



Bridging Strategy and Data



Data Security Considerations – Protection of Sensitive Data and Compliance with Privacy Laws

Presented to: Software Industry Conference
July 16th, 2009

Data Privacy Laws – Today and Tomorrow

- Present - Most States have reactive data privacy laws (e.g. California)
 - Generally don't require protection of data, just "appropriate safeguards"
 - Focus on informing consumer of breach, rather than preventing one
- Future - More proactive laws (e.g. Massachusetts)
 - Require protection of data
 - Any company that stores data about a MA resident is subject to the laws even if the company does not have an office in the state
 - 3rd party vendors used by the company are also required to comply
 - Companies are liable regardless of where the fault lies
 - Carry penalties when there are breaches
 - Fines when a breach occurs
 - Fines for each record breached – in some cases up to \$5000/record

Business Impact of Data Breaches

- Direct Financial Cost to the Company
 - \$197 average cost per compromised record*
 - \$98 Loss of Customers
 - \$69 Incident Response
 - \$30 Lost Productivity
 - Average cost per data breach “incident” - \$6.3 Million*
- Other Costs
 - Fines/Penalties
 - Potential Lawsuits
 - Negative Publicity
- Consumer Reaction
 - 19% terminated service
 - 40% considered terminating service
 - 24% were concerned
 - 14% were not concerned

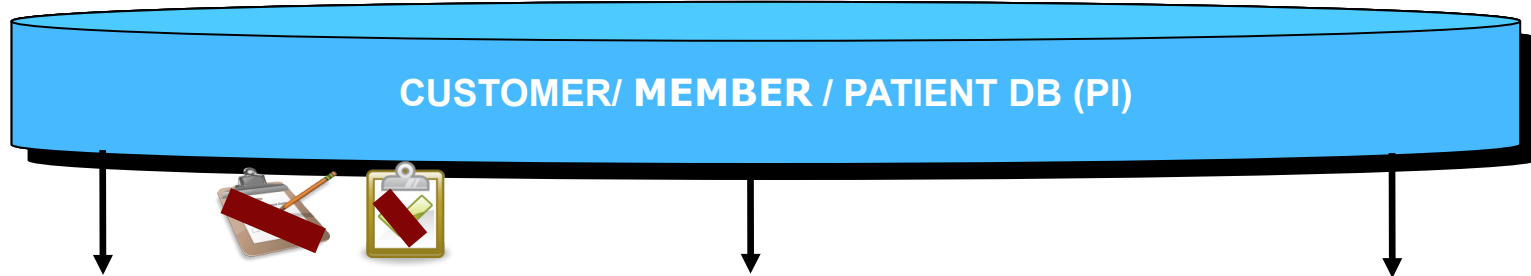
*Source: Ponemon Institute

Examples of Data Breaches

- Harvard University (3/12/2008)
 - Graduate School of Arts and Sciences web server may have compromised student and applicant data
 - 10,000 sets of personal information may have been compromised, including 6600 SSN's
 - Under new laws, could be a fine of up to \$50 million
- Lasell College (3/20/2008)
 - Hacker accessed data containing personal information on current and former students, faculty, staff, and alumni
 - Estimate of 20,000 records breached
 - Under new laws, could be a fine of up to \$100 million
- Local financial company (5/29/2008)
 - Computer equipment containing customer and employee information was stolen from a vendor hired to provide legal support services
 - Data included 45,500 names, addresses, and SSN's
 - Under new laws, could be a fine of up to \$227.5 million

*Source: Privacy Rights Clearinghouse (<http://www.privacyrights.org>)

