LERNER SOLUTIONS

IT PLAYBOOK WIRED FOR GROWTH

Field Guide to Scale from 1 to 100 Locations



Client Since 2020



WELCOME

What's Inside?

01 Strategy & Standards 3

Core Principles 4
Expansion Contexts 6
Process Overview 7
Project Management 8

02 Infrastructure Design 9

IT Design Overview 10
IT Design Parameters 12
ISP Strategy 15
Network Engineering 16
Security & Risk 19

03 Hardware & Systems 20

Hardware Overview 21
Core Hardware & Systems 23
End-User Devices 25
Integrated Systems 27

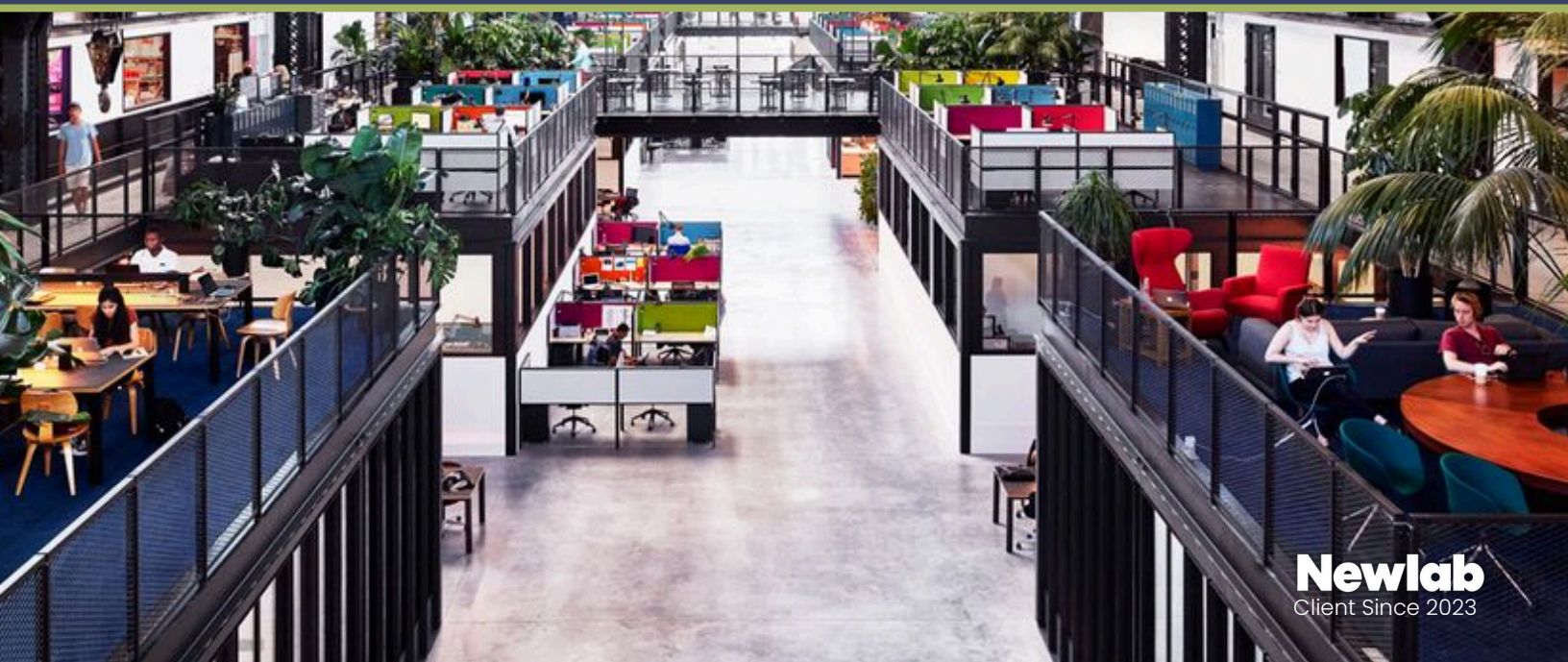
04 Deployment & Operation 30

Installation 31
Standards & Playbooks 33
Support & Maintenance 35

SETTING THE STAGE

01
SETTING THE STAGE

Core Principles
Expansion Contexts
Process Overview
Project Management



CORE PRINCIPLES



These are the foundational principles that determine whether your physical expansion becomes a repeatable growth engine—or a growing pile of exceptions, rework, and operational drag.

01 Make Expansion Boring Again

Early decisions are often made to get one location open quickly. At scale, those same decisions get repeated dozens of times. If a choice does not hold at 50 or 100 locations, it is a temporary solution—even if it works today. *The goal is not to make Site #1 perfect, but to make Site #100 boring.*

02 Design for Context

There is no single "best" IT design. Decisions must be driven by business context, not preference or habit. Design priorities should be determined by role of site in the business, industry (retail vs. warehouse vs. specialty), expansion velocity and other key context.

03 Hardware is a Design Input

Hardware is not an implementation detail. It is a design input. Decisions about networking gear, AV systems, access control, security, digital signage, and specialty equipment dictate space requirements, power, cabling, mounting, and lead times.

04 Supportability is a Design Input

Support is not downstream. It is a design input. If a system cannot be supported & managed remotely across dozens of locations, it should not be designed that way at the first site. Hardware choices, network architecture, and vendor decisions all determine how incidents are handled later.

05 IT as a Construction Discipline

IT for physical expansion is not a back-office function. It must be treated with the same rigor as architecture, electrical, and other mission critical trades. If IT is not included early or doesn't have detailed drawings incorporated into the blueprint, it will be improvised in the field.

06 Default to Scalability

Scalability manages the friction of growth. It requires commercial-grade infrastructure to provide the reliability and remote oversight needed to support a massive footprint with a lean team. If a solution requires manual "one-offs" to deploy or maintain, it isn't scalable. It's technical debt that kills expansion velocity.



Client Since 2018

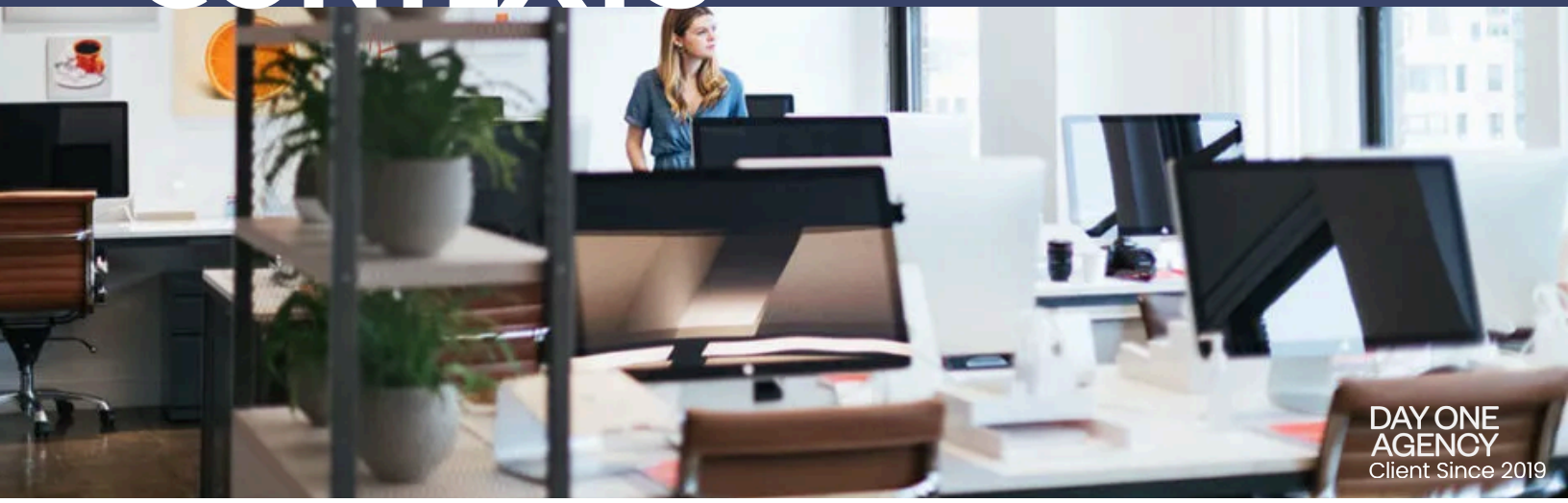
Expansion Reality Check

The Design Test
If you were starting construction on a new location tomorrow, could the GC build it and the install team implement it without clarification?

