openpath

Guide to Physical Security in the Workplace

Learn how to reduce risk and safeguard your space with our comprehensive guide to physical security systems, technologies, and best practices.

The modern business owner faces security risks at every turn

As technology continues to advance, threats can come from just about anywhere, and the importance of physical security has never been greater. While many companies focus their prevention efforts on cybersecurity and hacking, physical threats shouldn't be ignored. Every breach, big or small, impacts your business, from financial losses, to damaged reputation, to your employees feeling insecure at the office. Even for small businesses, having the right physical security measures in place can make all the difference in keeping your business, and your data, safe.

What is physical security?

Let's start with a physical security definition, before diving into the various components and planning elements. Physical security measures are designed to protect buildings, and safeguard the equipment inside. In short, they keep unwanted people out, and give access to authorized individuals. While network and cybersecurity are important, preventing physical security breaches and threats is key to keeping your technology and data safe, as well as any staff or faculty that have access to the building. Without physical security plans in place, your office or building is left open to criminal activity, and liable for types of physical security threats including theft, vandalism, fraud, and even accidents.

In the built environment, we often think of physical security control examples like locks, gates, and guards. While these are effective, there are many additional and often forgotten layers to physical security for offices that can help keep all your assets protected. A comprehensive physical security plan combines both technology and specialized hardware, and should include countermeasures against intrusion such as:

- Site design and layout
- Environmental components
- Emergency response readiness
- Training
- Access control
- Intrusion detection
- Power and fire protection

From landscaping elements and natural surveillance, to encrypted keycards or mobile credentials, to lockdown capabilities and emergency mustering, there are many different components to preventing all different types of physical security threats in the modern workplace. You can use a Security Audit Checklist to ensure your physical security for buildings has all the necessary components to keep your facility protected from threats, intrusions and breaches.




Components of physical security controls

Before updating a physical security system, it's important to understand the different roles technology and barriers play in your strategy. The smartest security strategies take a layered approach, adding physical security controls in addition to cybersecurity policies. This means building a complete system with strong physical security components to protect against the leading threats to your organization. The four main physical security components are:

1. **Deterrence** – These are the physical security measures that keep people out or away from the space. Deterrent security components can be a physical barrier, such as a wall, door, or turnstyle. Technology can also fall into this category. Access control systems and video security cameras deter unauthorized individuals from attempting to access the building, too.
2. **Detection** – Just because you have deterrents in place, doesn't mean you're fully protected. Detection components of your physical security system help identify a potential security event or intruder. Sensors, alarms, and automatic notifications are all examples of physical security detection.
3. **Delay** – There are certain security systems that are designed to slow intruders down as they attempt to enter a facility or building. Access control, such as requiring a key card or mobile credential, is one method of delay. Smart physical security strategies have multiple ways to delay intruders, which makes it easier to mitigate a breach before too much damage is caused.
4. **Response** – These are the components that are in place once a breach or intrusion occurs. Examples of physical security response include communication systems, building lockdowns, and contacting emergency services or first responders.

Together, these physical security components work to stop unwanted individuals from accessing spaces they shouldn't, and notify the necessary teams to respond quickly and appropriately. Your physical security plans should address each of the components above, detailing the technology and processes you'll use to ensure total protection and safety.

How do physical security policies impact cybersecurity and data protection?

Today's security systems are smarter than ever, with IoT paving the way for connected and integrated technology across organizations. However, cloud-based platforms, remote and distributed workforces, and mobile technology also bring increased risk. In fact, 97% of IT leaders are concerned about a data breach in their organization. But cybersecurity on its own isn't enough to protect an organization. That's why a complete physical security plan also takes cybersecurity into consideration.

Cyber and physical security convergence merges these two disparate systems and teams for a holistic approach to security. Even with stringent cybersecurity practices, like encryption and IP restrictions, physical security failures could leave your organization vulnerable. Gaps in physical security policies, such as weak credentials or limited monitoring capabilities, make it easier for people to gain access to data and confidential information.

Take a look at these physical security examples to see how the right policies can prevent common threats and vulnerabilities in your organization.

- Restrict access to IT and server rooms, and anywhere laptops or computers are left unattended
- Use highly secure access credentials that are difficult to clone, fully trackable, and unique to each individual
- Require multi-factor authentication (MFA) to unlock a door or access the building
- Structure permissions to employ least-privilege access throughout the physical infrastructure
- Eliminate redundancies across teams and processes for faster incident response
- Integrate all building and security systems for a more complete view of security and data trends
- Set up automated security alerts to monitor and identify suspicious activity in real-time

Determining your risk level

Before implementing physical security measures in your building or workplace, it's important to determine the potential risks and weaknesses in your current security. Detection is of the utmost importance in physical security. While it is impossible to prevent all intrusions or physical security breaches, having the right tools in place to detect and deal with intrusions minimizes the disruption to your business in the long run.

