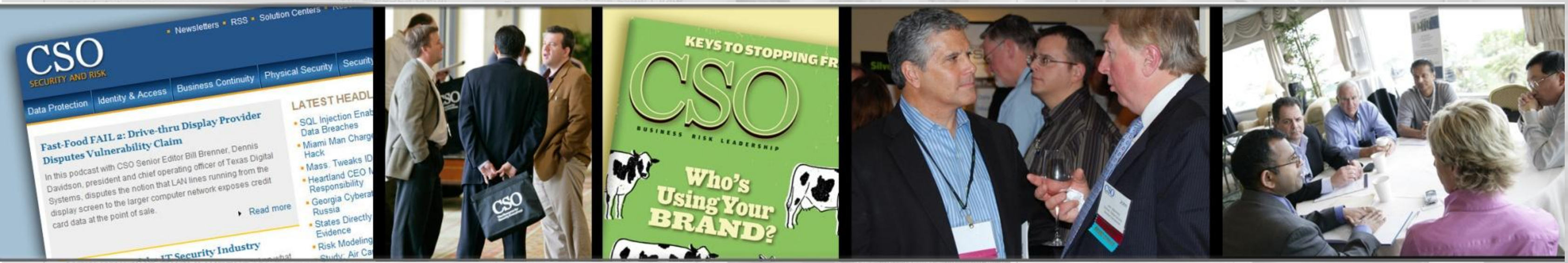
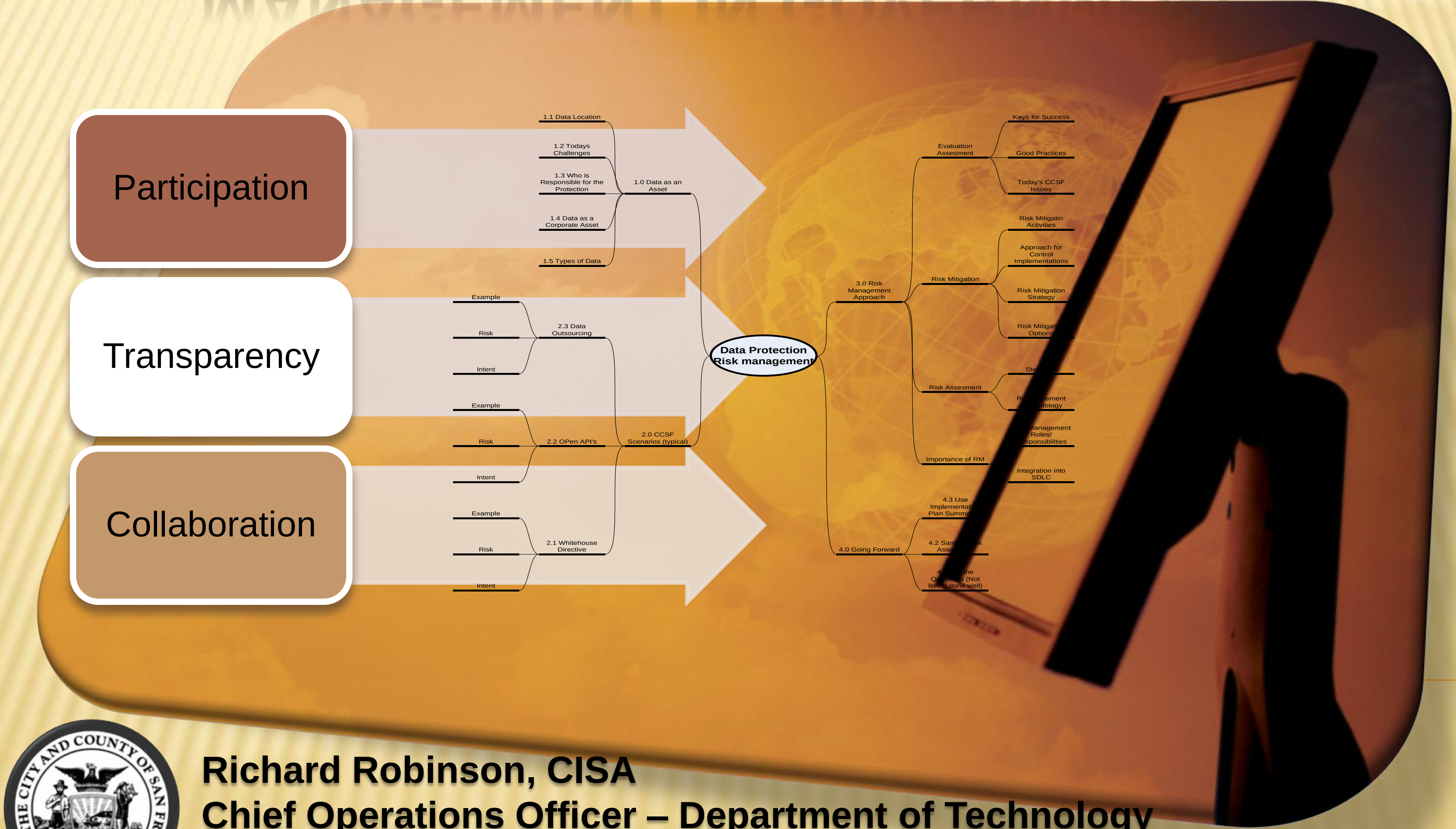


