TIZOR

Database Auditing and Forensics for Privacy Compliance: *Challenges and Approaches*

Bob Bradley
Tizor Systems, Inc.

December 2004

TIZOR

Problem Statement

- **You're a DBA for an information asset domain consisting of multiple servers, multiple Oracle 8i/9i/10g databases across three locations**

- **You work in an organization that is:**
  - Regulated
  - Updating corporate business process policies/ practices
  - Or Both

- **Your Chief Compliance/ Privacy Officer has executive mandate to insure that "best practices" regarding *information privacy protection* are implemented worldwide by Q2 2005**

TIZOR

Given your current staff, workload, budget, and timeframe, how do you approach this task?

Understand the Requirements: Privacy Compliance

Commercial Requirements:

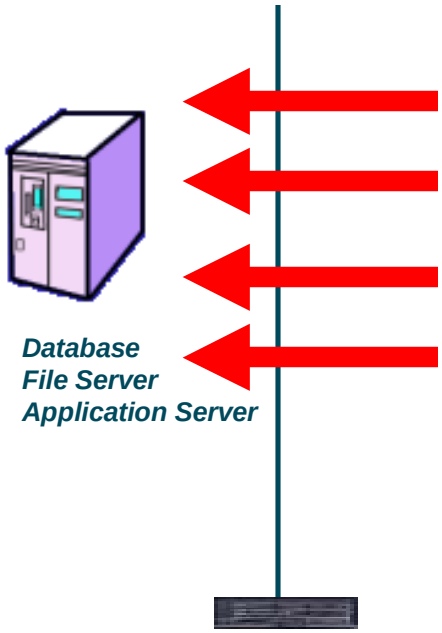
- **Source/direction may come from:**
  - **Regulation (HIPAA; SB 1386)**
  - Best Practices Recommendations
  - Internal Business Compliance Directive

Example: *Implement procedures to regularly review records of information system activity, such as **audit logs**, **access reports**, and **security incident tracking reports**.*

***I**mplement **hardware, software, and/or procedural mechanisms** that record and examine activity in information systems that contain or use electronic protected health information.*

HIPAA Security
Technical Safeguards
Clauses 164.308; 164.312

Understand the Requirements: Privacy Compliance



Auditing access to information assets

Requirements (Auditing):

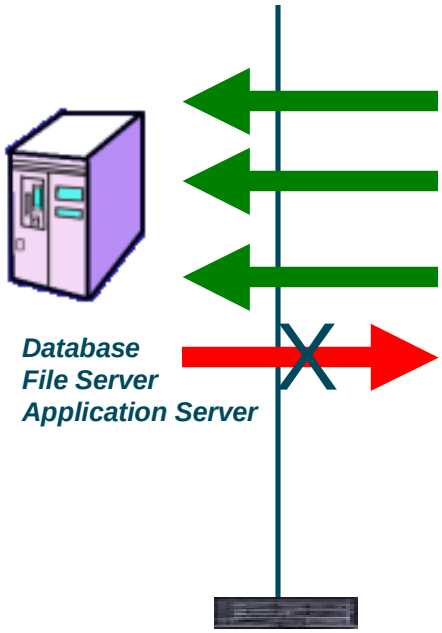
- **Source/direction may come from:**
  - Regulation (HIPAA; SB 1386)
  - **Best Practices Recommendations**
  - Internal Business Compliance Directive

Example: *Use physical and technological security safeguards as appropriate to protect personal information, particularly higher-risk information such as Social Security number, driver's license number, California Identification Card number, financial account numbers and any associated passwords and PIN numbers, other financial information, and health information, in paper as well as electronic records..*

- *Activate all auditing software if not already activated.*

California Department of Consumer Affairs (for SB 1386)
Office of Privacy Protection

Understand the Requirements: Privacy Compliance



Auditing unauthorized accesses & disclosures

Requirements (Unauthorized Access and Disclosure):

- **Source/direction may come from:**
  - Regulation (HIPAA; SB 1386)
  - **Best Practices Recommendations**
  - Internal Business Compliance Directive

Example: *Use physical and technological security safeguards as appropriate to protect personal information, particularly higher-risk information such as Social Security number, driver's license number, California Identification Card number, financial account numbers and any associated passwords and PIN numbers, other financial information, and health information, in paper as well as electronic records..*

