Privacy Protection is not just the Law - It's Good Business!

THE POWER OF ENTERPRISE DATA MANAGEMENT

Data Masking & Transformation Techniques to Protect Privacy in the Test Environment

Tom Rydz – Vice President
Princeton Softech Inc.

princeton softech

Agenda

- About Protecting Privacy
- What's at Stake?
- The Easiest Way to Expose Private Data
- Data Privacy Alternatives™
- Data Masking Techniques
- Success Stories
- About Princeton Softech

Disclaimer

This presentation is intended to provide general background information, not regulatory, legal or other advice. Princeton Softech, Inc. cannot and does not provide such advice. Readers are advised to seek competent assistance from qualified professionals in the applicable jurisdictions for the types of services needed, including regulatory, legal or other advice.

Privacy News – The US Government is Involved

US Senate Bill Holds IT Managers Responsible for Privacy Breaches

By Scott M. Fulton, III, BetaNews

February 8, 2007, 8:09 PM

A bill introduced in the US Senate on Tuesday by Judiciary Committee Chairman Patrick Leahy (D - Vermont), along with one independent and one Republican backer, aims to strengthen security requirements for all private databases accessible online that may hold personal information. Reintroducing language that had been stalled since 2005, if passed, the bill could hold IT managers accountable and responsible for security breaches where personal information is pilfered.

US Government Activity

- State
  - 31 states have enacted legal requirements for notifying the public regarding security breaches involving personal information
- Federal
  - Bill introduced in Summer 2006 would require companies that store information on more than 10,000 people to formally train employees in security practices, perform vulnerability tests, and ensure adequate security is practiced by third-party service providers.

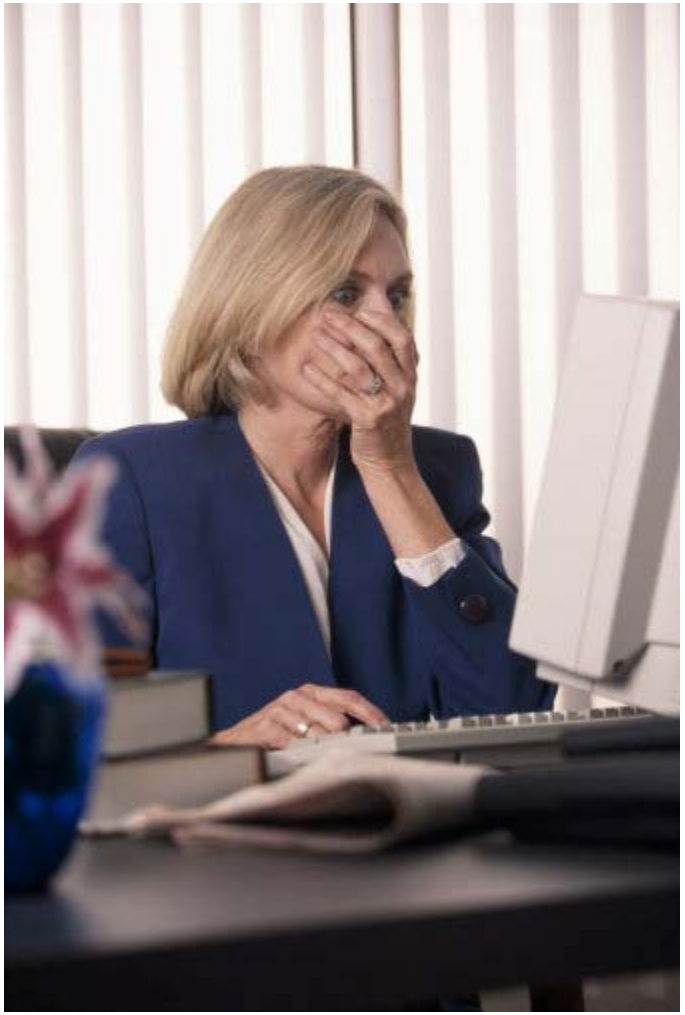
Common Legislative Themes

- Government regulations protect consumers
  - USA: HIPAA, Gramm-Leach-Bliley Act (GLB), California Security Breach Notice Statute
  - European Union: Personal Data Protection Directive 1998
  - UK: Data Protection Act of 1998
  - Australia: Privacy Amendment Act of 2000
  - Canada: Personal Information Protection and Electronic Documents Act
  - PCI Data Security Standard
- Fines and penalties focus on criminal misconduct
  - FDIC may levy fines from $5,000 to $1,000,000 per day
  - GLB sections 501 & 503 enable criminal penalties

