IBM

Information Security & Privacy Solutions
Enabling Information Governance

LYNDA KEITANY
IM SALES SPECIALIST

July 11, 2012

What's at Stake?

- **Damage to company reputation**
  - "Brand equity" damage; negative publicity
  - Loss customer loyalty

- **A privacy breach – or the threat of one**
  - Intellectual property loss
  - Increased operations cost
    - Average cost of a data breach incident is $6.7 million ($204 per compromised record)*

- **Loss of revenue & share price erosion**

- **Audits and the possibility of being fined**
  - FDIC may levy fines of $5,000 to $1,000,000/day
  - GLB sections 501 & 503 enable criminal penalties

* Sources: Ponemon Institute, 2009

What's the Risk?

Confidential data inadvertently exposed or otherwise available to unauthorized viewers.

February 2010: About 600,000 customers of a major NYC bank received their annual tax documents with their Social Security numbers (combined with other numbers & letters) printed on the outside of the envelope.

SQL injection is fast becoming one of the biggest & most high profile web security threats.

July 2010: Hackers obtained access to the user database and administration panel of a popular website by exploiting several SQL injection vulnerabilities. The exposed data included user names, passwords, e-mail addresses and IPs.

Unprotected test data sent to and used by test/development teams as well as third-party consultants.

February 2009: An FAA server used for application development & testing was breached, exposing the personally identifiable information of 45,000+ employees.

Confidential data that should be redacted can be hidden or embedded

April 2010: A PDF of a subpoena in the case of "United States vs. Rob Blagojevich" was posted to public website. However, the "redacted" text simply had black box placed on top to hide the content – the actual text was still available.

Securing and Protecting Your Information Supply Chain

- **Understanding the "what & where" of enterprise data**
- **Protecting the data across the enterprise, both internal and external threats**
- **Knowing who's accessing your data when, how and why**
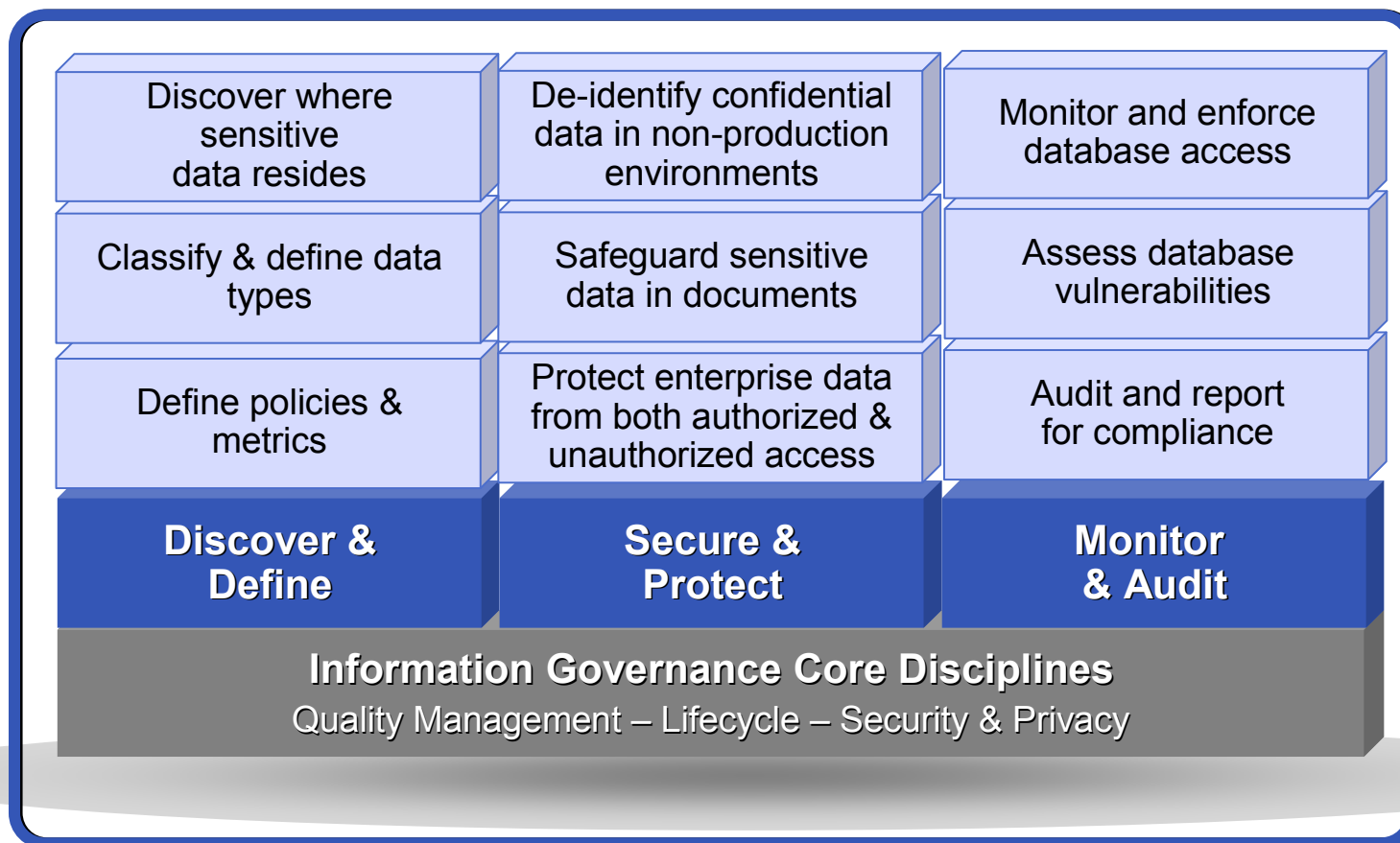- **Monitoring and reporting on database access for audit purposes**
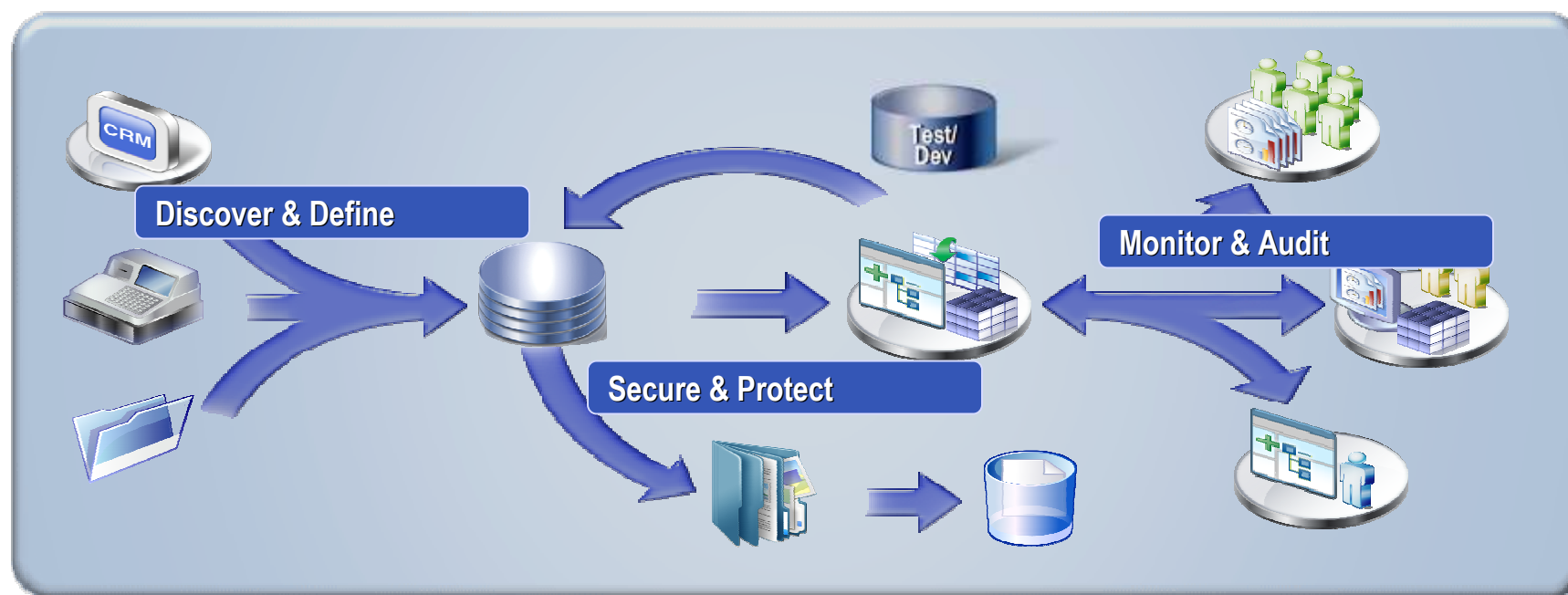
Can Today's Organizations Successfully Protect their Information?

