CSF 434/534: Advanced Network and System Security

Week 11 - Review

Michael Conti

Department of Computer Science and Statistics
University of Rhode Island

Sources: Professor Messer's CompTIA SY0-501 Security+ Course Notes

Disaster Recovery Sites

Disaster Recovery Sites

Cold site

☑ No hardware - Empty building

☑ No data - Bring it with you

☑ No people - Bus in your team

Warm site

☑ Somewhere between cold and hot - Just enough to get going

☑ Big room with rack space - You bring the hardware

☑ Hardware is ready and waiting - You bring the software and data

Disaster Recovery Sites

Hot site

☑ An exact replica
  - ☑ Duplicate everything

☑ Stocked with hardware
  - ☑ Constantly updated
  - ☑ You buy two of everything

☑ Applications and software are constantly updated
  - ☑ Automated replication

☑ Flip a switch and everything moves
  - ☑ This may be quite a few switches

Application Recovery

Application Recovery

Order of restoration

- ☑ Not all applications have the same priority
  - ☑ Some are more important than others
- ☑ This list should be defined well before it’s needed
  - ☑ Organization management sets the priority
- ☑ The order may change based on the calendar
  - ☑ Monthly/quarterly applications may take priority

Application Recovery

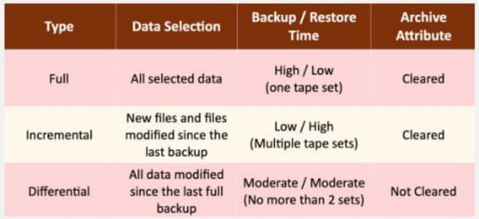
Backup strategies

- ☑ Backup technologies - Tape, disk, optical
- ☑ Database backups - Replication - Online duplicates
  - ☑ Online backups - Specialized backup process for databases
- ☑ Email database backups
  - ☑ Provide server, database, mailbox, or message backup/restore
- ☑ Snapshots
  - ☑ Operating system volume snapshots or hypervisor snapshots
- ☑ System backups
  - ☑ Bare metal backup using images

Application Recovery

Backup Types

- ☑ The archive attribute
  - ☑ Set when a file is modified
- ☑ Full
  - ☑ Everything
  - ☑ You’ll want this one first



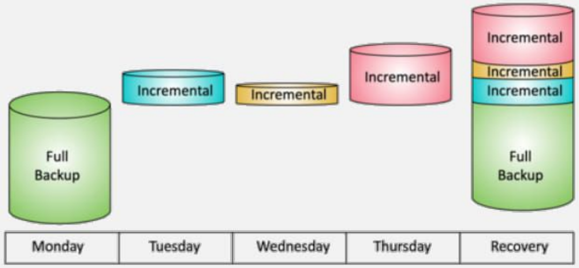
Type	Data Selection	Backup / Restore Time	Archive Attribute
Full	All selected data	High / Low (one tape set)	Cleared
Incremental	New files and files modified since the last backup	Low / High (Multiple tape sets)	Cleared
Differential	All data modified since the last full backup	Moderate / Moderate (No more than 2 sets)	Not Cleared

- ☑ Incremental
  - ☑ All files changed since the last incremental backup
- ☑ Differential
  - ☑ All files changed since the last full backup

Backup and Recovery

Incremental Backup

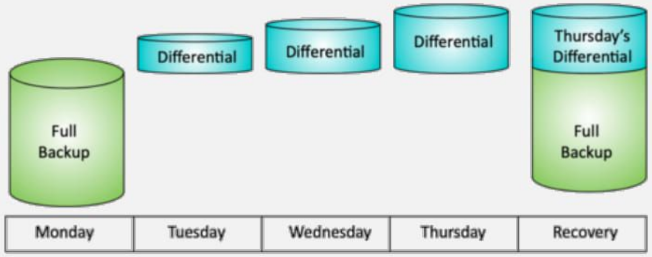
- ☑ A full backup is taken first
- ☑ Subsequent backups contain data changed since the last full backup and last incremental backup
  - ☑ These are usually smaller than the full backup
- ☑ A restoration requires the full back and all of the incremental backups