princeton softech

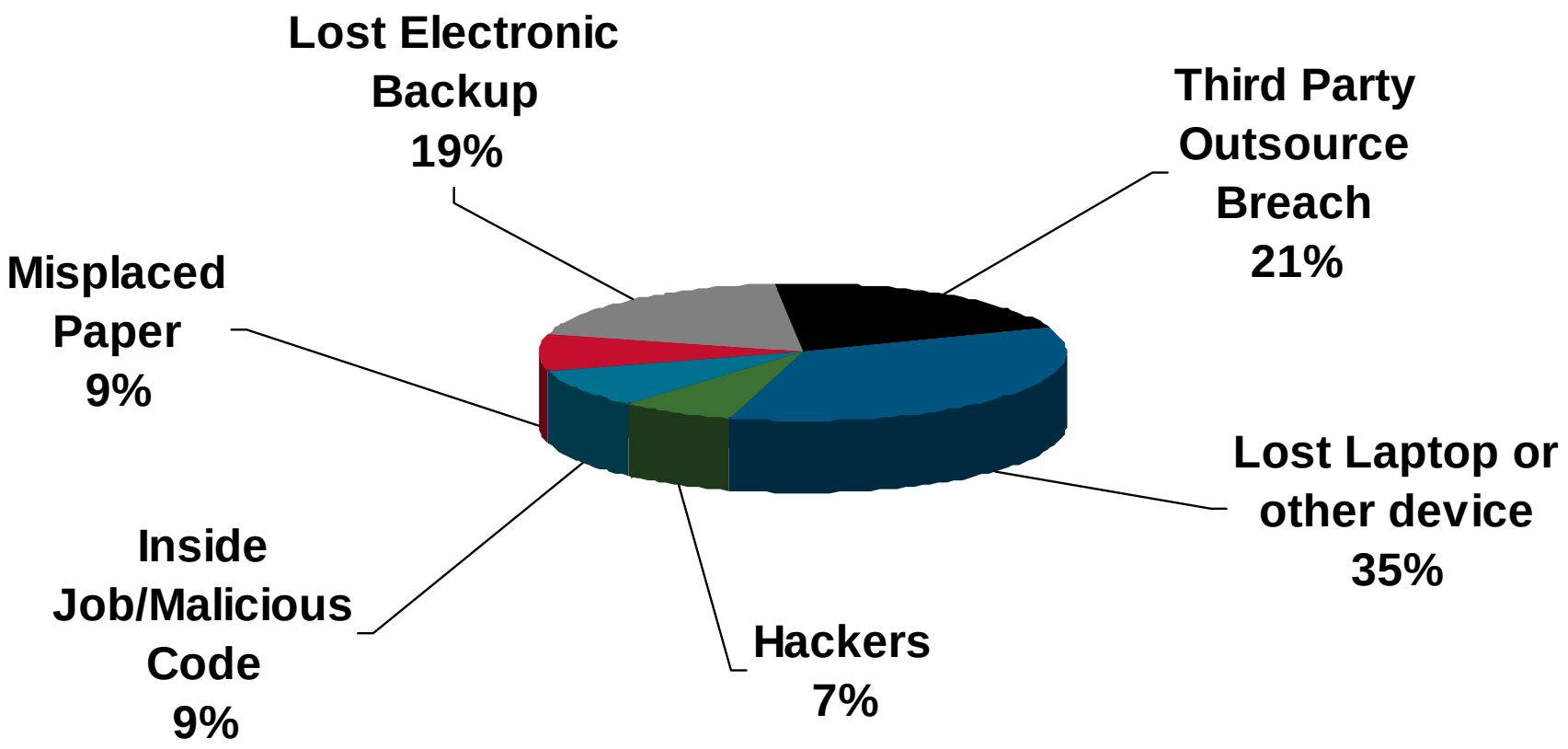
What's at Stake?

- Fines and penalties
- Loss of customer loyalty
- Loss of revenue
- Share price erosion
- Negative publicity
- "Brand equity" damage
- Damage to company reputation
- Increased operations costs