The Scale Test
If you doubled your location count in the next 12 months, would your IT design, hardware choices, and support model still hold—or would exceptions start to pile up?

The Visibility Test
If a critical system went down at a live site right now, could you diagnose the issue remotely and know exactly who owns resolution within minutes?

EXPANSION CONTEXTS



TL;DR Context determines which IT decisions actually matter, because the same hardware or network choice can be either harmless or catastrophic depending on how fast you're scaling and what failure costs the business.

The Pros & Cons of Using Industry As Context

Industry is often the first lens used to guide IT decisions, and it can be a useful starting point when making early assumptions about risk, scale, and operational needs.

Pros

- Short-hand signal on common uptime sensitivities and exposure patterns
- Reasonable baseline for device density, security posture, and support
- Useful shorthand during early planning, budgeting, or vendor discussions

Cons

- Breaks down with scale as operating models diverge within the same industry
- Ignores expansion velocity, which often matters more than industry itself
- Encourages over- or under-engineering when treated as a primary input

Another Way to Think About It

A more reliable way to make IT decisions is to focus on expansion velocity and what failure actually costs you. These factors determine how much standardization, redundancy, and operational rigor are required, regardless of industry.

- **Expansion Velocity:** Determines how much variance, discretion, and installer judgment the organization can tolerate
- **Downtime Impact:** Determines how much redundancy, automation, and cost are justified

Together, they're a lens that maps to hardware standards, network design, and security posture.

PROCESS OVERVIEW

1 Design Phase
IT Design Team + Client + Architect

When: Once site assumptions are known, running in parallel with architectural design

Role of IT: Help client understand possibilities; recommend systems & preliminary bill of materials; Ensure IT requirements are in floor plans, ceilings, elevations, and back-of-house layouts

Key Output: "Design Set" to incorporate into architectural drawings

Key rule: "Design Set" must remove ambiguity before construction drawings are finalized.

2 Construction Set
IT Design Team + Client + Architect

When: Once finishes, wall types, and ceiling conditions are locked

Role of IT: Lock exact bill of materials, including device SKUs/quantities; finalize mounting details, cable paths, rack layouts, and termination points. Coordinate with architects so IT elements are buildable and permitted

Key Output: Convert the "Design Set" into a "Construction Set"

Key rule: If it is not in the "Construction Set," it will be decided in the field.



3 Handoff to PMs
IT Design → PM

When: Once "Construction Set" and bill of materials are approved

Role of IT: Transition ownership to project management. Validate scope boundaries, source of truth, and responsibilities across trades

Key rule: Design ownership must transfer cleanly, or decisions will drift.

4 Field Install
PM + GC + Field Install + Vendors

When: Once construction and installation activities begin on site

Role of IT: Ensure installers execute against the approved "Construction Set." Prevent design decisions from being made in real time. Route all deviations through project management

Key rule: Installers execute designs. They do not improvise without approval.

PROJECT MANAGEMENT

TL;DR The most expansion failures are coordination failures, not technical ones. Clear ownership, disciplined handoffs, and tight change control matter more than tool choice once construction starts.

Project Management as Driver

IT success during expansion is less about technology choices and more about execution discipline. Most failures do not come from choosing the wrong hardware or platform; they come from unclear ownership, missed handoffs, and decisions drifting downstream into the field. Without tight coordination, IT decisions get made implicitly—by architects, GCs, or installers, often without full context, which leads to expensive rework.

Ownership & Coordination

Expansion succeeds when ownership is explicit and handoffs are structured. Without this rigor, IT decisions are made implicitly by architects or GCs without the necessary technical context.

- **Explicit Ownership:** Clearly define which stakeholders own design, procurement, configuration, and field validation to eliminate accountability gaps.
- **Scope Boundaries:** Document clear lines of responsibility between IT, Facilities, and external vendors to prevent "mid-build" surprises.
- **Field Trust but Verify:** Use trusted technicians for repeating work to ensure the "Lerner Standard" is maintained without constant oversight.



Design Integrity & Handoffs

PM Involved Early
Project Management must be involved early on during the design phase to ensure alignment.

Pre-Install Review
Validate scope, drawings, and schedule with the GC and installers before field work begins to identify site constraints early.

Integrity Enforcement
All field deviations must be routed back through Project Management for formal review rather than allowing ad hoc fixes that create permanent variance.

The Inefficiency Tax
Effective governance recovers the ~12% of project budgets typically lost to coordination failures and poor management practices.

02
INFRASTRUCTURE DESIGN & SECURITY

IT Design Overview
IT Design Parameters
ISP Strategy
Network Engineering
Security & Risk



Client Since 2024

IT DESIGN OVERVIEW

TL;DR IT design defines the big decisions that must be locked before construction and installation begin. Its job is to translate business context into a repeatable technical intent that can be executed consistently across sites.

Design Is Where Scale Is Decided

In physical environments, flexibility disappears early. Once walls, power, ceilings, and conduit paths are set, most IT decisions are effectively frozen. Treating IT as something that can be "figured out during install" works for one site. At scale, it guarantees variance.

Good design is not just documentation—it is early decision-making that removes ambiguity from execution.

The 2 Stage Design Process

Because physical expansion locks decisions in stages, we intentionally split IT design into two sets.

- **Design Set (Early / Conceptual):** The design set defines device locations, coverage assumptions, system types, cable/rack locations, and budgetary scope early, while preserving flexibility for vendor and product changes.
- **Construction Set (Final / Buildable):** The construction set locks exact models, quantities, cable/rack details (e.g., ports) and mounting details so the site can be permitted, built, and installed without interpretation.

What IT Design Must Decide

Network Architecture
Designed in tandem with the NetEng team to define topology, segmentation, and redundancy posture based on transaction criticality, security requirements, and expected expansion velocity.

Hardware Classes
Lock network, AV, security, access control, and specialty system classes early to align cost, lead times, and operational support across all locations.

Closet Strategy
Determine IDF/MDF locations, sizing, power, cooling, and access based on site role, square footage, and long-term serviceability.

Pathways & Mounting
Specify conduit paths, backer requirements, ceiling conditions, and mounting assumptions to support current use cases and future technology additions.

