How to maintain security control of data outside of organizational boundaries, including across international boundaries.

2011 FedCASIC Conference

March 23, 2011

NORC at the UNIVERSITY of CHICAGO

Speaker BIO

Diana Salazar – NORC Security Compliance

- 20+ years in IT (consulted at 50 companies: Fortune 1000, small to large enterprises)
- 6 years as employee at NORC at the University of Chicago, federal contractor
  - IT Engineering Managing: System Architecture - Servers, SAN, VMware, Databases, Software Deployments
  - NORC IT Security since 2007

Overview

- Managing Data Life Cycle
- Multi-layered Approach
- Going Beyond Boundaries
- Essential Technologies

Managing Data Life Cycle

Why secure the data?

- Confidentiality and Privacy Requirements
  - Personally Identifiable Data (PII)
  - Health Insurance Portability Act (HIPAA)
  - Confidential Business Data
  - Assurance to Respondents of the Confidentiality of their Data

- Decision makers depend on sensitive data to make important decisions that affect
  - Living Conditions
  - Societies
  - Global Economy

Managing Data Life Cycle

Three States of Data

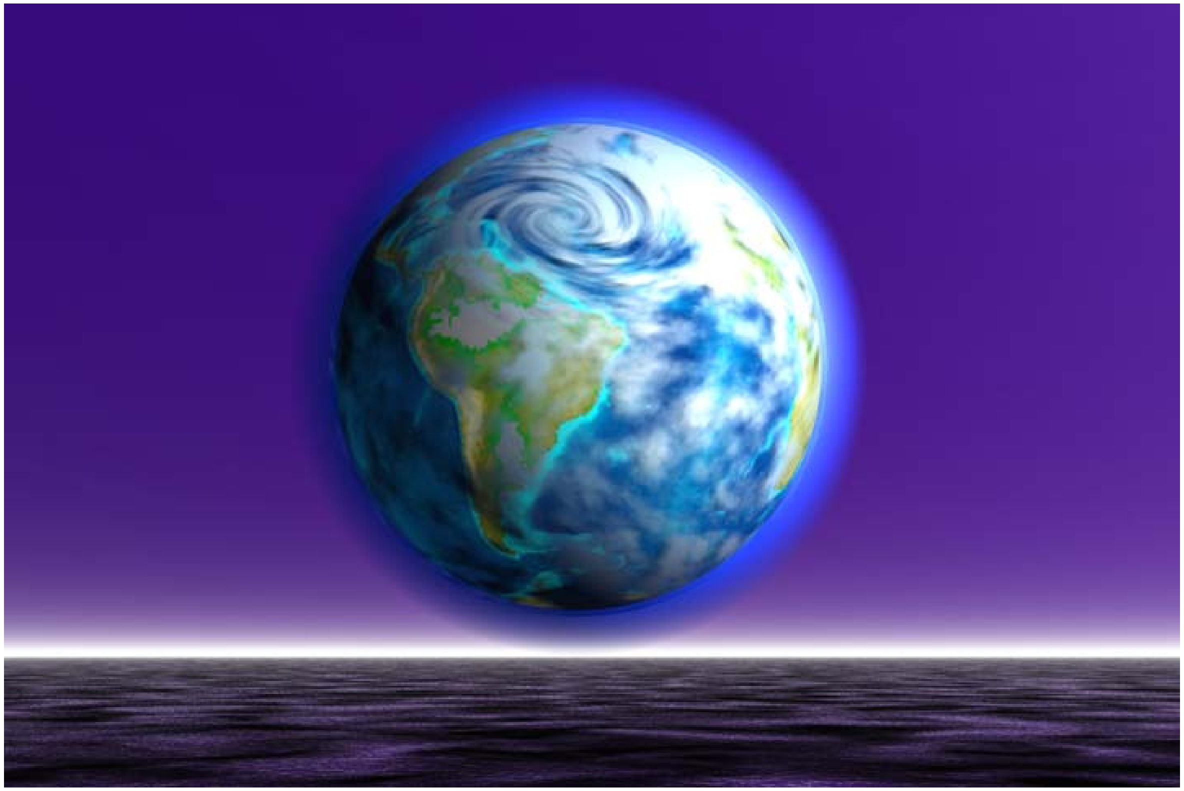
- **Data in use** is data on endpoints being used by personnel to do their jobs.
- **Data at rest** is information stored on endpoints.
- **Data in motion** is data sent over network

