Conference Presentation

Identity Theft: Enterprise-Wide Strategies for Prevention, Detection and Remediation

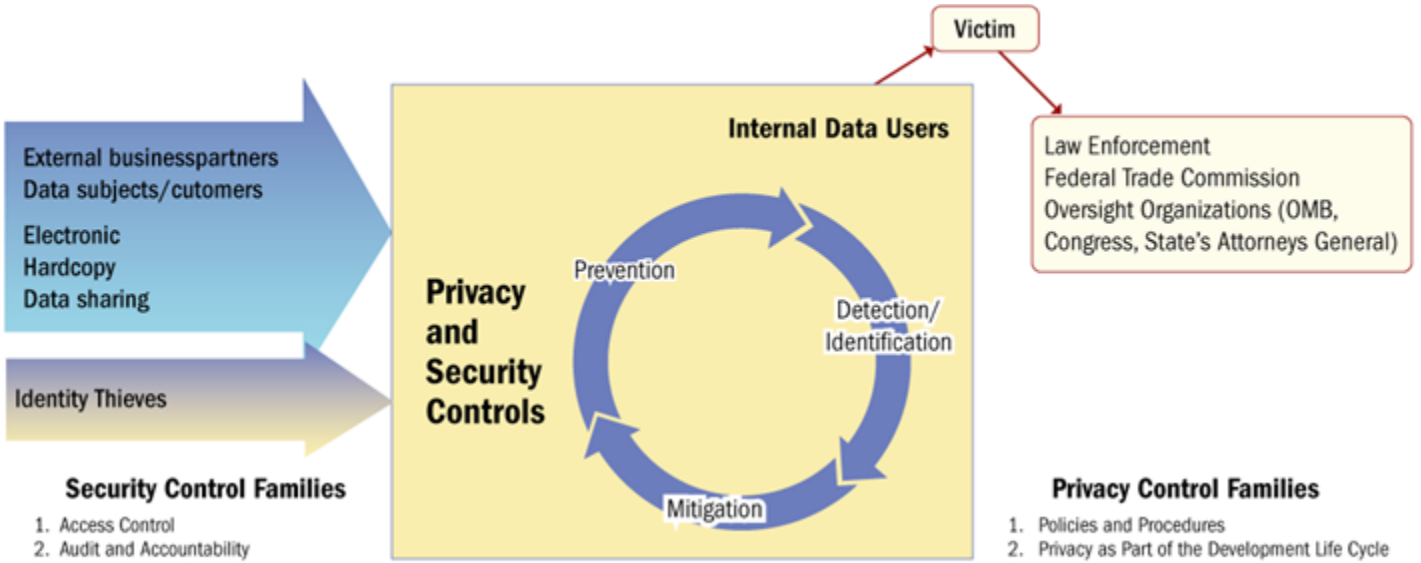
Kris O'Neal
Dan Steinberg
Harvard Privacy Symposium
August 20, 2008

We offer the usual disclaimer for the contents of this presentation and any verbal comments we make during its delivery.

Any and all opinions expressed are solely our own, and should not be attributed to Booz Allen Hamilton, the Office of the National Coordinator for Health Information Technology, or any other business or agency.

Table Of Contents

Identity theft strategies must take into account multiple actors, platforms, and stakeholders…



Security Control Families

1. Access Control
2. Audit and Accountability
3. Awareness and Training
4. Certification, Accreditation, and Security Assessments
5. Configuration Management
6. Contingency Planning
7. Identification and Authentication
8. Incident Response
9. Maintenance
10. Media Protection
11. Personnel Security
12. Physical and Environmental Protection
13. Planning
14. Risk Assessment
15. System and Communications Protection
16. System and Information Integrity
17. System and Services Acquisition

Privacy Control Families

1. Policies and Procedures
2. Privacy as Part of the Development Life Cycle
3. Assigned Roles, Responsibilities, and Accountability
4. Monitoring and Measuring
5. Education: Awareness and Role-based Training Programs
6. Public Disclosure
7. Notice
8. Consent
9. Minimum Necessary
10. Acceptable Use
11. Accuracy of Data
12. Individual Rights
13. Authorization
14. Chain of Trust
15. Risk Management
16. Reporting and Response
17. Security Measures

