Privacy – Its All the Rage

An Overview of a Privacy Implementation Model

March 12, 2007

Donna Ebling and Carmalita Morgan

Agenda

- Collaboration Activity
- Introduction
- Legislation
- Implementation
- Privacy Model
- Case Study
- Summary

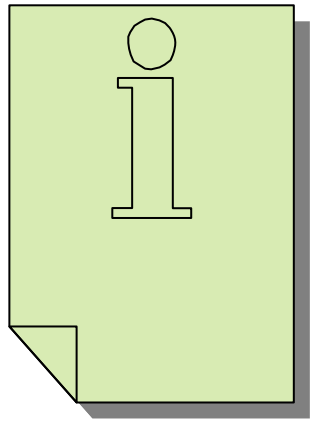
Collaboration Activity

Introduction

- Privacy
  - New buzz word or cause
- Privacy defined
  - In Webster's: "freedom from unauthorized intrusion"
  - Using a variety of security controls (management, operational, technical) to protect the public's information in identifiable form that an organization may collect, store, transmit, or use;
- Encompasses many areas or disciplines
  - Personal
  - Health/Medical
  - Financial
  - Business (proprietary)

What is Personally Identifiable Information (PII)?

- Data that identifies or can be used to identify, contact, or locate the person to whom such information pertains
- Examples:
  - Name, social security number, driver's license number, e-mail address, phone number, date of birth, home address, personal financial records, username/password
  - Exceptions granted for "life or death," research, and law enforcement situations



Security Concerns Addressed via Training Programs

- Training is the critical component for ensuring the security of our systems and information
- A critical security concern is the ability of agency personnel to protect information
- Requires an on-going effort in order to meet the ever changing challenges of those determined to obtain unauthorized access of that information
- Agency technology and education must keep pace with the these new challenges
- Important to understand the current status of a security program and its controls to make informed judgments and investments to mitigate risks to an acceptable level
- Personnel must be aware of their responsibilities for protecting systems and information

Approach to Meeting Security Challenges

- Process driven methodologies, proven best practices, and experienced personnel

Legislation

Privacy Regulations

Why Legislation?

- Promotes fair information practices
- Dictates that agencies must keep private information private
- May address implementation
- Protects personal information of individuals
- Allows individuals a choice in how their information is used
- Protects individuals from harm that might be imposed upon them if certain information were to be released without their consent

Legislation Helps to …

- Ensure that an individual's personal information is accurate, secure, and current and that individuals know about the uses of their data
- Ensure compliance
- Protect against data breaches
- Ensure:
  - All information is only used for the purpose for which the information was obtained
  - When performing daily job related activities, individuals to not have access to information they do not need

Privacy Legislations (not inclusive)

- ***Privacy Act***: provides guidance for collecting, using, managing, and disclosing PII; prohibits disclosure of PII without the individual's written consent (12 exceptions including: need to know within an agency, statistical data, and routine use)
- ***Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule:*** restricts use and disclosures of personal health information and grants individuals access to records
- ***E-Government Act 2002, Title II and III***: requires federal agencies to assess impact of privacy for systems that collect information about members of the public
- ***Children's Online Privacy Protection Act (COPPA):*** requires parental consent for certain websites who knowingly collect PII on children under 13
- ***Agency Guidance***: regulatory agencies provide guidance to implement privacy legislation (OMBM-06-1, OMB M-06-16, OMB M-06-19)

More Privacy Legislations (not inclusive)

- ***Graham-Leach Bliley Act***: requires U.S. financial institutions to establish safeguards to ensure confidentiality and integrity of customer records and information
- ***Office of Management and Budget (OMB) M-06-19:*** memorandum that sets guidelines for reporting security incidents involving PII
- ***OMB M-10-15***: memorandum that emphasizes roles and responsibilities of departments and agencies in safeguarding PII as outlined in the Privacy Act
- ***OMB M-06-16:*** memorandum issued to Heads of Departments and Agencies outlining a checklist for protecting sensitive agency information
- ***OMB M-03-22***: memorandum that provides guidance to agencies in implementing the privacy provision of the E-Government Act of 2002

