COMPTIA SECURITY+ SY0-701 · WEEK 10

Protecting Data, Resilience, and Recovery



Objectives 3.3 and 3.4 · 90-minute lesson

Presenter: Trapper Brown

What you will be able to do in 90 minutes

1. Identify data types, from regulated data to trade secrets, and what makes each sensitive.
2. Apply the six data classification labels to an organization's data.
3. Match a protection method to each data state: at rest, in transit, and in use.
4. Compare encryption, hashing, masking, tokenization, and obfuscation and pick the right one.
5. Distinguish load balancing from clustering, and hot, warm, and cold sites.
6. Plan backups that meet a stated RPO and RTO, and choose how to test them.
7. Explain how capacity planning, generators, and UPS support continuity of operations.

AGENDA

3 min	Why data protection and resilience go together
8 min	Data types
7 min	Data classifications
8 min	Data states, sovereignty, and geolocation
10 min	Methods to secure data
10 min	Exercise 1: label it, state it, protect it
7 min	High availability: load balancing vs clustering
8 min	Site considerations
8 min	Diversity, multi-cloud, COOP, and capacity
6 min	Testing resilience and recovery
12 min	Backups and power
3 min	Wrap-up

Know what kind of data you hold

Data type	What it is	Clinic example
Regulated	Governed by law or binding rules	Patient records under HIPAA
Trade secret	Valuable because it stays secret	Proprietary scheduling method
Intellectual property	Creations protected by copyright or patent	Patient education videos it produced
Legal information	Contracts, case files, legal advice	Malpractice case files
Financial information	Payment card, bank, and billing data	Card numbers under PCI DSS
Human, non-human readable	Text people read vs codes and binary	Visit notes vs a barcode or DB file

Labels tell people how to handle data

Public

Approved for anyone; no harm if disclosed.

Office hours, website text

Private

About individuals; personal and often regulated.

Staff home addresses

Sensitive

Harm if disclosed; needs handling rules.

PII, PHI

Confidential

Approved people only; disclosure causes damage.

Payer contracts

Restricted

Tightest access; named people only.

Encryption keys, legal holds

Critical

Needed to operate; loss stops the business.

EHR database

States, sovereignty, and geolocation

Consideration	Meaning	Typical control
Data at rest	Stored on disks, databases, and backups	Full disk or database encryption
Data in transit	Moving across a network	TLS, IPSec VPN
Data in use	In memory and being processed	Access control, secure enclave
Data sovereignty	Subject to the laws where it is stored	Choose cloud regions by law
Geolocation	Where a user, device, or data is	Block sign-ins from unexpected places

Change the data or limit who reaches it

Transform the data

- Encryption: reversible with the right key
- Hashing: one way; proves integrity
- Masking: hide part, such as all but the last 4
- Tokenization: swap for a token; a vault maps it
- Obfuscation: make data or code hard to read

Restrict access

- Permission restrictions: least privilege on data
- Segmentation: sensitive data in its own zone
- Geographic restrictions: block by location

Label it, state it, protect it



10

MINUTES · PAIRS

For each Lakeside item, give its data type, classification, current state, and the single best protection method.

1. Patient visit notes stored in the EHR database
2. Card numbers the front desk takes for copays
3. A lab result sent to a hospital's system
4. The clinic's hours and phone number
5. A support vendor viewing a patient chart on screen
6. Patient data copied for a developer to test new software
7. Backups kept with a cloud provider in another country

Load balancing and clustering differ

Load balancing

- Spreads requests across independent servers
- Health checks remove failed servers
- Scales out to handle more users
- Fits stateless web front ends

Clustering

- Several servers act as one, sharing state
- Active/passive: a standby takes over
- Active/active: every node shares the work
- Fits databases and file services

Hot, warm, or cold: pay for speed

Site	What is ready	Recovery time and cost
Hot site	Hardware, current data, network, all live	Minutes to hours; highest cost
Warm site	Hardware and network; data must be loaded	Hours to days; moderate cost
Cold site	Space, power, and cooling only	Days to weeks; lowest cost
Geographic dispersion	Sites far enough apart for separate disasters	Survives regional events

Plan for more than one way to fail

Platform diversity

Different vendors or systems so one flaw cannot stop all.

Two firewall vendors in series

Multi-cloud systems

Spread services across providers to survive an outage.

Backups in a second cloud

Continuity (COOP)

Keep essential functions running while systems recover.

Paper check-in during an outage

Capacity planning

Enough people, technology, and infrastructure for demand.

Cross-train a second admin

Test the plan before a disaster does

Tabletop exercise

Talk through a scenario; no systems are touched.

Ransomware at the clinic

Simulation

Act out an event with realistic injects and roles.

Mock outage drill with the staff

Parallel processing

Run the backup system alongside the primary; compare.

Recovery site processes a day's work

Fail over

Actually switch production to the backup system.

Move EHR to the standby server

Backups meet the RPO; restores meet the RTO

Choice	What it means	Watch for
Onsite and offsite	Local copy for speed, remote for disaster	Keep one copy offline or immutable
Frequency	How often a backup runs	Sets the best RPO you can meet
Encryption	Protects backup media and cloud copies	Lost keys mean lost backups
Snapshots	Point-in-time image of a VM or volume	Same storage; not a full backup
Replication, journaling	Copy changes live; log every write	Replication copies corruption too
Generator and UPS	UPS bridges seconds; generator runs hours	Test both under real load

REVIEW

Five questions: write your answers first

1. What is the difference between tokenization and encryption?
2. Name the three data states and one control for each.
3. Of hot, warm, and cold sites, which costs least and takes longest to recover?
4. Why is a VM snapshot not enough on its own as a backup strategy?
5. Backups run every 6 hours and a full restore takes 3 hours. What RPO and RTO can you meet?

TAKEAWAYS

Four things to take with you

01

Know the data first

Type and classification decide how hard you protect each data set.

02

Protect every state

Encrypt at rest and in transit; limit and watch data in use.

03

Buy recovery speed knowingly

Hot, warm, and cold sites trade cost against the RTO you can meet.

04

Untested backups are hopes

Time a real restore and compare it with the RPO and RTO.

NEXT Lab 10: Backup and restore test against an RPO and RTO