PI Data Requirements Issues in Business



INTERNAL, PRODUCTION







INTERNAL, NON-PRODUCTION



EXTERNAL USES

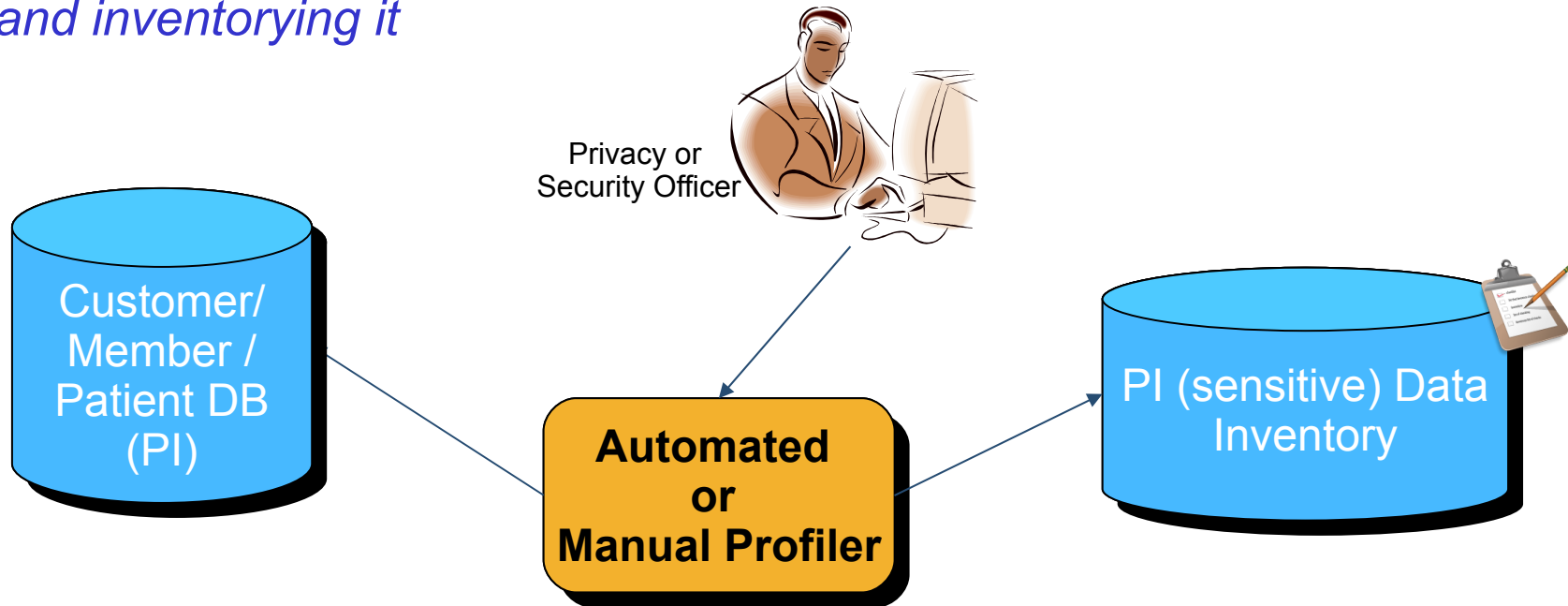


PI Data Requirements Issues

-  *PI is not inventoried and documented electronically*
-  *PI is not de-identified when provisioned*
-  *PI is not monitored so inappropriate access can be detected*
-  *No automated certification and documentation methods for audit purposes*