# Risk Management and Its Impact on Data Protection

**Richard Robinson,** CISA, Chief Operations Officer and Director, Enterprise Operations, Department of Technology, *City and County of San Francisco*

# DATA PROTECTION & RISK MANAGEMENT IN GOVERNMENT



Participation

Transparency

Collaboration

Data Protection Risk management

1.0 Data as an Asset
- 1.1 Data Location
- 1.2 Todays Challenges
- 1.3 Who is Responsible for the Protection
- 1.4 Data as a Corporate Asset
- 1.5 Types of Data

2.0 CCSF Scenarios (typical)
- 2.3 Data Outsourcing
  - Example
  - Risk
  - Intent
- 2.2 OPen API's
  - Example
  - Risk
  - Intent
- 2.1 Whitehouse Directive
  - Example
  - Risk
  - Intent

3.0 Risk Management Approach
- Evaluation Assesment
  - Keys for Success
  - Good Practices
  - Today's CCSF Issues
- Risk Mitigation
  - Risk Mitigatin Activities
  - Approach for Control Implementations
  - Risk Mitigation Strategy
  - Risk Mitigati Options
- Risk Assesment
  - Ste
  - Ri sement odology
- Importance of RM
  - Management Roles/ esponsibilities
  - Integration into SDLC

4.0 Going Forward
- 4.3 Use Implementati Plan Summa
- 4.2 Sam sk Asse
- 4 the Questions (Not Being done well)

**Richard Robinson, CISA**
**Chief Operations Officer – Department of Technology**
**City & County of San Francisco, California**

# OUTLINE/AGENDA

- *1.0 Data as an Asset*
- *2.0 CCSF Scenarios*
- *3.0 Risk Management Approach*
- *4.0 Going Forward*

# DATA AS AN ASSET

- 1.1 Types of Data
- 1.2 Data as a Corporate Asset
- 1.3 Who is Responsible for the Protection
- 1.4 Today's Challenges
- 1.5 Data Location

# Types of Data

- Census data
- Personal tax data
- Corporate tax data
- Military records
- National security intercepts (e.g. telephone/email intercepts by NSA)
- Law enforcement data (e.g. FBI investigative data)
- Prison records
- Passport applications
- Health records (Medical benefits programs)
- Transfer program records (e.g. Social Security, Food Stamps)
- Federal employee records
- Regulatory disclosures (e.g. trade secrets, required disclosures, results of inspections)
- Contracting, purchasing
- Sealed court records
- Immigration records

# DATA AS A CORPORATE ASSET

- Data no longer just an IT function (Company Asset)
- Responsibility falls to Legal & IT to protect like any other asset.
- Used in line with Internal & External Compliance & Controls
- Assets now digital (easily copied & transferred)
- Loss not always intentional (lack of awarness and training)

# WHO IS RESPONSIBLE FOR THE PROTECTION?

- Senior management
- CIO
- Security Officer
- IT System Owners
- Owners of Data
- Business & Functional Managers
- Application Programmers

# TODAY'S CHALLENGES

- Critical Data stored in digital format
- Redundant Physical/Virtual Access points
- Evolving technologies (cloud/virtualization)
- Budgetary Pressures
- Training & education of staff
- Executive Directives
- Legislation/Legislation/Legislation…..

