System Administration
CSCI 4417

Backups

Disaster Recovery

Security

East Tennessee State University
Department of Computing
Jack Ramsey, Lecturer

Section Overview

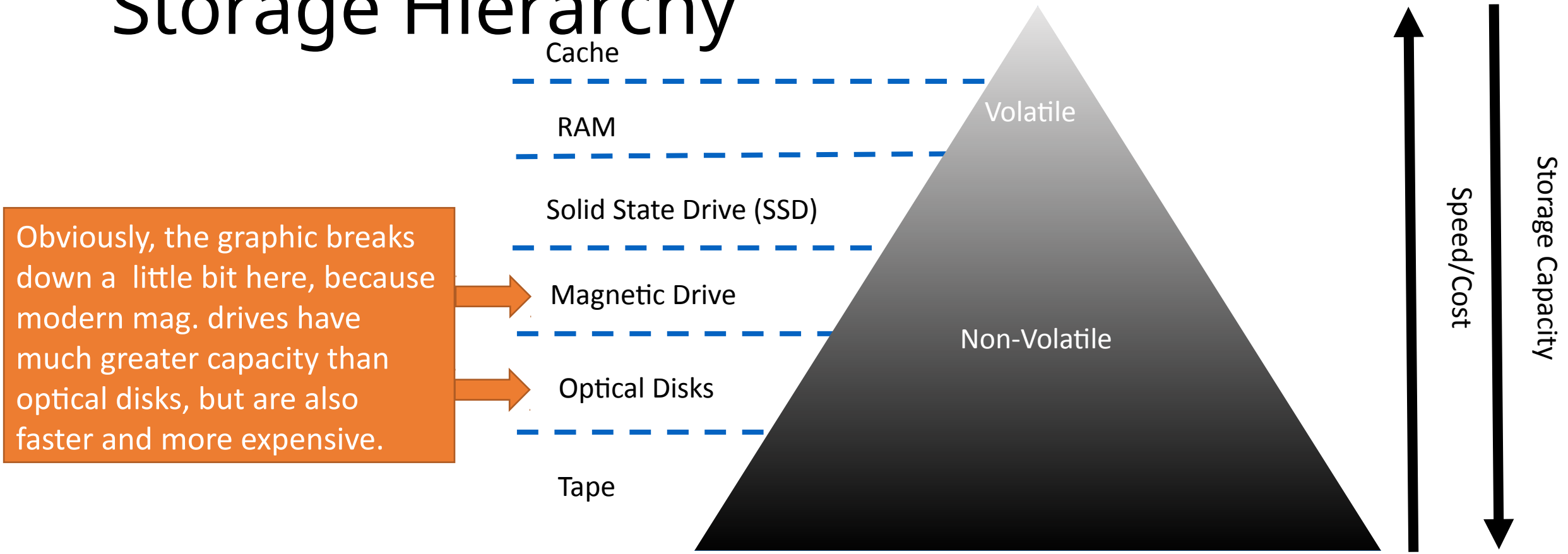
Storage Hierarchy

Backup Characteristics

Backup Media

Backups Tools and Plans

Storage Hierarchy



Obviously, the graphic breaks down a little bit here, because modern mag. drives have much greater capacity than optical disks, but are also faster and more expensive.

Why Backups?

Accidental deletions or modification

Hardware failures

Upgrades and Migrations

Security incidents

Disaster Recovery

Lawsuits?

Backup Plan Characteristics

Ease of use

- Automation of backups
- Selective file/directory restores

Time scheduling

Backup verification

Offsite copies

Portability

Media Lifecycle!!!

