



# The Future of Physical Security

How Physical Security and Logical Security Come  
Together

Lise Patton



# Table of contents

	<b>The Future of Physical Security</b>
03	Introduction
	<b>Fundamentals of Physical Security</b>
04	Traditional Physical Security
04	Physical Security Readers
04	Limitations of Traditional Physical Access Control Readers
05	Modern Physical Access
	<b>Modernizing Physical Security</b>
06	What does Modernization look like?
06	Benefits of Modernization
07	How to Achieve a Modern Physical Security Program
08	Cybersecurity
	<b>Key Components of Modern Security Programs</b>
09	Cybersecurity Technology Components
09	Consolidated Processes and Procedures
09	Cybersecurity Services

# The Future of Physical Security

## Introduction

The future of physical security is, in consolidation with logical access control systems, to provide users and organizations with a single solution used to manage all access across the organization.

Physical access security programs and cybersecurity systems, such as Identity and Access Management solutions, are often managed as separate silos of operations. However, when an organization decides to modernize their solutions and integrate both their physical access security programs and cybersecurity solutions, they can see significant benefits in the areas of threat detection and response capabilities, reduction in costs, and improvement of the organization's overall security posture. Consolidating physical security and IT cybersecurity can shine a light on blind spots, uncover vital insights, and improve organizational efficiency.

