

# Security and Privacy Strategic Direction

May 28, 2008

Mary Beth Joubanc

[www.azgita.gov/sispo](http://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 Information Security in the 21<sup>st</sup> Century
- The Security/Privacy Partnership



# 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



# 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



# EO 2008-10

- EO covers
  - All State Executive Branch agencies
  - Expectation: others comply → best practice
  
- January 14, 2008
  
- WHEREAS;
  - Prevention cheaper than mitigation
  - Protect citizen 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

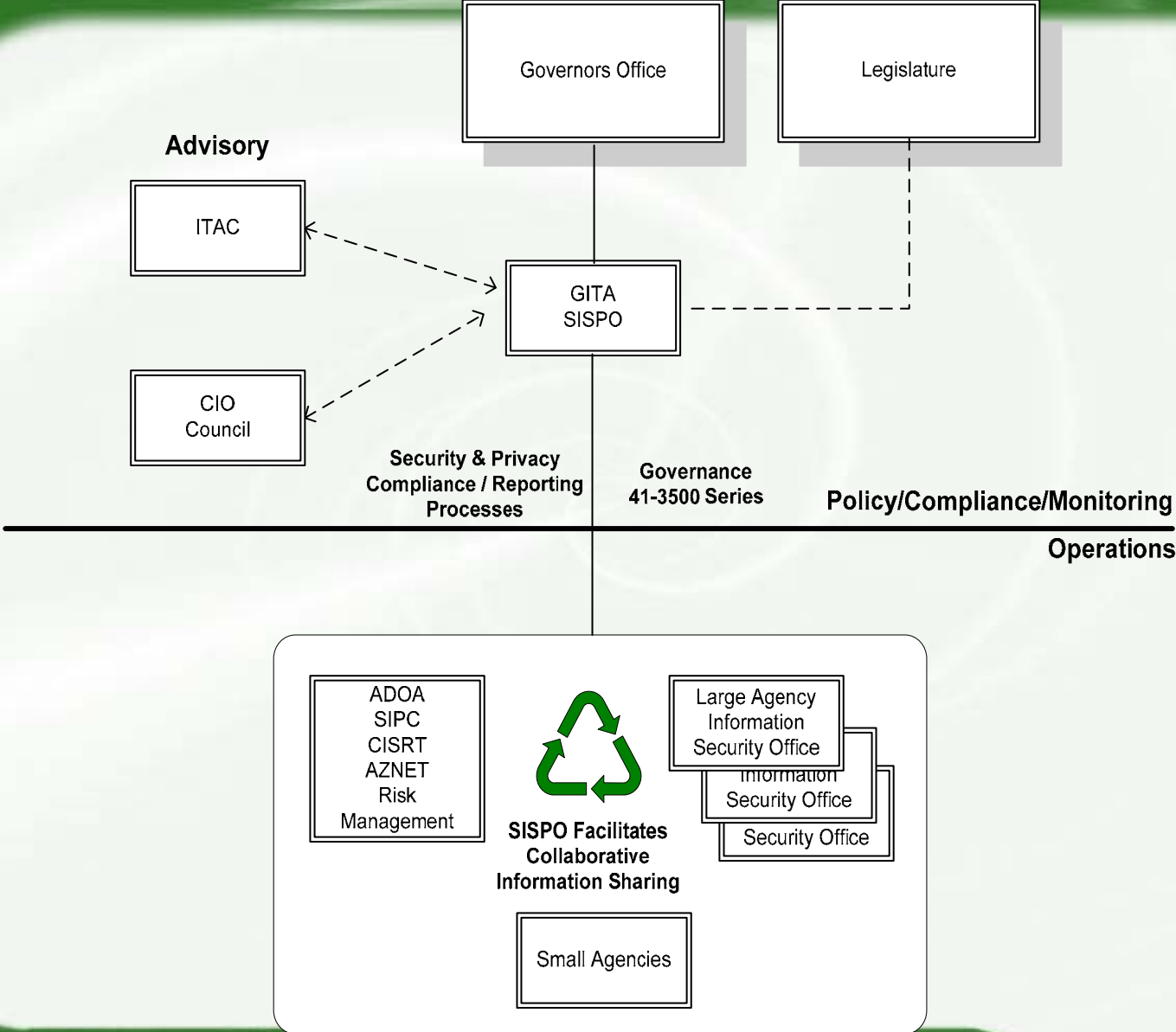


# EO 2008-10

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 Organizational Framework



# David VanderNaalt – BIO Highlights

- Arizona's Chief Information Security Officer
  - Governor announced appointment Sept. 05, 2007
  - Appointed September 17, 2007
    - Head Statewide Information Security & Privacy Office
- NYC Dept. of Investigation 1999-2007
  - Director Citywide Information Security (CISO)
  - Director Digital Crimes Investigation Unit
  - Director Citywide Continuance Planning (OEM)
  - Yes → 09-11-01
- American Express, World Wide 1985-1996
  - Corporate Information Security Officer (1989)
    - *Ponemon Institute; Distinguished Fellow*
    - *Certified Information Security Manager*



