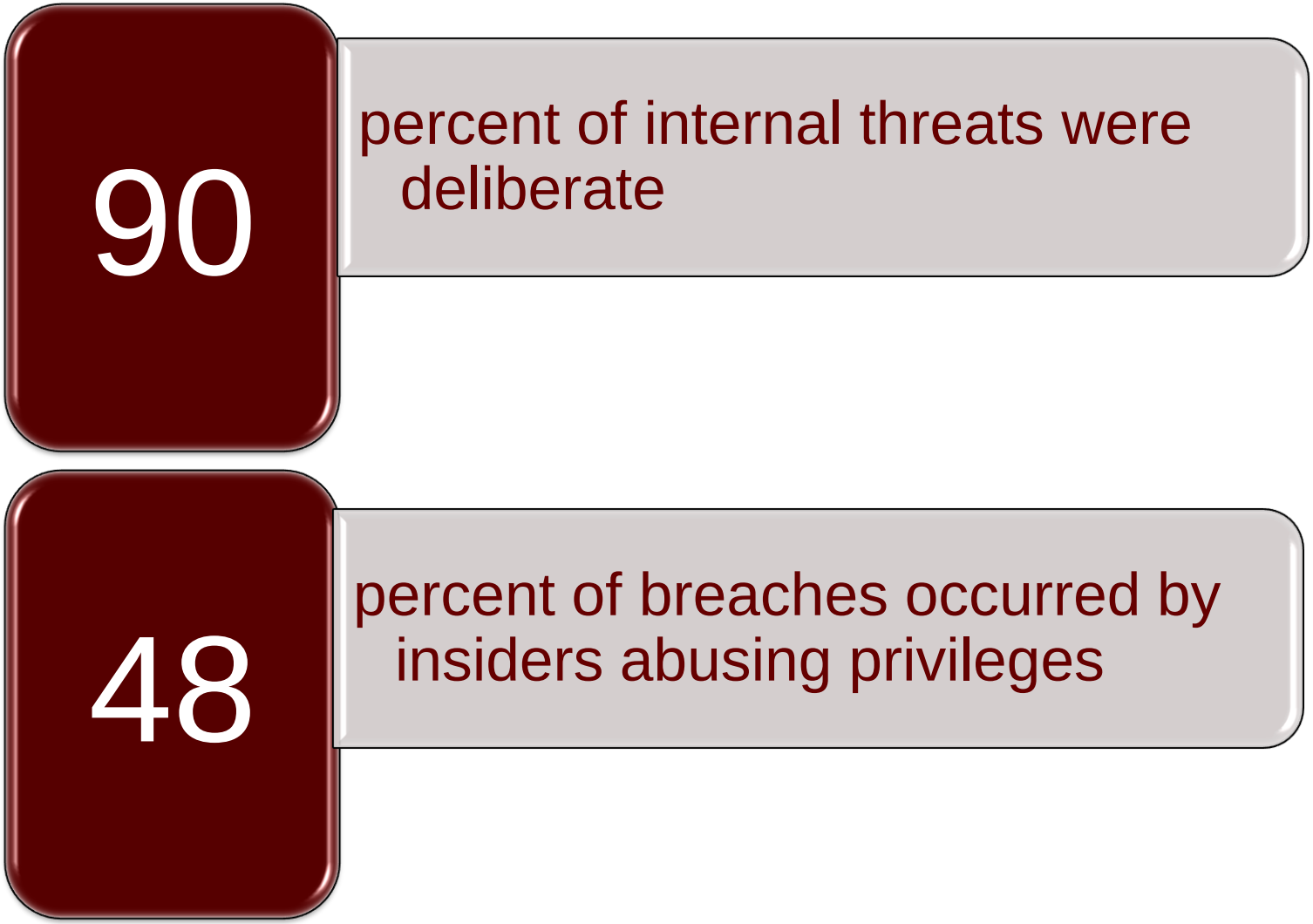
- Unpatched Databases = Exploitable Vulnerabilities
  - Attacks on DBMS are increasingly sophisticated, but can be done
  - More subtle methods that defy traditional intrusion detection mechanisms
  - Exploit scripts posted to the web within hours of a patch release

Public exploit code + slow patch cycle = High risk DBMS exposure

Database Risks for 2011

- Misconfigured Databases
  - DBA's understand things, we just don't
  - We understand things, DBA's don't