Deduplication

Backup Media

USB Hard Drives/Sticks

CD-R/RW and DVD±R/RW Drives

Disks

Tape

Libraries/Stackers/Jukeboxes

Linux Backup tools

`dump` and **`restore`**

- filesystem backups
- Support for incremental backups

`tar`

- File by file backups (archives)
- Easy to recover selected files

`dd` – Duplicate “raw” devices

`mt` – Control tape devices

Compression tools

- **`compress`**
- **`gzip`**

Backup Strategies

Full Backups – Backup entire system

Partial Backups – Selective backup

Differential – Backup files modified since last full backup

Incremental – Backup files modified since last incremental backup

Snapshots v. Backup

State/image of the storage device at a specific point in time

Snapshots useful for restoring data locally in the event of loss or corruption

Snapshots stored locally / backups can (should) be stored off-site

Snapshots require same storage medium as original / backups do not

Backups can be done over secure network connection

Amazon S3 / Glacier

Data/Disaster Recovery

Create restore location/mount point

Restore from last full backup first

Restore from most recent lowest level incremental

Increase level and repeat

Should plan backup schedule to keep restore time manageable

Disaster Recovery

East Tennessee State University
Department of Computing
Jack Ramsey, Lecturer

Disaster Recovery

Developing DR strategies

Regarding disaster recovery strategies, ISO/IEC 27031, the global standard for IT disaster recovery, states, “Strategies should define the approaches to implement the required resilience so that the principles of incident prevention, detection, response, recovery and restoration are put in place.” Strategies define what you plan to do when responding to an incident, while plans describe how you will do it.

Things to Consider

People

availability of staff/contractors

training needs of staff/contractors

duplication of critical skills so there can be a primary and at least one backup person

available documentation to be used by staff

follow-up to ensure staff and contractor retention of knowledge

Things to Consider

Physical facilities

availability of alternate work areas within the same site

at a different company location

at a third-party-provided location

employees' homes or at a transportable work facility

then consider site security, staff access procedures, ID badges and the location of the alternate space relative to the primary site

Things to Consider

Technology

access to equipment space that is properly configured for IT systems

with raised floors

suitable heating, ventilation and air conditioning (HVAC) for IT systems

sufficient primary electrical power

Things to Consider

Technology

access to equipment space that is properly configured for IT systems

suitable voice and data infrastructure

distance of the alternate technology area from the primary site

provision for staffing at an alternate technology site; availability of failover (to a backup system) and failback (return to normal operations) technologies to facilitate recovery; support for legacy systems; and physical and information security capabilities at the alternate site

Things to Consider

Data -- Areas to look at include

backup of critical data to a secure storage area

method(s) of data storage (disk, tape, optical, etc)

connectivity and bandwidth requirements to ensure all critical data can be backed

data protection capabilities at the alternate storage site

availability of technical support from qualified third-party service providers

Things to Consider

Suppliers

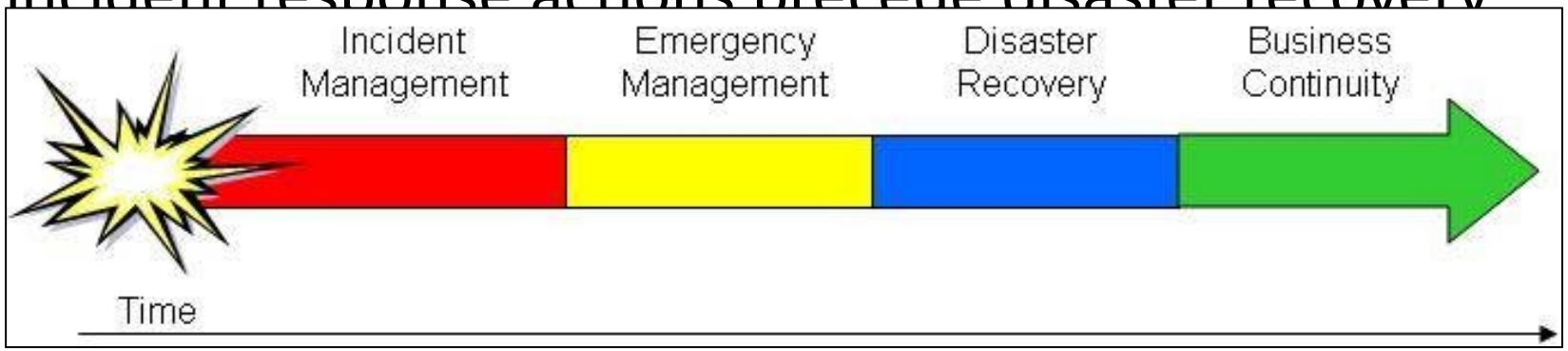
identify and contract with primary and alternate suppliers for all critical systems and processes

key areas where alternate suppliers will be important include:

- hardware (such as servers, racks, etc)
- power (such as batteries, universal power supplies power protection, etc)
- networks (voice and data network services)
- repair and replacement of components
- multiple delivery firms (FedEx, UPS, etc)

Incident Response

In addition to using the strategies previously developed, IT disaster recovery plans should form part of an incident response process that addresses the initial stages of the incident and the steps to be taken. This process can be seen as a timeline, in which incident response actions precede disaster recovery actions.



