Privacy and Security: A Strategic Direction

ATIC
September 18, 2008

Mary Beth Joublanc

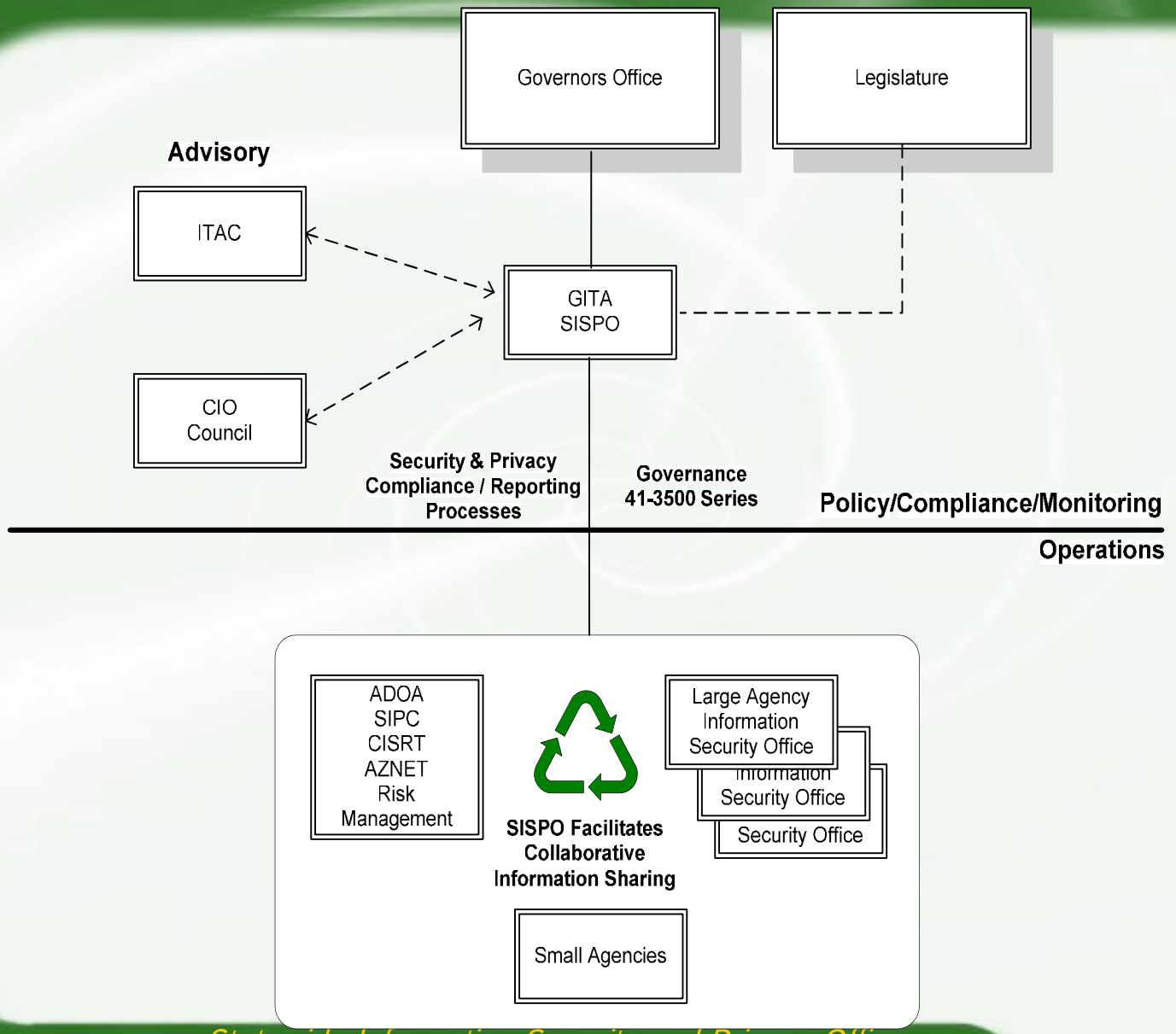
www.azgita.gov/sispo

Privacy is the goal
Security is the journey
Technology can help
People are the key

Agenda

- What is “SISPO”?? (animal, vegetable or mineral)
- Navigating the Privacy Maze
- Strategies for Privacy and Information Security in the 21st Century

SISPO Organizational Framework



A.R.S. 41-3501 et. seq.