# DATA LOCATION – DO YOU KNOW WHERE YOUR DATA IS?

- File Servers
- Email Servers
- Thumb drives
- CD’s/DVD’s
- Hard drives
- Laptops/Cell Phones
- Networks
- Printers
- Managed Storage Networks
- Cloud Providers

# CCSF SCENARIOS (COMMON)

- 2.1 Whitehouse Directive
- 2.2 Open API's
- 2.3 Data Outsourcing

# WHITEHOUSE DIRECTIVE

- Intent (White House Directive Open Data)
- 45 days identify and publish online in an open format at least three high-value data sets and register those data sets via Data.gov. These must be data sets not previously available online or in a downloadable format.
- 60 days create an Open Government Webpage located at http://www.[agency].gov/open to serve as the gateway for agency activities related to the Open Government Directive and maintain and update that webpage in a timely fashion.
- 120 days publish an agency-wide open government plan that will describe and enforce transparency initiatives and will improve public participation and accountability. The section headings of the Directive provide a clear outline of the document.

# WHITEHOUSE DIRECTIVE - RISK

- Data released accidentally due to human error or mis-configured software or application;
- Insider access in excess of defined permissions and/or for private purposes;
- Malfunctioning or wrongly designed software;
- Outside hackers, viruses, Trojan horses;
- Purportedly anonymized data releases that can be reverse engineered to create personally identifiable data (not unknown in the private sector, but of particular concern relating to census data);
- Foreign spying (contrast to industrial espionage in the private sector

# WHITEHOUSE DIRECTIVE -

**Government Data Breaches Expose 2500% More Records in 2009**

December 2009 – by Doug Pollack

- It has been reported that 2009 has been the year of the mega-data breach. Recently reported statistics by the Identity Theft Resource Center (ITRC) would seem to bear this out as far as our federal government and military is concerned as well.
- Government Technology, commenting on the report noted that "the breaches so far in 2009 have compromised more than 79 million records, whereas fewer than 3 million were hacked in 2008. A sobering upswing, to say the least. " This represents a staggering 2500% growth in number of individuals who's personal information was exposed via our federal government in 2009 (year to date) vs. 2008.

# GOVERNMENT OPEN API'S

- Intent
  - Open Government applications and services through Open API’s to…
  - Increase use of government data and content
  - Let citizens and constituents build applications and become the value added network
  - Integrate content into other applications (i.e., mash ups, mobile applications, etc.)

# GOVERNMENT OPEN API'S

- Risk
  - Risk to Core Systems
  - API abuse
  - Performance / Demand
  - Management, support and oversight
  - Control
  - Loss of Support
  - SLA’s/Liabilities
  - Data Privacy
  - Distributed Dependencies and Failure Points

# GOVERNMENT OPEN API'S

- The data confirmed what has become somewhat obvious to those who follow data breach situations and that the increasing mobility of data and data access significantly contributes to the risks of loss.
- While there are technology solutions to the problems, the adoption and use of social media, mobile devices and open systems seems to be outpacing organizations' ability to address the new risks.

# GOVERNMENT DATA OUTSOURCING

- Intent
  - Outsourcing is cheaper
  - Outsourcing is easier
  - Better Service

# GOVERNMENT DATA OUTSOURCING

- Risk
  - Licensing & Copyright
  - Standard of Work
  - Lack of Quality Control
  - Customer Service
  - Risks to Confidential Data & Personal Data
  - Increasing long term cost
  - Security
  - Fraud

# 3.0 RISK MANAGEMENT APPROACH

- 3.1 Importance of RM
- 3.2 Risk Assessment
- 3.3 Risk Mitigation
- 3.4 Evaluation Assessment

# IMPORTANCE OF RISK MANAGEMANT

- Identify Risk
  - " Net Negative Impact of the Exercise of a Vulnerability, considering both the probability and the impact of the occurrence"
- Assess Risk
- Take Steps to Reduce Risk to Acceptable Levels

