



Database Security Standards and Audit Implementation

With:

James Sortino, Director of Western Operation

Agenda

- Database security and compliance
- Business benefits of IT frameworks
- Addressing security and compliance
- Meeting audit requirements
- Conclusions

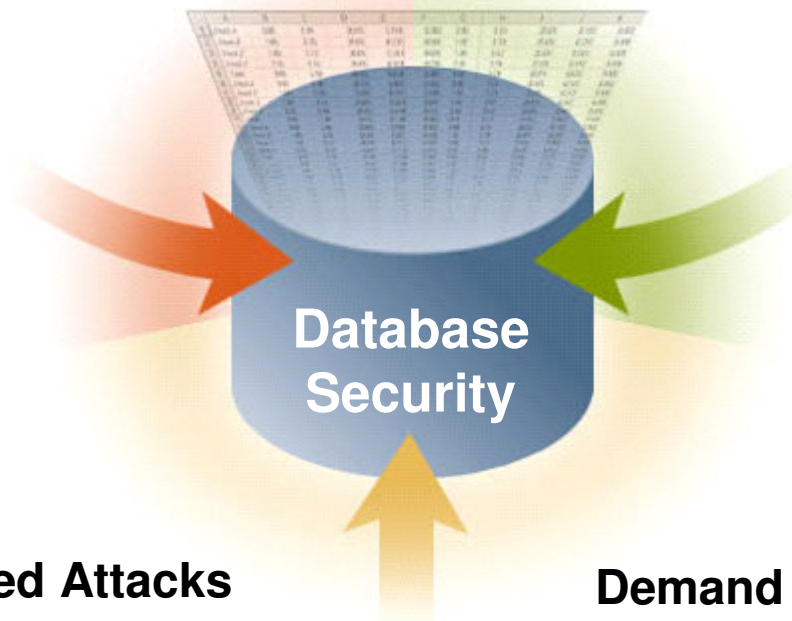
Forces Driving Database Compliance Efforts

Compliance Requirements

- Data lives in Db apps (90%+):
 - Privacy / confidentiality
 - Integrity

■ Compliance must be:

- Repeatable
- Demonstrable
- Automated



Increasingly Focused Attacks

- Directly on applications (75%!)
- Including insiders (80+%!)
- Financially motivated

Demand for Pervasive Access

- By anyone
- To any application
- Increasingly direct

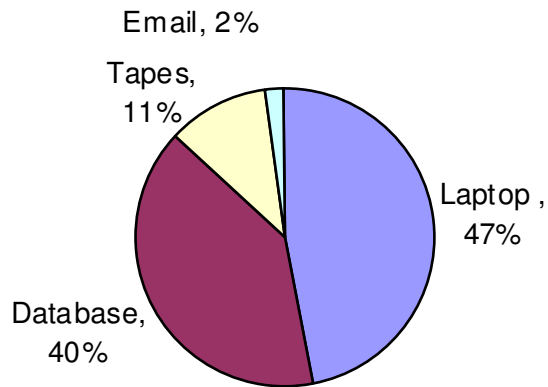
Market Overview: Databases Are Under Attack

■ January 2005 to March 2008

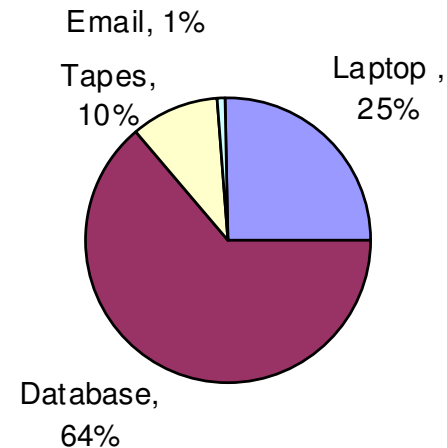
Total Affected Records: 223,142,082

- Literally hundreds of incidents
- Victims include financial institutions, government agencies, retailers, healthcare providers, universities, manufacturing, consulting and audit firms,

