DATA SECURITY: Securing Data Securely

Dr. Denise C. Walker

Chief Emergency Management Officer

(formerly Chief Security Officer)

Lone Star College System

Challenges

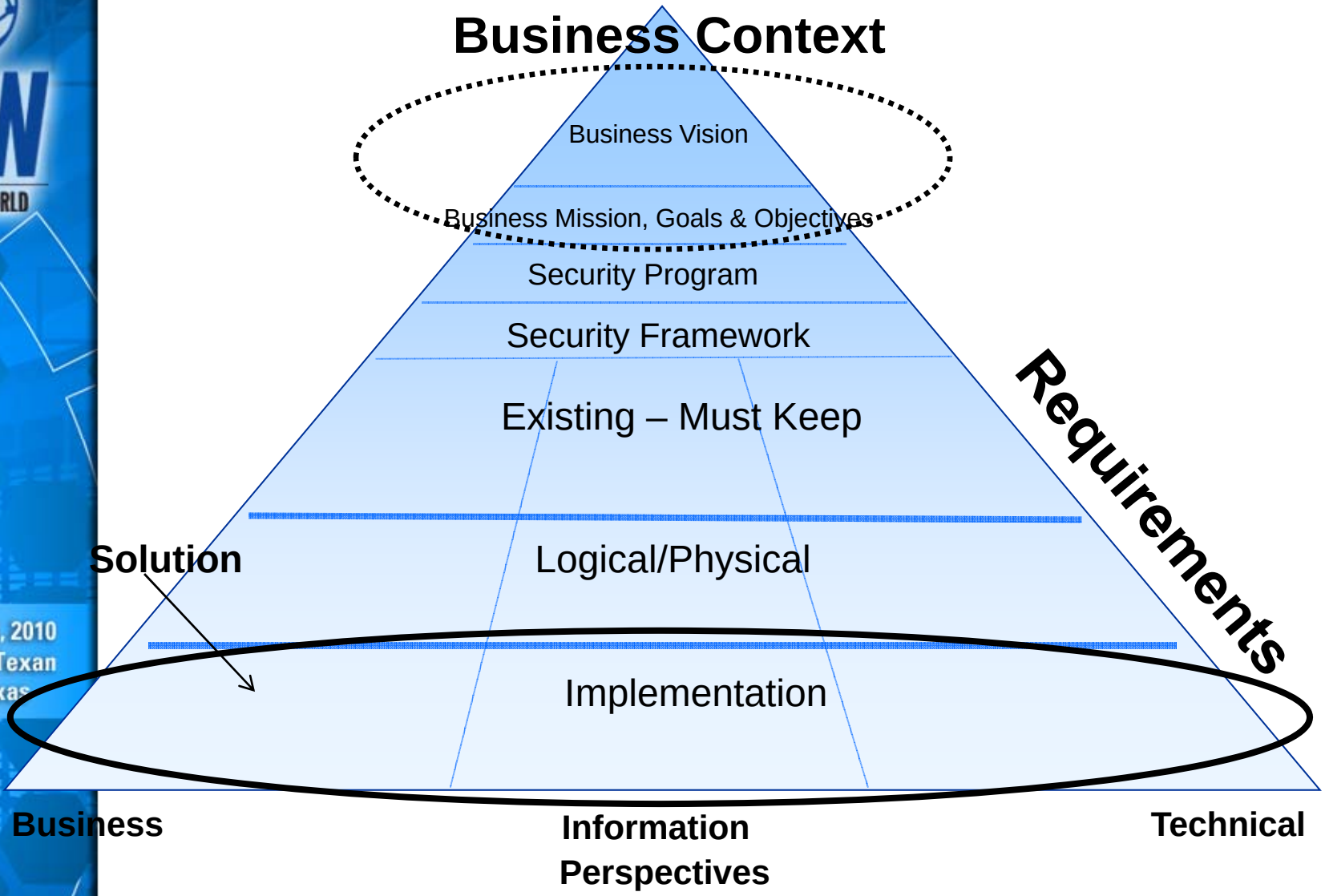
- Customers/business partners expect you to operate at all times
- Disaster, human error, or malicious acts cannot be totally prevented
- ***Threats to confidentiality, integrity, and availability of data***
- Information security should be based on analysis of your business functions and acceptable risks

How much can you afford to lose or accessed inappropriately?

Other Challenges

- **Budget constraints**
- **Laws, rules, regulations, standards**
  - FERPA, GLBA, HIPAA, FACTA, PCI DSS, etc.
- **Culture**
- **Technology**
  - e-Discovery, security controls, cloud computing, identity management, legacy applications, etc.