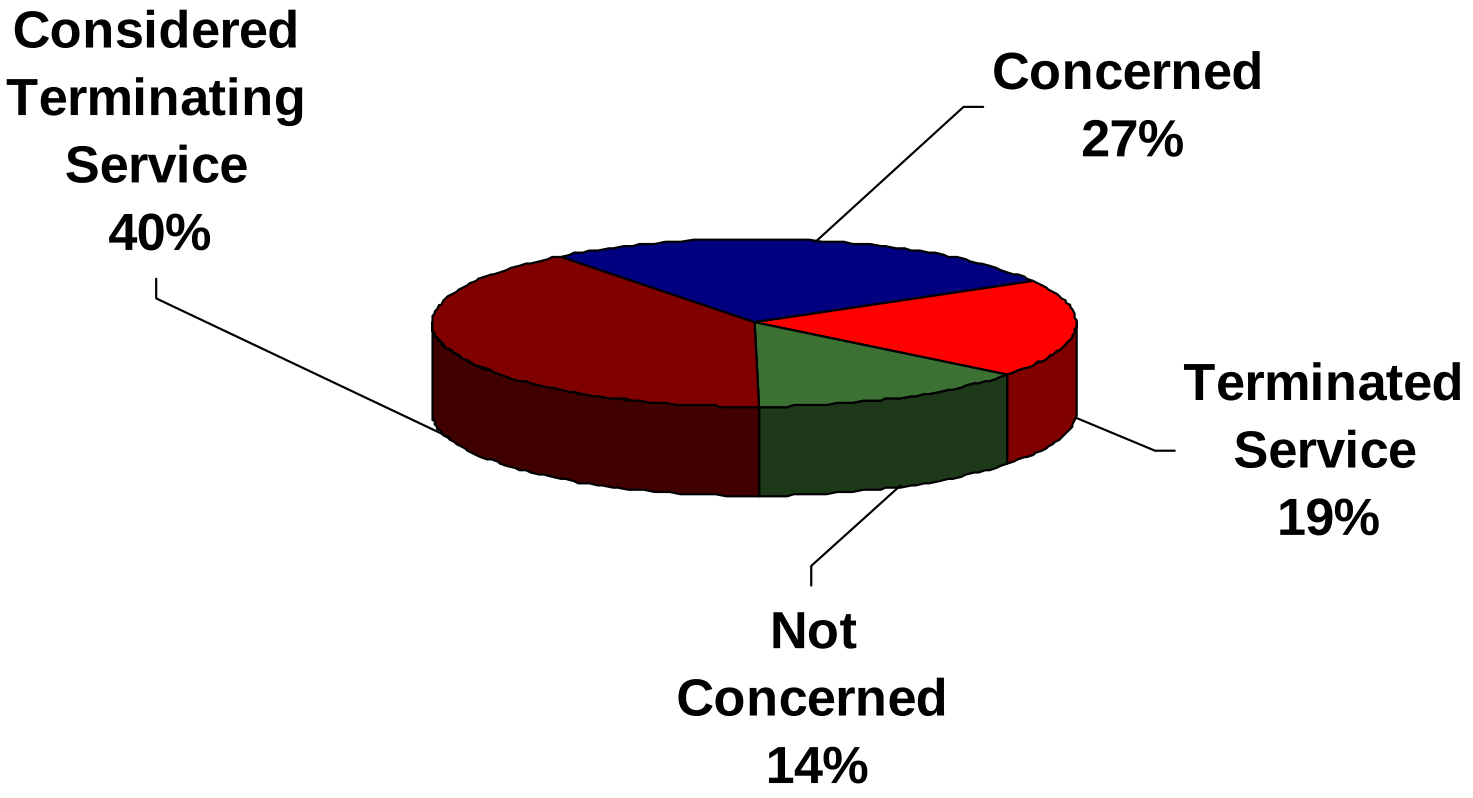


To date, personal information for at least 53 million US citizens has been lost, stolen or compromised