Backup and Recovery

Differential Backup

- ☑ A full backup is taken first
- ☑ Subsequent backups contain data changed since the last full backup
  - ☑ These usually grow larger as data is changed
- ☑ A restoration requires the full back and the last differential backup



Geographic Considerations

Geographic Considerations

Selecting offsite recovery options

- ☑ Your building can be the disaster
  - ☑ Fire, flood, water pipe burst, hurricane, tornado
  - ☑ Plan for the worst
- ☑ Hedge your bets by keeping data offsite
  - ☑ You'll always have another copy of your data
- ☑ Recovery sites can host you in a different location
  - ☑ Get up and running quickly

Geographic Considerations

Off-site backups

- ☑ Vaulting
  - ☑ Send your backup media to an outside storage facility
  - ☑ E-vaulting - Send the data electronically
- ☑ Organization-owned site or 3rd-party
  - ☑ Usually a secure facility
- ☑ Backups require extensive protection
  - ☑ Data loss and theft is a significant concern
- ☑ Many compliance mandates
  - ☑ Sarbanes-Oxley (SOX)
  - ☑ Federal Information Systems Management Act (FISMA)
  - ☑ Health Insurance Portability and Accountability Act (HIPAA)

Geographic Considerations

Distance

- ☑ A balancing act
  - ☑ Recovery vs. accessibility
- ☑ The recovery site should be outside the scope of the disaster
  - ☑ Natural disasters can affect a large area
- ☑ Travel for support staff
  - ☑ And for employees
- ☑ Unique business requirements
  - ☑ Specialized printers, bandwidth availability

Geographic Considerations

Location selection

- ☑ Legal implications
  - ☑ Business regulations vary between states
  - ☑ For a recovery site outside of the country, personnel must have a passport and be able to clear immigration
  - ☑ Refer to your legal team
- ☑ Data sovereignty
  - ☑ Data that resides in a country is subject to the laws of that country
  - ☑ Legal monitoring and court orders
  - ☑ Where is your data stored?
  - ☑ Your compliance laws may prohibit the moving data out of the country

Continuity of Operations

Continuity of Operations

Tabletop exercises

- ☑ Performing a full-scale disaster drill can be costly
  - ☑ And time consuming
- ☑ Many of the logistics can be determined through analysis
  - ☑ You don't physically have to go through a disaster or drill
- ☑ Get key players together for a tabletop exercise
  - ☑ Talk through a simulated disaster

Continuity of Operations

The scope of a tabletop exercise

- ☑ Decide on complexity
  - ☑ Invite local first responders or just discuss internally?
- ☑ Determine the scope of the disaster
  - ☑ Water main break? Death and injuries?
- ☑ Involve everyone
  - ☑ Perhaps even make the discussion a surprise
- ☑ Don't assume that every piece of information is going to be available in a disaster
  - ☑ The tabletop exercise should find the gaps

Continuity of Operations

After-action reports (AAR)

- ☑ Exercise scope and objectives - What's the endgame?
- ☑ Methodology - Detailed explanation of the exercise
- ☑ What worked? What didn't work? - The good and the bad
- ☑ Next steps
  - ☑ Update procedures, add a new set of tools
  - ☑ Prepare for the next exercise

Continuity of Operations

Failover

- ☑ Recovery site is prepped
  - ☑ Data is synchronized
- ☑ A disaster is called
  - ☑ Business processes failover to the alternate processing site
- ☑ Problem is addressed
  - ☑ This can take hours, weeks, or longer
- ☑ Revert back to the primary location
  - ☑ The process must be documented for both directions

Continuity of Operations

Alternate business practices

- ☑ Not everything goes according to plan
  - ☑ Disasters can cause a disruption to the norm
- ☑ We rely on our computer systems
  - ☑ Technology is pervasive
- ☑ There needs to be an alternative
  - ☑ Manual transactions
  - ☑ Paper receipts
  - ☑ Phone calls for transaction approvals
- ☑ These must be documented and tested before a problem occurs

Security Controls

Security Controls

Security controls

- ☑ Security risks are out there
  - ☑ Many different types to consider
- ☑ Assets are also varied
  - ☑ Data, physical property, computer systems
- ☑ Prevent security events, minimize the impact, and limit the damage
  - ☑ Security controls