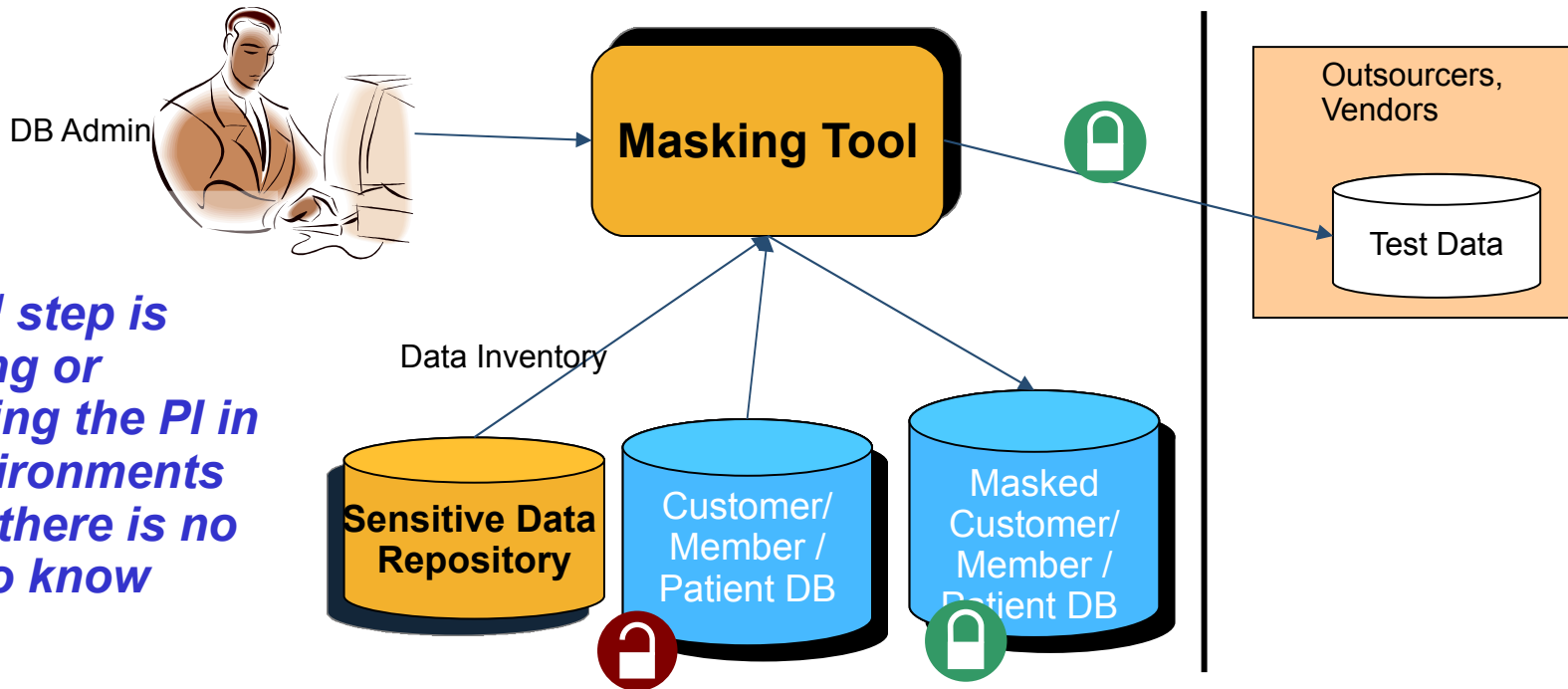
Inventory Personal Information (PI)

The 1st step to protecting PI is locating and inventorying it



Data Requirements Met	Automation Benefits
<ul style="list-style-type: none"> ✓ Identify and document all repositories storing PI 	<ul style="list-style-type: none"> • PI can be inventoried so the locations and amounts are well-understood • PI locations are documented and available for query and reporting