### CISA - Cybersecurity and Physical Security Convergence

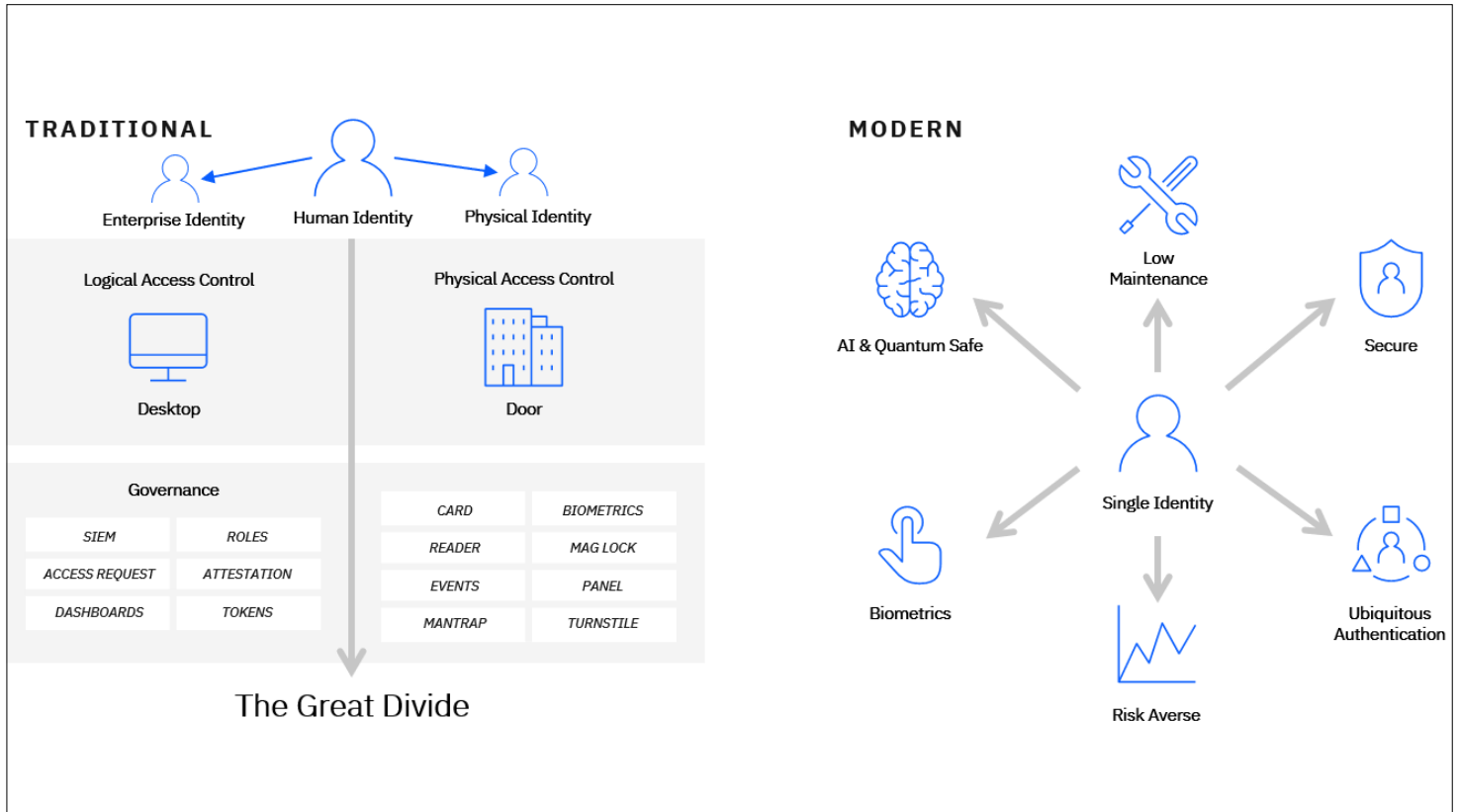


Figure 1: Traditional versus Modern Access Control

# Fundamentals of Physical Security

## Traditional Physical Security

Traditional Physical Access control leveraging biometric template on-card access is described above. This is the most commonly used architecture that traditional implementations have adopted.

## Physical Security Readers

Physical access control readers serve as the backbone of enforcing security. They prevent unauthorized entry, safeguard assets, sensitive information, and protect people within buildings and restricted areas.

These readers regulate who can enter specific spaces, ensuring that only authorized individuals gain access. Whether it is an office, data center, or warehouse, they play a critical role in maintaining order and safety.

## Limitations of Traditional Physical Access Control Readers

- **Costly Infrastructure:** Traditional systems often require specialized hardware, including control boxes and wiring (for power and network communication). Installation and maintenance can be expensive due to the need for multiple hardware interfaces, degradation through usage over time and building infrastructure changes that may impact placement and signal quality due to the proximity limitations of network/control boxes and power supplies.
- **Location-Specific Design:** Each control box is tailored for a specific area. Moving or reconfiguring them is cumbersome and requires additional effort.
- **Limited Integration:** Self-contained by nature, these systems struggle to integrate with other functions or technologies. Expanding capabilities beyond access control becomes challenging.

Traditional access control systems rely on High Frequency iClass cards or something similar, often supplemented by biometric templates stored directly on the cards. While this approach has served its purpose, it faces several limitations:

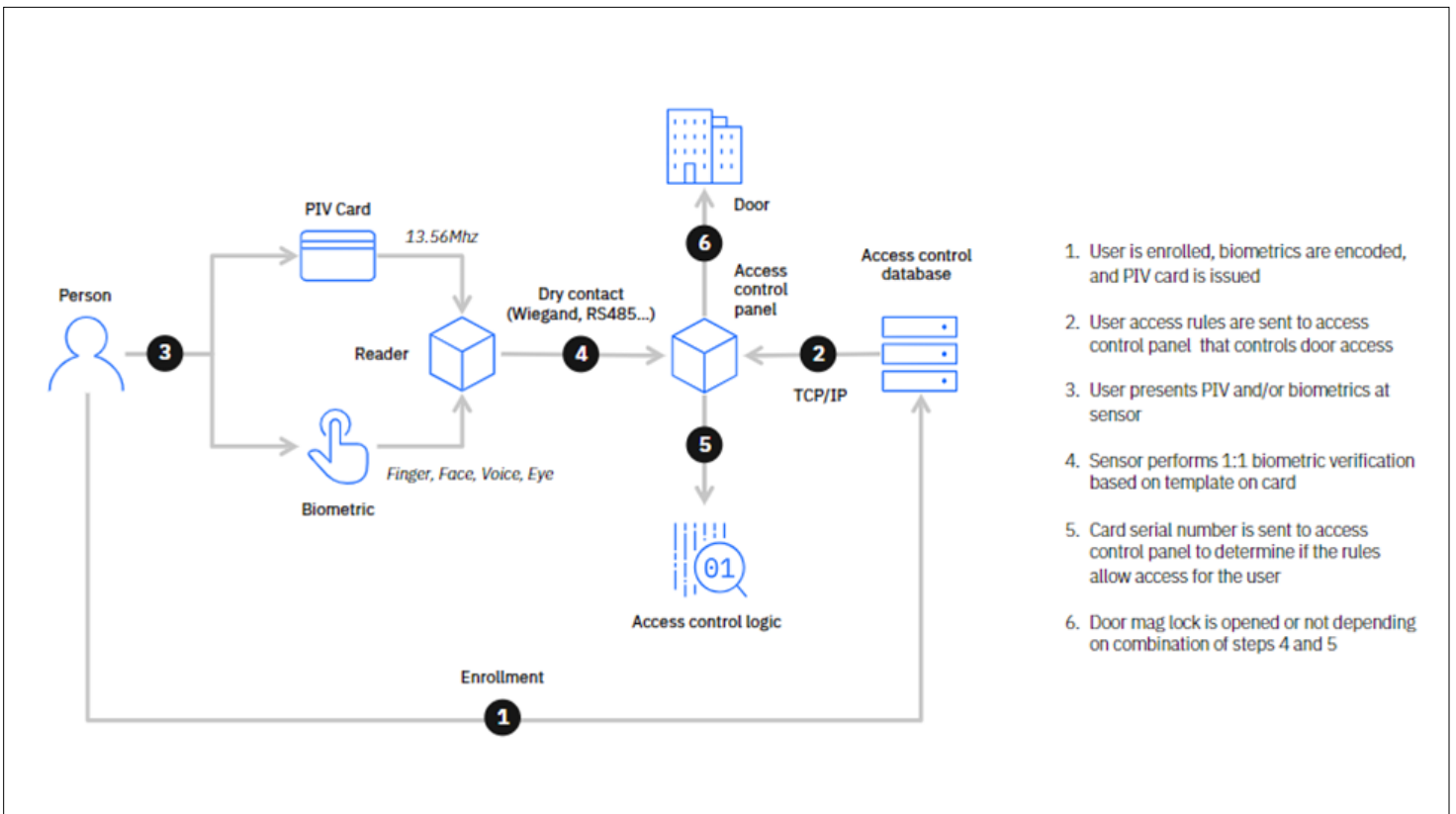


Figure 2: Traditional physical access control architecture.

## Modern Physical Access

Modern access management solutions can still leverage a secure physical access card. Access cards using FIDO (Fast IDentity Online) authentication is an authentication standard that uses public key cryptography to create a login experience that is more secure, phishing-resistant and convenient than passwords.

Organizations should pursue physical access solutions that work today and into the future.

A key component of ensuring that a solution is future proof is by leveraging modern security access cards. FIDO authentication mechanisms are standardized within the direction of the industry. These FIDO badges provide faster and easier personal identification. FIDO ID badges are used by employees for identification and enable specific employees to gain physical access to restricted areas using readers. These badges can also be used for logical access to computers and applications, making logins simple and quick, and bringing considerable benefits to organizations.

Biometrics can also be incorporated into the physical and logical access solutions, and is a function of the card provider organizations select. FIDO2 devices or badges can add biometrics (i.e. fingerprint) validation prior to unlocking the private key used to sign the challenge, exactly how Mac TouchID/Windows Hello works. For logical computer access, once the access request is made using the access card/biometric authentication, the central IAM solution does a standard FIDO2/Passkey interaction with the browser to grant the user access.

Modern credentials should seamlessly integrate with various reader types—whether proximity, smart card, or biometric readers. Scalability ensures consistent access across different entry points within an organization. Examples: MIFARE DESFire EV2 cards, which support multiple applications and encryption levels, or HID iCLASS SE cards with flexible encoding options.

Beyond physical doors, credentials should extend to desktop authentication. Employees can use the same card or biometric data to log in to workstations, enhancing the user experience and security. Examples: PIV (Personal Identity Verification) cards, commonly used in government agencies, serve both physical and logical access needs.