Security Controls

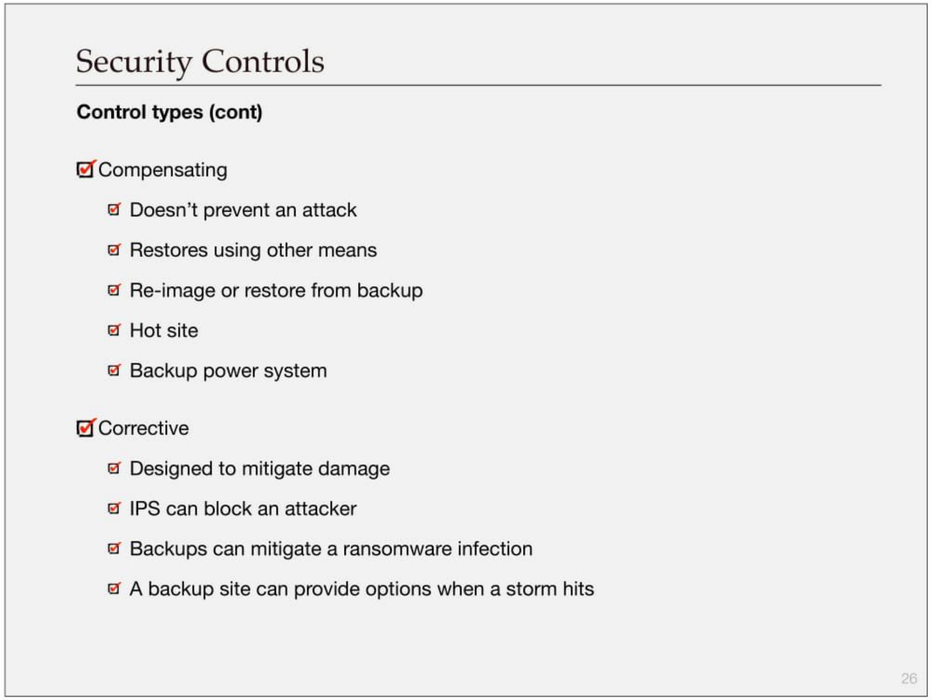
Control types

- ☑ Technical control types
  - ☑ Controls implemented using systems
  - ☑ Operating system controls
  - ☑ Hardware devices
- ☑ Administrative
  - ☑ Controls that determine how people act
  - ☑ Security policies
  - ☑ Standard operating procedures
- ☑ Physical
  - ☑ Fences, locks, mantraps
  - ☑ Real-world security

Security Controls

Control types (cont)

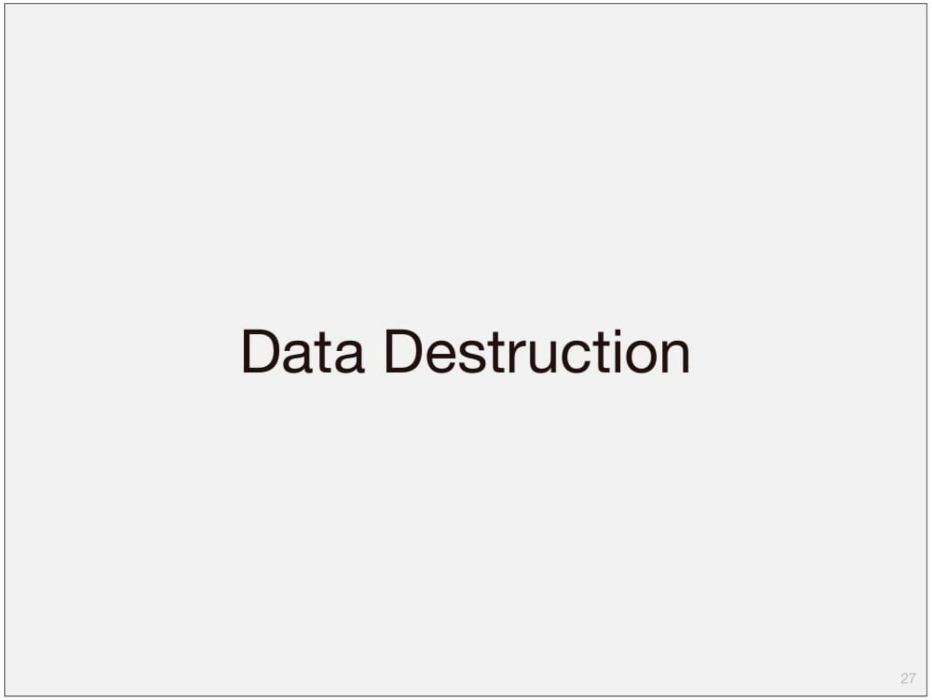
- ☑ Deterrent
  - ☑ May not directly prevent access
  - ☑ Discourages an intrusion attempt
  - ☑ Warning signs, login banner
- ☑ Preventive
  - ☑ Physically control access
  - ☑ Door lock
  - ☑ Security guard
  - ☑ Firewall
- ☑ Detective
  - ☑ May not prevent access
  - ☑ Identifies and records any intrusion attempt
  - ☑ Motion detector, IPS