- *Monitor employee access to higher-risk personal information procedures to ensure rapid detection of unauthorized access to higher-risk personal information.*
- *Use intrusion detection technology and procedures to ensure rapid detection of unauthorized access to higher-risk personal information.*

California Department of Consumer Affairs (for SB 1386)
Office of Privacy Protection

TIZOR

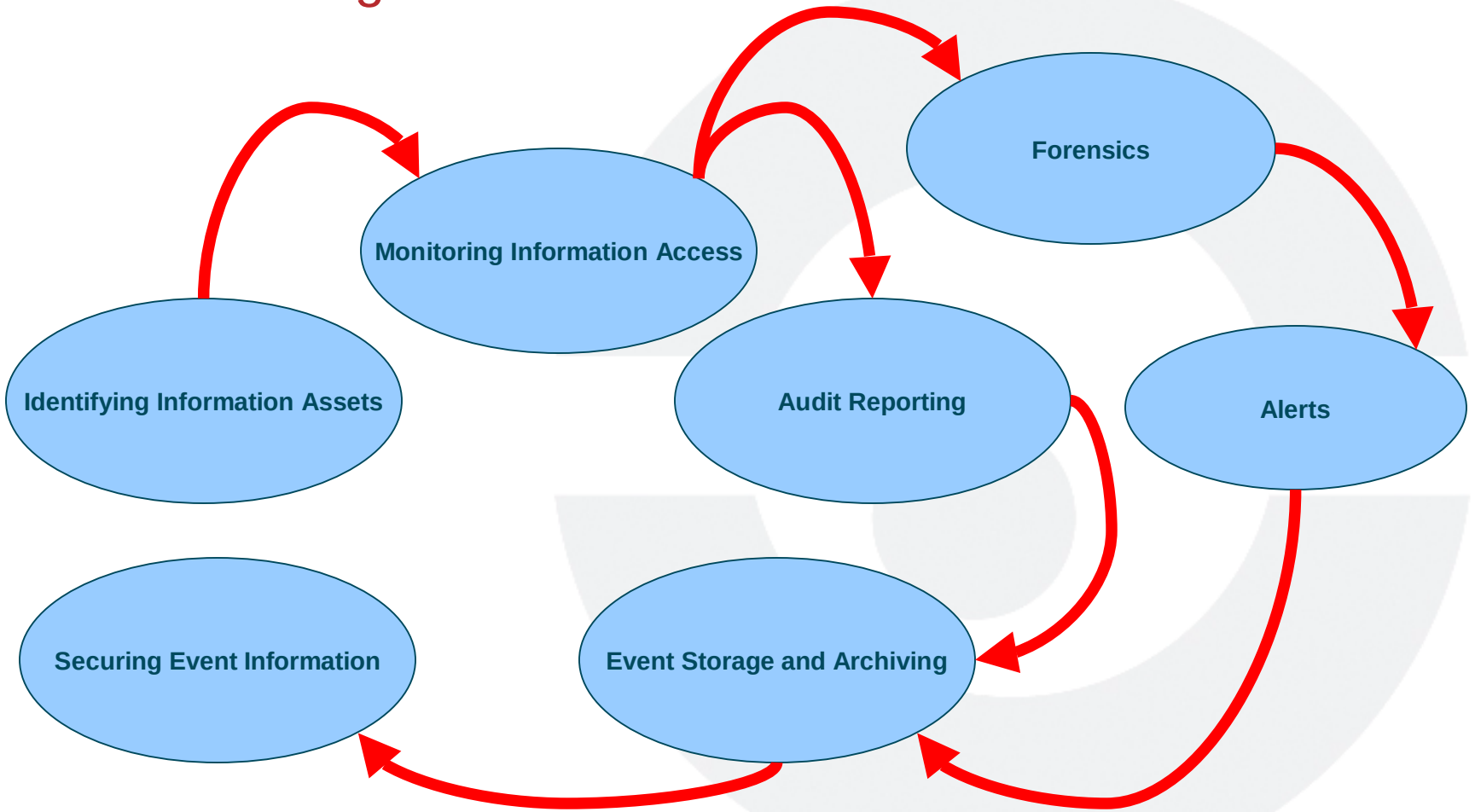
Defining an Approach: Regulation Compliance

- **Deploy *comprehensive auditing* of identified information assets providing information protection**