Security Architecture Framework



Focus Areas

…your response determines your directions

The Process

- Involve stakeholders early
- Determine what can be managed internally or outsourced
- Identify project sponsor and an owner high up in the organization
- ***Conduct risk analysis***
- Prioritize key deliverables and milestones
- Obtain funding
- Develop project plan
- Kickoff Program

Solution should fit the business rather than the business fitting into the solution!

Risk Assessment

- Negative effects on credibility
- Health, welfare, & detriment to stakeholders
- Violation of information privacy or confidentiality rights
- Accessibility and integrity of data
- Laws, regulations or contracts violations
- Operational impact
- Financial consequences
- System controls perform as designed

Information Security Risk Analysis

Do you have ...

- Processes and infrastructure that meet your **compliance** demands including ***information confidentiality***?
- Defined **testing** program for **goodness** and recovery with goals and measures in place (***information integrity***)?
- Change management and other policies tied directly to ***information availability*** plans?

Unauthorized Release of Data

Most common causes of unauthorized release of sensitive data appears to be ***lost backup tapes and unencrypted devices***

- **Fail to encrypt** sensitive information contained on tapes that travel from data centers to off-site storage
- With **access** to the right hardware and software, retrieving sensitive information from tape is relatively easy.
  - Shared passwords
  - Administrators with keys to the kingdom
  - Disgruntled employees separated from company and access remains active
  - Passwords stored insecurely

Backup v. Archival Storage

Backup

- A copy of electronic information maintained for use if there is loss/damage to original (incl. DR purposes)

Archival Storage

- Primary copy of records (not for DR purposes)
- Permanent maintenance of electronic information valuable to organization
- Focus on data that will no longer change
- Must be maintained uncorrupted and usable for a period of time
- 1 Master + 1+ Duplicates

Pros & Cons of Media Types – Writable Media

Type	Pros	Cons
Tape	• Inexpensive • Can be used repeatedly • Good for daily backups	• Relatively slow • Sensitive to heat and magnetism
CD / DVD	• Compact • Inexpensive • Portable	• Sensitive to heat • Unusable if mishandled • Rapidly evolving technology makes today's storage media outdated
External Hard Drive	• Most incl. backup software • Can be automated • Can be used to replace faulty drives	• Expensive • Maintaining compatibility with your source systems • Sensitive to heat and magnetism
Flash Drives	• Easily portable • Fast data transfer	• Easy to lose • Can be expensive • Difficult to label • Sensitive to heat and magnetism
Online Backup (remote server, upload via Internet)	• Easy data transfer • Can be automated	• Expensive • Provider system can be compromised • Provider can go out of business • Reliant on provider standards

Risk Analysis

- *Backups*
  - Understand flow of information
  - Cost of temporary/permanent data loss
  - Is encryption needed
  - Can compression be used to save space
  - How many versions of backups are needed to ensure retrieval of damaged/destroyed data
  - Labeling and naming convention of backed-up files
  - Frequency and types of backups
  - Full, incremental and differential backups
  - What to backup
    - Software, application files and settings, sensitive data

Risk Analysis

- *Archival Storage*
  - What to store
  - How many duplicates are needed
  - Where to safely store and for how long
  - **Should not be compressed or encrypted**
  - Address information security for data at rest
  - Media migration or refreshing at defined basis
    - Life expectancy of media
    - Retention of data
    - Climate conditions and reuse
    - Common file formats to use (i.e., TIFFs)

Data Storage, Backup & Recovery Risk Analysis

Do you have an understanding of ...