- Where does your clients sensitive data reside across the enterprise?
- How can their data be protected from both authorized and unauthorized access?
- Can your confidential data in documents be safeguarded while still enabling the necessary business data to be shared?
- How can access to your enterprise databases be protected, monitored and audited?
- Can data in your non-production environments be protected, yet still be usable for training, application development and testing?

" *Larry Ponemon, founder of the group that bears his name, said that survey shows a shift in the way C-level executives think about security software. Investing in data protection, he said, is now seen as less expensive than recovering from a data breach.* **-- InformationWeek**

Protecting Information Security & Privacy Across the Enterprise

Discover where sensitive data resides	De-identify confidential data in non-production environments	Monitor and enforce database access
Classify & define data types	Safeguard sensitive data in documents	Assess database vulnerabilities
Define policies & metrics	Protect enterprise data from both authorized & unauthorized access	Audit and report for compliance
Discover & Define	**Secure & Protect**	**Monitor & Audit**

Information Governance Core Disciplines
Quality Management – Lifecycle – Security & Privacy

Success: Leading Technology Company Simplifies Enterprise Security

Challenges

- **Improve database security for SOX, PCI & SAS70**
  - Environment: Oracle & SQL Server on Windows, Linux; Oracle E-Business, JD Edwards, Hyperion plus in-house applications
- **Simplify & automate compliance controls**
  - Previous solution consisted of traces & auditing with in-house scripts, which impacted DBA resources, and lead to massive data volumes, supportability issues and SOD issues

Solution

- IBM InfoSphere Guardium

Business Benefits

- Enterprise-class scalability, **deployed to 300 DB servers in 10 data centers in 12 weeks (deployed to additional 725 database servers in phase 2).**
- **Addressed critical needs for automated compliance reporting; real-time alerting; and centralized cross-DBMS policies.**
- **Closed-loop change control with Remedy integration**

"The Guardium architecture offers a noninvasive, network-based, database-independent platform for continuously monitoring and analyzing database traffic in real time to help immediately identify unauthorized or suspicious activities."