GITA's Roles and Responsibilities

- Strategic oversight of State IT infrastructure
- Establish Statewide IT Policies & Standards
  - Develop / Monitor compliance
  - Includes Information Security & Privacy
- Statewide Coordinator IT projects
- Evaluate Agency IT Plans
- Develop & Implement a Statewide IT Plan
- Inventory IT Assets of the State
- Oversight of Agency IT Projects ($25k - $1M+)
  - Project Investment Justification (PIJ)
  - Approve / Disapprove / Suspend
  - Information Technology Authorization Committee (ITAC)
    - If project is $1M or more, ITAC must approve

SISPO Team

- Chief Information Security Officer and Manager:
  - David VanderNaalt
- Chief Privacy Officer:
  - Mary Beth Joublanc
- Manager Awareness & Training:
  - James Dzierzanowski
- GITA Manager IT Homeland Security:
  - Jim Ryan

A.R.S. 41-3507

41-3507. Statewide information security and privacy office; duties; suspension of budget unit's information infrastructure

A. The statewide information security and privacy office is established in the government information technology agency. The statewide information security and privacy office shall serve as the strategic planning, facilitation and coordination office for information technology security in this state. Individual budget units shall continue to maintain operational responsibility for information technology security.

B. The director shall appoint a statewide chief information security officer to manage the statewide information security and privacy office. The statewide chief information security officer shall report to the director pursuant to section 41-3503.

C. The statewide information security and privacy office shall develop, implement, maintain and ensure compliance by each budget unit with a coordinated statewide assurance plan for information security and privacy. The statewide information security and privacy office shall:

1. Direct information security and privacy protection compliance reviews with each budget unit to ensure compliance with standards and effectiveness of security assurance plans as necessary.

2. Identify information security and privacy protection risks in each budget unit and direct agencies to adopt risk mitigation strategies, methods and procedures to lessen these risks.

3. Monitor and report compliance of each budget unit with state information security and privacy protection policies, standards and procedures.

4. Coordinate statewide information security and privacy protection awareness and training programs.

5. Develop other strategies as necessary to protect this state's information technology infrastructure and the data that is stored on or transmitted by such infrastructure.

D. The statewide information security and privacy office may temporarily suspend operation of information infrastructure that is owned, leased, outsourced or shared in order to isolate the source of, or stop the spread of, an information security breach or other similar incident. A budget unit shall comply with directives to temporarily discontinue or suspend operations of information infrastructure.

E. Each budget unit and its contractors shall identify and report security incidents to the statewide information security and privacy office immediately on discovery and deploy mitigation strategies as directed.

A.R.S. 41-3507

SISPO's Roles and Responsibilities

- Strategic planning & coordination
- Individual budget units continue operations
- Compliance plan for InfoSec & Privacy
  - ➢ Temporarily suspend information infrastructure
  - ➢ Agency required to report incidents
    - Coordinate
    - Review
    - Mitigation
- Training & Awareness Program
  - Web based e-Learning
  - Leverage programs already in place

Executive Order (EO) 2008-10

- Signed January 14, 2008
  - All State Executive Branch agencies
  - Expectation: others comply→ best practice

- Goals:
  - Prevention of loss
  - Protect citizen and other state held or controlled information

EO 2008-10

Each Agency shall:

1. Appoint Agency ISO = Technology
2. Appoint Agency PO = Business (note option)
3. Work with SISPO to develop protections
   - Digital
   - Paper
4. Deploy encryption
   - RFP completed (HB 2785 Section 23)
     - GITA Notice of Intent (NOI)
5. Telecommute procedures
   - Proper physical & logical security

EO 2008-10

6. Redaction procedure
7. Report all incidents (S855)
   - Any information loss or misuse
   - Any technology infrastructure attack
8. Data breach notification procedure (ARS 44-7501)
9. Physical security
10. Training & Awareness programs
    - Privacy
    - Information Security

SISPO Activities

- Developing employee certifications
  - AZ Certified InfoSec Practitioner
  - AZ Certified Privacy Practitioner
- Developing online incident reporting
  - framework / tree / system
  - provide metrics – dashboard view
- Health-e Connections
  - Privacy sub-committee
  - Security sub-committee
- Developing Privacy Assessment
  - Annual & year over year trend reporting
- Statewide Risk Assessment