- **Attributes:**
  - Approach is **consistent with** internal practices; infrastructure
  - Monitor both **internal and external users' access** to compliance controlled information
  - Provide a **flexible policy definition language** that can codify regulations directly and easily
  - Provide **comprehensive audit trails**
  - Provide **real time analytics and forensics** to detect unauthorized data access
  - Be **manageable** across an enterprise deployment

TIZOR

The Auditing Process



TIZOR

Identifying Information Assets and Defining Audit Policies

Problem:

* Not all information assets (tables, columns) require compliance monitoring

Challenge:

* Performing “pragmatic” risk assessment e.g. costs of coverage
* Specify and target critical assets criteria
  - systems
  - schema

Approach:

* Policy based approach simple enough for DBAs yet comprehensive enough for IT/Security personnel
* Definition language that can easily abstract assets (databases, tables, columns)
* Provides for composite definition of “sensitive” assets (e.g. PHI is “A” and “B” seen together)

TIZOR

Monitoring Information Access

Problem: *How* to monitor?

Challenge:

* Approach should not impact system performance, network performance or integrity, and require application changes
* Different database types, SQL commands

Approach:

* Deploy “outside” the database servers
* Non-intrusive, network centric
* Monitors different databases
* Centrally managed
* Minimize performance impact & storage costs
* Augments existing database auditing tools

TIZOR

Audit Reporting

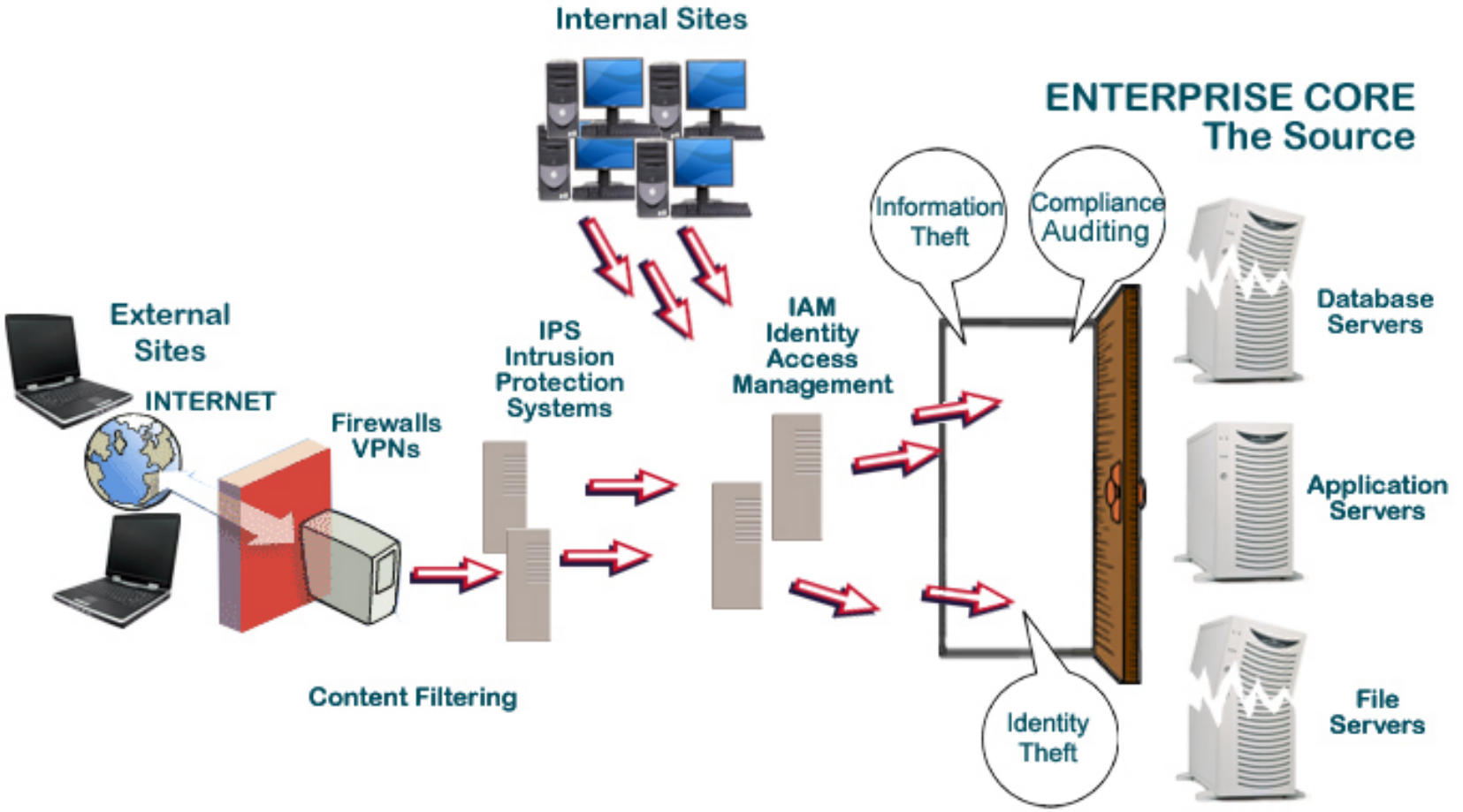
Problem: * How do I achieve reporting needed by compliance?