Credentials should prioritize standard security features:

- **Biometrics:** Fingerprint or facial recognition ensures strong authentication.
- **Secure Elements:** Embedded chips enhance encryption and protect against cloning.
- **Customizable Access:** Credentials can be programmed for specific areas and timeframes.
- **Traceability:** Record who accessed an area for audits and investigations.
- **Revocability:** Easily revoke or modify access rights.

Examples: FIDO U2F Security Keys, which combine biometrics and secure elements, or Smart Cards with cryptographic features.

FIDO Research - Bringing Confidence to Biometric Systems →

# Modernizing Physical Security

## What does Modernization look like?

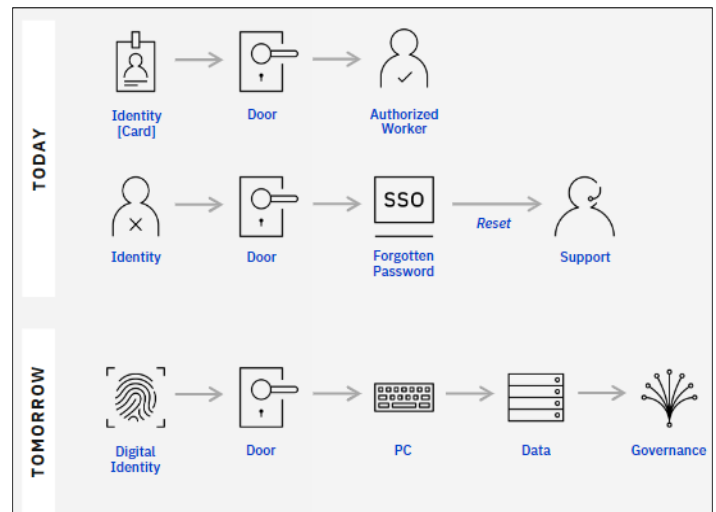
Organizations looking to modernize their physical security program should pursue consolidating their physical security solution with a logical Identity and Access Management Solution (IAM). Another key element of ensuring a successful consolidated solution is to properly incorporate cybersecurity in order to ensure the end state solution is protected and secure.

## Benefits of Modernization

When an organization decides to consolidate physical access control with enterprise logical access security programs and cybersecurity solutions, several benefits emerge:

- **Enhanced Threat Detection and Response Capabilities:** By combining physical and logical access controls, an organization gains a holistic view of security events. This integrated approach allows for more effective detection of threats, whether they originate from physical breaches or cyberattacks.
- **Cost Reduction:** Operating separate security silos can be expensive due to duplicated efforts, redundant technologies, and disjointed processes. Integrating physical and logical security streamlines operations, reduces overhead costs, and optimizes resource allocation.
- **Improved Security Posture:** The synergy between physical and logical security enhances the overall security posture. Insights from physical access logs can inform cybersecurity strategies, and vice versa. For example, anomalies detected in physical access patterns might correlate with suspicious user behavior in the digital realm.

There are significant benefits to modernizing and consolidating an organization's approach to both physical and logical cybersecurity. This modernization should also address a number of pain points within an organization.



Why Your Identity Is the Key to Modernizing Cybersecurity →

**Pain Point**

**Future Benefit of Modernization**

Vulnerabilities in older systems pose long-term security risks. Legacy Access Control Hardware introduces limited support for emerging security protocols, which may require eventual hardware upgrades which can be a costly experience especially without a phased transition

Modern credentials can offer backwards compatibility with older systems making it ideal and more cost effective for phased transitions and are designed to support future security standards making them effective for future proofing. As newer systems emerge, compatibility and scalability are more cost effective and secure.

Disjointed processes required to grant user access to physical, resulting in possible disconnects between systems and delays in provisioning and de-provisioning.

Grant/restrict/block access immediately to both physical locations and application accesses.

Possible security exposure due to user created passwords, including re-use of passwords and use of simple passwords.

Phishing-resistant passwordless authentication, prevents costly data breach, insecure passwords, and phishable MFA solutions.

Significant time and money are spent performing password resets for users in the field.

