

# Identity Management: The Responsible Information Management Perspective

---

Dr. Larry Ponemon  
Digital ID World Conference  
May 10, 2005

# My Agenda

- The responsible information management (RIM) perspective
- From the RIM perspective, what are the “seven deadly sins” of identity management?
- What do recent consumer studies by Ponemon Institute, Unisys and other learned sources tell us about responsible ID management practices?
- What is the moral of our story?

## Unisys & the Security Leadership Institute

- **Mission:** To help organizational leaders advance security practices that build stakeholders' confidence and trust across the enterprise.
  - Launched by Unisys, we are an independent group working to advance best practices in the security risk management space.
  - Composed of leaders from national security, intelligence, IT, business, law enforcement, & academia.
  - Dedicated to the proactive security solutions such as identity management.

## **Responsible Information Management**

- ✓ A process for engendering trust and confidence in how an organization manages sensitive, private and confidential information.
- ✓ RIM requires the alignment of key stakeholders' privacy and data protection preferences with business and technologies across the organization.
- ✓ RIM requires the holistic management of privacy, security, IP protection, confidentiality, data quality (accuracy) and IT efficiency.

## **RIM in the IdM Space**

- RIM is important because it requires companies to balance the end-user experience with ever-increasing security requirements.
- Implementation of a RIM process would highlight areas that should enhance the effectiveness of IdM within a complex environment.
- Implementation of a RIM process would identify IdM solutions that are not meeting targeted goals.

## Keep in Mind ...

- RIM is not about making IdM solutions better in a technical sense.
- IdM deployment usually fail because of two non-technical reasons:
  - Mismatched or ill-defined technology solution.
  - Poor supporting manual controls.

## What's Next?

- When IdM fails to consider the human factor.

# Seven Deadly Sins of IdM

1. Rigor reduces productivity
2. Tighter security motivates shortcuts
3. Easy IdM decreases trust among end-users
4. Over collection of PII creates privacy risks
5. Poor manual practices increases social engineering risks
6. Too much autonomy creates opportunity for malicious insiders
7. Forgetting about low-tech risks

# 1. More rigor reduces productivity

- **Case**
  - FS company's consumer service (CS) department implements new IdM system.
  - IdM requires everyone to change password from four-digit number to a seven digit alphanumeric code. New passwords are changed every 60 days.
  - IdM locks out employees after three failed attempts.
- **Consequences**
  - Many CS employees did not remember passwords
  - The IT help desk was overrun with calls and complaints
  - CS department productivity plummeted

## 2. Tighter security motivates shortcuts

- **Case**
  - Same FS company.
  - Employees took shortcuts that put the organization at great risk.
- **Consequence**
  - CS Employees started to share passwords
  - CS Employees used post-it notes to record 8+ digit codes
  - CS Employees develop simple heuristics to remember passwords or PIN (that can be easily guessed).
- Lesson: When you engineer the IdM solution don't over estimate ability to remember passwords and PINs

## 3. Ease decreases confidence

- **Factoid**

- Ponemon Institute’s recent online banking study shows that customers attach a higher level of “trustworthiness” when they view the IdM solution as “rigorous”.
- When customers view IdM as overly simplistic or too easy, they start suspecting privacy and security risks.
- The balance between convenience and trust depends on various factors, including industry requirements, the nature of the customer transaction, sensitivity of information shared, and access needs.

## 4. Over collection of PII

- **Case**

- Information collected for IdM such as DOB, SSN and other sensitive data elements should not be used for secondary purposes or shared without consent.
- In the IdM space, more may not be better than less. Collecting too much data may tempt others within the organization to reuse sensitive personal information for secondary purposes such as marketing.
- Ponemon Institute study shows that people are willing to share more personal facts about themselves and their households for authentication purposes than for marketing or online personalization.

## 5. Poor manual practices

- **Case**
  - Serious IdM enrollment failures at non-US governmental entity issuing biometric-enabled credential for airline workers.
  - Poorly trained contract personnel did not follow general inspection procedures, allowing criminals to show false documents to obtain smart cards.
  - Because of mistakes, seriously “bad” criminals and possibly terrorists have “legitimate” public credentials and access rights.

## 6. Monitoring the insider

- **Case**
  - Data base administrator (DBA) has significant responsibility and autonomy in the company's data center.
  - DBA controls the IdM system
  - What happens when the DBA gets mad? Or, is laid-off as a result of off-shoring the IT function?
- Lesson: Know the people who “control” the IdM solution and watch them closely. The monitoring issue becomes more salient when the IdM function is outsourced.

## 7. Ignoring low-tech risks

- **Case**
  - Data brokerage company has solid IT security controls.
  - Bad guys learn about the company, and register as business customers.
  - Criminals access over 300k+ individual records containing enormous amounts of sensitive personal information.
- **Case**
  - Identity thieves obtain low-level positions in corporate call centers giving them access to thousands of customer records. This may become a trend in off-shoring relationships (and could happen anywhere).

## What We've Learned

- ID management should be easy and efficient. People don't want to face overly complex passwords or multiple tiers of access controls.
- Despite identity theft concerns, consumers continue to share private information with unknown entities, even over the telephone or Internet. Despite excellent IdM solutions, the public's willingness to share PII makes companies vulnerable to continued criminal attacks.
- Consumers will share more and better information about themselves with companies that they trust, and especially for IdM purposes.

## What We've Learned

- Organizations that collect sensitive personal information for IdM purposes should provide notice about possible secondary uses.
- In the event of a privacy or data security breach, the public expects the organizations to provide personalized notice by either phone or e-mail.
- We expect different types of organizations, such as airlines, credit card companies, banks, and health care providers, to have stronger IdM and verification methods than other organizations such as retailers.

## What We've Learned

- From our IS tracking studies, many large companies under perform on the IdM front despite the availability of excellent, low cost technology solutions.
- The public appear to prefer Web channels for registration and credentialing than by telephone.
- The public's impressions about biometrics is improving.
- The public appears to be warming up to the idea of a universal identity management program.

# The Moral of the Story

- If done right, good identity management is an opportunity to create end-user trust and confidence
  - Strictly limit secondary uses of PII
  - Don't over-engineer the IdM solution
  - Consider biometrics—people are receptive to it
  - Most importantly, have RIM practices that support technology