Source of Breach



Records Lost



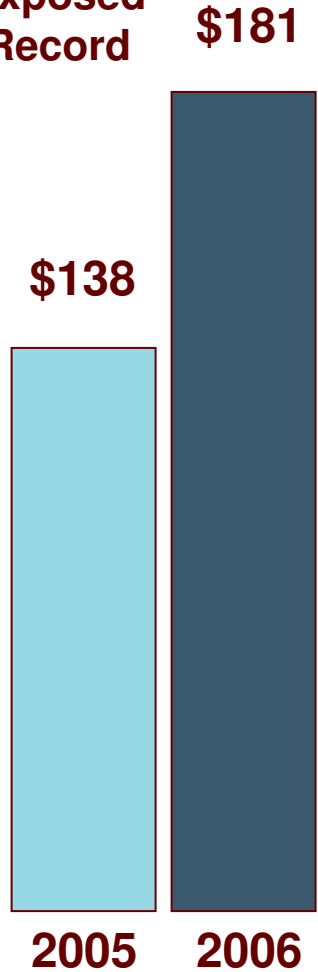
<http://www.privacyrights.org/ar/ChronDataBreaches.htm>

**Privacy Rights
CLEARINGHOUSE**

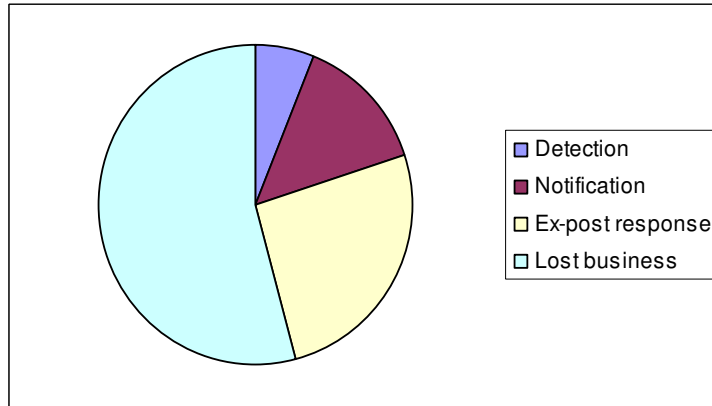
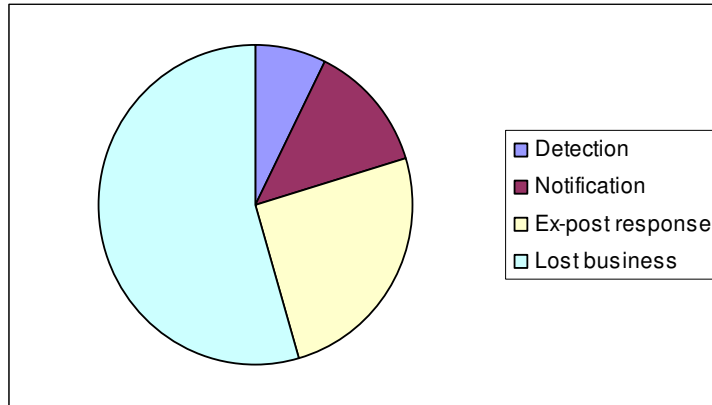
Market Overview: Data Breach Costs Are Rising

TJ1

Cost Per Exposed Record



Ponemon Research



223 million records breached
X 65%

145 million records attributed to database breaches

145 million records
At \$181 per record

Equals

\$26.2 billion in database related costs

Slide 5

TJ1

get updated data
ted julian, 3/21/2008

Common Compliance Control Frameworks

Compliance Requirements

- Sarbanes-Oxley
- PCI
- HIPAA
- FISMA
- Gramm Leach Bliley
- Basel II
- California SB 1386

IT frameworks for security control

- CoBiT
- 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

Business benefits of database compliance:

- Document known vulnerabilities and database risks
- Well-defined roles and responsibilities for IT personnel and people who have access to the database
- Regular review of user activity
- System of alerts on suspicious activity
- Keep policies up-to-date and streamline management review
- Operational efficiencies
- Improved threat intelligence

Payoffs of Control Frameworks in IT

Organizations need to consider ways to transition to more efficient processes:

- From manual to automated controls
 - From detective to preventative tools
 - From comprehensive to targeted testing
 - From unpredictable to managed costs
-
- Reducing ongoing operating costs
 - Better aligning IT with business needs
 - Lowering audit, compliance, and security costs
 - Improving how companies use existing resources (people and assets)

Performance gains from compliance initiatives:

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

- Reduction of data loss from security events
- Increased detection of security breaches via automated controls
- 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?	Prioritize efforts through risk assessment and gap analysis.
Have risks been addressed? Are there policies and controls in place that meet the standard appropriately?	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

What is PCI?