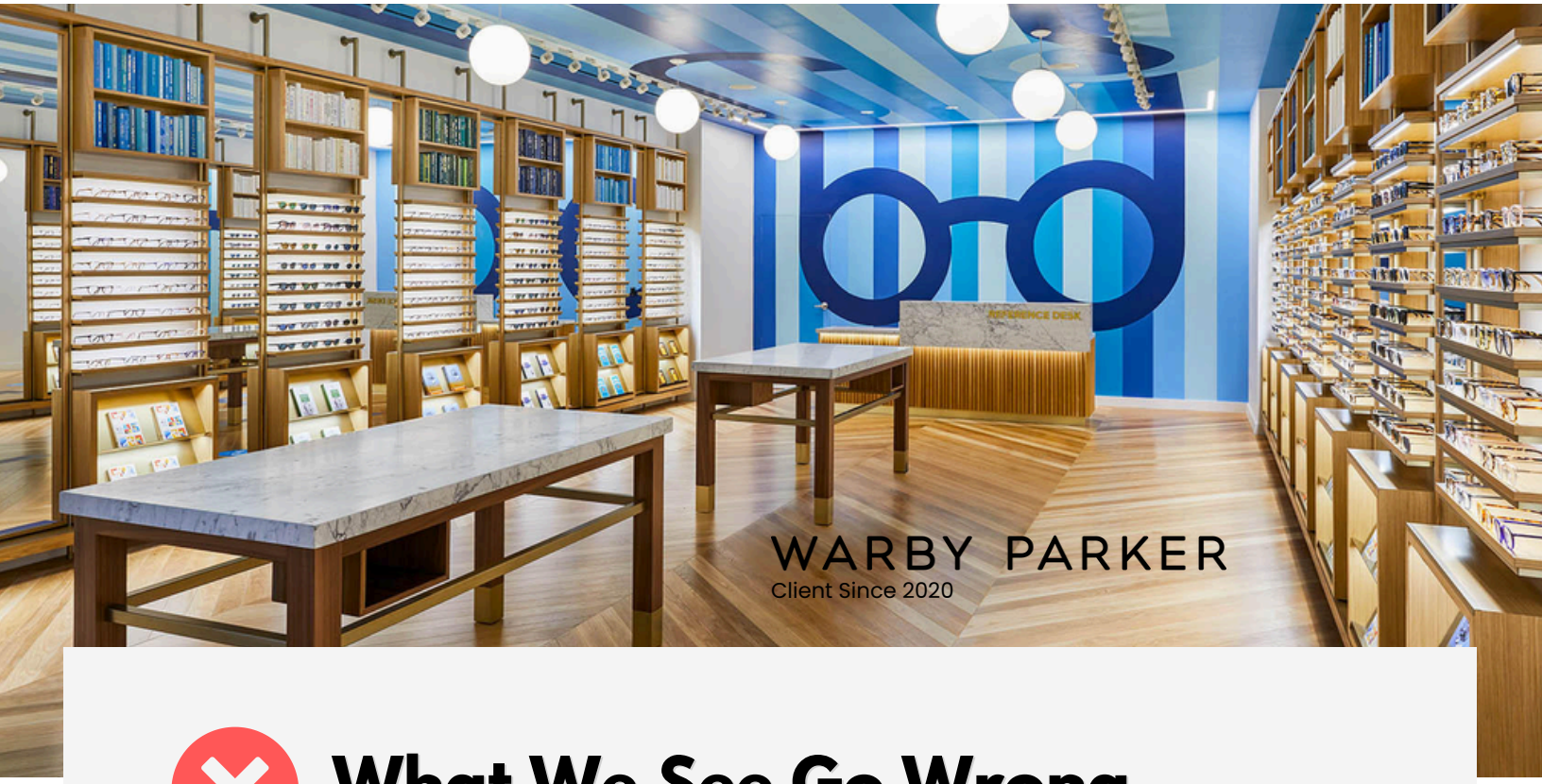
ISP Assumptions
Establish primary connectivity, failover strategy, and carrier lead times in line with downtime tolerance, site criticality, and go-live timelines.

Design Details That Enable Efficiency & Scale

Effective IT design produces artifacts that non-IT teams can execute against:

- Annotated floor plans and ceiling plans
- Standard detail sheets (APs, cameras, displays)
- Reusable site templates by location type
- Bill of materials aligned to drawings

If design lives in email, tickets, or tribal knowledge, it will not scale.



What We See Go Wrong

Reactive Timeline
IT design often begins only after architectural drawings are finalized, forcing expensive retrofits and compromising infrastructure placement.

Deferred Hardware Decisions
Critical equipment choices are frequently delayed until the installation phase, leading to disorganized site execution and unpredictable costs.

Siloed Vendor Scopes
Specialty vendors often design in isolation, creating a fragmented stack that lacks cohesive integration and centralized management.

Support-Light Design
Systems are frequently optimized for the speed of the immediate opening rather than the long-term repeatability and remote serviceability required at scale.

IT DESIGN PARAMETERS

TL;DR Design parameters convert intent into specific, enforceable constraints that eliminate installer judgment. They define the exact inputs that must appear on plans so execution can be repeated without reinterpretation.

Basic vs. Advanced IT Design

Advanced IT design is the differentiator between a site that is merely "connected" and one that is strategically built for scale.

While basic designs focus on coverage, advanced design focuses on environmental constraints—thermal, structural, and spatial—that are often ignored.

Working with a qualified partner like Lerner ensures that these "invisible" details are codified directly into the construction plans, eliminating the suboptimal field improvisation that leads to permanent operational drag.

Design Integrity Checklist

Mechanical Schedule
Does the HVAC schedule explicitly account for the IT closet's BTU/hr load?

Dedicated Circuits
Are IT receptacles labeled on the Electrical plan as specified amperage & outlet type?

Blocking Detail
Does the Architectural "Wall Type" schedule specify 3/4" fire-rated plywood for IT walls?

Path of Travel
Is the conduit route from the MPOE to the MDF clearly traced on the floor plan?



PELOTON
Client Since 2013

What Must Appear on Design Plans

The following are design details that should be visible on drawings, not implied or handled verbally. These are commonly missing from low-rigor designs. If these details are not on the plans, they will be decided suboptimally on site.

Devices & System Assignment
- Device type and role
- Device quantity per area
- Association to system class

Device Placement & Mounting
- Exact placement, not just schedule
- Mounting surface and orientation
- Mounting heights by device type

Closets, Racks & Physical Layout
- Exact rack location and orientation
- Front and rear service clearances
- RU allocation by system class
- Wall-mounted vs floor-mounted
- Door swing conflicts resolved

Power & Electrical
- Circuit quantity and type per rack
- Protected vs unprotected loads
- PoE budget assumptions per switch
- UPS placement and supported equipment

Ceiling & Mounting
- Mounting heights by device type
- Ceiling condition (ACT, hard lid, open)
- Backing or bracing requirements
- Plenum vs non-plenum cabling assumptions

Pathways & Cabling
- Conduit routes and sizes
- Homerun vs consolidated cabling strategy
- Service loop expectations



THE 15% RULE

Every rack and patch panel should be designed with 15% open capacity. This prepares for specialty tech (sensors, AI cameras, new POS) that will be added mid-lease; the cost of over-provisioning a rack today is 1/10th the cost of an uprade later.

Lessons Learned by Lerner Solutions

- **Serviceability Zones:** Drawings must include a "Hatched Service Zone" (36" deep) in front of all racks. This provides a visual "No-Fly Zone" for other trades (plumbing, electrical) to prevent encroachment on the IT service path.

- **MPOE Pathing Ownership:** Don't let the carrier "figure it out." Specify the exact 2" conduit path from the street to the MDF on the site plan; without this, carriers will take the path of least resistance, often creating "nightmare" cable runs through public spaces.

- **BOH Drop Density**: Always double the data drops at the manager's station and staging areas. Underspecifying Back-of-House (BOH) leads to the "Spiderweb Effect"—unmanaged 5-port switches and power strips that become the highest source of failure.

- **Growth Headroom:** Growth headroom must be explicitly reserved across core systems (rack space, switch capacity, PoE budget, AP density, and power) so expansion does not require redesign or field retrofits.

Technical Design Standards

A qualified design firm takes a stance on these variables to eliminate "tribal knowledge." Below are the recommended engineering standards that must appear on the Construction Set to ensure site-to-site uniformity.

Parameter	Recommendation	Why it Matters	Allowable Exception
Mounting Heights	Explicitly specified per device and per location	Eliminates field guesswork and ensures brand aesthetic across 100+ sites.	ADA-specific requirements or landlord-mandated height restrictions.
Closet Minimums	4' x 6' footprint; No shared storage with janitorial/wet utilities.	Prevents hardware overheating and accidental water/chemical damage.	Micro-sites using secure, ventilated wall-mount swing racks.
Rack Orientation	Side-mount or Center-room; 36" front clearance.	Ensures technicians can service cabling without dismantling the rack.	Shallow 2-post racks in space-constrained closets.
Ceiling Mounts	T-Bar clips for drop ceilings; Threaded rod for open-plenum.	Prevents "drifting" APs and cameras; ensures rigid alignment for AV.	Industrial warehouses requiring custom beam-clamp mounts.
Termination	Category 6; ANSI/TIA-568-C.2 B-Wiring standard.	Standardizes signal pair logic for remote cable testing and POE delivery.	Existing legacy cabling (must be tested/certified to pass).
UPS Strategy	Double-Conversion Online; Minimum 30-min runtime at 50% load.	Cleans "dirty" power and ensures transaction continuity during brownouts.	Temporary pop-ups using basic surge-protected power strips.
Thermal Load	Mandatory BTU/hr calculation; 24/7 dedicated cooling.	Prevents equipment throttling during off-hour HVAC setbacks.	Uncooled closets allowed only for passive gear.
Conduit Diameter	Explicitly specified on wire schedule & fill calculations	Ensures enough "pull-space" for future fiber or additional cabling.	0.5" flex allowed for short "last-inch" drops to furniture.



