APPLICATION SECURITY, INC.

ISACA Houston:

Grounding Security & Compliance Where The Data Lives

Mark R. Trinidad
Product Manager
mtrinidad@appsecinc.com
March 19, 2009

Agenda

- Understanding the Risk
  - Changing threat landscape
  - The target organizations
- Security and Compliance
  - Common control frameworks
  - Business benefits
  - Addressing audit requirements
- Defending the Database
  - Techniques and best practices

Database Security Threats Continue to Increase

- The database security landscape has changed:
  - Corporations increasingly grant access to a growing number of users: employees, contractors, suppliers, partners and 3rd party vendors to name a few
  - 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, enterprises often have little-to-no protection at the database application layer
- 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

Records Lost/Stolen Per Year

Year	Records Lost/Stolen	Records Per Second
2008	15,121,267	1.0803
2007	162,565,103	5.1549
2006	49,679,333	1.5753
2005	55,986,942	1.7753
2004	31,895,900	1.0114
2003	6,405,000	0.2031
2002	4,960	0.0002

CA SB 1386 goes into effect

-Source: http://etiolated.org/statistics

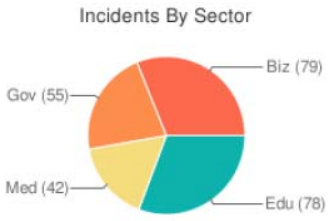
What's the source of the breach?

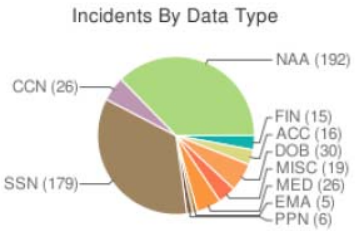
- ~1/3 laptops / hard drives, most incidental
- ~1/3 database breach
- ~1/3 we'll never know

-Source: AppSecInc analysis of media coverage

The Target Organizations—Everyone is at Risk

Target industries included: Banking, finance, retail, government, education, manufacturing, telecommunications, entertainment, media, nonprofits, insurance, pharmaceuticals, healthcare and transportation**—every leading sector**





Source: *Data Loss DB 2008 Report; www.datalossdb.org*

Changing Landscape Yields Greater Risks

- The evolving threat
  - From notoriety to profit motive
- The productivity machine
  - Business enhancements = risk
- Security costs growing 3x faster than IT budgets
  - Point product approaches no longer scale
- Accelerated growth of IP-aware networks
  - Accelerates IT risk
- Rapid growth in data
  - Data is the new currency
- Compliance mandates
  - Driving costs and spending

Common compliance control frameworks

Compliance Requirements

- Sarbanes-Oxley
- PCI
- HIPAA
- FISMA
- GLBA
- Basel II
- California SB 1386
- NERC/FERC
- Massachusetts Data Protection Law
- TARP?

IT frameworks for security control

- CoBiT
- COSO ERM
- NIST 800-53
- ISO 17799

Why combine compliance and database security?

Security best practices at the database level must address risk from inside and outside threats.

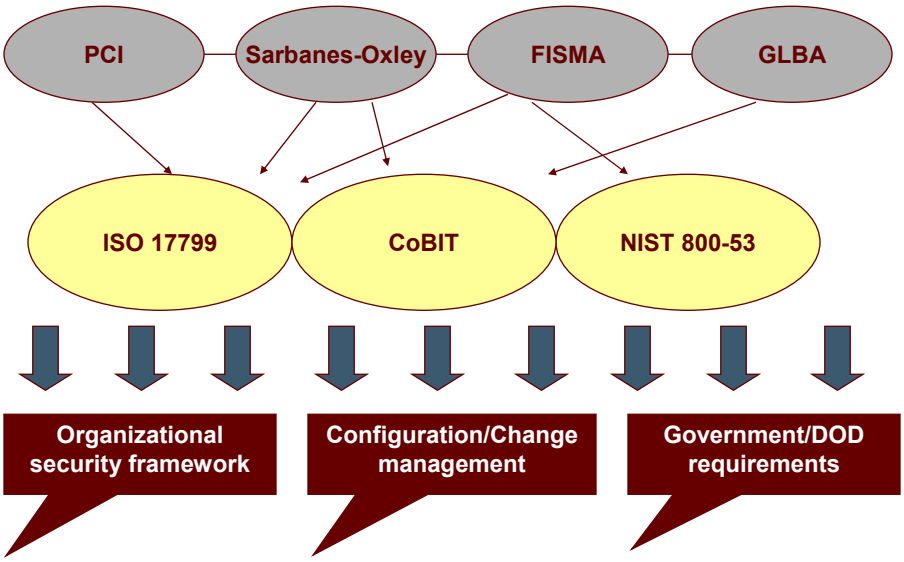
Risk mitigation begins with:

- Assessing risk
- Addressing known vulnerabilities
- Benchmarking progress against goals
- Continuous monitoring in real-time

Key benefit of combining compliance and database security:

Successful, predictable audit performance

Mapping Compliance Initiatives to Controls and Standards



Business benefits of database compliance

- Documentation of known vulnerabilities and database risks
- Defined roles and responsibilities for individuals who have access to the database
- Means to review user activity and user entitlement
- Improved threat intelligence
- System of alerts on suspicious activity
- Ability to keep policies up-to-date and to streamline management review
- Operational efficiencies

Payoffs of control frameworks in IT

Organizations are striving to become more efficient:

- Reduce ongoing operating costs
- Better align IT with business needs
- Lower audit, compliance, and security costs
- Improve resource management

Performance gains from compliance initiatives

Organizations that leverage a security framework in their compliance efforts experience:

- Increased detection of security breaches via automated controls
- Reduction of data loss from security breaches
- Operational efficiencies
  - Reduction of unplanned work
  - More servers per system administrator

Source: *IT Controls Performance Study, IT Process Institute (www.itpi.org), 2006*

What auditors ask and how to answer

What auditors ask	How do you prepare to answer
Has the organization assessed the environment? Is enough information being captured?	**Assess** the environment. Identify protected data sources
Does the audit trail establish user accountability? Is the audit process independent? Does the organization have a plan in place to maintain and constantly improve compliance efforts?	**Prioritize** efforts through risk assessment and gap analysis.
Have risks been addressed? Are there policies and controls in place that address and meet standards and compliance?	**Fix** and remediate known issues.
Is the scope and detail of the audit trail sufficient? What monitoring is in place for ongoing assessment? Is there a way to identify changes to the data?	**Monitor** systems through ongoing compliance analysis and documentation

1: ASSESS the environment

Identify systems and processes that store, create, view, change, transmit or destroy data

Review existing system documentation and process flows

Create process flows if none exist

Results:

- List of systems and processes that use relevant information
- List of business units and departments that use information
- New process flow documentation
- A means to identify key controls

2: PRIORITIZE how to address risks

Conduct Risk Assessment dealing with confidentiality, availability and integrity of information

- Survey of IT, business staff and users of information
- Identify threats and vulnerabilities to the information
- Identify Controls

Establish Risk Profile (High, Medium, or Low) based on threats, vulnerabilities and controls

Conduct Gap Analysis against the relevant standards

Results:

- Risk Assessment Report
- Gap Analysis Report
- Remediation Recommendations

3: FIX and remediate existing issues

Address the gaps identified in Step 2

Identified problems must be remedied, mitigated, or transferred to another entity

- Example: Organizations that are not capable of correctly securing PCI data have begun to shift functions (like credit card processing) to third parties to avoid compliance issues.

Conduct Gap Analysis against the relevant standards

Results:

- Improved security and data risk management
- Compliance

4: MONITOR for ongoing compliance

Full ongoing analysis against the relevant standards

- Repeatable
- Demonstrable
- Automated

Results:

- Proactive policy protections
- Comprehensive reporting and analysis
- Real-time intelligence, information and alerts

APPLICATION SECURITY, INC.

Database Security Best Practices

Develop a Risk Framework

Assess Security Posture
- Assess database security risks
- Determine impact
- Establish and prioritize work

Measure Impact
- Document risks and controls
- Align business and IT goals
- Develop business case

Deal with Impact
- Direct costs
- Indirect Costs
- Cross-departmental buy-in

Establish Controls
- Facilitate accountability
- Establish reporting framework
- Implement access controls
- Integrate policies and procedures

What's likely to happen
- Opportunity level
- Expertise required – business
- Expertise required - technical

How to Protect Against Attacks

Set a good password policy:
- Use strong passwords or passphrases.

Keep up to date with security patches:
- Try to install patches as fast as you can. Database vulnerabilities are serious and sometimes a database server can be easily compromised with just a simple query.
- Always test patches for some time on non-production databases

Protect access to the database server:
- Allow connections only from trusted hosts and block non used ports and outbound connections. Establish exceptions for special instances like replication, linked databases, etc.

Disable all non used functionality:
- Excess functionality can lead to vulnerabilities

Use selective encryption:
- At network level: use SSL, database proprietary protocols.
- At file level for backups, laptops, etc.

Periodically Audit Database Systems

Check for object and system permissions:

▪Check views, stored procedures, tables, etc. permissions. Check file, folder, registry, etc. permissions. Changes on permissions could mean a compromise or mis-configuration.

Look for new database installations:

▪Third party products can install database servers and this new installed servers could be installed with blank or weak passwords, un-patched, mis-configured, etc. Detect new database installations and secure or remove them**.**

Search for users with DBA privileges:

▪This helps to detect intrusions, elevation of privileges, etc.

Audit database configuration and settings:

▪If security configurations or settings are changed for instance by a system upgrade, patch, etc. your databases could be open to attack. If they change and there wasn't a system upgrade then it could mean a compromise.

Check database system objects against changes:

▪If you detect a change in a system object and you haven't applied a fix or upgrade to your database server it could mean that a rootkit is present.

Summary

- Database risks are real and increasing
- Organizations must address vulnerabilities to minimize risk
- Good things happen when compliance efforts are grounded in the database — where data lives
- Leverage compliance initiatives to better mitigate risk and protect data where it resides — in the database
- Use regular audits and assessments to continue to demonstrate compliance

Resources

White papers:

http://www.appsecinc.com/techdocs/whitepapers/research.shtml

- SQL Server Forensics
- Arrest the Threat: Best Practices for Monitoring Privileged Database Users
- Hunting Flaws in Microsoft SQL Server

Security alerts:

www.appsecinc.com/resources/mailinglist.html

Other database resources:

Oracle

- Project Lockdown www.oracle.com/technology/pub/articles/project_lockdown/index.html
- Security Checklist www.oracle.com/technology/deploy/security/pdf/twp_security_checklist_db_database.pdf

SANS Institute (SysAdmin, Audit, Network, Security)

- Oracle Database Checklist www.sans.org/score/checklists/Oracle_Database_Checklist.doc

Microsoft

- SQL Server 2005 Security Best Practices www.microsoft.com/technet/prodtechnol/sql/2005/sql2005secbestpract.mspx

SQLSecurity.com

- SQLSecurity Checklist

APPLICATION SECURITY, INC.

Thank you!

Questions?

Application Security, Inc.
1-866-9APPSEC (1-866-927-7732)
Sales@appsecinc.com