…but privacy efforts remain central to identity theft strategies

Table Of Contents

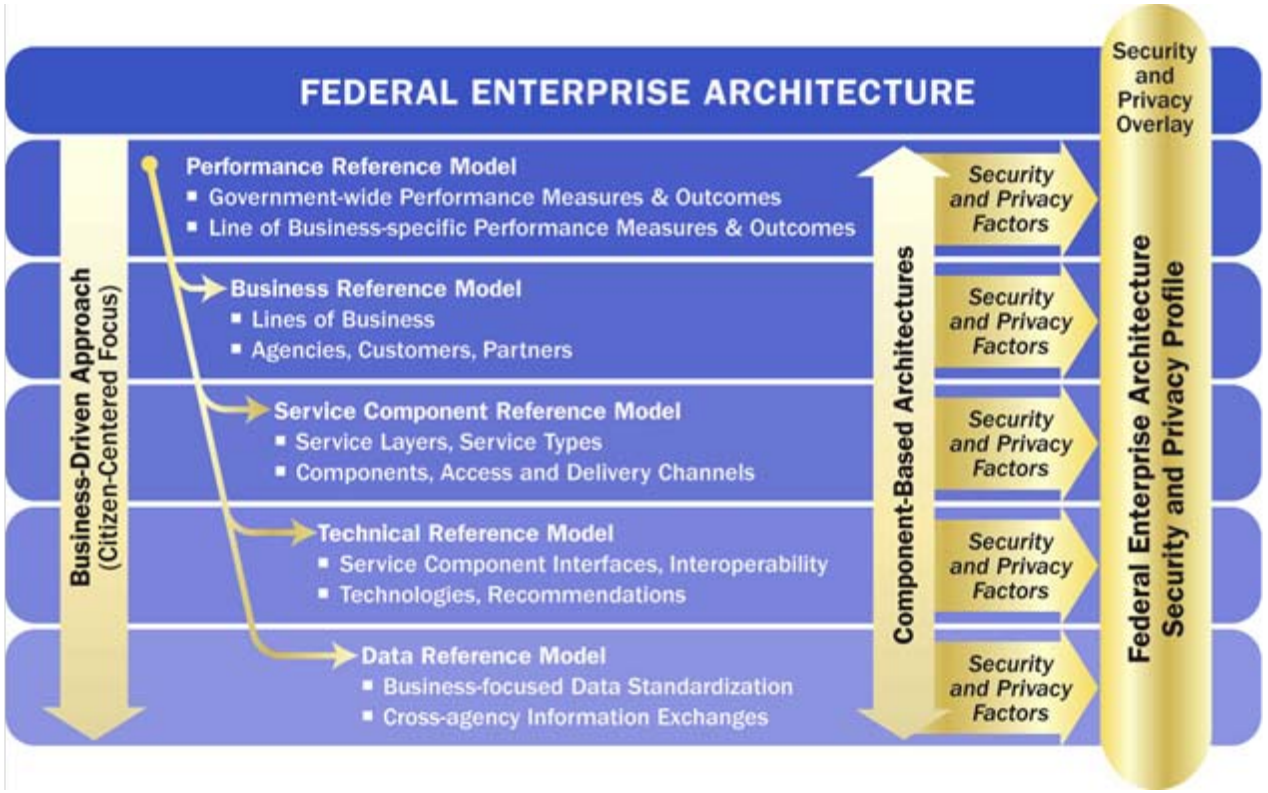
- Enterprise View of Identity Theft
- Enterprise Identity Theft Prevention Strategy
- Medical Identity Theft: Detection and Mitigation

Prominent activities that can help prevent identity theft include data minimization, accuracy, and individual rights

- Eliminate PII where possible, especially social security numbers (SSNs)
  - SSNs and other PII may need to be used because of secondary and ancillary needs, such as correlating records
- Ensure information is accurate
  - Validate data received from business partners where possible
  - Implement authentication schemes
- Be prepared to serve the customer
  - When your organization is the subject of a data breach
  - When the customer has been the victim of identity theft elsewhere

Identity theft prevention requires strong privacy and security controls—at all levels and sectors of the enterprise

- Understand existing technologies within your organization and deploy tools to enforce privacy and security
- Ensure the business components understand expectations for implementing privacy, security and identity theft strategies
- Establish performance metrics for privacy and security and use that data to drive decisions



Take a cross-organizational and cross–functional approach by recruiting senior officials to communicate their strong support for privacy and security activities

