MODULE 3 · STUDY NOTES

Data Center Physical Infrastructure - Space

How a data center keeps the wrong people out and uses every square foot: physical security, layered access control, and the white and gray spaces inside

A data center is a physical facility, and this module is about the two things that facility has to get right: keeping the wrong people out, and using every square foot well. The first half builds physical security from the outside in — the three kinds of data center security, the written security policy behind them, and the layered defense that puts a checkpoint at every gate from the perimeter to the server room, combining human access management (access lists, secure access points, biometric access) with technology-based measures (video surveillance and RFID). The second half turns to the room itself, dividing it into white space, where the revenue-generating IT equipment lives, and gray space, where the cooling, power, and mechanical systems that support it live. Because demand for space never stops growing yet the building cannot grow forever, the module closes with the strategies that squeeze the most performance out of both spaces without overcrowding, overheating, or overspending.

LEARNING OBJECTIVES

- Recognize the types of access controls and technology-based measures supporting physical security in a data center
- Recognize the white and gray spaces in a data center
- Identify the best strategies to optimize the use of white and gray spaces in a data center

3.1 Three kinds of data center security

Security and access control are essential components of any data center, and they come in three kinds. **Data security** relates to the information stored within the data center — standards and protocols define the maturity level of each facility. **Network security** defines the security of the network elements installed in the data center and their end connectivity. **Physical security** — this module's subject — targets the internal and external threats to the data center's physical infrastructure.

THE THREE KINDS OF SECURITY

- **Data security** — protects the information stored in the data center; governed by standards and protocols that set each facility's maturity level.
- **Network security** — protects the network elements installed in the data center and their end connectivity.
- **Physical security** — protects the facility and its equipment from theft and physical damage, and ensures only authorized personnel can enter sensitive locations such as the server room.

Physical security measures help ensure two things: that the facility and its equipment are protected from theft and physical damage, and that only authorized personnel can enter the data center and reach sensitive locations such as the

server room. Achieving that reliably takes a *perfect blend of technology, automation, and human intervention* — no single control is enough on its own.

3.2 A layered physical security policy

No data center in the world is secure without a clearly defined physical security policy. The policy's primary goal is to define the protocols and procedures for physically accessing the data center — and it applies to everyone who works there, including external vendors, utility management personnel, and security staff. The specific procedures follow from the kind of **layered security** the data center implements.

> **WHAT THE SECURITY POLICY COVERS**
>
> - Defines the protocols and procedures for **physically accessing** the data center.
> - Applies to all personnel — external vendors, utility management personnel, and security staff.
> - Specifies the procedures to follow based on the data center's chosen layered-security approach.

Layered security offers a level of security at *each* access-control gate. It spans the perimeter of the data center's main gate all the way to the actual server room, ensuring there is no unauthorized access to the innermost layers. Because a single checkpoint could be bypassed, defense is repeated at every zone — main gate, parking lot, lobby, administrative space, utility rooms, and finally the server room. Layered security is built from two elements that work together: **access management** and **technology-based security**.

> **COMMON PITFALL**
>
> Layered security is not one hardened front door. It repeats a level of security at every access-control gate from the perimeter inward, so that breaching an outer layer still leaves an intruder locked out of the inner ones.

3.3 Access management

Access management is the human-facing half of layered security, and it has three parts: the access list, secure access points, and biometric access.

TABLE 3.1 The three parts of access management

PART	PURPOSE	EXAMPLES
Access list	Determines who can access the premises and equipment	Employees, security guards, contractors (technicians, maintenance, gardeners); updated weekly or monthly
Secure access points	Restrict access to sensitive zones and prevent outside intrusion	Badged entry, secured doors, animal traps; sensitive/non-sensitive zones with proximity alerts
Biometric access	Uses personal attributes to digitally identify a person and grant access	Fingerprints, voice recognition, facial recognition; logs entry/exit; verifies background via national ID systems

DETAILS WORTH REMEMBERING

- The **access list** should be updated weekly, monthly, or as often as security accesses change — that is, as staffing needs change.
- **Secure access points** can include creating sensitive and non-sensitive zones that alert staff when someone is nearby.
- **Biometric access** can record the exact time staff enter and exit, and can verify individuals' backgrounds when connected to national ID systems.

3.4 Technology-based security measures

The technology-based half of layered security adds two measures on top of access management: video surveillance and RFID.

Video surveillance protects the exterior and interior walls of the building by recording activity on **closed-circuit television (CCTV)**. Cameras can be placed across many access-control areas — the main gate, parking lot, administrative space, lobby, lift-access areas, utility rooms, and server rooms. The equipment should be able to store data for incident reporting and should include cameras that can pan, zoom, or freeze frames. As a leading practice, recordings are digitally backed up and the surveillance can be controlled remotely.

RFID (radio-frequency identification) aims to alert the responsible management personnel when any asset IDs have been tampered with or are due for maintenance. Each RFID number is connected to a central server and can track assets *without being scanned or checked in*, providing automated, up-to-date statuses.