Restricting Access to PI



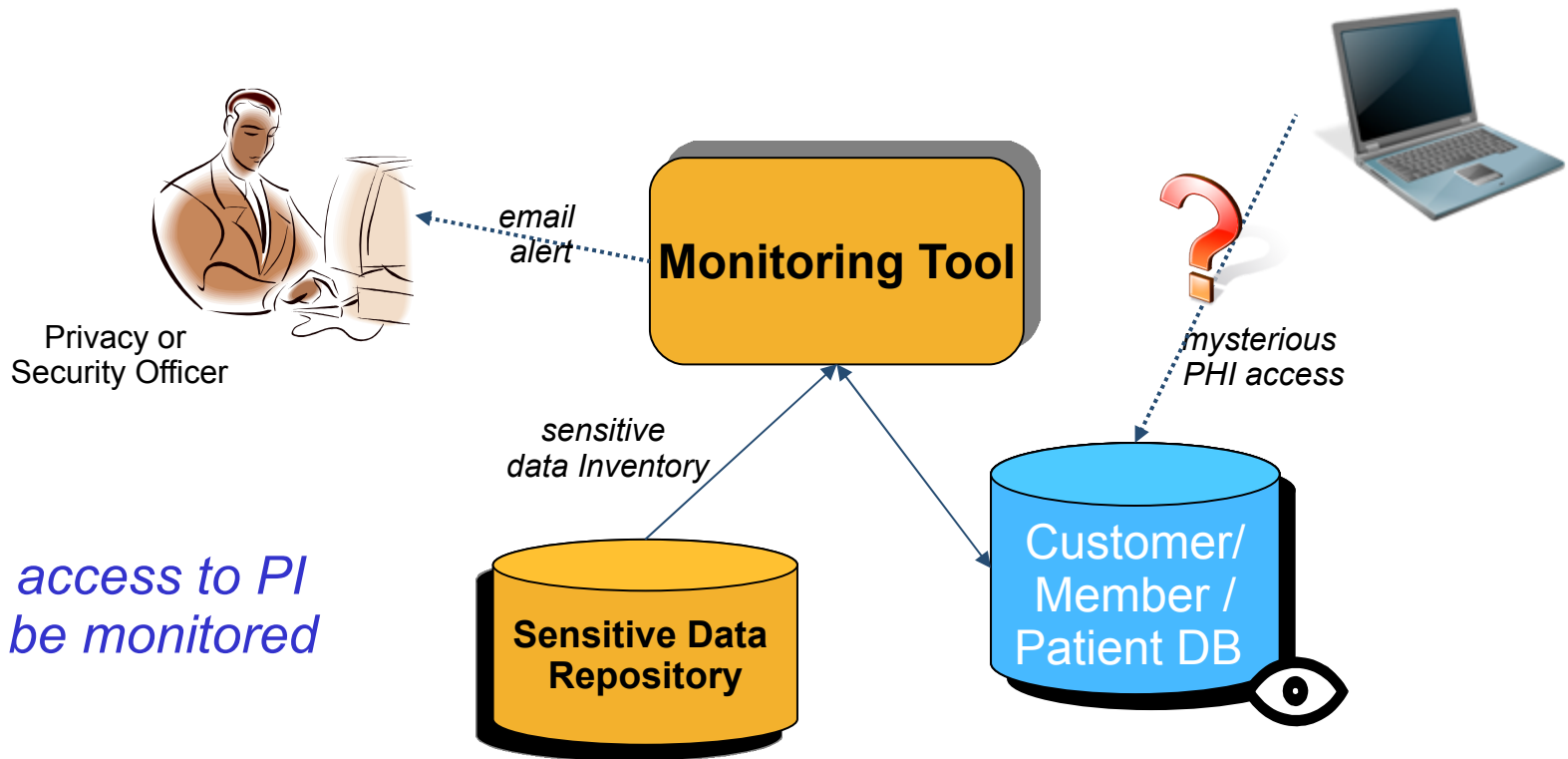
The 2nd step is masking or redacting the PI in all environments where there is no need to know

Data Requirements Met	Masking Tool Benefits
<ul style="list-style-type: none"> ✓ PI data should be de-identified (masked) or reduced to minimal levels in non-production environments ✓ PI data should be masked before sharing with business and technical partners 	<ul style="list-style-type: none"> • Automates Compliance with privacy and security rules when sharing data internally and externally • No application re-engineering required • Creates a measurable, documented, and repeatable process for protecting PI • Common approach leads to minimal impact on integration testing • Provides clearly auditable result

Restricting Access to PI (continued)

