FEDCASIC
Walking the Tightrope:
Balancing Security Requirements with Operational Efficiency Mandates

Welcome & Introduction

Paul Blahusch
Bureau of Labor Statistics

Bill Connet
University of Michigan

BLS
BUREAU OF LABOR STATISTICS
U.S. DEPARTMENT OF LABOR

Welcome & Agenda

- Introduction
  - Paul Blahusch, BLS

- Presentations
  - Taylor Cooper, Westat
  - Jennifer Durbin & McKinlay Jeannis, RTI
  - Diana Salazar, NORC

Housekeeping

- 30-35 minutes for each presenter
- Questions for the end
- 10 minute break @2:45
- Presentations will be available on the FedCASIC site

Introduction

Walking the Tightrope: Balancing Security Requirements with Operational Efficiency Mandates

As organizations seek to drive down the cost of information technology by leveraging so-called “shared services”, the traditional fortress models and methods of securing information are no longer adequate.

Background

- OMB *Cloud-First* policy – “going forward, when evaluating options for new IT deployments, OMB will require that agencies default to cloud-based solutions whenever a secure, reliable, cost-effective cloud option exists.”

- FISMA – Agencies are responsible for providing information security protections for “information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency”

BLS

Background

- Combine & Consolidate
  - Data Centers (DCCI)

    Vivek Kundra (Federal CIO) - “I envision three major federal data centers, Digital Fort Knoxes, that’s where we are headed.”

  - Outsource (“Cloud Computing”)

    OMB - Each agency must identify three services to move to the cloud. Agencies must move one of those services to the cloud in 12 months and the remaining two in 18 months.

Fear of “Outsourcing”

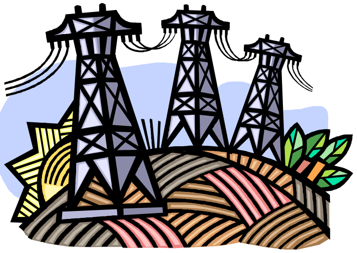
Fear of the Unknown

- Loss of Authority
- Loss of Control
- Loss of Relevance

But still all the responsibility!

Coping Method: Comparisons

- Electricity



- Air Travel

- Surgery

BLS

Comparisons/Differences

How is outsourcing to a shared service provider (“Cloud”) different from other examples?

- Utilities, commercial air traffic, and medical are regulated (statute, regulations, professional licenses)
  - Provider is legally bound and liable – both civil and criminal
- Shared service providers are not regulated
  - Outside of any contract provision, provider is not legally bound and liable – no criminal liability
  - Customer/user is, however, liable for any breach of their data – both civil and criminal

BLS

Coping Method: Knowledge

- Embrace the Unknown! The more you know about something, the less scary it becomes!

What is “Cloud” Computing

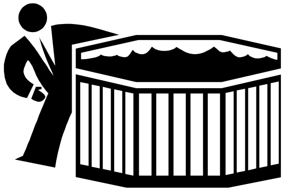
- The provision of computational resources on demand via a network.
- Offers computer application developers and users an abstract view of services that simplifies and ignores much of the details and inner workings.
- (NIST) A model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

Categories of “Cloud” Computing: Services Provided

- IAAS – Infrastructure as a Service
  - Hosted data center
  - Physical, environmental, and wiring
- PAAS – Platform as a Service
  - Virtual or Physical Server
  - Essentially disk, processing resources (Timeshare Computing?)
- SAAS – Software as a Service
  - Soup-Nuts
  - E-mail, Payroll, Purchasing

Categories of “Cloud” Computing: Provider Types

- Public Cloud
  - Computing resources used are owned and operated by a third-party with no direct management relationship to user
  - Generally open to all (who can pay)
  - Analogy: Public hot tub



- Private Cloud
  - Computing resources used are owned and operated by a unit within the organization with a direct management relationship to user
  - Generally closed to all but organizational users
  - Analogy: Family hot tub

Security Concerns with the “Cloud”

- Confidentiality – Who are all these people and is my stuff safe?
  - Only store non-sensitive information in the cloud
  - Encrypt/decrypt data locally
- Availability – What happens if provider goes out of business?
  - Plan for redundancy
- Integrity – Trust data hasn’t been modified and systems used are safe to access
  - Internal checks with hashes or checksums
  - Redundancy
  - Secure our client systems

Security Concerns with the “Cloud”

- Configuration Management
  - Are all (applicable) changes reviewed, tested, and approved prior to implementation? ... and by whom?
- Security Monitoring & Reporting
  - Responsibility for *continuous monitoring*
  - Incident reports to authorities (USCERT)
- Security Investigation Support
  - Can we have access to needed evidence in case of a (suspected) breach?
- Oversight ... verification
  - What sort of inspections or evaluations of provider controls am I allowed to perform?

Security Decisions Owning vs. Renting

- Agency Owned and Operated
  - "I own it, therefore I can adjust as needed as new requirements, threats, environments arise."
  - In-house security program management

- Provider Owned and Operated
  - "I rent it, therefore I better know up front what I need – both today and tomorrow – and I better make sure these are spelled out, and enforceable, in the contract."
  - Contract development and management

Help on the Way?

FedRAMP

(Federal Risk and Authorization Management Program)

- Joint initiative of GSA and the CIO Council
- To provide a standard approach to Assessing and Authorizing cloud computing services and products
- Provides a framework for the government to "approve once, and use often“, ensuring multiple agencies gain the benefit and insight of the security authorization and access to service provider’s authorization package
- Still incumbent on a purchasing agency to review authorization package and make its own risk-based decisions
- Not yet operational

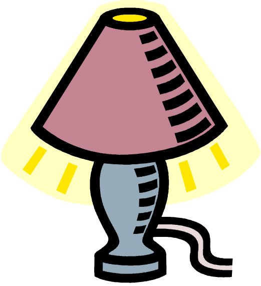
BLS

Knowledge Gained: Success Factors

- Engage Early
- Ensure inherent risks are understood
- Contribute Requirements
- Involve Contract Professionals, Legal, etc.
- Serve on Selection Panel
- Monitor and Hold Accountable

Success!

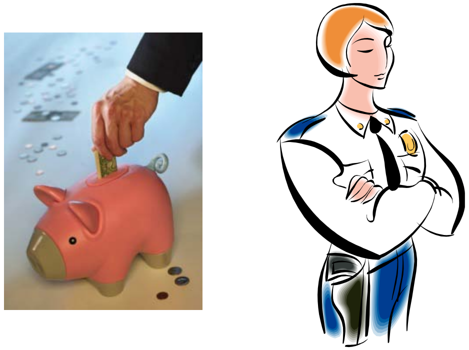
- Lights On



- Safe Landing

- Full Recovery

- Happy “Cloud” Customer



Solution: Group Therapy

THANK YOU!

BLS

Contact Information

Paul Blahusch
BLS IT Security Officer
blahusch.paul@bls.gov
202-691-7561

BLS
BUREAU OF LABOR STATISTICS
U.S. DEPARTMENT OF LABOR