Challenge: * Be able to “drill down” without “drowning in data”

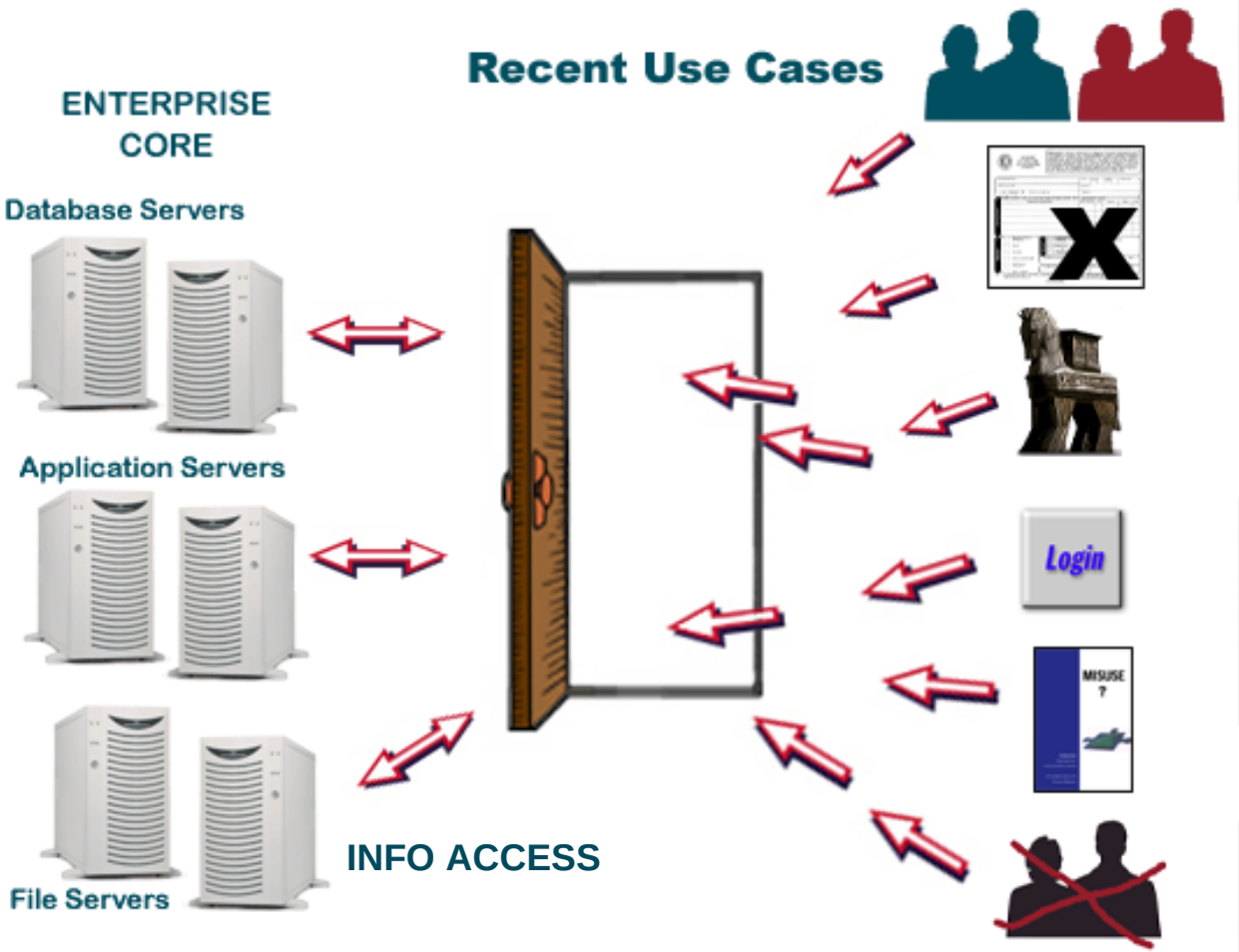
* Granular enough to report on “5 W’s”
  - **who = user**
  - **which = information asset**
  - **what = operation**
  - **when = time**
  - **where = location**
* Create simple but effective reports to distribute to compliance, security, and IT personnel