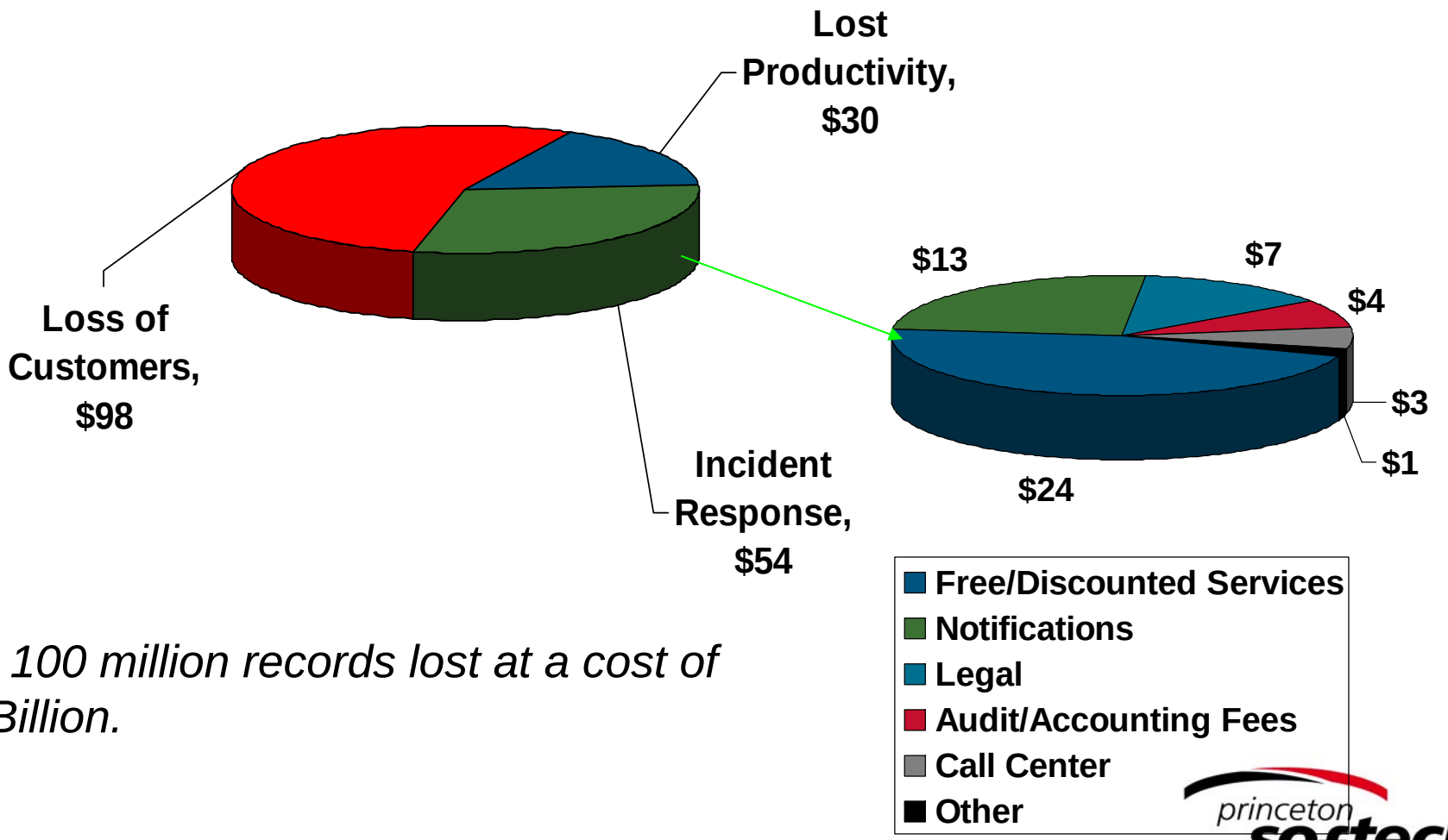
How Personal Data Was Lost



Consumer Reaction



Cost to Company per Missing Record: $182



Over 100 million records lost at a cost of $16 Billion.

Data Breach Examples

http://www.privacyrights.org

Company	Financial Impact
ChoicePoint	FTC Fine = $15M
Providence Health & Services	$7-9M (not including litigation)
BJ's WHOLESALE CLUB® Where values come to life.®	$10M and 3rd party audits every other year for 20 years
DSW	3rd party audits every other year for 20 years
Kaiser Permanente	State of CA fine $200,000 for a breach affecting 150 customers

princeton softech

What is Done to Protect Data Today?

- Production "Lockdown"
  - Physical entry access controls
  - Network, application and database-level security
  - Multi-factor authentication schemes (tokens, biometrics)
- Unique challenges in Development and Test
  - Replication of production safeguards not sufficient
  - Need "realistic" data to test accurately

How is Risk of Exposure being Mitigated?

- No laptops allowed in the building
- Development and test devices
  - Do not have USB
  - No write devices (CD, DVD, etc.)
- Employees sign documents
- Off-shore development does not do the testing
- The use of live data is ‘kept quiet’

The Easiest Way to Expose Private Data … Internally with the Test Environment

- 70% of data breaches occur internally (Gartner)
- Test environments use personally identifiable data
- Standard Non-Disclosure Agreements may not deter a disgruntled employee
- What about test data stored on laptops?
- What about test data sent to outsourced/overseas consultants?
- Payment Card Data Security Industry Reg. 6.3.4 states "Production data (real credit card numbers) cannot be used for testing or development"

princeton softech

Protecting Test Environments

Forrester Research:

"…IT's own access to customer and personnel data must be examined – strictly speaking, none should actually be necessary. *Test data must be "anonymized*…. " [sic]

Information Week:

"The search for consumer data and its uses doesn't stop at large production databases -- *it extends to application test data* and Web applications."

Encryption is not Enough

- DBMS encryption protects DBMS theft and hackers
- Data decryption occurs as data is retrieved from the DBMS
- Application testing displays data
  - Web screens under development
  - Reports
  - Date entry/update client/server devices
- If data can be seen it can be copied
  - Download
  - Screen captures
  - Simple picture of a screen

Exposure Points

- Are all test reports routinely shredded?
- Are test databases being sent to an outsourcer?
- Will employee NDAs deter a disgruntled developer?
- What is the risk of a lost laptop?
- Can test data be placed on portable devices?
  - Laptop
  - USB storage devices
  - CD
  - Hard drive