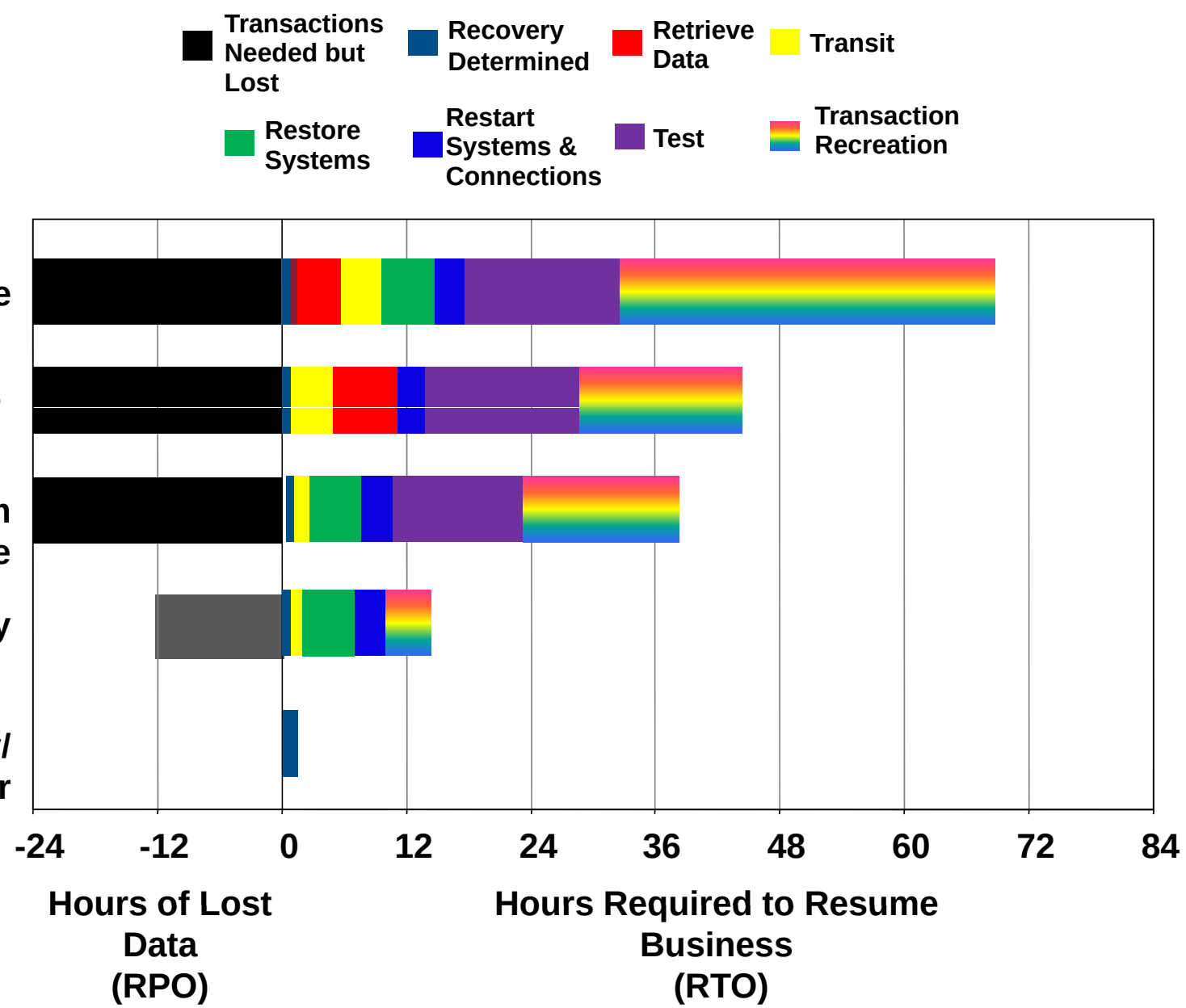
- Your business priorities and IT risks?
- What compliance means for your business?
- How long you can go if the primary source is no longer available, data is lost, corrupted, or compromised?
- Applications and hardware priorities required to support essential business functions?