SISPO Activities

- Review Incidents
  - Direct and coordinate
  - Internal controls & procedures
- Fulfill the Mandate of Executive Order 2008-10
  - Monitor compliance
- Update Cyber Terrorism response plan
    - AZ Incident Response (planning)
- Update Incident Reporting Procedures
- Policy & Standards
  - Review/update & formulate new
- TISA (Technology Infrastructure & Security Assessment)
  - Annual & year over year trend reporting
- Project Investment Justification (PIJ)
  - Update: Security / Privacy / Recovery

Partnerships

- Executive Agencies' Privacy and Information Security Officers (95+)
  - Arizona Department of Administration
- Legislative, Judicial Branch Agencies
- Universities
- Attorney General's Office
- AzNet
- Other Business Partners (e.g., Councils)

Current Projects

- Automated Incident Reporting, Response and Mitigation System
  - (IT-GRC)
- Privacy Framework and Assessment
- Compliance Infrastructure
- ID Theft Coordination and Resources
- Administrative Rule Development
- Web Resource Page:
  http://www.azgita.gov/sispo/

Navigating the Privacy Maze


PSSST!
PRIVACY
CONFERENCE.

Arizona Legislation

- AZ Health Information laws and the federal Health Insurance Portability and Accountability Act (HIPAA) (ARS 12-2291 to 12-2297; 45 CFR 160, 162, 164)
- Social Security Number Protection (ARS 44-1373 to 1373.03)
- Breach Notification Law (ARS 44-7501)
- Data Destruction (ARS 44-7601)
- Computer Tampering, Access, Security (ARS 13-2316 to 13-2316.02)
- Definitions of Personally Identifiable Information (ARS 13-2001 and above)

Health Information and HIPAA

- Arizona Medical Record Statute
  - ARS 12-2291 to 12-2297
  - Defines confidential information; third party and legal disclosure; retention

- Health Insurance Portability and Accountability Act (42 CFR 160, 162, 164)
  - Defines "protected health information," uses & disclosures; privacy rights
  - Electronic transactions
  - Information security regulations

Federal Waters are Deep!

- Privacy Act
- Gramm, Leach, Bliley Act
- Sarbanes Oxley Act
- Federal Information Security Management Act
- Family Education Rights Privacy Act
- More on the way….

Social Security Number
A.R.S. 44-1373

- A person or entity SHALL NOT:
  - Intentionally communicate an individual's SSN to the general public
  - Print a SSN on a card to receive products or services
  - Require use of a SSN on the Internet unless encrypted or transmission secure
  - Require a SSN to access an Internet web site unless other authentication means used
  - Print a SSN on a mailed materials unless state or federal law requires
- Civil penalties

Breach Notification Law
A.R.S. 44-7501

- Conduct business in AZ using unencrypted
  - personal information
  - unauthorized access or breach occurs
  - shall **notify** the individuals affected
- Personal data includes any combination:
  - Individual's name
  - Social Security number
  - Individual's driver license number
  - Credit or debit card number
    - security code
- Civil penalties

Data Destruction
A.R.S. 44-7601

- An entity shall not knowingly dispose of records w/o redacting or destroy documents containing first name or initial and last name in combination with:
  - SSN
  - Credit Card/Charge or Debit
  - Retirement
  - Checking, Savings or Securities
  - Driver License
- Civil penalty applies

Computer Tampering
A.R.S. 13-2316.02

- A person who acts w/o authority or exceeds authorization to commit computer tampering:
  - Access, Alter, Damage, Destroy, Defraud
  - Introduce Computer Contaminant into Computer or Network
  - Cause a Person to Suffer Emotional Distress
  - Obtain Confidential Records Operated by State, Political Subdivision or Medical Institution
  - Tamper with Critical Infrastructure
  - Use a Computer or Network in an Offense
  - Unlawful Possession of an Access Device
- Criminal penalties –
  - Class 6 felony release of proprietary
  - Class 4 felony if critical infrastructure

Personally Identifiable Information
A.R.S. 13-2001

- Means any written document or electronic data that provides information concerning:
  - Name
  - Signature
  - Electronic Identifier or Screen Name
  - Electronic Mail Signature
  - Biometric Identifier
  - Driver License Number
  - SSN, Tax ID
  - Employment, Citizenship Info/Status, Photo, DOB, Fingerprint, Retina Image, Photo, DNA…
  - Credit/Debit Card Info.

University of Colorado-Boulder, Leeds School of Business

Virginia Commonwealth University

University of Michigan

UCLA

University of Idaho

Rutgers-Newark University

Northwestern University

Loyola University

Yale University

University of Iowa – Psychology Dept.