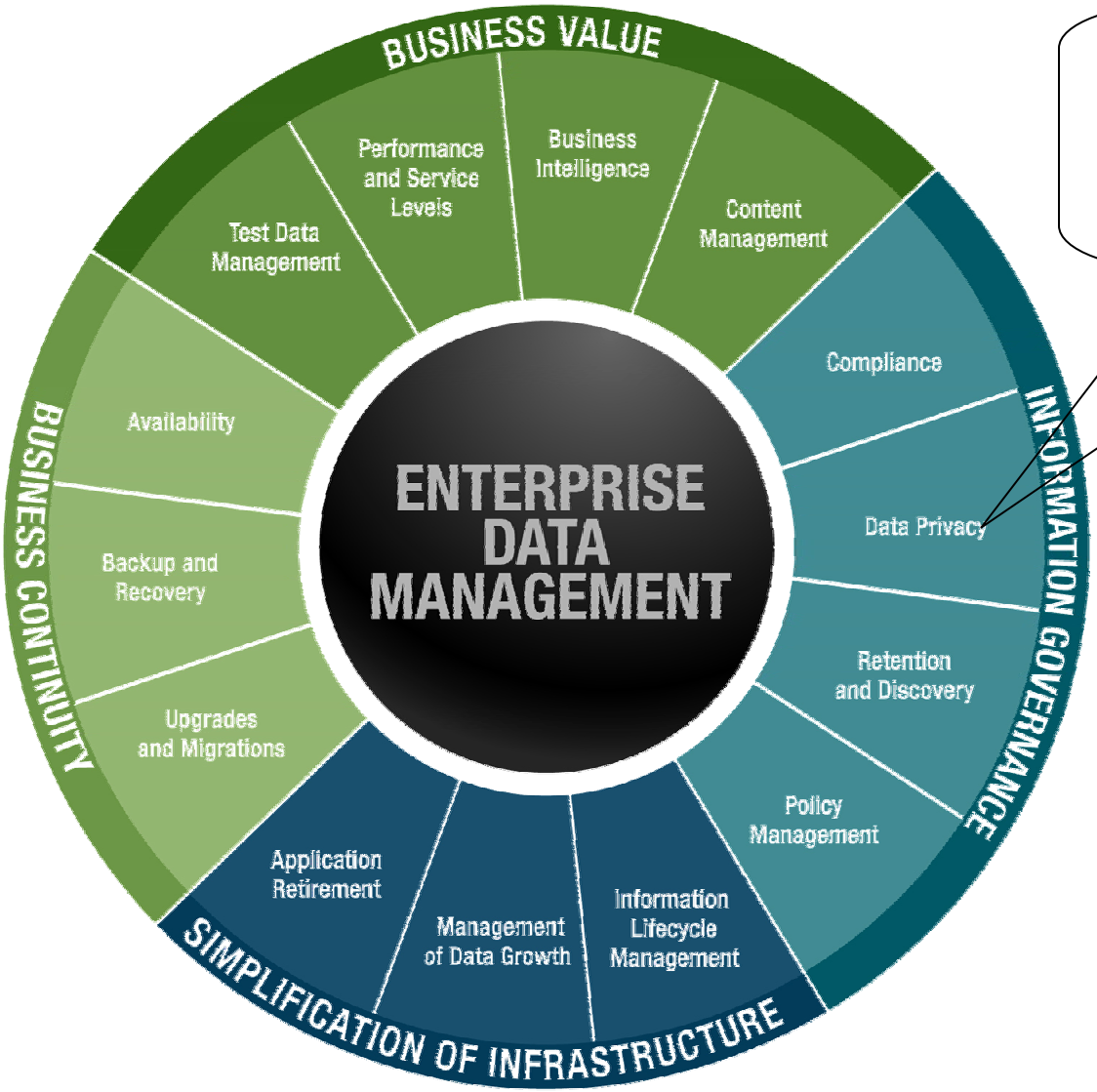
Best Solution: Optim to De-Identify Test Data

- Removing, masking or transforming elements that could be used to identify an individual
  - Name, address, telephone, SSN / National Identity number
- No longer confidential; therefore acceptable to use in open test environments
- No concern over off shore testing
- Loss or stolen hardware not a privacy breach
- Data has no value