WHO IS AFFECTED

- Covered entities comprise all Visa International, MasterCard Worldwide, Discover Financial Services, American Express, and JCB members, merchants, and service providers that store, process or transmit cardholder data. PCI regulates point-of-sale, telephone, online, and all other types of transactions.

WHAT IT COVERS

- All “system components” are covered. These are defined by the PCI DSS as “any network component, server, or application included in, or connected to the cardholder data environment.”

HOW IT'S ENFORCED

- Contractual penalties and/or sanctions, including fines of up to \$500,000 per incident and revocation of a company's right to accept or process credit card transactions.
- Validation requirements to maintain and demonstrate compliance.

Basics of PCI: Twelve Steps to PCI Compliance

CONTROL OBJECTIVES	COMPLIANCE REQUIREMENTS
Build and maintain a secure network	1. Install and maintain a firewall configuration to protect data
	2. Change vendor-supplied defaults for system passwords and other security parameters
Protect cardholder data	3. Protect stored data
	4. Encrypt transmission of cardholder magnetic-stripe data and sensitive information across public networks
Maintain a vulnerability management program	5. Use and regularly update antivirus software
	6. Develop and maintain secure systems and applications
Implement strong access control measures	7. Restrict access to data to a need-to-know basis
	8. Assign a unique ID to each person with computer access
	9. Restrict physical access to cardholder data
Regularly monitor and test	10. Track and monitor all access to resources and cardholder data
	11. Regularly test security systems and processes
Maintain an information security policy	12. Maintain a policy that addresses information security
* The Payment Card Industry Data Security Standard (PCI DSS) includes numerous sub-requirements not listed here. To see these, visit http://www.pcisecuritystandards.org .	

Why comply with PCI?

- **It's good security policy**
- The 12 PCI DSS requirements are basic information security policies that every business should already be following
 - PCI compliance isn't about just marking off a checklist; to be compliant, you really need to have strong information security in place
 - PCI remediation will genuinely improve information security within your organization overall, in addition to meeting the tactical goal of PCI compliance
- **Enhanced consumer confidence and public image**
- **Cost of non-compliance or breach**

Why Comply? The Risks are Real

Recently Reported Retail Attack Example

- Reconnaissance occurred over for 17 months
 - Encryption rendered useless as attackers accessed the keys.
- Over 45M records stolen; 30M valid records in total
 - The database holds the most up-to-date data and, if accessed, the data can often be harvested at will.
 - This was biggest data heist ever
- Theft took months to discover
 - Data thieves penetrated the database, took what they needed and then altered access logs to obscure the activity, frustrating investigations.
 - TJX did not know where all their sensitive assets were.
- Lack of monitoring and vulnerability scans were contributing factors in the attack
 - That figure is expected to grow, according to the Bankers Assn.
 - More than 60 banks were involved.

Remediation: Compensating Controls

Sometimes meeting a specific PCI requirement is unduly difficult or impossible. In such cases, an organization may consider compensating controls

- An alternative that achieves the objective of the PCI requirement, but in a different way than PCI specifies
- Compensating controls are applicable to most requirements
- Must meet the intent and rigor of the original PCI requirement

Example:

Companies unable to render cardholder data unreadable, for example by encryption, can use compensating controls instead

- Requires a risk analysis and legitimate technological or business constraints

What is SOX?

WHO IS AFFECTED

The Sarbanes-Oxley Act (SOX) is a federal regulation that impacts all publicly traded companies. The goal of SOX is to ensure the integrity of financial reporting.

WHAT IT COVERS

All financial records are covered. The act mandates that executives, auditor, securities analysts and legal counsel be accountable.

HOW IT'S ENFORCED

Stiff penalties including fines and imprisonment.

The Basics of SOX: Compliance Goals

The environment of accountability required by sections 302, 404 and 409 of the SOX act ensure that organizations can:

- Conduct ongoing security health assessments
- Maintain privacy through internal controls
- Prove claims
- Provide full disclosure when needed

The single common threat to SOX compliance is unauthorized data deletion, modification or access.

With the integrity of financial data at stake, compliance efforts must include securing data at its source — the database.

SOX: Why comply?

SOX is a federally regulated mandate. Non-compliance leads to various penalties including:

- Significant fines
- Incarceration

The regulation applies to any public corporation, large or small.