- All privacy offices must demonstrate the primary competency of fostering stakeholder collaboration
- Privacy and identity theft efforts must be integrated at the business level
  - Ideally, privacy governance will provide strong infrastructure
  - Even then, business units must ultimately support and implement solutions, and may even determine what approaches are needed and used
- Organization leadership must support the privacy and identity theft strategy
  - Bears ultimate responsibility for navigating challenges

Table Of Contents

- Enterprise View of Identity Theft
- Enterprise Identity Theft Prevention Strategy
- Medical Identity Theft: Detection and Mitigation

Medical identity theft is a new topic within identity theft with limited information available about its scope, depth, and breadth

- Occurs when a person:
  - Uses someone else's personally identifiable information (PII) or protected health information (PHI)
  - Without the individual's knowledge or consent
  - To obtain medical goods or services, or submit false claims for medical services.

- There is limited information available about the scope, depth, and breadth of medical identity theft

Year	Identity Theft Complaints	Medical Identity Theft Complaints
2001	86,000	1400
2005	256,000	4600

Source: Federal Trade Commission, *2006 Identity Theft Survey Report*

- Possible effects include loss of patient privacy; loss of health record integrity; slowed adoption of health IT (EHRs, PHRs, NHIN); and financial consequences to the patient, provider, or health care system.

Other health care fraud case studies are relevant to the exploration of “true” medical identity theft

Case Studies	Patient Record Integrity Threatened	Possible Financial Consequences	Change in Pattern: Patient Services Received	Change in Pattern: Provider Billing	Health Care Actually Provided	Patient Authentication Failure
Medical Identity Theft	✓	✓	✓		✓	✓
Medical Familial Identity Theft	✓	✓	✓		✓	✓
Phantom Provider/ Wholesale Fraud	✓	✓	✓	✓		
Upcoding	✓	✓	✓	✓	✓	

Anecdotal evidence provides examples of the kinds of fraud and identity theft techniques organizations must combat

- 2006: A Pennsylvania man stole a coworker's identification and used it to obtain over 40 prescriptions for Viagra.
- 2006: Another Pennsylvania man accessed a stranger's medical information and used it to pay for $140,000 in hospital charges.
- 2005: An unknown Washington State person stole the identity of a 3-week old baby to obtain large prescriptions of the often-abused painkiller, Oxycontin.
- March 2004: A Colorado man used a stranger's medical identity information to obtain surgery worth over $41,000
- 2003: Five health care providers in Milpitas, California provided elderly patients with checkups at a fake clinic, but also used their Medicare information to charge the program for $900,000 in services that were not delivered.

To understand beyond the anecdotal and to begin to scope the breadth and depth, the Office of the National Coordinator for Health Information Technology is studying this issue

- Medical identity theft has possible implications for the development of a National Health Information Network (NHIN)

- ONC is developing:
  - A comprehensive Environmental Scan of the medical identity theft problem in the U.S particularly focusing on the intersection of Health IT
  - A one-day Town Hall meeting to enable health care experts to share knowledge and experience of medical identity theft and how health IT can be utilized to prevent and detect medical identity theft.
  - A final report and roadmap

- Topics for exploration include:
  - Understanding the magnitude of the problem (cost, frequency)
  - Understanding its mechanisms (threats and vulnerabilities)
  - Available methods of prevention, detection, remediation

Solutions and controls must implemented and targeted at the full life-cycle: prevention, detection, and remediation.

- Categories of possible controls are identified for discussion purposes only

Possible and available categories of controls for:		
Prevention	**Detection**	**Remediation**
Incorporation into risk assessment	Exceptions or pattern recognition	Law enforcement (DOJ, FTC, HHS, CMS, State Attorneys General, FBI, others)
Education and awareness	Explanations of Benefits (EOBs) provided to patients	Incident response protocols and mechanisms
Patient authentication	Other victim reporting	Patient privacy principles: Notice, Choice, Access, Redress
Access controls	"Red Flag" validation of medical claims submitted	Health record corrections
Other security controls	Information sharing environments	Ongoing assessment

[1] No particular control or standard within each of these categories is endorsed by the ONC or Booz Allen

For More Information….

Kris O'Neal
Associate

Booz | Allen | Hamilton

Booz Allen Hamilton Inc.
8283 Greensboro Drive
McLean, VA 22102
Tel 703.377.1257
o'neal_kris@bah.com

Dan Steinberg
Associate

Booz | Allen | Hamilton

Booz Allen Hamilton Inc.
8283 Greensboro Drive
McLean, VA 22102
Tel 703.377.1261
steinberg_daniel@bah.com