To locate potential risk areas in your facility, first consider all your public entry points. Where people can enter and exit your facility, there is always a potential security risk. Baseline physical security control procedures, such as proper access control measures at key entry points, will help you manage who is coming and going, and can alert you to potential intrusions. Once inside your facility, you'll want to look at how data or sensitive information is being secured and stored. Do you have server rooms that need added protection? Are desktop computers locked down and kept secure when nobody is in the office? Do employees have laptops that they take home with them each night? Even USB drives or a disgruntled employee can become major threats in the workplace. List out all the potential risks in your building, and then design d security plans to mitigate the potential for criminal activity.

Most common threats to physical security

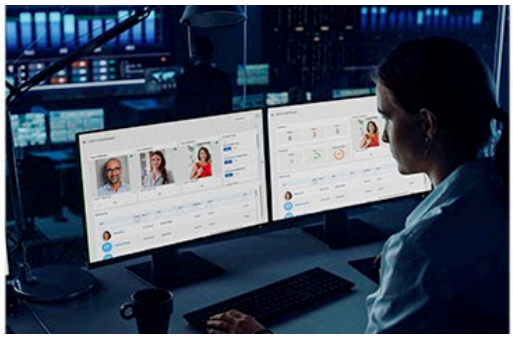
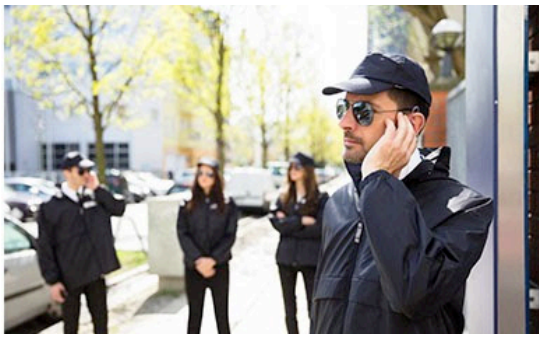
While your security systems should protect you from the unique risks of your space or building, there are also common physical security threats and vulnerabilities to consider. The top 5 most common threats your physical security system should protect against are:

- Theft and burglary
- Vandalism
- Natural disasters
- Terrorism or sabotage
- Violence in the workplace

Depending on where your building is located, and what type of industry you're in, some of these threats may be more important for you to consider. For example, if your building or workplace is in a busy public area, vandalism and theft are more likely to occur. If your building houses a government agency or large data storage servers, terrorism may be higher on your list of concerns.

The above common physical security threats are often thought of as outside risks. However, internal risks are equally important. Human error is actually the leading cause of security breaches, accounting for approximately 88% of incidents, according to a Stanford University study. Some of the factors that lead to internal vulnerabilities and physical security failures include:

- Employees sharing their credentials with others
- Accidental release or sharing of confidential data and information
- Tailgating incidents with unauthorized individuals
- Easily hacked authentication processes
- Slow and limited response to security incidents

Physical security technology

With a fundamental understanding of how a physical security plan addresses threats and vulnerabilities in your space, now it's time to choose your physical security technology options. With advancements in IoT and cloud-based software, a complete security system combines physical barriers with smart technology. The three most important technology components of your physical security controls for offices and buildings are access control, surveillance, and security testing methods. While the other layers of physical security control procedures are important, these three countermeasures are the most impactful when it comes to intrusion detection and threat mitigation.

Access control

Securing your entries keeps unwanted people out, and lets authorized users in. A modern keyless entry system is your first line of defense, so having the best technology is essential. There are a few different types of systems available; this guide to the best access control systems will help you select the best system for your building. The main things to consider in terms of your physical security are the types of credentials you choose, if the system is on-premises or cloud-based, and if the technology meets all your unique needs. When it comes to access methods, the most common are keycards and fob entry systems, and mobile credentials. Some access control systems allow you to use multiple types of credentials on the same system, too. Access control that uses cloud-based software is recommended over on-premises servers for physical security control plans, as maintenance and system updates can be done remotely, rather than requiring someone to come on-site (which usually results in downtime for your security system). Cloud-based technology also offers great flexibility when it comes to adding entries and users, plus makes integrating with your other security systems much easier.