Implementation

Implementing Privacy Within an Agency - Assumptions

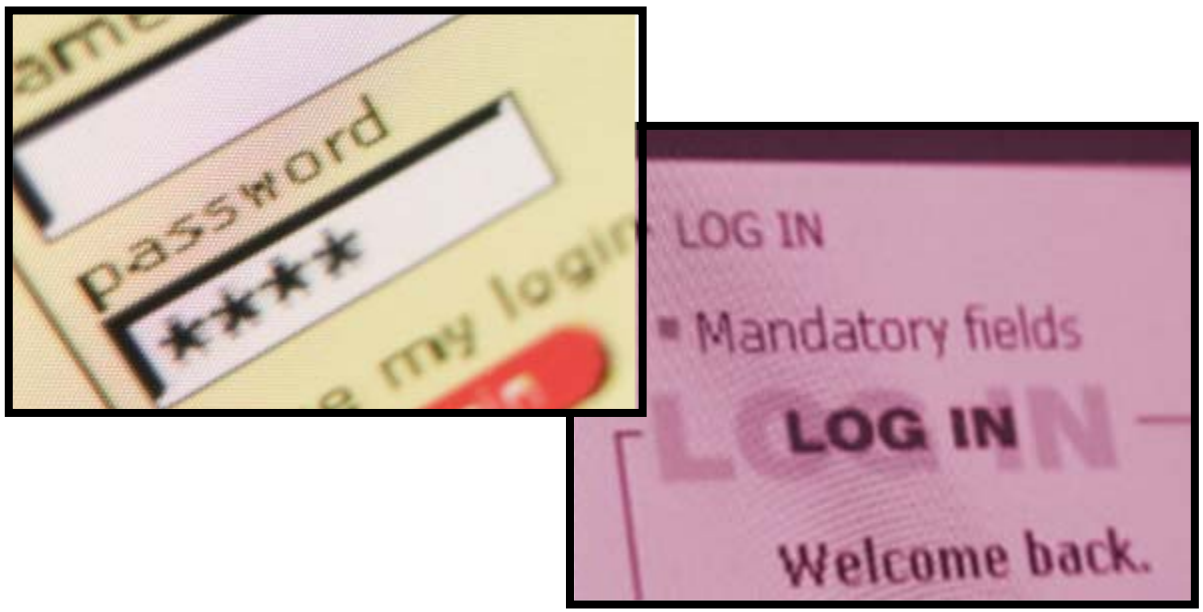
- A critical security concern is the ability of agency personnel to protect information
- Agency technology and education must keep pace with the these new challenges
- Requires an on-going effort in order to meet the ever changing challenges of those determined to obtain unauthorized access of that information
- Important to understand the current status of a security program and its controls to make informed judgments and investments to mitigate risks to an acceptable level
- Training is the critical component for ensuring the security of our systems and information
  - Personnel must be aware of their responsibilities for protecting systems and information

Implementing Privacy – Practices

- A Privacy Impact Assessment (PIA) is an analysis of how identifiable information is handled and privacy associated with information systems
  - Demonstrates that system owners and developers have consciously incorporated privacy protections throughout the entire life cycle of a system
  - Involves making certain that privacy protections are built into the system from the start, not after the fact when they can be far more costly or could affect the viability of the project
  - Other practices include: shredding, using strong passwords, and ensuring office equipment has security features that are enabled and current

Implementing Privacy –Technologies

- Spyware detection applications
- Intrusion Detection
- Anti-virus software
- Encryption
- Firewalls
- Authentication
- Authorization



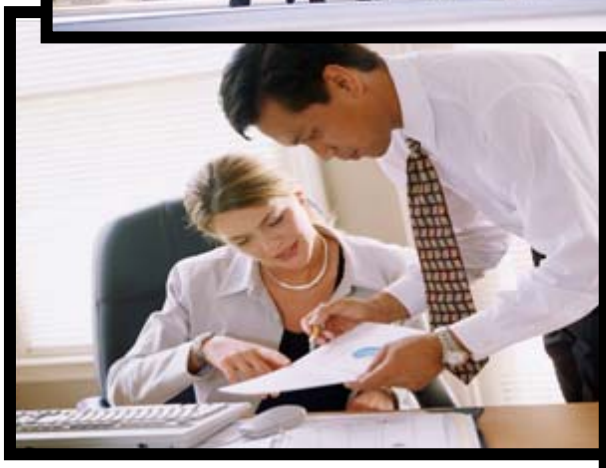
Implementing Privacy – What Else is Needed?