Consolidating physical and cybersecurity to use existing ID badges as a managed FIDO security key means time and money isn't spent on password resets.

Siloed view of user access to both physical locations and IT applications.

Organizations have full control over credential lifecycles and can create security policies that meet their cybersecurity needs based on internal use cases.

Lack of a consistent organizational wide cybersecurity approach results in inconsistent protection and in possible exposure to data breaches and cybersecurity attacks.

Implementing end to end cybersecurity by design ensures a consistent, effective approach to cybersecurity threat and risk management.

An integrated approach combines physical and logical access controls, leverages advanced encryption and secure elements, to significantly improve the security of access cards. The solution should be designed to seamlessly integrate with both physical and logical access controls, enabling users to securely access both physical spaces and desktop workstations using a single card.

Biometric data is stored centrally, reducing card-based vulnerabilities.

**Scalability and Interoperability:** A platform that seamlessly integrates with existing systems, allowing for efficient expansion and compatibility.

**What to look for in a solution:**

**Unified Identity Management:** By integrating physical and logical access, organizations ensure a holistic view of security events. Anomalies detected in physical access patterns can correlate with digital threats.

**How to Achieve a Modern Physical Security Program**

Modernizing an organization's physical security through consolidation with a logical identity management solution is a significant undertaking. A modernization program would need to be developed, consisting of both a planning and execution phase.

**Biometric Enhancement:** Solutions that leverage advanced biometrics for more accurate and secure authentication.

The planning phase would include a current state assessment, a future state vision and the development of a road map to bridge the gap between the two.



## Cybersecurity

A successful cybersecurity program encompasses many components, all of which contribute to the security posture within an organization. Some of these components are technology/tool based, others are process and governance driven. Some key components all cybersecurity programs should include are:

1. Cybersecurity Governance, Policies, and Procedures
2. Identity and Access Management
3. Network device security
4. Endpoint device security
5. Data protection
6. Threat monitoring and detection
7. Third-party risk management
8. Business continuity and disaster recovery planning
9. Regulatory compliance
10. Continuous improvement

A unified security solution is developed from the ground up utilizing a Security by Design approach, based on cybersecurity and physical security leading practices. This ensures that new risks are mitigated rapidly, and that organizations have clear visibility over their cybersecurity and physical security environment's hardening.

Successful security solution design incorporates data security and privacy measures to be applied throughout the environment. From collection and storage to usage, sharing, retention, and disposal, it is important to make security and privacy foundational, scalable, and integrated into an organization's ecosystem rather than an after thought or siloed capabilities.

The best approach is use-case driven, ensuring that requirements are tailored to an organization's needs and environment, incorporating a variety of tools and strategies such as:

1. **A security and privacy framework which is designed to align to multiple standards and regulations**, such as ITSG-33, NIST Privacy, NIST CSF, GDPR, and CCPA, to facilitate alignment with industry leading practices and compliance with requisite regulations, ensuring that our solutions incorporate security and privacy by design.

The Importance of Understanding and Adopting a Cybersecurity Framework →

2. **Integrating vulnerability assessments (VA) and privacy impact assessments (PIAs) into the design and change management phases**, allows an organization to systematically identify and implement appropriate controls that address potential security and privacy risks and help ensure both cybersecurity and personal privacy considerations are embedded throughout the project lifecycle.

3. **Access control measures tailored to specific use-cases:** Employing Role-Based Access Control (RBAC), Attribute-Based Access Control (ABAC), and Policy-Based Access Control (PBAC) through the use of a central Identity and Access Management (IAM) solution. This enables IT and physical access management to be governed based on roles, attributes, and policies, ensuring alignment with principles of least privilege and zero trust.

An Identity First Approach to Infrastructure Security →

4. **Best-ecosystem approach** for efficient integration within an organization's diverse environments. Unlike the best-of-the-breed approach, which often will result in siloed capabilities, a best-ecosystem strategy prioritizes interoperability within an organization's existing infrastructure. This enables solutions to be compatible with and enhance current systems, leveraging the ecosystem's strengths and optimizing resource utilization.
5. **Quantum Safe Cryptography** is an important factor to include in any security by design architecture. As the use of quantum computing becomes more accessible to bad actors, it will become critical that sensitive data is secured with Quantum Safe encryption algorithms, both in transit and at rest. Ensuring that this is included in the design of the end-to-end solution will reduce the need for costly remediation at a later date. Quantum safe cryptography is particularly important when consolidating personal employee data as the impact of a data breach is exponentially increased when data is aggregated in one location.

