Top 10 Mistakes in Physical Security Installations (and How to Avoid Them)

OGS TECHNOLOGY
TOTAL IT SOLUTIONS

Overview

In the world of physical security, one small oversight can compromise an entire system. As technology advances from IP-based surveillance and biometric access control to integrated command centers it's critical to remember that even the most advanced security setup is only as strong as its design and installation.

---

1. Treating Security as an Afterthought

Many projects treat security as something to "add later," once construction or networking is done. This is one of the biggest mistakes. Security should be integrated from the design phase, alongside electrical, IT, and architectural planning.

How to Avoid It:

Include security consultants early in the design process. Coordinate cable pathways, power requirements, and device locations before walls are closed or ceilings sealed.

---

2. Poor Camera Placement and Field of View

Cameras that face direct sunlight, are mounted too high, or miss blind spots provide a false sense of security, where expensive cameras captured nothing but the tops of people's heads.

How to Avoid It:
Conduct a **site walk** with both a physical layout plan and camera visualization tools. Consider lighting, weather exposure, and mounting height. Always verify the **field of view (FOV)** before finalizing mounts.

3. Ignoring Network Infrastructure

Modern CCTV, access control, and alarm systems rely heavily on **network performance**. Poor switch selection, unmanaged traffic, or lack of VLAN segmentation can cripple your system or open cybersecurity holes.

How to Avoid It:
Use **enterprise-grade PoE switches**, assign **dedicated VLANs for security devices**, and ensure sufficient bandwidth and redundancy. Always coordinate with the IT/networking team for scalability.

4. Using Consumer-Grade Hardware

It's tempting to cut costs by using cheap cameras or unmanaged recorders, but consumer-grade gear lacks the resilience, cybersecurity, and compatibility needed for professional deployments.

How to Avoid It:
Stick to **commercial or industrial-rated equipment**. Look for products with proper certifications, vendor support, and firmware update lifecycles.

5. Neglecting Power and Backup Planning

A system is only reliable if it stays online during outages. Many installers forget to account for **UPS, surge protection, and redundant power supplies**, especially for critical components like recorders and access controllers.

How to Avoid It:
Design a power map for the entire system. Include UPS units, surge protection, and isolated circuits for core equipment. Periodically test your failover plan.

6. Poor Cable Management

Loose or exposed cables don't just look bad they make troubleshooting harder and invite signal interference or damage.

How to Avoid It:
Follow structured cabling standards (TIA/EIA-568). Use **labeled, color-coded, and neatly dressed cables** in conduits or raceways. Maintain accurate as-built drawings for future maintenance.

7. Failing to Secure Network Devices

Many integrators leave default passwords or open ports on security devices. That's an open invitation for hackers.

How to Avoid It:
Change all **default credentials**, disable unused services, and keep firmware updated. Integrate with firewalls, access lists, and monitoring tools to detect unauthorized access.

8. Skipping System Testing and Commissioning

Installing devices isn't the finish line. Without structured testing, you'll miss issues like latency, camera dropout, or faulty sensors.

How to Avoid It:
Perform a **final commissioning checklist**:

- Verify every camera feed.
- Test door access under power loss.
- Confirm alert notifications.
- Validate all configurations against design specs.

Document the results it's part of professional installation.

9. Lack of Integration Between Systems

Access control, CCTV, and intrusion detection often work in silos. This reduces situational awareness and response time.

How to Avoid It:
Design for **integration from day one**. Use platforms that can **unify multiple systems** into a central management dashboard allowing operators to view, control, and respond in one interface.

10. Ignoring Maintenance and Lifecycle Planning

Even the best installation will degrade without proper maintenance. Cameras get dirty, batteries age, and firmware becomes outdated.

How to Avoid It:
Schedule **preventive maintenance** every 6–12 months. Maintain a system health log, plan for

periodic upgrades, and replace aging equipment before it fails.

About OGS Technology

At **OGS Technology**, we believe that precision, planning, and integration are what separate good systems from great ones. Avoiding these ten mistakes isn't just about saving time and cost it's about ensuring peace of mind and long-term reliability.

Contact Us

Email us at: info@ogstechnology.com

OGS Technology.

Address: 155 Meadow Street, Branford, CT 06405.

Phone: (203) 433-4145

Website: www.ogstechnology.com