After Action Meeting/Report

Security

East Tennessee State University
Department of Computing
Jack Ramsey, Lecturer

The Basics

Two basic patterns

- Perimeter: Physical security, firewalls
- Defense in depth: Security measures at all points in the network
  - Firewall – attacks from the Internet
  - Antivirus system scanning all emails
  - Antimalware on each PC
  - Encryption between computers to ensure privacy and authentication

The Basics

Design Considerations

- Simplicity – Complexity obscures errors or chinks in the armor
  - People will often circumvent complex security protocols, leaving the system vulnerable
  - Should be built in to the system, not “bolted on” at the end
- Usability
  - Security vs. Convenience
  - Single-sign-on

Ask the Right Questions

Questions

- What are you trying to protect?
- From whom should it be protected?
- What are the risks?
- What is it worth to the company?

Decisions made through informed discussion with executive management

Document & review with management

Information Protection

Information as an asset

Classification determines what level of security is applied

- Public – Marketing information, user manuals, etc.
- Company confidential – Organizational charts, phone lists, internal newsletters, source code, security policies, etc.
- Strictly confidential – Contract negotiations, employee information, product-development details, etc.

Information Protection

Protecting Information

- Malicious alteration
- Deliberate & accidental release of information
- Theft
- Destruction

Service Availability

If a company relies on the availability of certain electronic resources to conduct its business, part of the mission of the security team will be to prevent malicious DoS attacks against those resources

Theft of Resources

Intruders stealing IT resources

Hidden FTP or chat servers in the infrastructure

Documentation

Policies are the foundation for everything that a security team does

Must be created in cooperation with people from other departments

HR

- Acceptable-use
- Monitoring
- Privacy

Documentation

Policies are the foundation for everything that a security team does

Must be created in cooperation with people from other departments

Legal

- Tracking and prosecution of intruders
- When to involve law enforcement

Documentation

All policies need the support of upper management

Documentation

Acceptable Use Policy (AUP) – identifies legitimate users & what they are permitted to use system resources for

Monitoring and privacy policy – describes company's monitoring of computer and network resources

- Network traffic, email, web browsing, audit trails, & log monitoring

Remote access policy – should explain risks associated with unauthorized access to the network, protecting private information, provide a way to report lost or stolen remote access tokens

Documentation

Network connectivity policy – describes how the company sets up network connections to other entities or shared resources for access by a third party

Log-retention policy – what is logged and how long logs are stored

Centralize Authority

Decisions that relate to security

- Business decisions
- Policy making
- Architecture
- Implementation
- Incident response
- Auditing

State of Security

Must-haves (bare minimum)

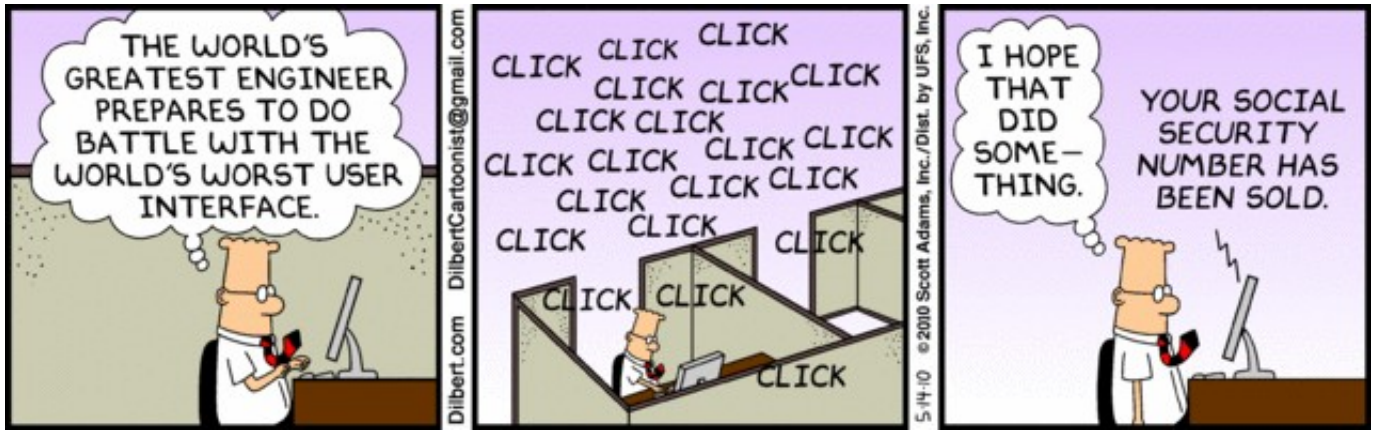
- Firewalls
- Email filtering
- Malware protection
  - Viruses
  - Spyware
  - Worms
- VPNs