# Key Components of Modern Security Programs

## Cybersecurity Technology Components

A key aspect of the consolidation of physical and cybersecurity is the design of the technical solution. Technology tools that need to be incorporated into the end-to-end solution include:

- A central IAM solution which would leverage workflows to provision user access to both IT applications, and to provision physical access through a FIDO card access management tool.
- Cybersecurity tools to ensure the security of the consolidated data and workflows. Components of the Cybersecurity solution should include network device security, endpoint protection, data loss prevention. A SIEM should also be included in the solution to allow the monitoring and identification of threats to the environment.

## Consolidated Processes and Procedures

In order to ensure the long-term success of a consolidated physical and cybersecurity solution it is important to implement processes and procedures that are aligned to a security and privacy framework which is designed to align to multiple standards and regulations, such as ITSG-33, NIST Privacy, NIST CSF, GDPR, and CCPA. This framework includes Cybersecurity Governance, Policies, and Procedures; Third-party risk management; Incident Response Planning, Business continuity and disaster recovery planning; Continuous improvement

## Cybersecurity Services

There are a number of cybersecurity services which should be included in a consolidated physical and logical security program. These additional cybersecurity services ensure that safety of the consolidated data, and help to protect the organization from threats, both internal and external.

**Tabletop Exercises:** As part of Incident Response Planning, it is recommended that an organization undertake bi-annual tabletop exercises in order to test and procedure their Incident Response Plan. This is most effectively accomplished in a third-party location with the facilities to emulate a cyber attack. A cyber range is recommended for these tabletop exercises. Having a local location available to perform these tabletop exercises ensures participation from all key stakeholders.

**Incident Response Retainer:** An additional consideration for Incident Response Planning is to engage a partner with significant experience assisting organizations during a cyber

incident on a retainer so that in the event of a cyber incident an immediate response is available.

**Managed Security Services:** The engagement of a third-party organization to provide managed security services allows an organization to focus on their core business with the assurance that their environment is being monitored 24/7 by cybersecurity professionals who have an in-depth knowledge of cybersecurity tools, and attack vectors. For organizations that have elevated security needs a critical consideration when selecting a Managed Security Services provider is to ensure that the provider is staffed locally, by government security cleared resources, and that all data remains in the country of origin.

## About the author



### **Lise Patton**

Associate Partner, Public Sector

IBM Consulting | Cybersecurity Services

Lise is a strong and detail-oriented leader with extensive experience driving successful results for enterprise-wide programs. Lise has extensive experience working within the public sector implementing support services to large and complex organizations. She has a proven track record of successfully managing operational and project related programs and is known for delivering results. Lise is an outstanding communicator and team motivator.

## Additional Citations

[Gartner - Identity-First Security Maximizes Cybersecurity Effectiveness](#) →

This Gartner report highlights the strength and impact of taking an identity-first security approach. It dives into a changing mindset and approach to cybersecurity, and how it can enhance an organization's posture and cyber resilience, with identity at the core.

[Physical Security to Cybersecurity \(Challenges and Implications in the Modern Digital Landscape\)](#) →

This study dives deep into the shift from purely physical based security to cybersecurity and its importance and relevance in the modern world. It shines light on where physical security beings to fall short, and why physical and cybersecurity need to evolve and work as a cohesive system to protect key data and assets,

© Copyright IBM Corporation 2024

IBM Corporation  
New Orchard Road  
Armonk, NY 10504

Produced in Canada  
October 2024

IBM, the IBM logo, and IBM Security Verify, are trademarks or registered trademarks of International Business Machines Corporation, in the United States and/or other countries. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on [ibm.com/trademark](https://ibm.com/trademark).

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT.

IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