Backup & Recovery Readiness Risk Analysis

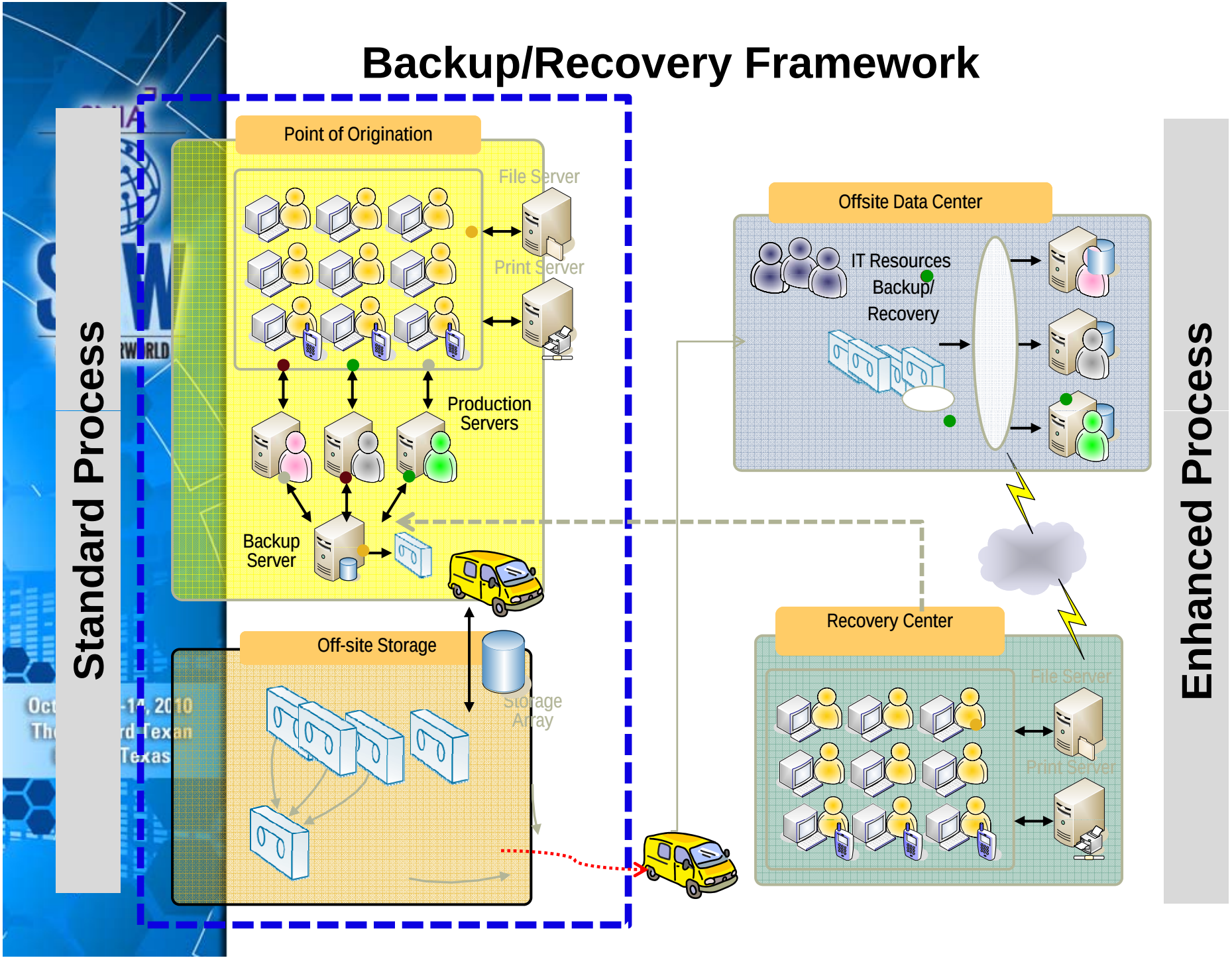
Do you have ...

- Detailed procedures to respond to an attack that penetrates your network or device?
- Backup strategy that supports both operational issues and disaster recovery?
- Documented responses to a disruption of a critical business unit?
- Alternate facility from which to recover and conduct business and/or IT operations?

RPO & RTO: Types of Recovery Processes



Backup/Recovery Framework



Guidelines for Secure Backup

- Back up data at regular intervals
  - Employees make important files available for inclusion
  - Individual backup procedures also needed
- Verify data has been backed up
- Store backup media in a secure, safe place
- Verify the ability to restore
- Test, test, test

Encryption

- **What**
  - a process of transforming information to an unreadable format using an algorithm (called cipher) to anyone except those possessing special knowledge, usually referred to as a key.
- **When**
  - Sensitive data in transit and at rest
- **Who**
  - Anyone with a device that is used to access sensitive data
- **Why**
  - to minimize opportunity for unauthorized access to electronic sensitive data

Encryption concerns

- **View by end users:** *a move towards "over-kill“ and not welcomed by stakeholders*
- **Expensive and intrusive:** *Encrypting all production data without looking at the value or hot it fits into the overall data protection strategy*
- Causes **degradation in performance**
- Data loss if encryption keys are lost or disgruntled former employees refuse to provide passwords
- Another password prompt for information access
- Management of encryption systems - certificates, keys, passwords, additional storage requirements
- IS personnel must work closely
- Finding the right balance among locking data down, discomfort, and acceptable risk.

Other processes to secure data from the threat within

- Forensics analysis
- Digital rights management
- Security policy management
- Protect intellectual property
- Enforcement policies

The dreaded hacker:

(16%) isn't much of a menace

v. insiders (69% = 39% human error + 30% malicious)

(Ponemon Institute's 2004 Data Security Tracking Study)

Conclusions

- Effective governance with clear accountabilities for **ownership & use**
- Aligning backup policy and controls with business needs – new risks will surface
- Previously mitigated risks may become a concern again
- Create/maintain awareness throughout the organization
- Measure/report on the value of securing data securely

Conclusions

- Develop/use an architecture that includes existing and emerging technology and business scenarios
- Regularly review schedules, scopes, information classifications, etc.

Technology is important however the most advanced technology is useless if not tested and incorporates the needs of the business.

Contact Information:
Dr. Denise C. Walker
Lone Star College System
Denise.c.walker@lonestar.edu

THANK YOU!


COMPUTERWORLD
SNIA
SNW
OCTOBER
11-14
2010
The Gaylord Texan, Dallas, Texas