KNOWLEDGE CHECK – MATCH THE MEASURE TO ITS PURPOSE

The lesson maps each security element to what it prevents: **RFID-based asset management** → prevent tampering with data center assets; **video surveillance** → secure the perimeter walls; **biometric access** → prevent unauthorized access at each layer; **secure access points** → prevent intrusions from the outside.

COMMON PITFALL

RFID does more than label equipment. It actively alerts management to tampering and upcoming maintenance and reports asset status automatically, from a central server, without anyone scanning or checking the asset in.

3.5 The data center as a physical space

A data center is a physical facility that houses IT equipment — servers and storage equipment, network equipment, and various communication equipment — along with the supporting devices that manage IT operations for one or more organizations. To drive efficiency, the facility requires well-coordinated communication between the IT equipment and those supporting devices.

ORGANIZING THE SPACE

- **IT equipment** must be organized in cabinets and racks, accounting for the heat generated, the airflow required, and the power input each cabinet and rack needs.
- **Supporting devices** also need the proper amount of space to perform their various functions.
- The space requirement is **not constant** — it increases as the amount of data increases.

Demand for space keeps rising because data-centric operations keep growing, yet it is not possible to expand a data center endlessly. The remaining option is to make the best use of the *existing* space — but with care. Overcrowding equipment lowers efficiency: crowded equipment generates more heat, which can demand more cooling, which increases cost. To manage space efficiently you first have to know its categories: every data center divides into **white space** and **gray space**.

> **COMMON PITFALL**
>
> Filling every gap to fit more equipment backfires. Overcrowded equipment generates more heat, forces more cooling, and raises cost while lowering efficiency — optimizing space is not the same as cramming it.

3.6 White space

White space is the area dedicated to IT equipment — servers, storage devices, power distribution systems, air-conditioning units, racks, and other network devices. It is the *productive* area of the data center, so during expansions it fills quickly with servers and associated equipment. Fitting an ever-increasing number of servers into a confined area is one of the biggest challenges data center administrators face.

> **ANALYZING THE WHITE SPACE REQUIREMENT**
>
> - Analyze the requirement based on **high, medium, and low equipment density**, then focus on the best use of the analyzed space.
> - Include a well-laid **rack plan** and determine the **rack units** at the initial design stage.
> - Remember that racks and cabinets **do not share the same specifications** — even cabinets of a similar size vary in internal structure by make.
> - Consider **future requirements, cost, and power consumption** when choosing racks and cabinets.

INCREASING THE WHITE SPACE	DESIGNING THE WHITE SPACE
white space is the productive, revenue area ▪ Maximize the amount of white space during the initial design phase. ▪ Use **virtualization** to replace less efficient IT equipment with a smaller amount of highly efficient equipment. ▪ Focus designs on the best space use — more white space means more revenue. ▪ Adding physical locations forces adding equivalent gray space, which raises cost — not the optimal way to grow.	*hard to change once cables are in* ▪ Lay a **cable structure** that fits present and future power consumption. ▪ Plan areas so **airflow is not obstructed**. ▪ Weigh **environmental factors** — temperature, humidity, seismic zone, atmospheric disturbances. ▪ Match **cabinets and racks** to the data center's actual needs.

DESIGNING FOR ENVIRONMENTAL RISK

Environmental factors shape where and how white space is built. Ideally a data center is not located near a seismic zone or in areas frequently hit by floods and storms; if it is, special measures apply — for example, setting up a **disaster recovery (DR) site** in a different seismic zone or on the cloud. Building precautions include sourcing information from meteorological departments, installing pumps to remove flood water, and fitting backflow valves to stop flood water entering from the sewage system.

COMMON PITFALL

The intuitive way to get more white space — add another building — is the wrong one. Each new white space demands an equivalent new gray space to support it, which drives cost up; virtualization and efficient equipment increase usable white space without that penalty.

3.7 Gray space and its relationship to white space

Gray space holds the various electrical and mechanical equipment that makes up a data center's backend support systems: cooling systems, switchgears, generators, uninterruptible power supplies (**UPSs**), and chillers. Uninterrupted performance depends on well-installed, well-maintained gray-space equipment, so it is important to hire qualified engineers who are experts in installing and maintaining it.

TABLE 3.2 White space vs gray space

DIMENSION	WHITE SPACE	GRAY SPACE
Houses	All IT equipment — the productive area	Electrical and mechanical backend support systems
Examples	Servers, storage, racks, network devices, power distribution systems, AC units	Cooling systems, switchgears, generators, UPSs, chillers
Role	Runs the workloads that generate revenue	Powers, cools, and supports the white space — and monitors it
Sizing	Maximize during initial design — more white space, more revenue	Sized in proportion to the white area; grows as servers grow

HOW WHITE AND GRAY SPACES RELATE

- The equipment in the white area is **handled and monitored from the gray area**.
- The gray area is **sized based on the size of the white area** — it is a dedicated support area for the white space.
- If the number of servers in the white space increases, the **support equipment in the gray space increases in proportion**.
- Existing space must be optimized to achieve **efficient white and gray spaces**.

KNOWLEDGE CHECK – WHICH SPACE?