# Mary Beth Joubanc – BIO Highlights

- Arizona's Chief Privacy Officer
  - Appointed January 15, 2007
  - Licensed AZ Attorney & member of AZ State Bar
  
- Chief Health Insurance Portability and Accountability Act (HIPAA) Compliance Officer (ADHS)
  - Created HIPAA Privacy and Security compliance program
  - Member of the Statewide HIPAAZ Workgroup
  - Chairperson Human Subjects Research Review Board
  
- Appointee to National Academy of Science, Institute of Medicine Committee on HIPAA and Research



# SISPO Team

- Chief Information Security Officer (SISPO)
- Chief Privacy Officer (SISPO)
- Manager Awareness & Training (SISPO)
- Manager IT Homeland Security (GITA)
- Agency POs & ISOs (Approximately 120 agencies)
  
- Future
  - Compliance Reviews
  - Vulnerability and Threat Assessments
  - Incident Response Coordination
  - COOP Consulting (EPOC / State COOP / Tech DRP)



# 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



# 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 Relationships

## ❖ Ongoing Interactions

- Governor's Cabinet
- Agency executives
- Agency CIOs
- Agency CISOs
- Agency CPOs
- Legislators
- Committees
- Other branches of AZ Gov't
- Other state CISOs & CPOs

## ❖ Communicate

- G1 Deputy Directors
- G2 Directors
- Agency CIOs
- Agency POs
- Agency ISOs

## ❖ Universities

## ❖ Key Industry Groups

## ❖ Leading Companies



# Identity theft prevention

- ↪ SISPO is focused on information protection
- ↪ Creating a state level workgroup
  - ① Law enforcement
  - ① Attorney General Office
  
  - ② Privacy Officers
  
  - ③ Private companies
  - ③ Service providers
- ↪ New web page for ID Theft resources



# Navigating the Privacy Maze



# 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.



# 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



# Privacy IS Good Business!

- Trust = Good Government Business
- Privacy culture empowers employees and reduces turnover
  - Respect
  - Participation
- Privacy Plan is integrated with business strategies and operations



# 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

- 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



# 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

- 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

## ➤ 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.



# 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



# Information Security....

## And

# The 21<sup>st</sup> Century



# 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.**



Univ. of Pittsburgh, Med. Center

Manhattan Veteran's Affairs Medical Center & New York Harbor Health Care System

Beaumont Hospital

*Sisters of St. Francis Health Services via Advanced Receivables Strategy*

Swedish Medical Center

Univ. Calif. Irvine Medical Center

Group Health Cooperative Health Care System

Mercy Medical Center

DCH Health Systems

Johns Hopkins Hospital

Beacon Medical Services

Allina Hospitals and Clinics

Prudential Financial Inc.

Seton Healthcare Network

University of Pittsburgh Medical Center

DePaul Medical Center

McAlester Clinic

Kaiser Medical Center

& Veteran's Affairs Medical Center

Highland Hospital

Akron Children's Hospital

Cleveland Clinic

Back and Joint Institute of Texas

Gulf Coast Medical Center

*Emory University Hospital, Emory Crawford Long Hospital, Grady Memorial Hospital, Geisinger Health System, Williamson Medical Center*

Jacobs Neurological Institute

Erlanger Health System

*via Electronic Registry Systems*

Deaconess Hospital

Westerly Hospital

Health Resources, Inc.