GAMES

Client Since 2020

ISP STRATEGY

TL;DR Design ISP connectivity for failure, not optimism. Default to dual-path internet where downtime matters, prioritize symmetric business-class circuits, and treat LTE/5G as failover—not primary. If the site can't survive an ISP outage, the strategy is wrong.

ISP Strategy is Design, Not Procurement

ISP strategy must be defined before construction, not when the site is "almost ready." Ignoring ISP lead times is one of the most common causes of delayed openings. Key decisions include:

- Selection aligned to industry, downtime tolerance, site role, and expansion velocity
- Primary connectivity type (fiber, cable, fixed wireless)
- Failover approach (terrestrial vs. cellular)
- Carrier lead times and install dependencies
- Demarc location and power requirements

Circuit Standards by Site Context

Large Office (HQ/Regional):
- *Primary Circuit*: Dedicated Fiber (DIA)
- *Secondary Circuit*: Business Broadband Fiber

Warehouse / Industrial
- *Primary Circuit*: Dedicated Fiber (DIA)
- *Secondary Circuit*: Business Broadband Fiber

Showroom / Small Office
- *Primary Circuit*: Business Broadband Fiber
- *Secondary Circuit*: LTE / 5G Failover

Retail / Restaurant
- *Primary Circuit*: Business Broadband Fiber
- *Secondary Circuit*: LTE / 5G Failover

Readiness Check

Physical Path Diversity
Confirm primary and secondary circuits enter the building through different conduits to prevent a single backhoe cut from taking down both links.

Static IP Allocation
Ensure the primary Fiber circuit includes a /29 or at least one static IP to maintain stable VPN tunnels and remote management reach-back.

Cellular Penetration
For sites relying on LTE/5G failover, verify signal strength inside the MDF; if signal is below -90dBm, consider alternative plan.

Contract Lead Times
Align fiber install dates with the "Power On" date; if the carrier quote exceeds 90 days, immediately trigger the cellular hardware as the "Day-1" temporary primary.

NETWORK ENGINEERING

TL;DR Engineer the network for predictable failures and scale, not theoretical elegance. Standardize segmentation, routing, and QoS patterns so sites behave the same under load and during outages. If behavior differs by site, troubleshooting will fail.

The Logical Foundation

While the physical layer defines the hardware, this section defines the Intelligence of the site: how traffic is segmented, prioritized, and routed both inside the site and across the footprint. These engineering decisions directly determine the "blast radius" of a security event, the site's overall security posture, and the mean-time-to-recovery (MTTR) when a failure occurs.

Core Engineering Standards

These standards define the non-negotiable network behaviors every site must exhibit, regardless of size or location. They exist to constrain blast radius, prevent lateral movement, and ensure issues can be diagnosed and fixed remotely without site-specific knowledge.

- **Layered Segmentation:** Separate Corp, Guest, Devices, AV, and Management into distinct segments to prevent cross-domain impact during outages or compromises
- **Policy at the Edge:** Enforce access by role and segment at the boundary rather than relying on endpoint settings or user behavior
- **Template-First Configs:** Require every site to inherit from a standard baseline; deviations must be justified and tracked to prevent drift
- **Fail Closed:** Place unknown or misclassified devices into restricted segments by default rather than granting broad access due to misconfig

If segmentation differs across comparable sites, standards are not being enforced



Network Engineering Patterns by Site Type

Site Type	Hardware Redundancy	Network Segmentation	Security Policy
Large Office (HQ / Regional)	Redundancy in MDF and all IDFs. Redundant edge and critical switching, UPS for core gear, redundant MDF–IDF uplinks.	Function-based VLANs for Corp, Voice, Guest, Exec, Security, AV, and IoT. Designed to scale across floors and IDFs.	Strict isolation between segments. Guest is internet-only. Management access limited to IT admins with centralized logging.
Warehouse / Industrial	MDF doubled where downtime stops ops. IDFs may use single switches unless justified. Redundant edge only for critical sites. UPS for MDF/core.	Minimal VLANs (Corp, Scanners, OT, Security). OT (robotics/conveyors) and Scanners (WMS tools) are separated to ensure low-latency performance.	OT is logically isolated from Corp to prevent lateral movement. Scanners limited to required services. Guest access typically disabled.
Showroom / Small Office	No blanket redundancy. Single firewall, switch, and APs. Add redundancy only where revenue impact requires. UPS for edge/switching.	Simple segmentation on the firewall. Small number of VLANs separated by firewall (e.g., data, POS, AV, physical security, guest, infrastructure)	Block guests from everything but public internet. Employees lack access to POS and backend infrastructure.
Retail / Restaurant			Guests internet-only. Limited employee access to AV and surveillance. No employee access to POS or core infra.

Day 1 Readiness Check

Segmentation Enforced
Verify device classes land in the correct segments and cannot laterally traverse.

IP Overlap Prevention
Verify that the new site's IP range does not conflict with existing HQ or VPN-connected sites to prevent routing "black holes".

IP Space Allocation
Ensure network segments are sized for 2x the anticipated peak client count to account for future growth.

Perform Wifi Validation Survey
Ensure that wifi signal is strong across all required locations.

Perform Failover Tests
Simulate ISP and power failures and confirm critical systems still operate (e.g., POS).

Quality of Service (QoS) Verified
Stress test with bulk traffic to confirm voice and video remain stable.

Wireless Engineering Defaults

Wireless is often the most visible and criticized layer of the network. These engineering defaults ensure predictable roaming and stable performance while eliminating troubleshooting ambiguity across the fleet.

- **SSIDs by Function:** Use dedicated SSIDs for Corporate, Guest, and Headless Devices (IoT) to ensure authentication methods and security policies match the specific usage.
- **Enterprise Authentication:** Mandate certificate-based or SSO-backed authentication for the Corporate SSID to eliminate shared credentials and improve auditability.
- **Minimum RSSI Enforcement:** Enforce strict signal thresholds to prevent "sticky clients"—where a device stays connected to a distant AP—which reduces roaming-related performance issues.
- **Plan for Stability:** Prefer lower channel widths to avoid WiFi interference and collisions.
- **Plan for Future:** Prefer using WiFi 7 capable WAPs

Fail Condition: Users routinely "fix the Wi-Fi" by toggling their device radios or reconnecting, indicating a fundamental RF misconfiguration or roaming failure.



WARBY PARKER
Client Since 2020

QoS & Traffic Prioritization

Quality of Service (QoS) ensures that real-time business functions degrade last during network congestion or partial impairment. If all traffic is treated equally, latency-sensitive video, voice, and POS workflows will be the first to fail.

- **Protect Real-Time Traffic:** Tag and prioritize VoIP (Voice) and Video Conferencing packets so call quality remains stable even under heavy network contention.
- **Deprioritize Bulk Traffic:** Automatically push large file backups, OS updates, and background syncs below interactive workloads in the priority queue.
- **Guest Last:** Ensure all traffic on the Guest VLAN is always assigned the lowest priority, preventing it from impacting core site operations.

Fail Condition: Routine file uploads or background cloud syncs cause noticeable disruptions, such as jitter or freezing, during voice or video calls.

SECURITY & RISK

TL;DR Security spans both cyber and physical domains. Network controls limit digital blast radius, while access control and surveillance prevent physical compromise and persistence.