Surveillance tools

Surveillance is crucial to physical security control for buildings with multiple points of entry. The most common type of surveillance for physical security control is video cameras. Video management systems (VMS) are a great tool for surveillance, giving you visual insight into activity across your property. When adding surveillance to your physical security system, choose cameras that are appropriate for your facility, i.e. exterior doors will need outdoor cameras that can withstand the elements. For indoor cameras, consider the necessary viewing angles and mounting options your space requires. Another consideration for video surveillance systems is reporting and data. To get the most out of your video surveillance, you'll want to be able to see both real-time footage, as well as previously recorded activity. In physical security control, examples of video surveillance data use cases include running audits on your system, providing video footage as evidence after a breach, using data logs in emergency situations, and applying usage analytics to improve the function and management of your system. If you're using an open-platform access control system like Openpath, you can also integrate with your VMS to associate visual data with entry activity, offering powerful insights and analytics into your security system. Because Openpath runs in the cloud, administrators are able to access the activity dashboard remotely, and setting up new entries or cameras is quick and efficient.

Emergency preparedness and security testing

Education is a key component of successful physical security control for offices. If employees, tenants, and administrators don't understand the new physical security policy changes, your system will be less effective at preventing intrusions and breaches. Once your system is set up, plan on rigorous testing for all the various types of physical security threats your building may encounter. You should run security and emergency drills with your on-site teams, and also test any remote features of your physical security controls to make sure administrators have the access they need to activate lockdown plans, trigger unlock requests, and add or revoke user access. Communicating physical security control procedures with staff and daily end users will not only help employees feel safer at work, it can also deter types of physical security threats like collusion, employee theft, or fraudulent behavior if they know there are systems in place designed to detect criminal activity.

What the rise in cloud-based technology means for physical security

Cloud-based physical security technology is quickly becoming the favored option for workplace technology over traditional on-premise systems. The main difference with cloud-based technology is that your systems aren't hosted on a local server. Instead, it's managed by a third party, and accessible remotely. But how does the cloud factor into your physical security planning, and is it the right fit for your organization?

Increased flexibility

By migrating physical security components to the cloud, organizations have more flexibility. In terms of physical security, examples of that flexibility include being able to make adjustments to security systems on the fly. Changes to door schedules, access permissions, and credentials are instant with a cloud-based access control system, and the admin doesn't need to be on the property. This is especially important for multi-site and enterprise organizations, who need to be able to access the physical security controls for every location, without having to travel.

Support for remote access and monitoring

The cloud has also become an indispensable tool for supporting remote work and distributed teams in recent years. When you can't have every employee onsite at all time, whether due to social distancing or space limitations, remote access to your physical security technology is essential. Let's look at the scenario of an employee getting locked out. With remote access, you can see that an unlock attempt was made via the access control system, and check whose credentials were used. With video access control or integrated VMS, you can also check video footage to make sure the person is who they say they are. Then, unlock the door remotely, or notify onsite security teams if needed. All on your own device without leaving the house.

Being able to monitor what's happening across the property, with video surveillance, access activity, and real-time notifications, improves incident response time and increases security without additional investment on your part.