Villanova University students & staff

Via Insurance broker

Purdue University

Mississippi State University

University of Missouri

Berry College

via consultant Financial Aid Services Inc.

Georgia Tech Univ.

Louisiana State Univ

Ohio State Univ.

University of Minnesota

University of South Carolina

Johns Hopkins University

Montana State University

Notre Dame University

University of Texas at Arlington

Texas A&M University

University of California, Davis

University of Virginia

University of Texas - Dallas

New Mexico State Univ.

University of Nebraska

Connors State College

University of Toledo

Texas Woman's University

Georgia Institute of Technology

University of New Mexico

Eastern Illinois University

Radford University

Westminster College

De Anza College

Univ. of Montana - Western

City College of San Francisco

UC San Francisco

Black Hills State Univ.

Cal State Los Angeles

Nassau Community College

Metropolitan State College of Denver

Central Connecticut State University

Montgomery College

Bowling Green State University

Adams State College

Los Rios Community College

Goshen College

Stony Brook University

Community College of Southern Nevada

Highlands University

Penn State Univ. - USMC

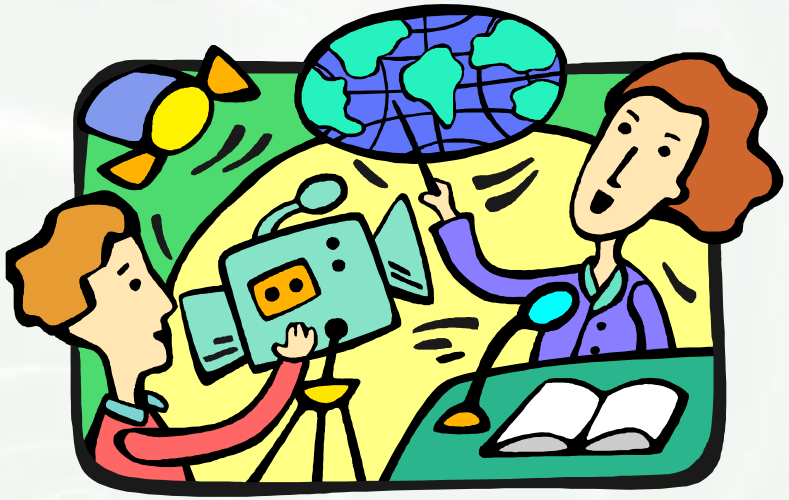
Carolina University

Vanguard University

Gadsden State Community College

Grand Valley State University

MEDIA HYPE OR A REAL PROBLEM?



DATA BREACH

Some of the reported incidents that occurred in 2007…

Dr. Marilyn Prosch

ASU School of Global Management & Leadership
ARIZONA STATE UNIVERSITY

FEDERAL TRADE COMMISSION

- Arizona is #1 in Identity Theft….not where we want to be!
- Has settled 14 cases "challenging **faulty data-security practices** by companies that handle sensitive consumer information."
- They almost always require a **security audit every 2 years for the next 10-20 years**.

Uncertainty of Data Breach Detection

Ponemon Institute & Compuware

- 75% breach caused *negligent* insider
- 26% breach by *malicious* hacker
- PrivRigthClr → 225,786,657 records
- Cost of data breach = $197 per record
  - Nov 2007 – 3rd annual report

Example

http://thedailywtf.com/Articles/Oklahoma-Leaks-Tens-of-Thousands-of-Social-Security-Numbers,-Other-Sensitive-Data.aspx

- Oklahoma → Department of Corrections
  - Public facing web site
  - Sexual & Violent Offender Registry (SVOR)
    - ✓Federally mandated registry
    - ✓Publically available
  - Poor coding & even poorer QA
    - ✓Displayed every type of offender
    - ✓Displayed SSN
- 💣UP FOR 3 Years

Uncertainty of Data Breach Detection

Ponemon Institute & Compuware

- Recommendations:
  - Establish data breach governance
  - Process to determine scope of breach
  - Investigative & forensics tools
  - Determine root cause of breach
  - Include portable devices in security
  - Tools to detect

Information Security….