- Front End
 - Ensure Identity and Access Management is in place
 - Perform regular user entitlements reviews
 - Maintain a mapping of user entitlements to PI
- Back End
 - Identify where PI resides
 - Leverage existing data inventory
 - Buy/build tool to scramble/obfuscate PI data
 - Needs to be masked in such a way that it can be used by IT folks in place of production data
 - Deploy process to your environments in a rolling fashion
 - Need to allow IT folks to verify that masked data meets the needs of their work
 - Put a process in place to ensure scrambled data is always used and deter exception requests to use real data

Monitoring Access



Finally, access to PI should be monitored

Data Requirements Met	Benefits
<ul style="list-style-type: none"> ✓ User access to PI data should be monitored and reported ✓ Encrypt External Transmissions and Storage ✓ Monitoring controls should be considered "lockdown" for PI where scrambling/masking won't work 	<ul style="list-style-type: none"> • Ensure only authorized personnel are accessing PI • Enables immediate action for PI security breaches • Email, Laptops, Smart Phones, Remote Access, USB Storage and Data Feeds need to be secured • Monitoring can be costly so a surgical approach works best • Products are available on the market that can assist with database monitoring/mapping to IDAM systems

Common Data Masking Concerns

1. **Post-Masking Stress Disorder** – coping with the loss of real production data
2. **You Sunk My Database** – referential integrity is the tip of the iceberg
3. **A Zero business value project** – showing ROI
4. **Prove it** – showing results to ISOs, auditors, regulators, and sponsors
5. **Not in *my* backyard** – where masking fits into your information security framework
6. **Cleaning up this mess** – integrating masking into the SDLC

Post-Masking Stress Disorder

- Challenge
 - “We won’t be able to test! The application won’t work. I can’t do my job like that...”
- Solution
 - Make target data look and act realistic.
 - “Let us show you – just give us a sandbox, then check out the results before giving approval.”
- Benefit
 - Empower development teams in the process.
 - Provide development teams with usable data.

You Sunk My Database

- Challenge
 - “These applications need to talk to each other even after they’re masked.”
- Solution
 - Determine which systems:
 - Must be masked in synch.
 - Need to be masked first, then used to feed downstream applications.
 - Identify data elements that must be preserved.
 - Address interrelated fields.
 - Select the best technique to mask each data element (context-dependent.)
- Benefit
 - Applications work and interact seamlessly.

A Zero business value project – showing ROI

- Challenge
 - “This is going to slow down and complicate my work.”
- Solution
 - Place more stringent controls on Production data.
 - Employ automation wherever possible.
- Benefit
 - A major benefit of an automated approach is that it creates greater efficiency in maintaining data masked
 - With a better understanding of how the application and its data, bug- and break-fixing becomes faster and easier.

Prove it – showing results to stakeholders

- Challenge
 - “We did masking last year, so we’re all set.”
- Solution
 - Employ smart tools, process, automation and audit trails in the ongoing monitoring and periodic testing of masked environments.
- Benefit
 - Make it easy to keep and show that a masked environment is still ‘clean.’