WellPoint's Anthem Blue Cross Blue Shield

Kaiser Permanente Colorado

South County Hospital

Providence Alaska Medical Center

Gundersen Lutheran Medical Center

Swedish Urology Group

Intermountain Health Care

St. Mary's Hospital, MD

Concord Hospital

Stevens Hospital

WorkCare Orem

*via billing company Med Data*

Wellpoint's Empire Blue Cross/Blue Shield NY

*Sky Lakes Medical Center via Verus Inc*

*Segal Group of New York*

St. Vincent Hospital


*via web site of Vermont state agency*

Healing Hands Chiropractic

*Statewide Information Security and Privacy Office*

Georgia Dept. of Community Health

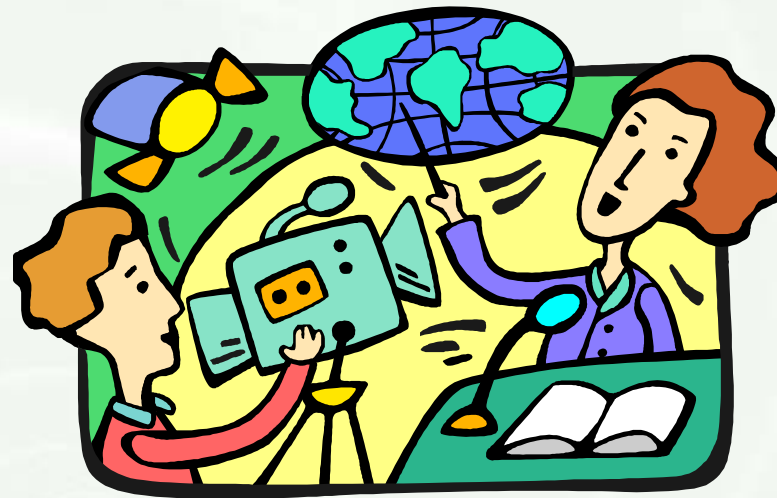


Cuyahoga County Dept. of Development	Los Angeles County Child Support Services	Chicago Board of Elections
Tuscarawas County and Warren County	Fresno County	Chicago Voter Database City of Chicago via contractor Detroit Water and Sewerage Department
Orange County (FL) Controller	Champaign Police Officers	City of Savannah
Santa Clara County Employment Agency	Huntsville County Hidalgo County Commissioner's Office	Bowling Green Police Dept. Lynchburg City Port of Seattle
Washiawa Women, Infants and Children program (HI)	ChildNet Pima Co. Health Dept.	Fort Monroe City of Encinitas Metropolitan St. Louis Sewer District
Fresno County/Refined Technologies Inc.	Johnston County, NC	City of Visalia, CA Cleveland Air Route Traffic Control Center
<i>Berks Co. Sheriff's Office via contractor Canon Technology Solutions</i>	Cumberland County, PA	New York City Financial Information Services Agency City of Lubbock
		City of Wickliffe, OH City of Grand Prairie Poulsbo Department of Licensing
Indianapolis Public Schools	Harrison County Schools	Chicago Public Schools via All Printing & Graphics, Inc.
Jackson Local Schools	Waco Independent School District	Willamette Educational Service District
San Diego Unified School District	Chicago Public Schools	Greenville County School District
Shamokin Area School District	Clarksville-Montgomery County Middle and High Schools	Germanton Elementary School Riverside High School NC
Cedarburg High School	St. Mary Parish	Big Foot High School, WI
San Juan Capistrano Unified School District (CA)	Iowa Dept. of Education	Troy Athens High School
Leominster Chaffee School	Yuma Elementary School District	Clay High School, OH
	St. Vrain Valley School District (CO)	39

University of Colorado-Boulder, Virginia Commonwealth University University of Michigan  
 Leeds School of Business  
 UCLA University of Idaho Rutgers-Newark University Northwestern University  
 Loyola University Yale University University of Iowa – Psychology Dept.  
*Villanova University students & staff* Purdue University Mississippi State University  
*Via Insurance broker* University of Missouri Louisiana State Univ Ohio State Univ.  
*Berry College* Georgia Tech Univ. University of Minnesota University of South Carolina  
*via consultant Financial Aid Services Inc.* Johns Hopkins University Notre Dame University  
 Montana State University Texas A&M University University of California, Davis  
 University of Texas at Arlington University of Texas - Dallas New Mexico State Univ.  
 University of Virginia University of Toledo Connors State College  
 University of Nebraska Georgia Institute of Technology University of New Mexico  
 Texas Woman's University Eastern Illinois University Radford University Westminster College  
 Eastern Illinois University De Anza College City College of San Francisco  
 Univ. of Montana - Western Black Hills State Univ. UC San Francisco  
 Cal State Los Angeles Nassau Community College Metropolitan State College of Denver  
 Bowling Green State University Montgomery College Central Connecticut State University  
 Adams State College Stony Brook University Los Rios Community College Goshen College  
 Community College of Southern Nevada Highlands University Penn State Univ. - USMC  
 Carolina University Gadsden State Community College Vanguard University  
 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



# 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 – 3<sup>rd</sup> annual report



# 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



# Critical priorities and steps

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



# The Information Security and Privacy Partnership:

- » Reduces duplicate effort
- » Builds trust
- » Sustains the organization



# 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



# 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



# Partner InfoSec with Privacy

- Define Policy & Standards
- Awareness Program
- Lock up laptops (not trunk / back seat)
  - Specific procedure for handling information in transit
- Gather metrics
  - Assessment
  - Compliance
- Information Inventory
- Retention network, databases, back-ups
- Encrypt, Encrypt, Encrypt!
- Secure paper documents



# 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



# Future Asset Protection

## Asset protection – Senior Executive

- Privacy
- Information Security
- Technology Infrastructure protection
- Physical security
- Risk Management
- Legal compliance  
(local/state/federal/international)
- External investigation
- Internal investigation



# Remember

**Privacy is the GOAL**

**Security is the journey**

**Technology can help**

**People are the key**



# Contact

**Mary Beth Joubanc, 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

[mbjoubanc@azgita.gov](mailto:mbjoubanc@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](mailto:dvandernaalt@azgita.gov)