Sorting equipment into the two categories: a **server** → white space; a **power distribution system** → white space; a **switchgear** → gray space; an **uninterruptible power supply (UPS)** → gray space. The rule of thumb: revenue-producing IT gear is white; the electrical and mechanical systems that support it are gray.

3.8 Space-use strategies

Seamlessly integrating the white and gray spaces gives a data center better performance and throughput. The strategies split by which space they optimize.

OPTIMIZE WHITE SPACE USE	OPTIMIZE GRAY SPACE USE
get more work out of the productive area	*get more out of the support systems*
▪ **Virtualization software** — an interface between the IT equipment and managers that surfaces performance data. ▪ **Infrastructure management tools** — DCIM software for estimates, predictive analysis, and cost-efficient methods. ▪ **Proper planning** — a thorough layout for every entity and piece of equipment avoids complications. ▪ **Making use of the cloud** — centrally manage related resources and equipment. ▪ **Adopting SSDs** — faster storage, very low latency, higher reliability and durability. ▪ **Avoiding old power strips** — new equipment should use the strips its own specs recommend.	▪ **Momentum** — machinery that keeps moving during power fluctuation produces extra power the UPS can use; **flywheel** technology boosts this momentum. ▪ **Solar energy** — a renewable, cost-effective source where geography and climate allow. ▪ **Cooling alternatives** — economizer modes that use outdoor air in colder months, cutting investment and running costs.

ECONOMIZER MODE, CONCRETELY

Instead of an expensive cooling solution running full time, a data center can use several *economizer modes* matched to the local climate. During colder months it draws in outdoor air, which lets refrigerant-based components such as chillers and compressors shut off or run at reduced capacity — less investment and lower running costs.

COMMON PITFALL

On a "which optimize white space?" question, watch the distractors. **DCIM tools, the cloud, and avoiding old power strips** (plus virtualization, SSDs, and proper planning) optimize *white* space; **solar energy and cooling alternatives** optimize *gray* space; and **reducing power fluctuations** is not one of the strategies at all.

Module summary

- Data center security comes in three kinds — data, network, and physical; physical security protects the facility and equipment from theft and damage and keeps unauthorized people out, blending technology, automation, and human intervention.
- A written security policy defines the protocols for physically accessing the data center for all personnel; layered security then puts a level of protection at every gate from the perimeter to the server room.
- Layered security has two elements: access management (access list, secure access points, biometric access) and technology-based security (video surveillance on CCTV, and RFID asset tracking).

- Biometric access identifies people by fingerprint, voice, or face, logs entry and exit times, and can check backgrounds via national ID systems; RFID alerts staff to tampering or due maintenance and tracks assets from a central server without scanning.
- A data center is a physical facility housing IT equipment and supporting devices; space demand always grows but cannot expand endlessly, so the existing space must be optimized — overcrowding raises heat, cooling, and cost.
- White space houses all IT equipment (servers, storage, racks, network devices, power distribution systems) and is the productive, revenue-generating area; it is analyzed by equipment density and planned with rack units, cable structure, airflow, and environmental factors.
- Gray space houses the electrical and mechanical backend — cooling systems, switchgears, generators, UPSs, chillers; it is monitored from, and sized in proportion to, the white space, growing as servers grow.
- Optimize white space with virtualization, DCIM tools, proper planning, the cloud, SSDs, and correct power strips; optimize gray space with captured momentum (flywheels), solar energy, and economizer cooling modes.

Review questions

1. **What are the three kinds of data center security, and which one does this module focus on?**

   Answer: Data security (stored information), network security (network elements and connectivity), and physical security (the facility and equipment). The module focuses on physical security.

2. **What does a layered security approach achieve, and what are its two elements?**

   Answer: It provides a level of security at every access-control gate from the perimeter main gate to the server room, so no one reaches the inner layers unchecked. Its two elements are access management and technology-based security.

3. **Compare the roles of video surveillance and RFID.**

   Answer: Video surveillance records activity on CCTV to protect the building's exterior and interior walls and support incident reporting; RFID tracks assets from a central server and alerts management when asset IDs are tampered with or due for maintenance, without scanning or check-in.

4. **Distinguish white space from gray space, with examples of each.**

   Answer: White space is the productive area holding IT equipment — servers, storage, racks, network devices, power distribution systems. Gray space holds the electrical and mechanical backend — cooling systems, switchgears, generators, UPSs, and chillers.

5. **Why can't a data center simply keep expanding, and what problem does overcrowding cause?**

   Answer: Physical space cannot grow forever, so the existing space must be optimized; overcrowding equipment generates more heat, which requires more cooling and increases cost while lowering efficiency.

6. **Sort these into white or gray space: server, switchgear, UPS, power distribution system.**

   Answer: Server → white; power distribution system → white; switchgear → gray; UPS → gray.

7. **Give three strategies to optimize white space use and three to optimize gray space use.**

   Answer: White: virtualization software, DCIM tools, proper planning, the cloud, SSDs, avoiding old power strips (any three). Gray: capturing momentum with flywheels, solar energy, and economizer cooling modes.