TOP 10 PHYSICAL SECURITY MISTAKES *(AND HOW TO FIX THEM WITH CAMERAS & ACCESS CONTROLS)*

Physical security is the bedrock of a robust organizational defense. Overlooking its critical components can lead to significant vulnerabilities. Here are the top 10 most common physical security mistakes and how modern cameras and access control control systems can provide effective solutions.

1. NEGLECTING COMPREHENSIVE SURVEILLANCE

Mistake: Insufficient CCTV camera coverage, weak monitoring protocols, and failing to regularly review footage. This includes having "blind spots" or cameras that are improperly placed or maintained, as well as unreliable alarm systems.

Fix: Implement a professional-grade IP camera system with strategic placement to eliminate blind spots. Integrate these cameras with a centralized Video Management System (VMS) that offers advanced analytics (e.g., motion detection, facial recognition, anomaly detection) and real-time alerts. Utilize AI-powered monitoring for proactive threat detection and ensure redundancy for critical equipment.

2. LACK OF ROBUST ACCESS CONTROL

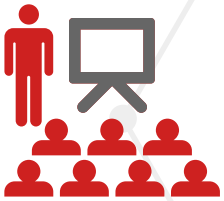
Mistake: Relying on traditional keys, inadequate lock systems, or failing to implement granular access permissions. This also includes issues like stolen identification and the lack of a proper visitor management system.

Fix: Deploy a modern, network-based access control system (ACS) utilizing keycard, biometric (fingerprint, facial recognition), or mobile credentials. Integrate ACS with HR systems for automated provisioning and de-provisioning. Implement multi-factor authentication for sensitive areas and leverage visitor management modules for secure guest entry and tracking.

330 Pony Farm Road, Suite 3
Oneonta, NY 13820

607-433-2200

www.directive.com



3. INADEQUATE EMPLOYEE TRAINING

Mistake: Relying on traditional keys, inadequate lock systems, or failing to implement granular access permissions. This also includes issues like stolen identification and the lack of a proper visitor management system.

Fix: Deploy a modern, network-based access control system (ACS) utilizing keycard, biometric (fingerprint, facial recognition), or mobile credentials. Integrate ACS with HR systems for automated provisioning and de-provisioning. Implement multi-factor authentication for sensitive areas and leverage visitor management modules for secure guest entry and tracking

4. IGNORING PHYSICAL BARRIERS

Mistake: Overlooking the importance of foundational physical barriers like fencing, proper lighting, and secure entryways. This includes failing to address "soft targets" in a building's design.

Fix: Conduct a thorough physical security assessment to identify vulnerabilities in the building's perimeter and interior. Enhance external lighting with motion-activated LEDs. Utilize cameras with low-light capabilities. Implement robust entry points with reinforced doors and access control integration. Design spaces with security in mind, minimizing hiding spots and maximizing visibility.

5. FAILURE TO PLAN FOR EMERGENCIES

Mistake: Lacking comprehensive emergency response plans for various scenarios (e.g., natural disasters, civil unrest, workplace violence, theft, vandalism) and a proper incident reporting system.

Fix: Develop and regularly update detailed emergency response plans. Integrate security cameras and access control systems with emergency communication platforms to facilitate rapid lockdowns, evacuations, and alerts. Implement a centralized incident reporting system that logs all security events and ensures timely response and investigation.

330 Pony Farm Road, Suite 3
Oneonta, NY 13820

607-433-2200

www.directive.com

6. NEGLECTING SECURITY AUDITS

Mistake: Infrequent security system testing, failing to address equipment failures promptly, and not conducting regular security audits.

Fix: Establish a schedule for regular security audits conducted by qualified professionals. Implement preventative maintenance programs for all cameras, access control hardware, and software. Utilize system health monitoring tools to detect and address equipment failures proactively, ensuring optimal system performance and reliability.

7. FAILING TO ADAPT TO EVOLVING THREATS

Mistake: Sticking to outdated security solutions and processes, and failing to update systems to counter new and emerging physical security threats.

Fix: Invest in scalable and future-proof security solutions that can integrate with emerging technologies. Regularly research and adopt new advancements in camera technology (e.g., 4K, thermal), access control (e.g., mobile credentials, cloud-based solutions), and security analytics. Continuously review threat intelligence to proactively adapt security strategies.

8. IGNORING SECURITY CONVERGENCE

Mistake: Treating physical security, cybersecurity, and operational technology (OT) security as separate, disparate domains. This includes failing to implement strong cybersecurity measures for physical security systems themselves.

Fix: Implement a converged security strategy that integrates physical security systems with the organization's cybersecurity framework. Secure all network-connected cameras and access control devices with strong passwords, encryption, and regular patching. Leverage unified platforms that provide a holistic view of security posture across all domains.

330 Pony Farm Road, Suite 3
Oneonta, NY 13820

607-433-2200

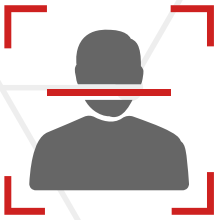
www.directive.com

9. OVERLOOKING SECURITY COMPLIANCE

Mistake: Failing to adhere to relevant industry-specific security compliance standards and regulations.

Fix: Identify all applicable industry and governmental compliance requirements (e.g., HIPAA, GDPR, PCI DSS). Configure camera retention policies, access logs, and data encryption to meet these standards. Maintain detailed audit trails and documentation to demonstrate compliance during inspections.

10. WEAK IDENTITY VERIFICATION



Mistake: Relaxing rules on ID requirements, not verifying identities effectively, and vulnerability to social engineering or stolen identification.

Fix: Enforce strict ID verification protocols at all entry points. Utilize access control systems that can verify credentials against a database in real-time. Implement multi-factor authentication for sensitive areas. For visitors, integrate ID scanning and photo capture with the visitor management system to ensure accurate identification and tracking.

Tackling physical security challenges protects your organization's assets, data, and people. By using modern cameras and access control systems, along with good training and regular maintenance, you can turn weaknesses into strong, proactive security. These integrated solutions deter threats and give you the intelligence and control to respond effectively to any incident, ensuring ongoing safety and compliance.

READY TO ENHANCE YOUR PHYSICAL SECURITY?

Don't leave your organization open to avoidable risks. Contact us today for a comprehensive security assessment and see how our **tailored camera and access control solutions** can give your business the protection it deserves.

330 Pony Farm Road, Suite 3
Oneonta, NY 13820

607-433-2200

www.directive.com