princeton softech

Strategic Issues for Implementing Data Privacy

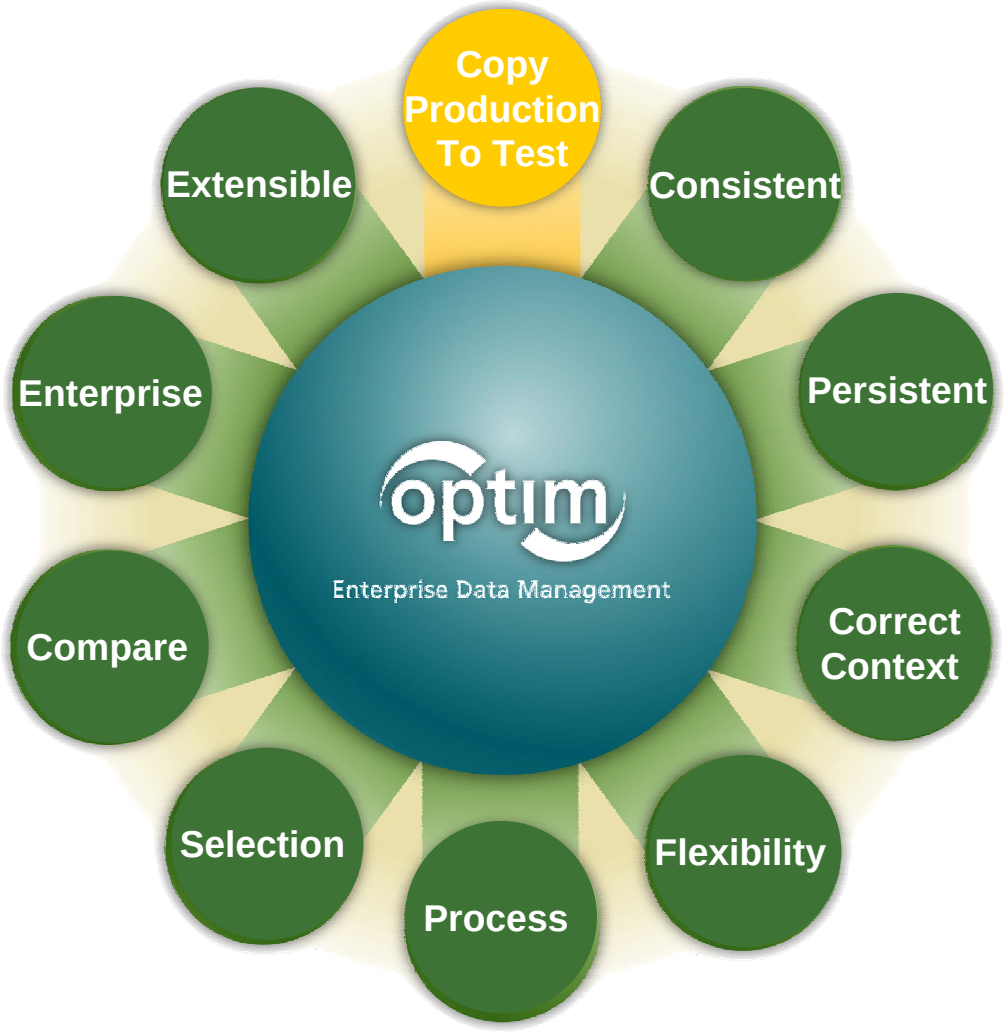
Optim Value across the Enterprise



Today's focus: Data Privacy

princeton softech

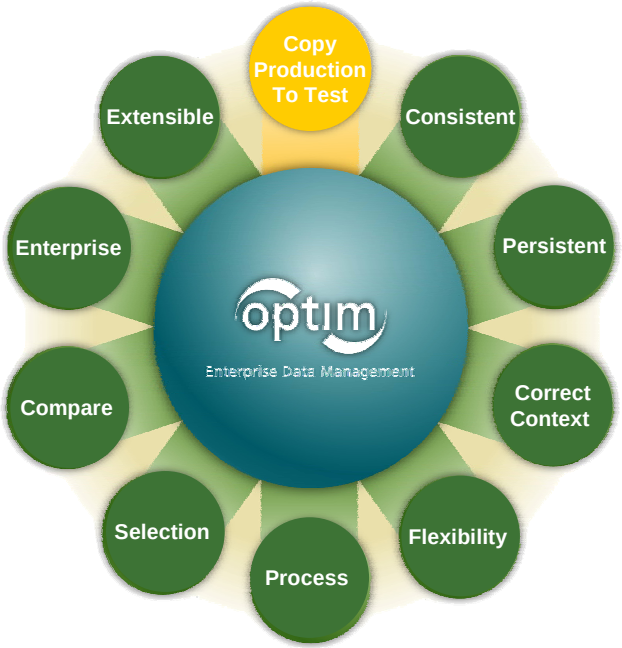
Components of an Privacy Project



- Masking is not a simple
  - Many DBMS
  - Legacy Files
  - Multiple platforms
- Meet system edits
- Existing processes
- Key fields
- Not a one time process
- Unknown ERP structure

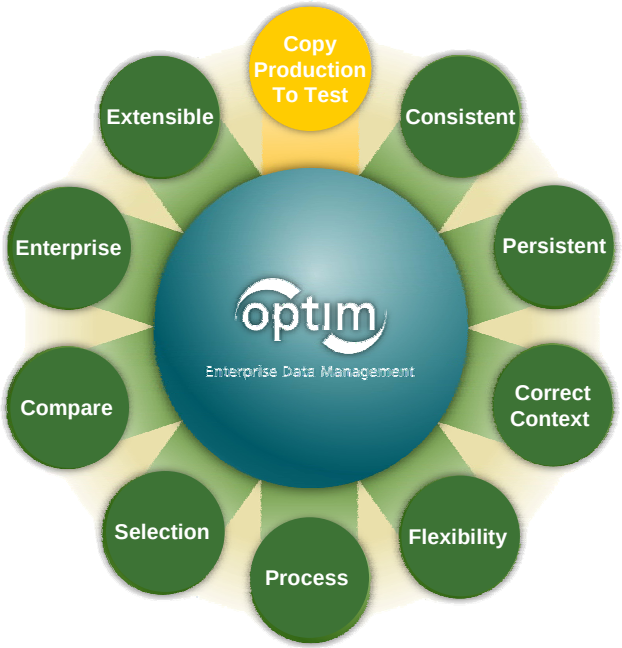
princeton softech

Consistency



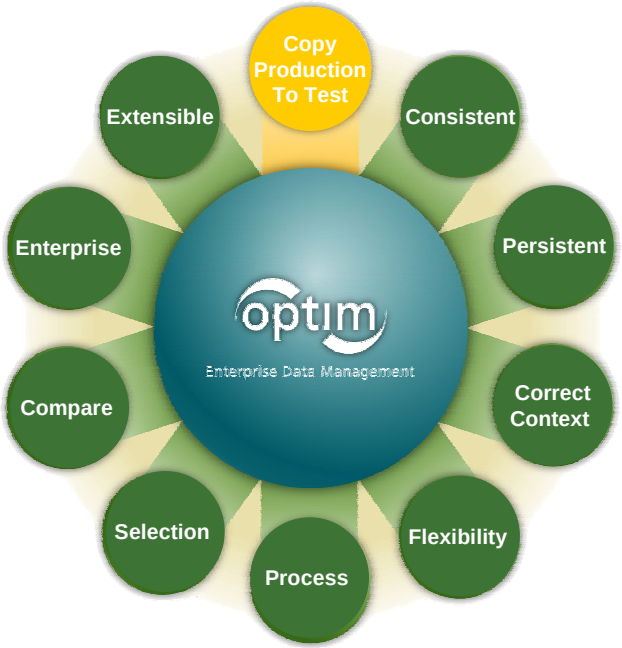
- Masking is a repeatable process
- Subsystems need to match originating
- The same mask needs to be applied across the enterprise
  - Predictable changes
  - Random change will not work
- Change all ‘Jane’ to ‘Mary’ again and again