Strategy & Recommendations

Cyber Security (Network, Identity, Systems)

- **Segmentation:** Users and devices receive only the access required for their function.
- **Identity as Primary Boundary:** Enforce strong identity controls, including MFA for privileged access. Block unknown or unmanaged devices.
- **Configuration:** Security controls are standardized and enforced via global configuration profiles, not local judgment.
- **Centralized Visibility & Logging:** All core systems log and alert to a centralized platform so events surface globally and immediately.

Physical Security (Access, Cameras, Facilities)

- **Unified Strategy:** Cameras, access control, and related systems are treated as security infrastructure, not facilities tooling.
- **Identity-Linked Access Control:** Physical access is tied to the identity lifecycle (SSO / directory), ensuring access is granted and revoked automatically.
- **Isolated Physical Security Networks:** Cameras and access systems operate on segmented networks with tightly controlled egress.
- **Central Monitoring & Auditability:** Physical events and access logs are centrally monitored and retained for investigation and compliance.

What We See Go Wrong

Default Password Breach
Deploying IoT devices or cameras with factory-default credentials, which are often indexed by automated botnets within minutes.

Network Lateral Movement
Failing to segment POS or security cameras from guest Wi-Fi, allowing a customer to scan and potentially exploit critical systems.

Unencrypted Hardware
Sending laptops to remote sites without disk encryption, turning a lost bag into a mandatory legal disclosure event.

Orphaned Physical Access
Failing to integrate the badge system with the corporate directory (SSO), leading to terminated employees retaining physical access.

03
HARDWARE & SYSTEMS

Hardware Overview
Core Hardware & Systems
End-User Devices
Integrated Systems



HARDWARE OVERVIEW

TL;DR Hardware decisions are context-dependent. The right hardware for a showroom, restaurant, warehouse, or office is different—but within each context, hardware should be standardized aggressively to preserve speed, supportability, and scale.

3 Hardware Layers, Different Constraints

- **Core Systems:** Networking, power delivery, and physical infrastructure form the utility layer of each site and must be standardized aggressively to ensure durability, remote manageability, and consistent installs.
- **End-User Devices:** Laptops, desktops, and peripherals should vary only by role and performance need, with fixed SKUs, defined lifecycles, and standardized accessories to reduce support load and redeployment friction.
- **Integrated Site Systems:** AV, access control, cameras, and signage should be selected based on site operation, but managed through standardized platforms and power models to maintain visibility and supportability at scale.

List of Common Hardware Requirements

Hardware Class	Examples
Network Infrastructure	Firewalls/routers, switches, wireless access points, LTE/5G failover devices
Compute & Edge Devices	On-site servers (if any), edge compute appliances, local controllers
AV & Digital Experience	Digital signage displays, media players, speakers, microphones, conferencing kits
Security & Surveillance	Cameras, cloud/NVR controllers, door controllers, sensors
Access Control	Electronic locks, badge readers, mobile credential readers, keypads
Point of Sale	POS terminals, receipt printers, scanners, payment peripherals
End-User Devices	Laptops, tablets, shared workstations, wall/floor-mounted devices
Closet & Rack Equipment	Racks, patch panels, UPS units, PDUs, environmental sensors
Power & Resiliency	Battery backups, surge protection, generator interfaces

Translating Hardware Strategy onto the Blueprint

Hardware strategy only works if it is translated into drawings that other trades , including the field install team, can execute against. At a minimum, blueprints should clearly communicate:

- **Device Locations:** Where each hardware class is installed, including wall, ceiling, floor, or rack placement.
- **Power Requirements:** PoE versus local power, outlet type, and which trade owns delivery.
- **Mounting Assumptions:** Backer, height, orientation, and clearance requirements.
- **Pathways & Terminations:** Conduit routes, homeruns, and which IDF or MDF devices terminate to.

If hardware appears only in a bill of materials and not on drawings, those decisions will be made in the field, introducing variance, delays, and rework.



What Strategy Must Decide

Hardware Classes by Context
Define approved hardware classes for each expansion context (e.g., showroom, transaction-critical, warehouse) so similar sites deploy the same device categories.

Power & Mounting
Standardize PoE model, wall vs ceiling mounts, rack vs distributed installs to prevent field improvisation and rework.

Procurement
Lock approved vendors, ordering paths, and expected lead times to avoid last-minute substitutions that break standardization.

Lifecycle Expectations
Define refresh horizons and end-of-life assumptions so hardware choices remain supportable as the footprint scales.



What We See Go Wrong

No PoE Standard
Devices rely on local power adapters, creating inconsistent installs, harder troubleshooting, and limited visibility as the footprint scales.

Integrated Tech Ignored
AV, security, access control, and specialty systems are layered in late, forcing compromises around power, mounting, and network design.

Late Hardware Decisions
Power, mounting, and placement assumptions are discovered during install instead of being locked during design.

No Replacement Discipline
Failures result in downtime because spares, lead times, and swap procedures were never defined by context.

CORE SYSTEMS & HARDWARE

TL;DR Core infrastructure hardware is the "utility layer" of site expansion. Scaling requires moving beyond simple hardware selection to a productized stack that enforces lifecycle discipline, predictable power footprints, and remote-first serviceability.

The Physical Foundation

This section defines the standard hardware backbone deployed at every site: routing, switching, wireless, and core physical systems. The goal is to minimize variance while preserving performance headroom and security telemetry.

The playbook provides default guidance, but hardware sizing and specific selections must reflect by its use case & context: site type (office, retail, warehouse, pop-up), business role (revenue-critical vs operational), downtime sensitivity, density, and expansion velocity.

This Section Covers

- Firewall / Router
- Access Switches
- Wireless Access Points
- Network Mgmt & Monitoring Platform
- Power and PoE Delivery
- Physical Security Controllers
- Physical Infra (racks & enclosures)

Hardware Tiering

- **Cisco Meraki (Optimal):** Our general recommendation because it delivers stronger security, a more mature cloud-management platform, and enterprise-grade monitoring and support
- **Ubiquiti UniFi (Adequate):** A tier 2 option that is more cost-effective if budget is the primary driver but you still want reliable performance and a modern network stack
- **Advanced: Cisco Catalyst / Palo Alto Networks:** While Meraki is the standard for 99% of the time, use these alternatives only for rare, high-density environments or hub-sites where specific regulatory, modular redundancy, or complex protocol requirements exceed Meraki's standard design envelope.



Client Since 2021

Hardware Recommendations by Context

Component	Large Office (HQ/Regional)	Warehouse / Industrial	Showroom / Small Office	Retail / Restaurant
Firewall / Router	Meraki MX95/105	Meraki MX85/95	Meraki MX67/68	Meraki MX67C/MX67CW
Switch	Meraki C9300	Meraki MS130/150	Meraki MS130	Meraki MS130
Access Points	Meraki CW9176I	Meraki CW9176I/MR46E	Meraki MR46/CW9172I	Meraki MR46/CW9172I
UPS / Power	Eaton Cloud-Connected UPS (1500VA)	Eaton Cloud-Connected UPS (1500VA)	Eaton Cloud-Connected UPS (750/1000VA)	Eaton Cloud-Connected UPS (750/1000VA)
Mgmt / Monitoring	Cloud Dashboards	Cloud Dashboards	Cloud Dashboards	Cloud Dashboards

Hardware Sizing

Use this as a last sanity check before ordering. If any item fails, expect rework or outages.

- **Firewall Effective Throughput:** Size models based on real-world traffic with all security features (IDS/IPS, AMP) enabled, not "headline" marketing speeds.
- **The 25% PoE Rule:** Ensure the physical switch maintains spare power budget after totaling peak draw for all APs, cameras, and access control.
- **AP Density vs. Square Footage:** Drive model selection by concurrent client count and high-bandwidth usage rather than square footage alone to avoid RF congestion.
- **Physical Infrastructure Clearance:** Confirm racks and cabinets accommodate Cat6A bend radii, provide sufficient airflow, and fit one future expansion cycle.
- **Management Visibility:** Require every core device to be natively visible and capable of alerting within a single primary management platform.