# IMPORTANCE OF RISK MANAGEMENT

- Risk Management Roles/Responsibilities
  - Senior Management –
  - Chief Information Officer –
  - System & Information Owners –
  - Business Managers –
  - ISSO –
  - IT Security Practitioners –
  - Trainers (SME's)

# RISK ASSESSMENT

- Risk Assessment Methodology
- Determine the extent of potential threat and risk associated with as system through the SDLC.
- Use Output to identify appropriate controls
- Determine likelihood of future adverse event
- Determine level of Impact
- Use Risk Assessment Methodologies

# RISK ASSESSMENT

- 1. System Characterization
- 2. Threat Identification
- 3. Vulnerability Identification
- 4. Control Analysis
- 5. Likelihood Determination
- 6. Impact Analysis
- 7. Risk Determination
- 8. Controls Recommendations
- 9. Results Documentation

# RISK MITIGATION OPTIONS

- Risk Assumption
- Risk Avoidance
- Risk Limitation
- Risk Planning
- Research & Acknowledgement
- Risk Transference

# RISK MITIGATION STRATEGY

- When vulnerability exists
- When vulnerability can be exercised
- When hackers cost is less than gain
- When loss is too great

# RISK MITIGATION - APPROACH

THE RULE:

“ Address the greatest risks and strive for sufficient risk mitigation at the lowest cost, with minimal impact on other mission capabilities”

# RISK MITIGATION - ACTIVITIES

- Prioritize Actions
- Evaluate Control Options
- Conduct Cost-Benefit Analysis
- Select Control
- Assign Responsibility
- Develop & Safeguard Implementation Plan
- Implement Controls

# EVALUATION ASSESSMENT

- Today's CCSF Issues

# EVALUATION ASSESSMENT

- Good Practices
  - Do formal risk assessments of entire organization every 2-3 years.
  - Integrate Risk management as part of your SDLC
  - Define a specific schedule for assessing and mitigating mission risks
  - Build security training & education into daily operations

# EVALUATION ASSESSMENT

- Keys for Success
  - Commitment from Senior Management
  - FULL Support and participation of the entire IT Team.
  - Competence of security team
  - Awareness and Cooperation of the user community
  - On-going evaluations and assessments of IT related mission risks.

# 4.0 Going Forward

- Ask the Questions (What is not being done well ?)
- Sample Risk Assessment
- Use Implementation Plan Summaries
- Final Comment

# *GOING FORWARD* - SAMPLE RISK ASSESSMENT

- Who are valid users?
- What is the mission of the user organization?
- What is the purpose of the system in relation to the mission?
- How important is the system to the user organization's mission?
- What is the system-availability requirement?
- What information (both incoming and outgoing) is required by the organization?
- What information is generated by, consumed by, processed on, stored in, and
- retrieved by the system?
- How important is the information to the user organization's mission?
- What are the paths of information flow?
- What types of information are processed by and stored on the system (e.g., financial,

personnel, research and development, medical, command and control)?

- What is the sensitivity (or classification) level of the information?

# GOING FORWARD

**Use Implementation Plan Summaries**

I. Introduction
- Purpose
- Scope of this risk assessment

II. Risk Assessment Approach
- The participants (e.g., risk assessment team members)
- The technique used to gather information (e.g., the use of tools, questionnaires)
- The development and description of risk scale (e.g., a 3 x 3, 4 x 4 , or 5 x 5 risk-level matrix).

III. System Characterization

IV. Threat Statement

V. Risk Assessment Results
- Observation number and brief description of observation (e.g., Observation 1: User system passwords can be guessed or cracked)
- A discussion of the threat-source and vulnerability pair
- Identification of existing mitigating security controls
- Likelihood discussion and evaluation (e.g., High, Medium, or Low likelihood)
- Impact analysis discussion and evaluation (e.g., High, Medium, or Low impact)
- Risk rating based on the risk-level matrix (e.g., High, Medium, or Low risk level)
- Recommended controls or alternative options for reducing the risk.

VI. Summary

# GOING FORWARD

- Final Comment

# QUESTIONS/COMMENTS?

- Thank you