- Education, best practices, and technologies are not enough…..
- An implementation model that encompasses all the essential elements is required if the implementation is to be effective and successful

Privacy Model

Culture of the Client

Technical Cyber Security Knowledge and Expertise



Instructional Systems Design Skills

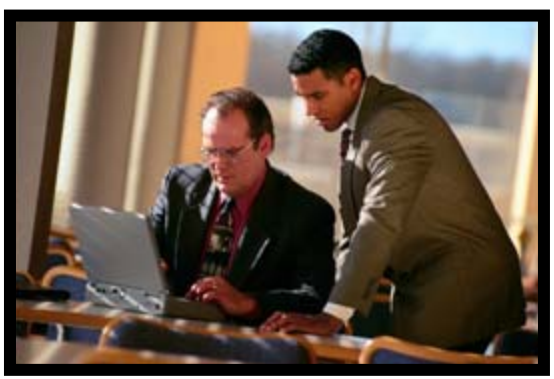
Communication and Collaboration with the Client

Culture of the Client

- Understand your client's mission and goals
- Know your target audience – be able to define the right implementations for the right people
- Bridge the gaps between the client environment and the required regulatory environment
- Know the client strengths and weaknesses for their various processes
- Understand the chain of command
- Understand the implications involved if your client's processes are centralized or decentralized

Technical Cyber Security Knowledge and Expertise

- Ensure members of your team are experienced, certified professionals who are knowledgeable and experienced in IT security and privacy
- Ensure that members of your team understand and can address both security and privacy issues
- Employ team members who are familiar with privacy best practices, privacy directives, and legislative requirements
- Design and develop programs and training materials and procedures to promote safe secure protection of agency information



Instructional Systems Design and Skills

- Apply ISD Process
  - Step 1 – Analysis
  - Step 2 – Design
  - Step 3 – Develop
  - Step 4 – Implement
  - Step 5 – Evaluation and maintenance

- Information assurance and instructional systems design provides a standardized process critical to successful training programs and ensures a best practices approach with an emphasis on quality

Communication and Collaboration with the Client

- Schedule regular meetings with the privacy implementation team and the client
- Complete weekly and monthly status reports for the client
- Do not hesitate to ask the client's thoughts on any ideas or concerns; always treat them with respect
- Ensure that all stakeholders for the client have an active role in periodic and final reviews
- Ask the client's stakeholders to state their expectations for the outcome and/or use of the product
- Ask the client's stakeholders to voice any concerns and ideas at the beginning of the project

Case Study

Case Study

- Client: extremely large civil agency that needed to do “damage control” after security breaches in the privacy arena were uncovered
- Mission: Damage control for security breaches in the privacy arena
- Goals:
  - Establish program that informed employees how to protect, use, store, and maintain private information
  - Avoid further breaches
  - Ensure compliance with privacy dictated federal regulations
  - Restore reputation and public’s trust

Case Study

- Client Team: consisted of the agency's Chief Security Officer and his staff, the stakeholders which included various members of the client's Training and Privacy teams

- Our Team: consisted of sub-teams with various areas of expertise: technologies and architectures, security controls, governance, training, communications, privacy, and program management (oversee the project and interact on a daily basis with the client)

- The Campaign: promote a privacy awareness campaign to all members of the agency; to inform about the importance of privacy and the use of agency established procedures, the duty of the agency to the members of the public, and the importance of compliance with federal regulations

Case Study

- The Method: while in constant contact with the client's team we re-established the importance of established procedures and created new ones, developed training materials and seminars, instituted a systematic approach to noting which systems contained PII and if their security controls were adequate

- The Products – consisted of Privacy guides, tutorials for entering privacy system information into the database, Privacy Awareness course (mandatory for all agency employees), Protecting Private Information tri-fold (made available to all agency employees), Privacy Implementation Plan, and Privacy role-based training courses
  - All were customized to ensure they reflect the agency's culture

- The Results – informed agency employees regarding Privacy, better protections of private information and information systems, and beginnings of regaining their reputation and ensuring public trust,

Case Study - Summary

- The Moral: Using all of the components of the Privacy Implementation model (Client Culture, Technical Cyber Security Knowledge and Expertise, Instructional Systems Design Skills, and Communication and Collaboration with the Client) allowed to act as a team with the client and to ensure that our solution and products reflected the agency's culture. The agency was more likely to heed our recommendations as we always kept them informed and respected their opinions and ideas. This project was truly a team effort.

Questions and Answers?

Q & A

Thank You For Attending our Presentation

Donna Ebling

Booz Allen Hamilton

(703) 377-6714

ebling_donna@bah.com

Carmalita Morgan

Booz Allen Hamilton

(703) 377-6878

morgan_carmalita@bah.com