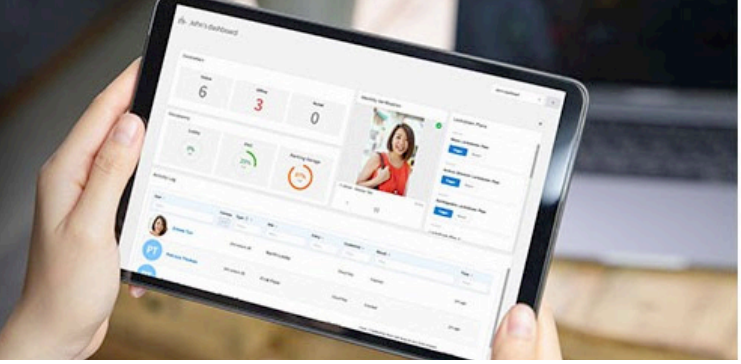
Greater scalability

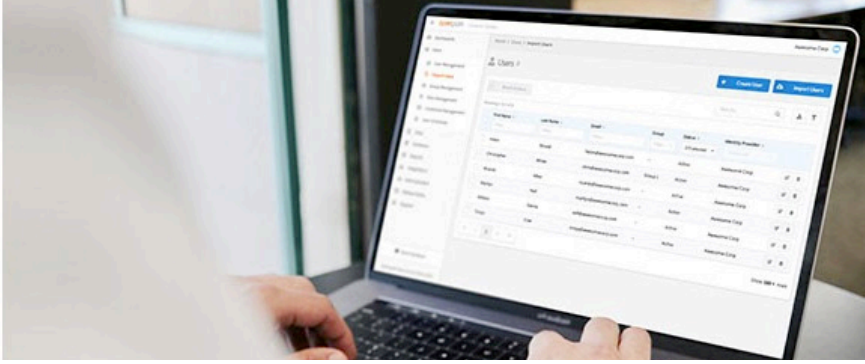
Physical security plans often need to account for future growth and changes in business needs. But it's nearly impossible to anticipate every possible scenario when setting physical security policies and systems. That's where the cloud comes into play. On-premise systems are often cumbersome to scale up or back, and limited in the ability to easily or quickly adapt the technology to account for emerging security needs. Cloud-based physical security technology, on the other hand, is inherently easier to scale. Because the entire ecosystem lives in the cloud, all software updates can be done over-the-air, and there aren't any licensing requirements to worry about if you need to scale the system back.

Improved ROI and future-proofing

All of these benefits of cloud-based technology allow organizations to take a proactive approach to their physical security planning. Rather than waiting for incidents to occur and then reacting, a future-proof system utilized automations, integrations, and data trends to keep organizations ahead of the curve. In short, the cloud allows you to do more with less up-front investment. With SaaS physical security, for example you only pay for what you use, and it's easy to make adjustments as business needs shift.

The seamless nature of cloud-based integrations is also key for improving security posturing. System administrators have access to more data across connected systems, and therefore a more complete picture of security trends and activity over time. Taking advantage of AI data analytics, building managers can utilize cloud-based technology to future-proof their physical security plans, and create a safer building that's protected from today's threats, as well as tomorrow's security challenges.





Benefits of physical security technology

Beyond the obvious benefit of physical security measures to keep your building protected, the technology and hardware you choose may include added features that can enhance your workplace security. Especially with cloud-based physical security control, you'll have added flexibility to manage your system remotely, plus connect with other building security and management systems.

- **Prevent unauthorized entry**
  Providing a secure office space is the key to a successful business. Nearly one third of workers don't feel safe at work, which can take a toll on productivity and office morale. Providing security for your customers is equally important. Not only should your customers feel secure, but their data must also be securely stored. Data breaches compromise the trust that your business has worked so hard to establish. Implementing a rigorous commercial access control system as part of your physical security plans will allow you to secure your property from unauthorized access, keeping your assets and employees safe and preventing damage or loss.
- **Proactive intrusion detection**
  As the first line of defense for your building, the importance of physical security in preventing intrusion cannot be understated. Installing a best-in-class access control system ensures that you'll know who enters your facility and when. With an easy-to-install system like Openpath, your intrusion detection system can be up-and-running with minimal downtime. Plus, the cloud-based software gives you the advantage of viewing real-time activity from anywhere, and receiving entry alerts for types of physical security threats like a door being left ajar, an unauthorized entry attempt, a forced entry, and more. With Openpath's unique lockdown feature, you can instantly trigger a full system lockdown remotely, so you take care of emergencies quickly and efficiently. Cloud-based and mobile access control systems offer more proactive physical security measures for your office or building
- **Scalable physical security implementation**
  With data stored on the cloud, there is no need for onsite servers and hardware that are both costly and vulnerable to attack. Cloud-based physical security control systems can integrate with your existing platforms and software, which means no interruption to your workflow. Both for small businesses experiencing exponential growth, and for enterprise businesses with many sites and locations to consider, a scalable solution that's easy to install and quick to set up will ensure a smooth transition to a new physical security system. Cloud-based systems are naturally more flexible compared to legacy systems, which makes it easier to add or remove entries, install new hardware, or implement the system across new building locations.
- **Seamless system integrations**
  Another benefit of physical security systems that operate in the cloud is the ability to integrate with other software, applications, and systems. While a great access control system is essential to any physical security plan, having the ability to connect to other security tools strengthens your entire security protocol. For example, Openpath's access control features an open API, making it quick and easy to integrate with video surveillance and security cameras, user management systems, and the other tools you need to run your business.
- **Audit trails and analytics**
  One of the benefits of physical security control systems is that the added detection methods usually include reporting and audit trails of the activity in your building. This data is crucial to your overall security. Being able to easily and quickly detect possible weaknesses in your system enables you to implement new physical security plans to cover any vulnerable areas. In the event that you do experience a breach, having detailed reports will provide necessary evidence for law enforcement, and help you identify the culprit quickly. Analytics on the performance of your physical security measures allow you to be proactive in finding efficiencies, enabling better management and lessening the burden on your HR and IT teams.