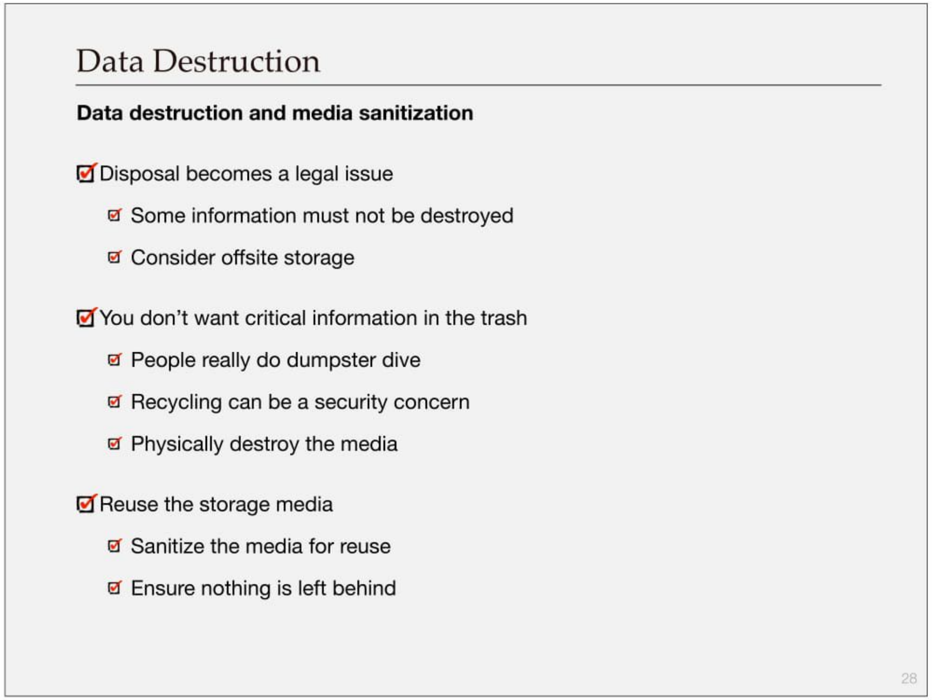
Security Controls

Control types (cont)

- ☑ Compensating
  - ☑ Doesn’t prevent an attack
  - ☑ Restores using other means
  - ☑ Re-image or restore from backup
  - ☑ Hot site
  - ☑ Backup power system
- ☑ Corrective
  - ☑ Designed to mitigate damage
  - ☑ IPS can block an attacker
  - ☑ Backups can mitigate a ransomware infection
  - ☑ A backup site can provide options when a storm hits



Data Destruction



Data Destruction

Data destruction and media sanitization

- ☑ Disposal becomes a legal issue
  - ☑ Some information must not be destroyed
  - ☑ Consider offsite storage
- ☑ You don’t want critical information in the trash
  - ☑ People really do dumpster dive
  - ☑ Recycling can be a security concern
  - ☑ Physically destroy the media
- ☑ Reuse the storage media
  - ☑ Sanitize the media for reuse
  - ☑ Ensure nothing is left behind