Meet Business Needs

No point in securing a company to the point where it can't conduct business

Need to understand:

- What the employees are doing
- How they are trying to do it
- What their workflow looks like



Meet Business Needs

The right solution

- Enables people to work effectively
- Provides a reasonable level of security
- Is as simple and clean as possible
- Can be implemented within a reasonable time

Know the Latest Attacks

Security bulletins from vendors

Advisories from organizations that track security issues

- Bugtraq: http://www.securityfocus.com
- CERT/CC: http://www.cert.org
- Computer incident Advisory Capability (CIAC): http://www.ciac.org
- Australian Computer Emergency Response Team (AUSCERT): http://www.auscert.org.au

Provide exploits that you can test on your own systems

Authentication & Authorization

Authentication – validates user's identity

- Factors: Something you know, something you have, something you are
- 2-Factor: Must be something from two of the above groups, not, for example, a password and a PIN (both represent something known)
  - Provides stronger authentication

Authorization – determines what that person can do

Vendors & Products

Security sensitive products – one or more of these qualities

- Used by any 3rd party having restricted level of access
- Part of the authentication, authorization, or access control system
- Accessible from the Internet or any untrusted network
- Has access to the Internet or any untrusted network
- Provides authenticated users access to sensitive data or systems

Vendors & Products - **Things to consider**

Confidence in degree of security provided

Simplicity

Open source/Proprietary

Usability

Functionality

Vendor issues

Integration

Cost

Futures

Auditing

Internal, External, Both

Checking whether security environments are in compliance with policies & design criteria

Checking employee and contractor lists against authentication & authorization databases

Making physical checks on machine rooms, wiring, and telecom closets for foreign devices

Auditing

Checking that relevant machines have up-to-date security patches

Scanning relevant networks to verify what services are offered

Launching sophisticated, in-depth attacks against particular areas of the infrastructure

- Clearly defined success criteria and limitations

Auditing

Logging & log processing

- Tracing what happened
- Detecting attacks
- Gauging attack seriousness
- Should be stored in highly secure central location

Auditing

Internal verification

- Check for anomalies on your network & important systems
- Strange routes on network
- Routes going in strange directions
- Traffic from unexpected sources
- Intrusion detection can make this easier