Multi-layered Approach

NORC at the UNIVERSITY of CHICAGO

- Technical (IT, systems, network)
- Operational/Organizational (management policies, protocols)
- Physical security, educational (data handling specific training)
- Legal protection (contracts, nondisclosure agreements (NDAs), Rules of Behavior (ROB))

Beyond Boundaries



Beyond Boundaries

- **In the ever-flattening work world, boundaries are vertical, horizontal, stakeholder, demographic and geographic.**

- **Any solution can have both advantages and disadvantages.**

- **There is always risk because of human error or technological issues.**

Essential Technologies

Technologies to protect data	
Encryption	• Full-disk encryption • USB, CD and removable media • Policy-based email encryption • File share encryption • Central key management and backup • Ability to audit encryption status
Threat protection	• Protect endpoint, email and web vectors with proven security. • Detect known and unknown malware proactively without the need for an update, including viruses, worms, Trojans, Spyware, Adware, suspicious files and behavior, potentially unwanted applications (PUAs)
Control Devices	• Storage: Removable storage devices (USB flash drives, PC card readers, and external hard drives), optical media drives (CD_ROM/DVD/Blu-ray, floppy drives. • Network: wireless (Wi-Fi interfaces, 802.11 standard), modems • Short range: Bluetooth interfaces, infrared (IRDA infrared interfaces)