Data Destruction

Protect your rubbish

- ☑ Secure your garbage
  - ☑ Fence and a lock
- ☑ Shred your documents
  - ☑ This will only go so far
  - ☑ Governments burn the good stuff
- ☑ Burn documents
  - ☑ No going back
- ☑ Pulp the paper
  - ☑ Large tank washing to remove ink
  - ☑ Paper broken down into pulp
  - ☑ Creates recycled paper

Data Destruction

Physical destruction

- ☑ Shredder / pulverizer
  - ☑ Heavy machinery
  - ☑ Complete destruction
- ☑ Drill / Hammer
  - ☑ Quick and easy
  - ☑ Platters, all the way through
- ☑ Electromagnetic (degaussing)
  - ☑ Remove the magnetic field
  - ☑ Destroys the drive data and the electronics
- ☑ Incineration
  - ☑ Fire hot

Data Destruction

Certificate of destruction

- ☑ Destruction is often done by a 3rd party
  - ☑ How many drills and degaussers do you have?
- ☑ Need confirmation that your data is destroyed
  - ☑ Service should include a certificate
- ☑ A paper trail of broken data
  - ☑ You know exactly what happened

Data Destruction

Sanitizing media

- ☑ Purge data
  - ☑ Remove it from an existing data store
  - ☑ Delete some of the data from a database
- ☑ Wipe data
  - ☑ Unrecoverable removal of data on a storage device
  - ☑ Usually overwrites the data storage locations
  - ☑ Useful when you need to reuse or continue using the media
- ☑ *Just because you delete something does not mean that data is gone*

Handling Sensitive Data

Handling Sensitive Data

Labeling sensitive data

- ☑ Not all data has the same level of sensitivity
  - ☑ License tag numbers vs. health records
- ☑ Different levels require different security and handling
  - ☑ Additional permissions
  - ☑ A different process to view
  - ☑ Restricted network access

Handling Sensitive Data

Data sensitivity labels

- ☑ Public / Unclassified
  - ☑ No restrictions on viewing the data
- ☑ Private / Classified / Restricted / Internal use only
  - ☑ Restricted access, may require a non-disclosure agreement (NDA)
- ☑ Confidential
  - ☑ Very sensitive - Must be approved to view

Handling Sensitive Data

Sensitive data types

- ☑ Proprietary
  - ☑ Data that is the property of an organization
  - ☑ May also include trade secrets
  - ☑ Often data unique to an organization
- ☑ PII - Personally Identifiable Information
  - ☑ Data that can be used to identify an individual
  - ☑ Name, date of birth, mother’s maiden name, biometric information
- ☑ PHI - Protected Health Information
  - ☑ Health information associated with an individual
  - ☑ Health status, health care records, payments for health care, and much more

Data Roles and Retention

Data Roles and Retention

Data roles

- High-level data relationships
  - Organizational responsibilities, not always technical
- Data owner
  - Accountable for specific data, often a senior officer
  - VP of Sales owns the customer relationship data
  - Treasurer owns the financial information

Data Roles and Retention

Data roles (cont)

- Data steward
  - Responsible for data accuracy, privacy, and security
  - Associates sensitivity labels to the data
  - Ensures compliance with any applicable laws and standards
- Data custodian
  - Manages the access rights to the data
  - Implements security controls
  - Sometimes the same person as the data steward
- Privacy officer
  - Responsible for the organization’s data privacy
  - Sets policies, implements processes and procedures

Data Roles and Retention

Data retention

- Keep files that change frequently for version control
  - Files change often
  - Keep at least a week, perhaps more
- Recover from virus infection
  - Infection may not be identified immediately
  - May need to retain 30 days of backups
- Consider legal requirements for data retention
  - Email storage may be required over years
  - Some industries must legally store certain data types
  - Different data types have different storage requirements
    - Corporate tax information, customer PII, tape backups, etc.

CSF 434/534: Advanced Network and System Security

Week 11 - Review

Michael Conti

Department of Computer Science and Statistics
University of Rhode Island

Sources: Professor Messer's CompTIA SY0-501 Security+ Course Notes