COVID-19 physical security plans for workplaces

All offices have unique design elements, and often cater to different industries and business functions. However, the common denominator is that people won't come to work if they don't feel safe. The coronavirus pandemic delivered a host of new types of physical security threats in the workplace. When offices closed down and shifted to a remote workforce, many empty buildings were suddenly left open to attack, with no way to manage who was coming and going. Once buildings reopen with limited occupancy, there are still challenges with enforcing social distancing, keeping sick people at home, and the burden of added facility maintenance.

Building and implementing a COVID-19 physical security control plan may seem daunting, but with the right technology investments now, your building and assets will be better protected well into the future. Because common touch points are a main concern for many tenants and employees upgrading to a touchless access control system is a great first step. Even if you implement all the latest COVID-19 technology in your building, if users are still having to touch the same turnstiles and keypads to enter the facility, all that expensive hardware isn't protecting anyone. Your access control system should also have occupancy tracking capabilities to automatically enforce social distancing in the workplace. Use a COVID-19 workplace safety checklist to ensure your physical security plans include all the necessary features to safeguard your building, employees, and data during the pandemic.

Top considerations for physical security planning

Physical security planning is an essential step in securing your building. Use this 10-step guideline to create a physical security plan that addresses your unique concerns and risks, and strengthens your security postuvring.

1. Identify the scope of your physical security plans. This should include the types of employees the policies apply to, and how records will be collected and documented.
2. Determine who is responsible for implementing your physical security plans, as well as the key decision-makers for making adjustments or changes to the plan.
3. Include the different physical security technology components your policy will cover.
4. State the types of physical security controls your policy will employ. Include any **physical access control systems**, permission levels, and types of credentials you plan on using.
5. List out key access points, and how you plan to keep them secure.
6. Define your monitoring and detection systems. What types of video surveillance, sensors, and alarms will your physical security policies include? Identify who will be responsible for monitoring the systems, and which processes will be automated.
7. Outline all incident response policies. Your physical security planning needs to address how your teams will respond to different threats and emergencies.
8. Scope out how to handle visitors, vendors, and contractors to ensure your physical security policies are not violated.
9. Create a cybersecurity policy for handling physical security technology data and records. Include your policies for encryption, vulnerability testing, hardware security, and employee training.
10. Address how physical security policies are communicated to the team, and who requires access to the plan.

Safety is essential for every size business whether you're a single office or a global enterprise. The physical security best practices outlined in this guide will help you establish a better system for preventing and detecting intrusions, as well as note the different considerations when planning your physical security control procedures. Here's a quick overview of the best practices for implementing physical security for buildings.

- Install perimeter security to prevent intrusion. Physical barriers like fencing and landscaping help establish private property, and deter people from entering the premises.
- Use access control systems to provide the next layer of security and keep unwanted people out of the building. When selecting an access control system, it is recommended to choose a cloud-based platform for maximum flexibility and scalability.
- Integrate your access control with other physical security systems like video surveillance and user management platforms to fortify your security.
- Employ cyber and physical security convergence for more efficient security management and operations.
- Regularly test your physical security measures to ensure you're protected against the newest physical security threats and vulnerabilities.
- Always communicate any changes to your physical security system with your team.

If you're looking to add cloud-based access control to your physical security measures, Openpath offers customizable deployment options for any size business.

About Openpath

On a mission to improve convenience and security in the built environment, Openpath creates smart, customizable access control solutions for the modern workplace. Designed with a laser-focus on the user experience, Openpath combines sleek, state-of-the-art hardware with cloud-based enterprise software for faster, more reliable access that's customizable to fit every level of security. Openpath is helping companies prepare for the "new normal" with contactless options and innovative features designed to make remote management easier than ever.

Openpath's unique mobile credentials give users a completely hands-free entry experience, without needing to remove the smartphone from their pocket. With encryption at every level and patented Triple-Unlock technology, Openpath is the first and only solution to achieve 94% mobile adoption.

LinkedIn	https://www.linkedin.com/company/openpath-security
Twitter	https://twitter.com/OpenpathSec
Facebook	https://www.facebook.com/GetOpenpath
Instagram	https://www.instagram.com/openpathsecurity