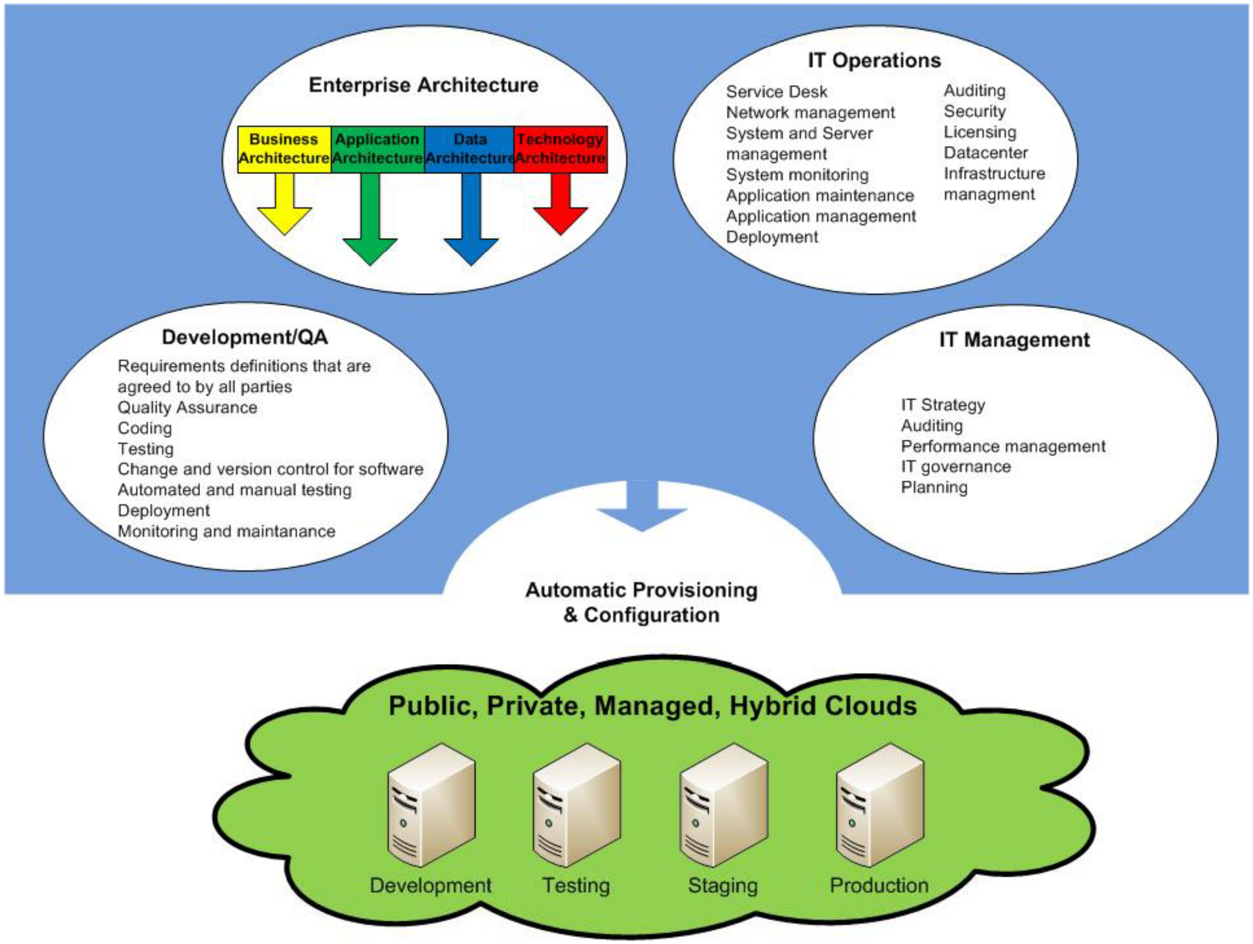
Essential Technologies

Technologies to protect data	
Policy Compliance	• Develop a list of applications that need to be controlled under all or certain circumstances to prevent the accidental transmission of sensitive data by email, IM, P2P, online storage, Smartphone synchronization and other frequently used communications applications. • Introduce and enforce methods of web control, as the internet is the source of most malware.
Data Loss Prevention	• Stop accidental data loss by scanning content for sensitive information sent by email or IM, and saved on storage devices with automatic rules • File matching rule: Specified action is taken based on the name or type of file a user is attempting to access or transfer. • Content rule: Specified action is taken if a user attempts to transfer data that matches one or more definitions.

ssential Technologies

NORC at the UNIVERSITY of CHICAGO

Cloud Computing Architecture



Enterprise Architecture

Business Architecture
Application Architecture
Data Architecture
Technology Architecture

IT Operations

Service Desk
Network management
System and Server management
System monitoring
Application maintenance
Application management
Deployment

Auditing
Security
Licensing
Datacenter
Infrastructure managment

Development/QA

Requirements definitions that are agreed to by all parties
Quality Assurance
Coding
Testing
Change and version control for software
Automated and manual testing
Deployment
Monitoring and maintanance

IT Management

IT Strategy
Auditing
Performance management
IT governance
Planning

Automatic Provisioning & Configuration

Public, Private, Managed, Hybrid Clouds

Development
Testing
Staging
Production

ssential Technologies

- Cloud Computing is increasingly being utilized to provide data outside the organizational boundaries.
- Common Models
  - Stand Alone
  - Shared Remote
  - Shared Data Center

ssential Technologies

nternational Services

- Rapid scalability and cost-effectiveness using partners across the world

Global Satellite Access

- Providers of voice, data, internet, video over satellite solutions for fixed or mobile communications

tional and International security ndards to meet control of data

- North America: NIST 800-53, Homeland Security, CMMI, Bill 3494/2000, Bill 3221/2004, Bill 198, COBIT, COSO, SAS 70, Sarbanes-Oxley, PCI
- South America: NBR 17799/27001, NTP 17799, NCH 2777, SB Regulations, Decree 83, Specific Local Requirements
- Asia: Japan Privacy, Japanese SOX, Basell II & FICS
- Australia and New Zealand: AS/NZS 4360, CLERP 9, PA & PAA
- nternational: ISO/IEC 27001:-27002, ISO/IEC 2000, ISO/WD 3100
- Europe: BS 25999, BS 7799-3, KongTraG, Basell II, DPA, EUDP, IAS, Companies Act, BDSG, LOP, Reg 357, Article 46, King II Report, Banking Act

ecurity Standards

Below is a list of regulatory schemes that may need to be part of a compliance framework:

- **NIST Guidance**
- **US Federal Security Guidance**
- **US Federal Privacy Guidance**
- **US State Laws Guidance**
- **ISO Guidance**
- **ITIL Guidance**
- **Healthcare and Life Science Guidance**

ecurity Standards

- **Energy Guidance**
- **US Internal Revenue Guidance**
- **Records Management Guidance**
- **EU Guidance**
- **UK and Canadian Guidance**
- **Other European and African Guidance**
- **Asia and Pacific Rim Guidance**
- **System Configuration Guidance**

esources

Citrix:
ttp://www.citrix.com/English/ps2/products/product.asp?contentID=23
04712

File Backup Services – FIPS 140-2 compliant
ttp://www.asigra.com/fips-140-2-certification-backup

USB Devices - FIPS 140-2 Level 3: IronKey, Spyrus

Disk Encryption FIPS 140-2 Certified : Check Point, WinMagic,
DESLock+

Security Standards List: http://www.compliancebuilding.com/what-is-your-scope-of-compliance/

Europe Cloud Computing Challenges:
ttp://www.cessda.org/project/doc/CESSDA_RI_SRA_FINAL.pdf

na Salazar – NORC Security Compliance
azar-diana@norc.org,312/759-2380

hank You!

NORC at the UNIVERSITY of CHICAGO

insight for informed decisions™