What We See Go Wrong

PoE starvation

Switches selected without accounting for AP density, cameras, or access control wattage requirements, leading to hardware brownouts when high-draw devices peak simultaneously.

The Prosumer Drift

Choosing non-enterprise gear to save upfront CAPEX, resulting in massive productivity losses when hardware fails without a 24/7 replacement SLA or support to resolve it.

Missing Out-of-Band Assets

Failing to include a network-managed UPS or an LTE-capable gateway on the initial build, leaving IT unable to remotely power-cycle or reach hardware during an outage.

Inconsistent Hardware SKUs

Slight model differences across sites that compound into physical spares complexity and "firmware drift" that prevents centralized bulk updates.

END-USER DEVICES

TL;DR Standardize user devices aggressively to reduce support load and onboarding friction. Prefer Apple or Dell business-class endpoints with fixed SKUs. Variance should be role-driven, not preference-driven.

The User Experience Baseline

User devices are one of the highest-volume hardware categories and the largest driver of ticket noise when unmanaged.

The objective is to minimize SKU sprawl, simplify provisioning, and ensure predictable performance across roles. Device choice should vary only by job function, performance requirement, and mobility needs, not individual preference or ad hoc purchasing.

This Section Covers

- Laptops
- Desktops
- Tablets
- Shared / kiosk devices
- Docking stations
- Peripherals (keyboard, mouse, etc.)

Spec Recommendations (2026)

Role	Model	Minimum Specs	Our Rationale
Standard Employee	MacBook Air 14" or or Lenovo T14	16GB RAM 256GB SSD	High-quality, reliable business-grade machines for 90% of roles (sales, marketing, ops, etc.)
Engineer / Designer	MacBook Pro 14" or Lenovo P16	32GB RAM 1TB SSD	These expensive hires. Don't slow them down with an underpowered machine
Executive / Corp	MacBook Air 14" or Lenovo Carbon X1	16-32GB RAM 512GB SSD	Lightweight but still powerful
Warehouse / Field	iPad Pro or Surface Go	Cellular Enabled / Rugged Case	Effective for mobile and high-latency warehouse environments.
Front Desk / POS	Mac Mini or Lenovo Tiny	16GB RAM / 256GB SSD	Dedicated, fixed-purpose hardware to prevent configuration drift at high-traffic entry points.

“Zero-Touch" Provisioning

Hardware selection is only half the battle; the procurement & provisioning method is the other.

- **Zero-Touch Enrollment:** You should mandate that all devices are purchased through a partner's "DEP" (Apple) or "Autopilot" (Windows) portal.
- **The Goal:** This ensures that as soon as a remote user unboxes a device and connects to Wi-Fi, the MDM (Mobile Device Management) profile is pushed automatically.

Peripheral Standards

Standardization fails if the "last inch" of connectivity is neglected.

- **Universal Docking:** Mandate USB-C / Thunderbolt 4 docks to ensure a single-cable experience for power, video, and data.
- **Monitor Standardization:** Standardize on 27" QHD (1440p) displays with integrated USB hubs to reduce desk-underneath cabling.
- **Input Devices:** Deploy "Logi Bolt" or standardized wired sets to avoid Bluetooth interference patterns in high-density offices.

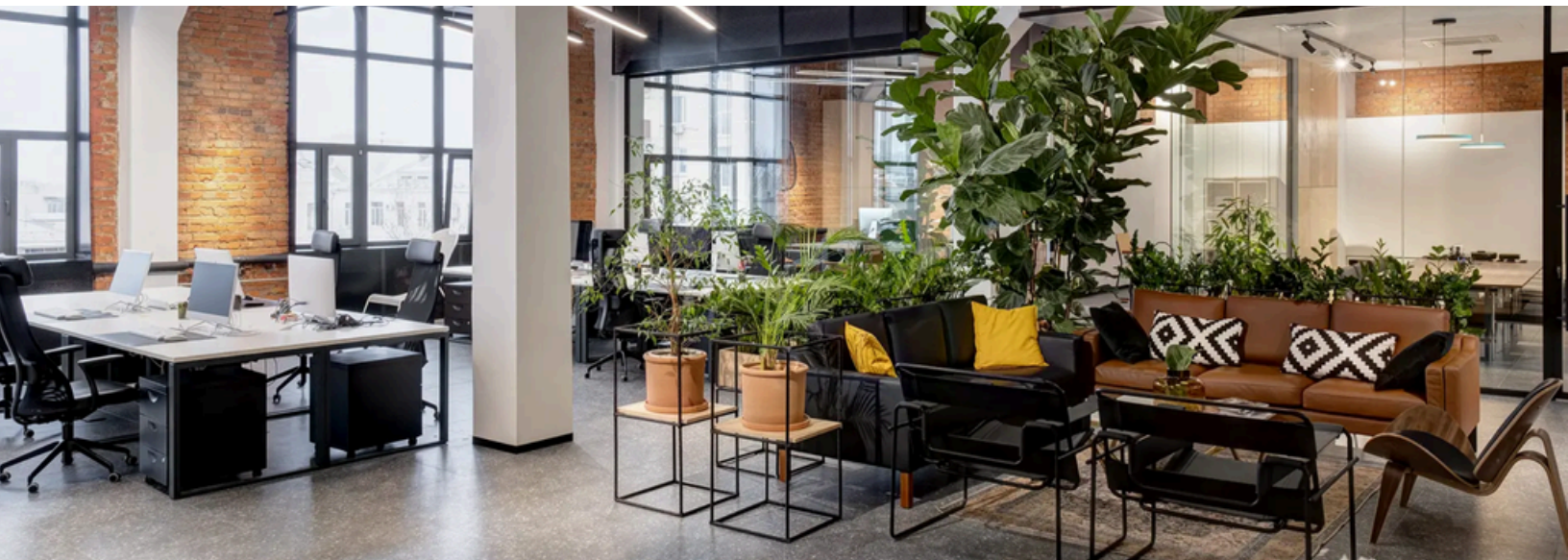
What We See Go Wrong

The Retail SKU Trap
Buying laptops from consumer retail stores that lack enterprise management chips and consistent driver sets.

Dongle Madness
Failing to standardize on a docking station, leading to localized desk-side "workarounds" that increase helpdesk tickets by an estimated 40%.

Under-Specced RAM
Ordering 8GB RAM to save upfront CAPEX, which results in hardware becoming obsolete and causing user frustration within 18 months of deployment.

Peripheral Chaos
Non-standard docks and chargers become the top failure point within months



INTEGRATED SYSTEMS

TL;DR Treat non-network systems as first-class infrastructure, not afterthoughts. Default to Verkada for access control and cameras to minimize vendor sprawl and simplify support. Standardize AV and signage to avoid fragile, site-specific installs.

Integrated Site Subsystems

These systems fail disproportionately when treated as "facilities problems." The objective is to standardize platforms, power, and management so installs are repeatable and issues are diagnosable remotely.

Hardware selection should vary by site type, business criticality, and uptime tolerance, not by GC preference or local vendor availability.

Every subsystem should be network-attached, centrally visible, and owned operationally by IT, even when installed by facilities or third parties.

This Section Covers

- Access Control
- Cameras
- AV / Conference Rooms
- Digital Signage
- Specialty Devices
- Other Sensors

Hardware Recommendations by Context

System	Large Office (HQ/Regional)	Warehouse / Industrial	Showroom / Small Office	Retail / Restaurant
Cameras	Verkada Dome (Indoor) / Bullet (Outdoor)	Verkada Bullet (High Retention/IK10 Rugged)	Verkada Dome (Standard)	Verkada Fisheye (360° Coverage)
Access Control	Verkada AC Controllers w/ HID Signo Readers	Verkada AC Series w/ Rugged Readers	Verkada AC Series (Cloud Managed)	Verkada AC Series (Mobile Credential Optimized)
Meeting / AV	Logi Rally Bar (Large) / Dual Displays	N/A (or Wall-Mount Tablet for Check-in)	Logi Rally Bar Mini (Huddle Rooms)	N/A (or Overhead Audio Interface)
Signage	Apple TV / BrightSign (Dual Screen)	BrightSign (High-Brightness Displays)	Apple TV (4K / MDM Managed)	Apple TV (Fixed Content Kiosk)

Hardware Sizing Validation Checks

Use this as a final sanity check before finalizing the subsystem BOM.