SOX: How to Comply

Unlike a standard like PCI, SOX compliance is organizationally driven. Tasks a SOX auditor will required to complete are:

- Assess the design and operating effectiveness of selected internal controls;
- Understand the flow of transactions, including IT aspects, sufficiently to identify points at which a misstatement could arise;
- Perform a fraud risk assessment;
- Evaluate controls designed to prevent or detect fraud, including management override of controls;
- Evaluate controls over the period-end financial reporting process;
- Scale the assessment based on the size and complexity of the company;
- Rely on management's work based on factors such as competency, objectivity, and risk;
- Evaluate controls over the safeguarding of assets; and
- Conclude on the adequacy of internal control over financial reporting.

Source: Auditing Standard No. 5 of the Public Company Accounting Oversight Board (PCAOB)

How do we know the process works?

We've done it. Companies have already achieved significant benefits by using the DbProtect solution, Database Security Lifecycle, and the compliance methods outlined in this presentation to streamline and improve their compliance efforts.

We help companies reduce risk, improve their internal controls and enhance their compliance efforts. Our customers achieve these goals:

- Precisely documented controls and policies that define roles, and control access to data assets
- Clearly defined boundaries between Sarbanes-Oxley and non-Sarbanes-Oxley controls
- Automated testing and validation checks to demonstrate system integrity
- Activity monitoring to identify and alert on suspicious actions

Summary

Good things happen when compliance efforts are grounded in the database—where data lives. Security improves as control deficiencies are addressed, weaknesses are identified and fixed, and monitoring is activated to identify and alert on potential database threats.

As a result of compliance initiatives like SOX and PCI, organizations are scrutinizing data protections and controls. Through this examination, they are identifying ways to improve data security and fulfill their commitment to protect consumer and financial information. By tying these efforts to security gains, organizations can leverage compliance initiatives to better mitigate risk and protect data where it resides—in the database.

Database Security Standards and Audit Implementation

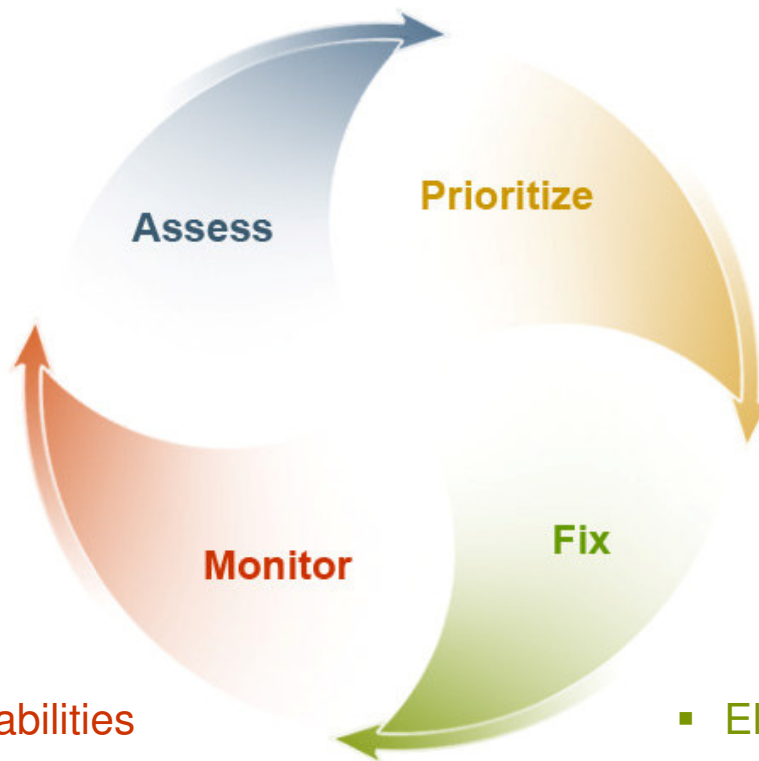
Best Practices



How Do You Secure Intellectual Property?

Apply the vulnerability management lifecycle...