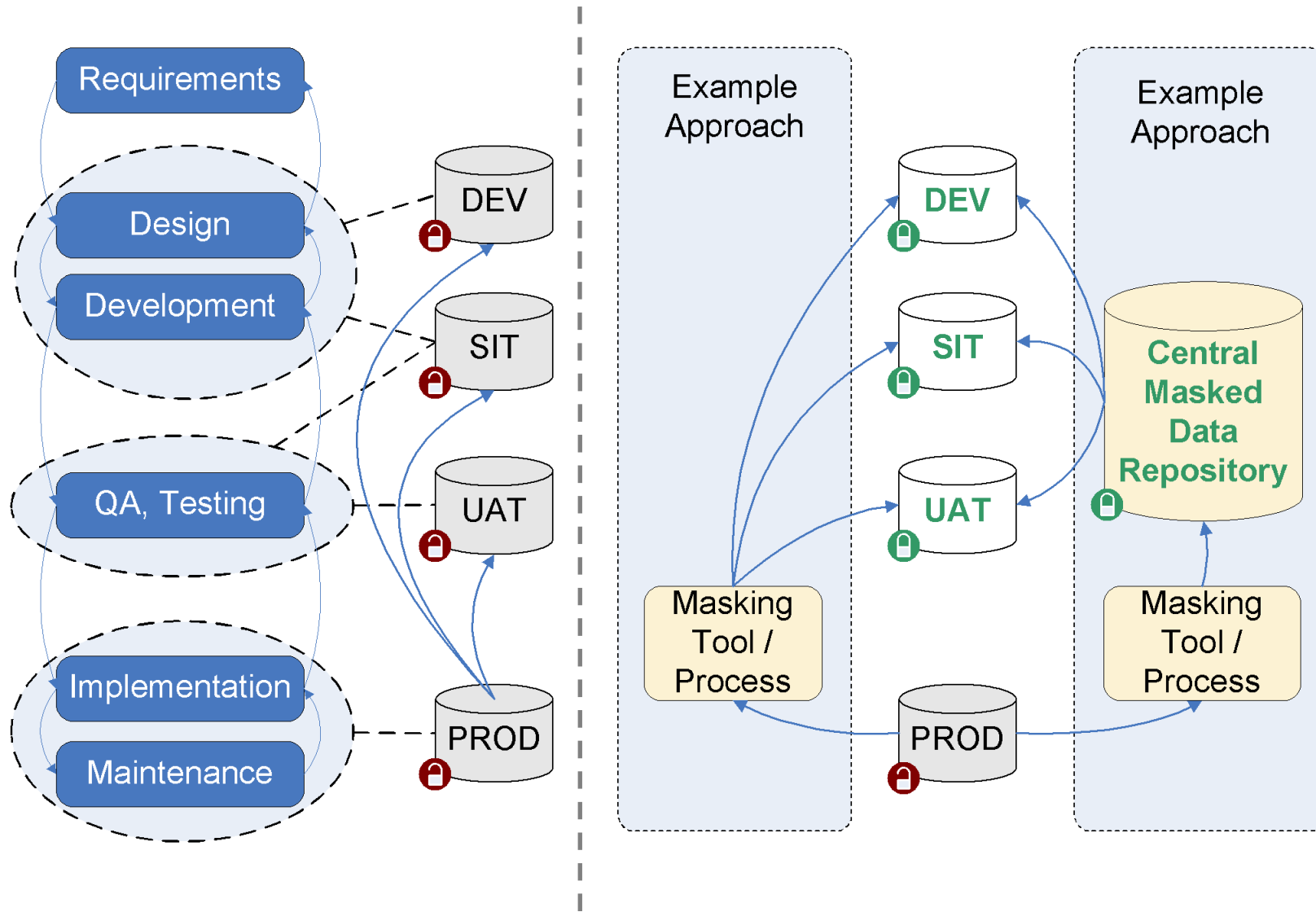
Not in my backyard – where masking fits

- Challenge
 - “We already don’t just give ‘anyone’ access...”
- Solution
 - Keep in mind that Data Masking is not a one-time event; it’s one of several tools in your Data Security Toolkit.
- Benefit
 - Knowing when and where to employ data masking versus other data confidentiality controls (RBAC, lockdown, etc.) helps your organization avoid a slow-down in productivity.

Cleaning up the mess

- Challenge
 - “How am I supposed to get my job done if I have to mask data at every step of the way?”
- Solution
 - Analyze each SDLC instance to determine the best potential ‘in point’ for data masking.
- Benefit
 - Data masking becomes part of the ongoing process, yet remains as behind-the-scenes as possible.

Integration of Masking with Development Cycle



TYPICAL REACTIONS & CONCERNS



Bridging Strategy and Data

Axis Technology, LLC

Boston • New York • Dallas

225 Franklin Street
Boston, MA 02110

(617) 217-2153

www.AxisTechnologyLLC.com

THANK YOU.