And

The 21st Century

Critical priorities and steps

Priority	Recommendation
1	**Data Inventory & Classification** *Figure out where the important date lives. Start there*
2	**Encryption** *Pick what works best for your business, critical data first*
3	**Awareness & Training** *For travelers/remote workers, critical data handlers & everyone else*
4	**Process, Process, Process** *Helpdesk authentication, termination process, contractor lifecycle*
5	**Segmentation & Separation of Duties** *Networks & employees– don't let the fox (or the hens!) watch the henhouse*
6	**Know Thy Perimeter** *Wireless audits & overall vulnerability management prevent "easy" hacks*
7	**Develop Secure Applications** *Cheapest and best means of protecting applications is to develop them securely*
8	**New Technical Solutions** *Cisco Security Agent sits on the host and blocks all anomalous behavior*

Critical Partnerships

- Develop relationships
  - Information Security
  - Privacy Office
  - General Counsel
  - Corporate Compliance
  - Procurement
  - Risk Management
  - Audit
  - Physical Security
  - Law enforcement
  - Chief Operating Officer
  - Marketing – information broker
  - Leader Technology

Your Privacy Plan

- Executive Management Actively Involved
- Customers and Personnel Information
- Electronic, Paper and Other Media
- Don't shelve policies and procedures– update them!
- Awareness training and updates for all employees—even executives
- Have a Retention Program (electronic, paper and other media)

Your Privacy Plan

- Develop a report of concern process
  - Non-punitive
  - Protect the identify of those reporting
  - Policies and practices are the same—no retaliation for those who report
  - Take reports seriously
  - Termination interviews—follow-up on concerns expressed

Your Privacy Plan

- Investigation
  - What information is missing (reconstruct)
  - How long?
  - Where from?
  - Who had access?
  - Must be prompt investigation
  - Notify risk management, legal counsel, executive management and if a state agency, SISPO
  - Lessons learned and remediation

Your Privacy Plan

- Contracts
  - Vendors use (prohibit research??)
  - Purchase Orders—be cautious!
  - Scope of Work (be specific with data, access and responsibilities)
  - Non-disclosure Agreements
  - Data breach notification—who's responsible to notify and pay for costs
  - Agency retains right to any part of investigation conducted by contractor

Your Privacy Plan

- Digitizing records and plan for use
  - Are these records being uploaded to web sites???
  - Have they been classified for purposes of the Arizona Public Records Act??
  - Is redaction permanent or vulnerable to recovery?
  - What's your retention plan?
  - E-discovery—include in your plan and policies.

E-Discovery Considerations

- Arizona Rules of Procedure Adopted:

- ✓ Duty to preserve and produce electronically stored information for pending or actual litigation

- ✓ Emails must be preserved
  - ✓ Plan to classify and retain

- ✓ Webmail/Virtual Office Capabilities

Information Security and Privacy

- Websites and Data Collection
- Contracts/Purchase Orders/Non-Disclosure Agreements/Subs
- Acceptable Use Policy and Updates
- Role-based Access (vendors, too) and Timely Network Termination Process
- Digitizing records and Plan for Use

Your Privacy Plan

- Personnel Records
  - What are supervisors keeping at desks—personal/medical information??
  - Special training for HR folks
  - HIPAA coverage
    - Generally not applied to employers (Preamble, December 28, 2000, Rules and Regulations, at 82485)
    - Will apply to records needed for work determinations
    - Will apply to sponsored and self-insured benefit plans
    - Don't use for employment decisions!!!

Your Privacy Plan

- Foster a Privacy Culture
  - Recognize who handles the information
    - Entry level personnel are critical
    - Important to engage in the program
    - Temps (special issues can arise)
  - Role based access and minimum necessary principles
  - Disclosure of information—is all personal information needed or only portions?
  - Have redaction training and procedures

Your Privacy Plan

- Culture of Privacy--Employees
  - Continued Awareness
    - Training on Hire and Annually
    - Special training for certain areas
    - Confidentiality and Non-disclosure statements
    - Employee evaluations
    - Supervisors accountable
    - Awards and contests for ideas

Remember

Privacy is the GOAL

Security is the journey

Technology can help

People are the key

Contact

Mary Beth Joublanc, JD

Chief Privacy Officer

State of Arizona

Statewide Information Security & Privacy Office

http://azgita.gov/sispo/

Government Information Technology Agency

100 N. 15th Ave. Suite 440

Phoenix, Arizona 85007

602.364-4537

mbjoublanc@azgita.gov

Contact

David VanderNaalt

Chief Information Security Officer and Manager

State of Arizona

Statewide Information Security & Privacy Office

http://azgita.gov/sispo/

Government Information Technology Agency

100 N. 15th Ave. Suite 440

Phoenix, Arizona 85007

602-364-0535

dvandernaalt@azgita.gov