Database Risks for 2011 – Insider Attacks



Source: Verizon 2010 Data Breach Investigations Report

Database Risks for 2011

- Insider Mistakes
  - Unintentional authorized user attack
  - Accidental deletion or exposure of data
  - Non-malicious security policy circumventions
    - Example: A user copies sensitive info to a thumb drive or notebook to take work home

Database Risks for 2011

- External Attacks
  - SQL Injection still reigns King!
  - Phising
  - Large Scale Recon

Database Risks for 2011

- Cloud Security
  - Uncertainty to data residing
  - What's the SLA from the public cloud vendor?
    - Amazon.com
    - Database.com
    - Many More…

What Can We Do? Database Security Tips for 2011

1. Devise a Database Security Plan
2. Fix Default, Blank and Weak Passwords
3. Regularly Patch Databases
4. Minimize Attack Surface
5. Review User Privileges
6. Locate Sensitive Information
7. Encrypt Sensitive Data in Rest and in Motion
8. Train and Enforce Corporate Best Practices

Database Security Tips for 2011

- Devise a Database Security Plan
  - Start with an established DBMS checklist
    - DISA STIG is an excellent starting point
    - DISA publishes detailed guidelines on how to secure and configure MS SQL server and Oracle
  - Customize to meet your orgs needs.
  - There may be industry regulations to follow – PCI, SOX, HIPAA
  - Once a DBMS security policy is established, build a roll-out plan
    - Pick one or two of the highest priority issues to remediate first
    - As you progress, layer on additional checks and tests

Database Security Tips for 2011

- Fix Default, Blank and Weak Passwords
  - Ensure all databases have complex passwords
  - Eliminate default, blank and weak passwords
  - Use separate passwords for each DBMS instance
  - Extend the same password policy to all N/W logins
  - If possible, consider using N/W authentication
- Regularly Patch Databases
  - Critical patches insure that vulnerabilities are remediated on a regular basis
  - Patching in conjunction with auditing and monitoring increases DBMS protection

Database Security Tips for 2011

- Minimize Attack Surface
  - The DBMS ships with many features that are not used
  - Some of these features have functionality that render a DBMS vulnerable to attack
  - Where possible, disable unused DBMS features
- Review User Privileges
  - Ensure employees only have access to the sensitive data required to do their jobs
  - Map job functions to privileges on IT assets
  - Never assign privileges to guest accounts or PUBLIC
  - Untangle the web of user entitlements

Database Security Tips for 2011

- Review User Privileges (cont.)
  - Implement compensating control for what cannot be fixed
  - Establish strong policy-based access and activity monitoring on critical systems
  - Use activity monitoring and auditing to alert on suspicious activity
  - Alerts can be filtered a disseminated to define groups or individuals based on policy

Database Security Tips for 2011

- Locate Sensitive Information
  - Determine where all sensitive info resides on the N/W
    - Secure the info in those databases first
  - Conduct a comprehensive analysis of:
    - Which users have access to each system
    - Which data and functionality they can access
    - Verify the level of access granted is appropriate based on their job function
  - Implement user entitlement best practices
  - Insure appropriate access and ownership rights to critical data

Database Security Tips for 2011

- Encrypt Sensitive Data at Rest and in Motion
  - Never store sensitive data in clear text in a DBMS where any DBA/IT staff can access it
  - Ensure the data is encrypted and not allowed to travel unencrypted on the network
  - Lock down DBMS vulnerabilities and monitor access to critical data stores to discover attacks
  - SQL injection attacks require a multi-layered defense
    - Protective measures architected with an end-to-end view
    - Web application and DBMS infrastructures scoped into the solution

Database Security Tips for 2011

- Train and Enforce Corporate Security Best Practices
  - Ensure all employees are aware of the orgs. security best practices
  - Create a training program and consistently reinforce policy
  - Extend critical protections at the network and application layer to the DBMS
  - Perform regular DBMS audits, pen tests and misconfiguration checks
  - Activity monitoring to ensure sensitive data is not downloaded or transferred

Actionable Takeaways

1. Target Critical Systems for an Audit
2. Review Password Profile Settings
3. Review Patch Levels and Patch Policy
4. Understand Who's DBA/Sys Admin
5. Understand Who Has Insert, Update, Delete Rights
6. Understand the Risk Involved from Entire System View

Mark Trinidad

mtrinidad@appsecinc.com