Approach: * Graphical and tabular reporting with detailed forensics
* Report export capabilities for data interchange

Forensics: Unauthorized Access & Information Theft



Forensics: Unauthorized Access & Information Theft



TIZOR

Forensics and Alerts

Problem:

* How do I detect unauthorized access?
* When do I alert?

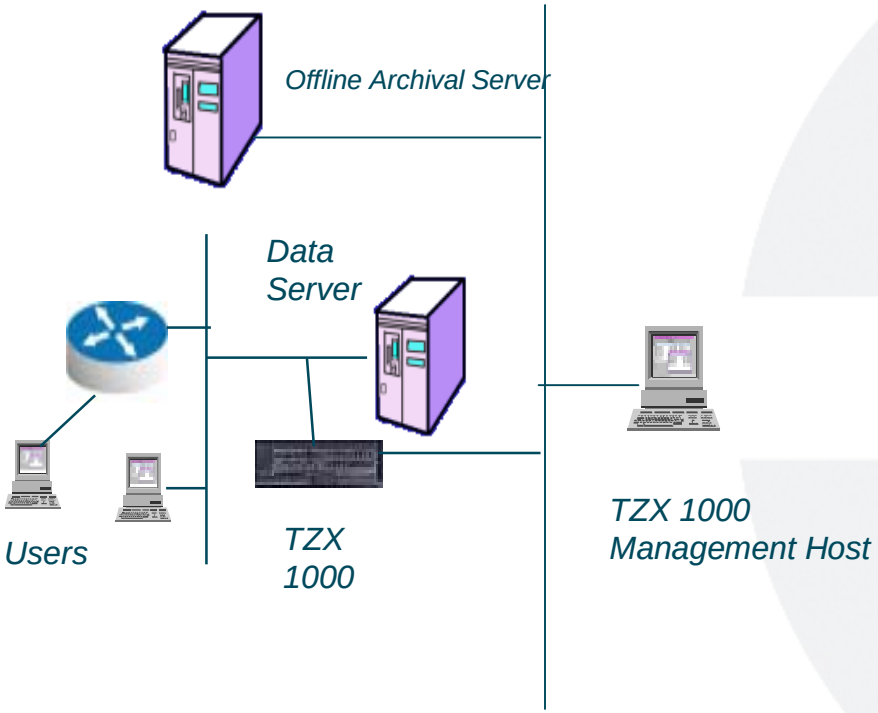
Challenge:

* Low false positives
* Low false negatives
* English like policy management
  example: ***operation = SELECT and content.table = 'SSN' and large (size)***
* Real time risk mitigation

Approach:

* Must understand users' pact activity
* Allow for data mining via event search
* Allow for signature creation for theft similar as used with worms, viruses)
* Detect and alert

Event Storage and Archiving



Problem: * How do I archive and store audit trail data for compliance ?

* What to store to provide adequate granularity?"

Challenge: * Short term vs. long term data storage

Approach: * Short term (1-3 months) on the appliance for report generation

* Longer term (> 3 months) automatically archived

TIZOR

Securing Event Information

Problem:

***** How do I ensure that my audit trails are secure enough for compliance purposes?

Challenge:

* Confidentiality
* Availability
* Non-reputability

Approach:

***** Authenticated access to audit trails
* Digital signature of local data
* Offline archiving of encrypted audit trails

TIZOR

Summary

- Privacy Compliance is an industry driver for *Information Protection*
  - ***Unauthorized disclosures*** **and** ***identity theft*** **are two** ***highly visible*** **manifestations of privacy violations**
  - **The risks to organizations are increasingly brand equity**

- *Real time* Information Access Protection can be achieved via a comprehensive auditing process

- There are evolving approaches and methodologies that can meet the auditing requirements for database, security, and compliance/privacy administration

Thank you!

Tizor Systems, Inc.
2 Clock Tower Place, Maynard, MA 01754
Phone: 978-823-5150 Fax: 978-823-5160
info@tizor.com www. tizor.com