- Inventory assets
- Identify vulnerabilities
- Develop baseline



- Prioritize based on vulnerability data, threat data, and asset classification
- Document security plan

- Monitor known vulnerabilities
- Watch unpatched systems
- Alert on other suspicious activity

- Eliminate high-priority vulnerabilities
- Establish controls
- Demonstrate progress

Database Security Best Practices

■ Vulnerability Assessment

- Discover & Create an accurate inventory
- Assess for known vulnerabilities
- Prioritize and remediate (...if possible)

■ Database Activity Monitoring

- Alert - users attempting to exploit vulnerabilities that can not or have not yet been remediated
 - (Patch-Gap management)
- Alert - suspicious, unusual or other abnormal activity
- Log - authorized access
 - which systems, when, and how
 - what was done (for both privileged/non-privileged user)

Best Practices – the What

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

Best Practices – the How

- **Vulnerability Assessment and Threat Monitoring**
 - Assess your database applications for known vulnerabilities
 - Alert in real-time users attempting to exploit these vulnerabilities
 - Alert in real time any other suspicious, unusual or other “abnormal” access
- **Database Activity Monitoring**
 - Determine who accessed which systems, when, and how
 - Determine what they did (both users and administrators)
 - Understand where the threat / risk originates and deploy the appropriate solution to defend against such threats
- **Change Auditing**
 - Establish a baseline policy for database; configuration, schema, users, privileges and structure, then track deviations from that baseline.

DbProtect: Complete Database Security



Proven technology

- More than 1,059 customers
- Database security leader since 2001
- More than 1,000,000 databases

Integrated database security

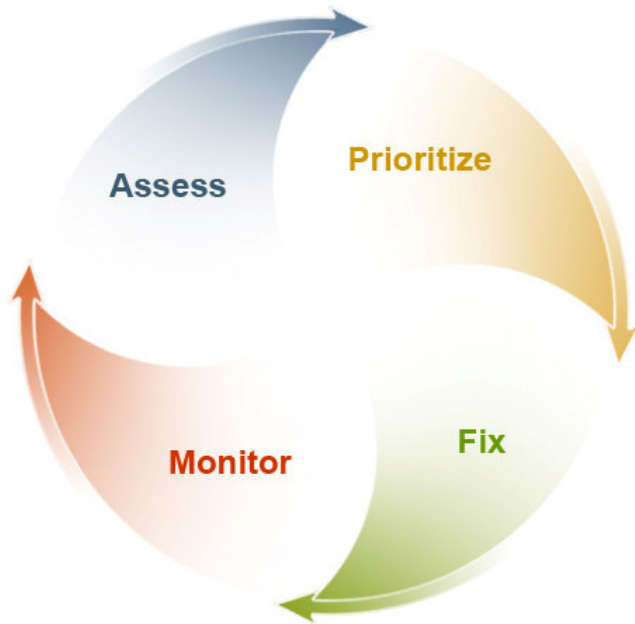
- Database activity monitoring
- Database vulnerability assessment
- Database intrusion detection

Enterprise class

- Multi-user centralized management
- Multi-tier distributed architecture
- Network and host based sensor flexibility
- Extensive templates and custom reports

“... the most comprehensive database security solution...” Forrester Research

Deployment Best Practices



1. **Discovery**
2. **Vulnerability assessment and prioritization**
3. **Remediation**
4. **Residual vulnerability mapping**
5. **Monitoring policy deployment**
 - Patch-gap policies
 - Privileged user monitoring policies
 - User and behavior policies
6. **Report customization and publishing**
7. **Vulnerability updates and policy tuning**
8. **Integration: SIM/SEM etc**

A Logical 3 Step Process

- **Vulnerability Assessment**
 - Per Engagement License
 - Corporate Audit License
 - AppDetective Pro
 - DbProtect AppDetective
- **User Activity Monitoring**
- **Encryption**

The Value of DbProtect

- Pre-formatted policies and compliance toolkits make deployment easy
- Operational efficiencies immediately realized
 - Automated scanning / monitoring vs. manual
 - Do more with your time and money
- Most up-to-date and comprehensive threat intelligence of any database security solution available
 - Knowledgebase of vulnerabilities, checks and filters
- Policy mapping via simple to use Wizard
- Automated reporting streamlines operations
- Get more value by integrating DbProtect feeds into your existing infrastructure views
 - ArcSight
 - SPIDynamics
 - OpsWare

Questions?

For more information contact:

James Sortino, CISSP
jsortino@appsecinc.com

Craig Whittington
cwhittington@appsecinc.com

Technical questions can be referred to:
asktheexpert@appsecinc.com