Persistence



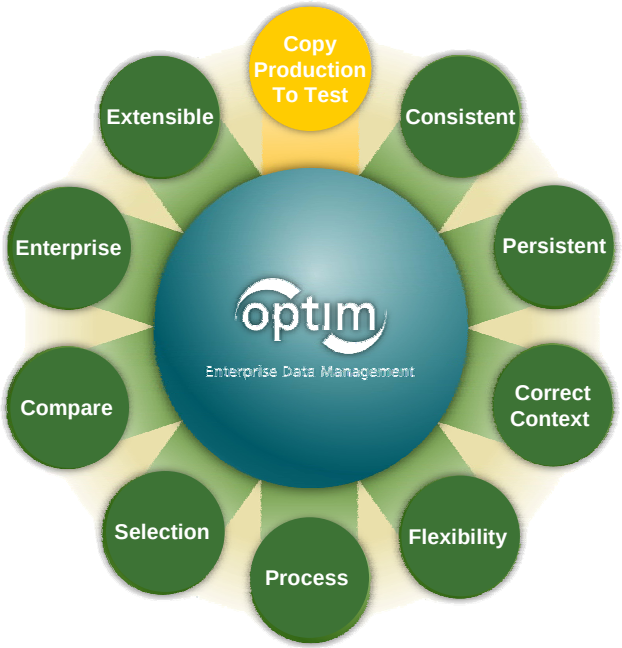
- One DBMS mask
  - Must match subsystem
- A single change must 'persist' to other DBMS
- A single change must 'persist' to other platform
- Physically separate DBMS systems need to be masked together

Contextually Correct



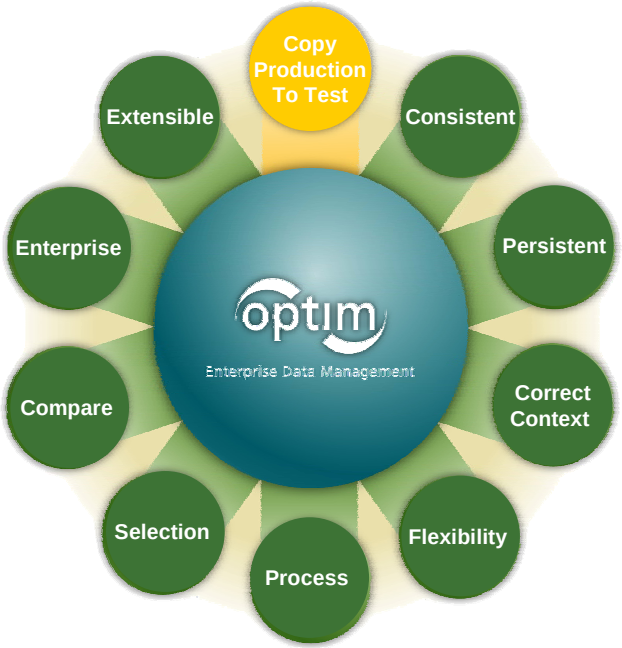
- A single mask will affect 'downstream' systems
- Column/field values must still pass edits
  - SSN
  - Phone numbers
  - E-mail ID
- Zip code must match
  - Address
  - Phone area code
- Age must match birth date

Flexibility



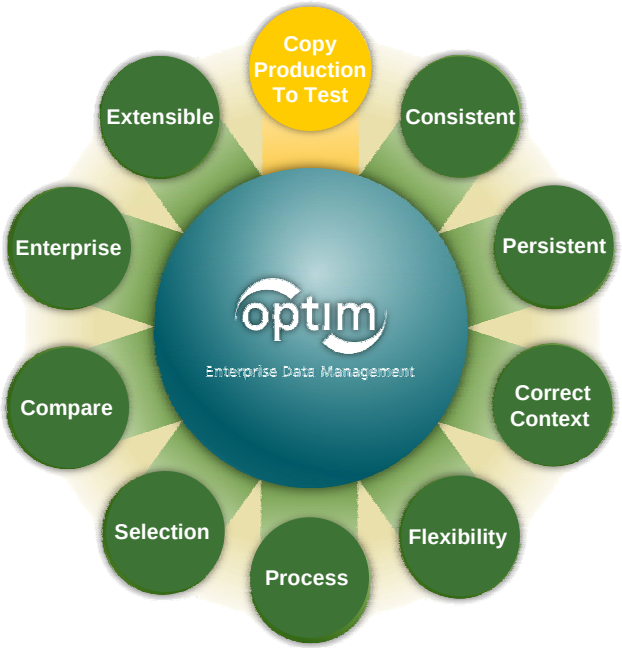
- Laws being interpreted
- New regulations being considered
- Change is the only certainty
- ERPs being merged
- Masking routines will change, frequently
- Quick changes will be needed