- **PoE+ Allocation:** Confirm the core switch has sufficient PoE+ budget (30W/port) for all cameras and door controllers.
- **Camera Retention:** Validate that onboard storage SKUs match regulatory requirements (e.g., 30/60/90 days) to avoid expensive cloud-backup costs.
- **AV Field of View:** Verify meeting room hardware matches room size; use Rally Bar Mini for huddle rooms and Rally Bar for medium/large rooms.
- **Signage Power**: Ensure every signage display has a designated recessed power outlet and data drop directly behind the mounting bracket.



Lerner's Lessons Learned

- Fewer platforms > marginal feature gains
- Cloud-managed > on-prem NVRs or controllers
- Replaceable components > custom installs



What We See Go Wrong

NVR Vulnerability
Using legacy analog or IP cameras that require a localized NVR, creating a single point of failure.

Franken-AV Rooms
Mixing different brands of webcams, speakers, and mics, leading to 20+ minute delays at meeting starts.

Proprietary Lock-in
Installing access control hardware that requires a localized server and proprietary wiring.

Power Neglect
Failing to put cameras and door controllers on a battery-backed PoE switch, causing the site to go dark during minor power flicks.

Security Controls by Site Type

Site Type	Identity & Access	Network & Physical Protections
Large Office (HQ / Regional)	MFA-backed mobile credentials for employees; automated access reviews on role change; no shared or standing admin accounts	Full east–west controls to block lateral movement; certificate-based authentication for Corp Wi-Fi; management and security systems isolated from user networks
Warehouse / Industrial	Primary identity model optimized for scanners and logistics accounts; ruggedized readers; vendor and admin access time-bound and audited	Hardened north–south controls; IoT and scanner devices confined to restricted VLANs; no direct access to Corp or management networks
Showroom / Small Office	Cloud-managed scheduling for vendor access; guest identities isolated and non-persistent	Client isolation enforced on Guest Wi-Fi; peer-to-peer traffic blocked; AV and demo systems restricted to outbound-only access
Retail / Restaurant	Locked-down kiosk mode for POS; strong identity for managers only; no shared store credentials	PCI-scoped traffic isolated from all non-payment systems; POS networks separated from Guest, Store, and Management; no shared routing or management paths

80%

of Breaches: Involve lost or stolen credentials, making MFA your most critical boundary.

$1.5M

estimated additional cost of a breach in environments without Segmentation Enforced.

25%

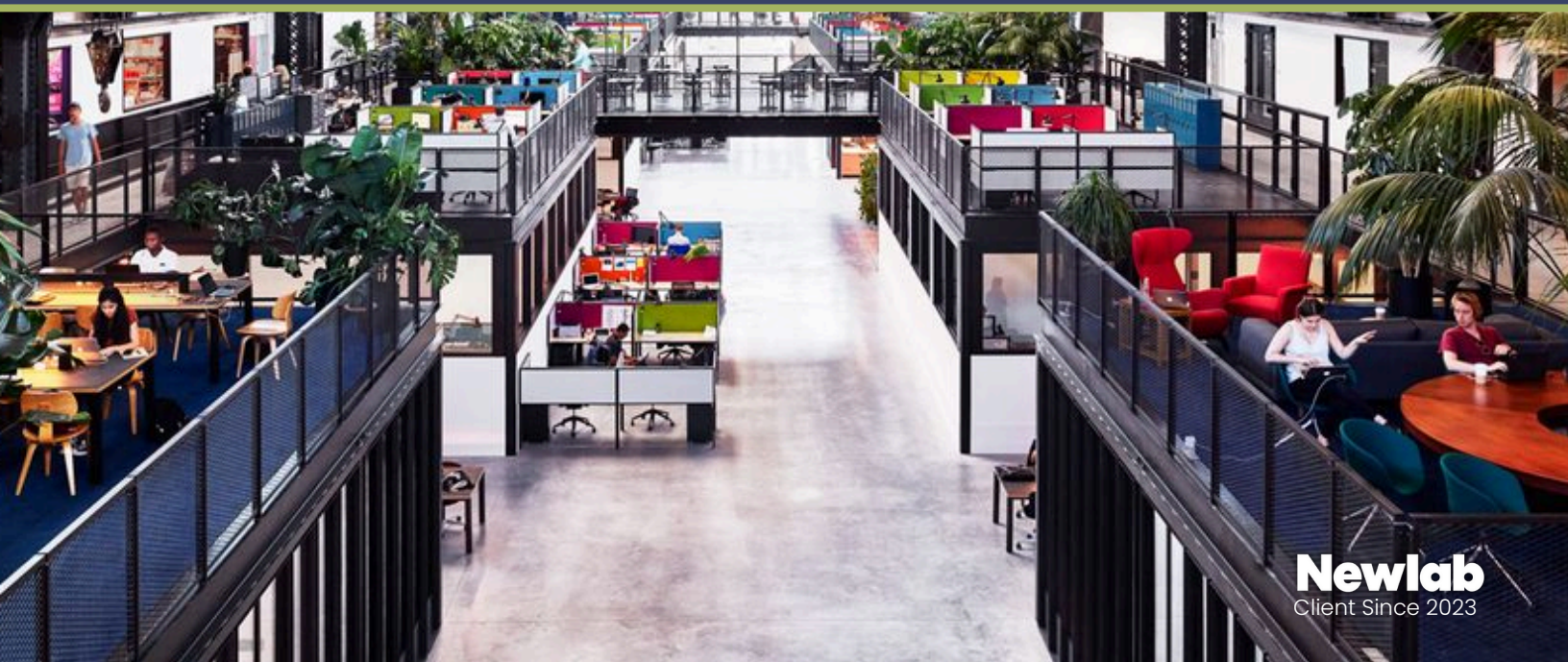
of incidents involve persistent access after role change, highlighting the need for automated access reviews.



LERNER SOLUTIONS

04
DEPLOYMENT & OPERATIONS

Installation
Standards & Playbooks
Support & Maintenance



INSTALLATION

TL;DR Installation is where disciplined design either gets executed cleanly or quietly eroded. Clear sequencing, proper staging, and systematic validation matter more than speed once work hits the field, especially at scale.

Executing the Design in the Field

Implementation should be boring. The objective is not to "solve problems on site," but to execute an approved design with minimal interpretation. At a minimum, effective installs require:

- Hardware staged and validated before arriving on site
- Install sequencing aligned to construction milestones
- Drawings and construction sets treated as the system of record
- No design decisions made by installers in real time

When installation deviates from this model, variance are difficult to unwind.

PM as the Control Plane

Installation succeeds when one owner controls communication, sequencing, and decision flow. The Project Manager is the single point of coordination between IT, trades, vendors, and the business.

- All field questions route through the PM, not solved ad hoc on site
- Design intent is clarified centrally and documented before work proceeds
- No installer judgment calls on power, mounting, placement, or cabling
- Changes require PM approval and update to the system of record
- PM enforces sequencing and validation gates before turnover

What We See Go Wrong

In-Field Decisions
Installers make on-the-spot changes to mounting, placement, or cabling when drawings are incomplete or inconvenient, creating site-by-site variance that is hard to unwind later.

Hardware Arrives Unstaged
Devices show up unconfigured, unlabeled, or mismatched to the drawings, slowing installs and increasing configuration errors under time pressure.

Poor Sequencing
IT work begins before power, ceilings, or finishes are ready, forcing rework and last-minute compromises to stay on schedule.

No Formal Validation
Sites open without systematic testing of network, devices, and integrated systems, pushing avoidable issues into live operations.

1 Before Anyone Shows Up

These prevent improvisation and rework.