Auditing

Per project verification

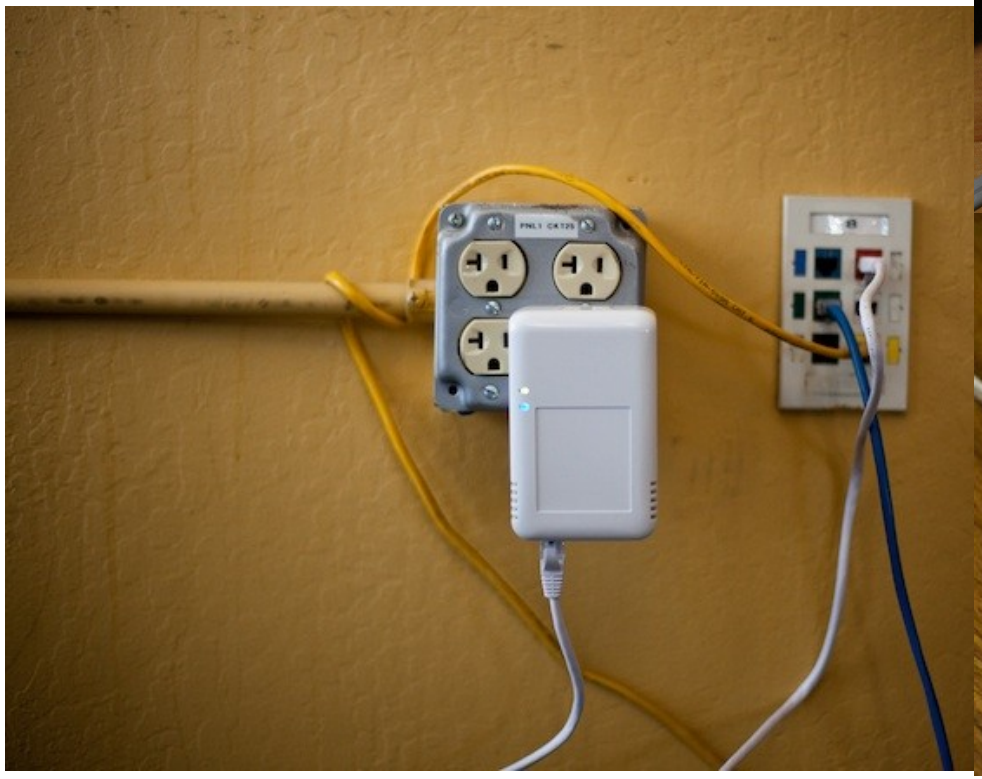
- Check that each security project for configuration changes
- Ensure that it still matches the design specifications
- Conforms to appropriate policies

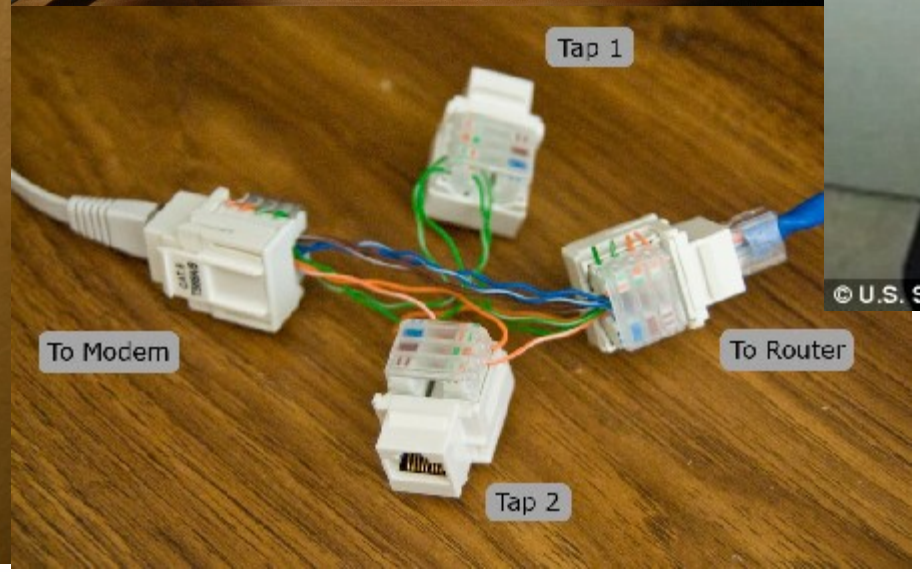
Auditing

Physical checks

- Key points – data centers, networking closets, telecommunications closets, videoconferencing rooms, wiring between such rooms, wired/wireless connections between buildings
- Look for additional devices

Auditing





East Tennessee State University
Department of Computing
Jack Ramsey, Lecturer

Best Practices

Make security pervasive

- Awareness campaigns
- Clean Desk Policy

Stay current: Contacts and Technologies

- Conferences
- New technologies, benefits, how they work, deployment/operational needs

Produce metrics

- Example: IDS log data indicating number of attacks or possible attacks, providing graph of level of protection

Copyrights

Presentation prepared by and copyright of John Ramsey, East Tennessee State University, Department of Computing . (ramseyjw@etsu.edu)