Process



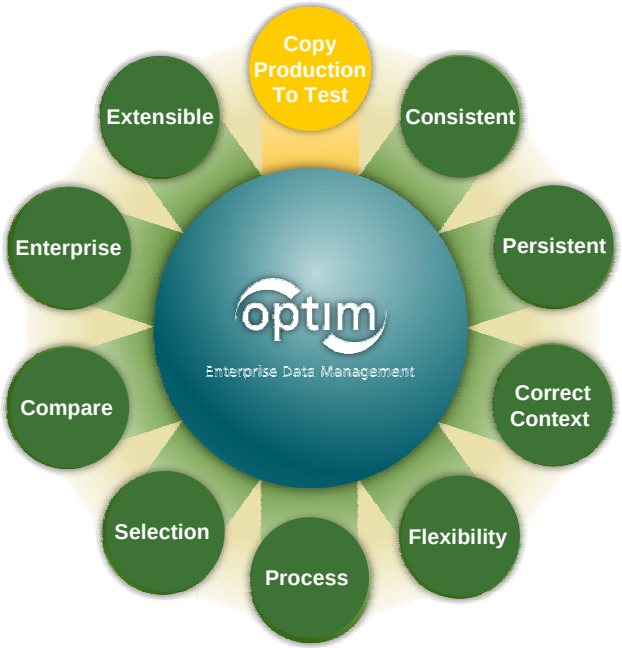
- Masking needs to be an integrated process
  - Batch test runs
  - Automated testing tools
- Not a one time process
- Masking of data is an ongoing process for the enterprise
- Management of routines required

Data Selection



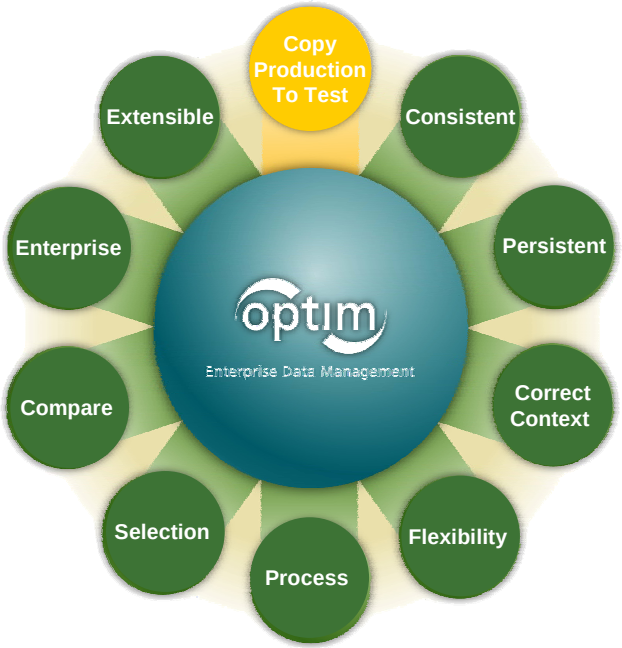
- Simply changing personal columns is not enough
- Value of some columns could lead to identity
- Privacy is maintained by excluding rows/records

Compare Masking Results



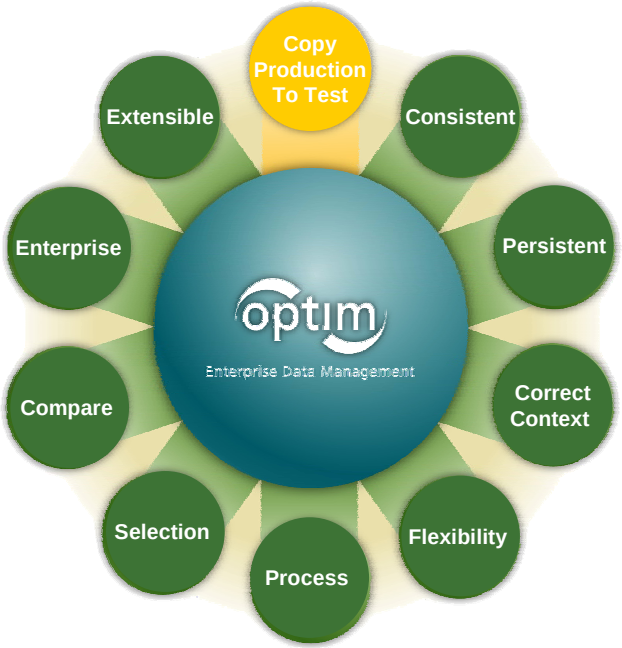
- Guess work leaves loopholes
- Must be sure masks are
  - Consistently applied
  - Persisted
  - Syntactically correct
- Testing of mask routines imperative

Enterprise



- Masking is not a point solution
- Systems are integrated
- Mask routines applied on
  - Legacy
  - Unix systems
  - Windows
  - I-Series

Extensible



- Masking routines are vendor supplied
- Industries have specific needs
- Global systems present more challenges
  - SSN in US
  - Codice Fiscale (National ID) in Italia
- Vendor solutions need extensible libraries

OPTIMIZE

Introducing Princeton Softech Optim™