- **Site Readiness Confirmed:** Demarc location, rack/cabinet, power, grounding, and pathways verified
- **Hardware Staged:** Firmware pinned, templates applied, labels printed
- **ISP Status Known:** Circuit delivery date confirmed; plan for temporary access
- **Access Coordinated:** Who can open doors, closets, ceilings is documented

2 During Installation

These ensure consistency across sites.

- **Template Enforcement:** No local config changes without approval
- **Clean Physical Install:** Proper mounting, strain relief, airflow, and labeling
- **Power Discipline:** Correct outlets used; no daisy-chaining or temporary power
- **Security by Default:** Unused ports disabled; default creds removed

3 Before Go-Live

A site is not live until it passes these checks.

- **Resiliency Verified:** Primary and failover paths tested; power outage simulated
- **Segmentation Verified:** Devices land in correct VLANs; no lateral access
- **Wireless Verified:** Validation survey; Corp/Guest/Device SSIDs tested under load
- **Monitoring Verified:** Alerts firing; devices visible centrally

4 Handoff Package

These convert an install into an operable site.

- **As-Built Summary:** What was installed, where, and why
- **Logical Diagram:** Segments, paths, and dependencies
- **Credentials & Access:** Stored centrally; no local secrets
- **Support Notes:** Known constraints, open items, next review date



snappy

Client Since 2020

STANDARDS & PLAYBOOKS

TL;DR Standardization is not about exerting control; it is about removing the friction that slows down a pipeline. By defining what is mandatory versus what is adaptable, you transform IT from a custom "project" into a repeatable, high-velocity "product".

How to Build a Playbook That Scales

A scalable playbook is built by capturing decisions as artifacts, not by writing guidance in isolation. The raw material of a playbook is real project work—designs, drawings, checklists, and handoffs that have already survived execution. Effective playbooks are built by:

- Converting recurring decisions into standards once they appear more than twice
- Capturing design intent in reusable design and construction sets
- Turning execution steps into checklists that remove interpretation
- Encoding ownership, scope boundaries, and review points explicitly
- Validating templates through live projects before formalizing them

Playbooks should evolve alongside expansion. Each site should either reuse an existing standard or produce a justified exception that informs the next revision. If a playbook requires explanation to be used correctly, it is not finished.

Playbook Reality Check

Substitution Test
Could a new PM, installer, or MSP execute a site correctly without verbal explanation?

Velocity Test
Does adding locations reduce decision time, or does every new site introduce new debates?

Drift Test
Are sites opening today materially different from sites opened six months ago—and if so, why?

Exception Test
When a site deviates from the standard, is the exception documented, justified, and fed back into the playbook—or quietly forgotten?

Failure Test
When something breaks, does the playbook tell you exactly how to respond, or do people improvise?



What to Standardize vs Where to Allow Variance

Category	Standardize	Allow to Vary	Variance Trigger
Network & Security	Hardware vendor (e.g., Cisco Meraki), core topology, segmentation model, monitoring and alerting standards	WAP counts and locations	Size & floorplan. Geographic serviceability; determine primary and secondary providers
ISP & Connectivity	Connectivity model (primary + failover), activation process, documentation	Access type (fiber, coax, fixed wireless, cellular)	Site location and carrier availability
Point of Sale	Core transaction hardware (POS terminals, printers, scanners), network isolation	Mounting, integrations	Brand aesthetic and store design requirements
Devices & Endpoints	Device classes, OS, security baseline, enrollment method	Size & mounting	Site role and operational workflow
Power & Rack	Rack unit layout, size, form factor, labeling, UPS standards, grounding	Rack location	Site footprint, landlord constraints, back-of-house space
Closet Strategy	IDF/MDF layout principles, access control, cooling assumptions	Closet location and size	Square footage, building layout, and lease constraints
Audio & Visual	Media players, content delivery method, control systems	Screen size, count, orientation	Ceiling height, sightlines, experiential density
Security & Surveillance	Camera platform, retention standards, access model	Camera count and coverage	Risk profile, regulatory requirements, store size
Access Control	Platform, credential type, integrations	Door and reader placement	Site size and access complexity
Integrated Tech	Integration, hardware vendor (e.g, Verkada), & expectations	Device quantity	Size & purpose of location
Installation Process	Sequence, validation, sign-off criteria	None	Process should not vary
Support & Monitoring	Monitoring stack, escalation paths, documentation standards	Onsite support presence	Site criticality and geographic dispersion



SUPPORT & MAINTENANCE

TL;DR Supportability is a design constraint, not a downstream task. A scalable support model relies on remote observability, standardized spares, and predictable failure modes to minimize downtime and eliminate "tribal knowledge" in troubleshooting.

The 5 Key Elements of Designing for Support

Most teams optimize IT for opening day and defer support thinking until problems appear; at scale, this creates brittle environments where small issues consume disproportionate resources. Supportability must be baked into the initial design to ensure long-term stability:

- **Remote Observability:** If a critical system goes down, the team must diagnose the root cause remotely without asking on-site staff to "check the lights" on a router.
- **Centralized Management:** Utilize commercial-grade, cloud-managed platforms to provide visibility into devices and traffic across dozens of locations from a single dashboard.
- **The Visibility Test:** Every site must pass a post-install audit to confirm that network health and device status are reporting correctly before the project is considered closed.
- **Tiered Spares Strategy:** Define a context-driven inventory—ranging from on-site "Crash Kits" for standard retail to "Full Cold Spares" for transaction-critical sites.
- **Field Response Model:** Establish clear SLAs and ownership boundaries between internal IT, Managed Service Providers (MSPs), and on-ground partners.

Support Reality Check

Visibility Test
Can you see network health, device status, and key alerts across every site from a single place?

Response Test
Can most issues be diagnosed and resolved remotely without waiting for site staff?

Repeatability Test
Do similar locations share the same hardware classes, configs, and naming conventions?

Escalation Test
Is ownership clear for what IT handles vs MSP vs vendor vs onsite, with predictable handoffs?

Eliminating Tribal Knowledge

A site is not supportable if it requires the original installer to troubleshoot it.

- **Uniform Configurations:** Establish standard naming conventions and configurations across all similar sites to make troubleshooting predictable.
- **Physical Labeling Standards:** Every cable and port in the MDF/IDF must be labeled to match construction drawings so any technician can understand the layout instantly.
- **The Rework Loop:** If a specific hardware failure recurs, the Design Set must be updated immediately to prevent the error from being "copied" into the next ten locations.
- **Refresh Horizons:** Establish 3–5 year end-of-life cycles to ensure the support model isn't crippled by legacy hardware that no longer supports centralized management

Support & Maintenance Operations Matrix

The following matrix recommends standards to maintain a physical footprint at scale

Sensitivity Context	Observability Standard	Spares Strategy	Field Response Model
Low Sensitivity Pop-ups Small Offices	**Reactive:** Basic cloud-dashboard alerts and email notifications for offline status.	**Next-Day Shipping:** No on-site inventory; rely on vendor RMAs and standard shipping.	**Remote-First:** Troubleshooting is handled 100% centrally; no dedicated field dispatch.
Medium Sensitivity Showrooms Standard Retail	**Proactive:** Real-time dashboard monitoring with automated ticketing for critical failures.	**On-Site "Crash Kit":** Local storage of high-fail, low-cost items (cables, power bricks, peripherals).	**On-Ground Partner:** Tier 1 support dispatched via local partner with a 24-hour SLA.
High Sensitivity Volume Transactions Medical Specialty	**Predictive:** Heartbeat monitoring and "Visibility Tests" to diagnose issues before site awareness.	**Full Cold Spares:** On-site backup for mission-critical gear (Firewalls, Switches, POS terminals).	**Priority Field Engineering:** Dedicated internal or elite MSP response with a 4-hour on-site SLA.



LERNER SOLUTIONS

v1.1

LET'S TALK

Lerner Solutions partners with growth-stage and multi-site businesses to design, deploy, and operate IT environments that scale predictably

Headquartered in New York, we support companies expanding physical footprints where uptime, security, and operational consistency are non-negotiable.

For design reviews, expansion planning, or execution support, contact our Founder & President, David Lerner, at david@lernersolutions.com

