AVIGILON™

WHAT IS PHYSICAL SECURITY?

Controls, methods and measures for commercial buildings

MOTOROLA SOLUTIONS

CONTROLS, METHODS AND MEASURES FOR COMMERCIAL BUILDINGS

In this day and age of technology, security is a top priority for businesses across every industry. With almost every organization now depending on IT infrastructure to carry out day-to-day business operations such as information exchange and monetary transactions, securing your digital network makes practical sense.

Because of the ever-changing landscape of digital infrastructure, it's natural for businesses to invest heavily in protecting their IT assets, especially as newer, more sophisticated threats are on the horizon. But are digital security measures enough?

Physical security systems are not a new concept, but they are as important as cyber security measures when it comes to protecting people, property and assets.

In this guide, you will learn the definition of physical security, its components, technologies, benefits and other information you should know to implement an effective physical security plan.

What is physical security?

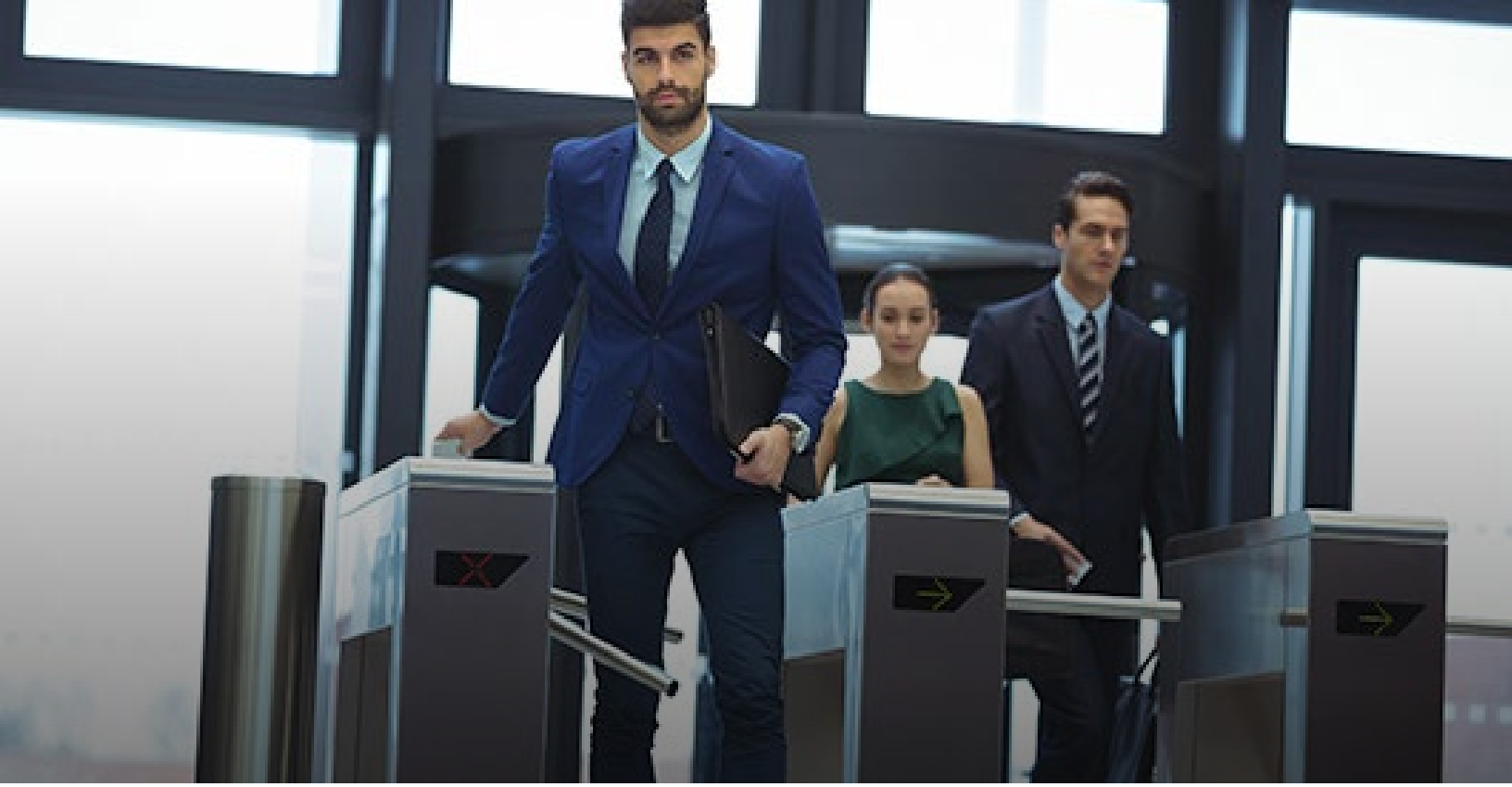
A common definition of physical security includes security measures designed to limit access to authorized individuals, as well as any resources that protect personnel from harm and property from damage.

So, in the simplest term, physical security is defined as the securing and protecting of organizational assets from coming to harm as a result of physical events. These events can range from natural disasters such as fires and floods, to human-inflicted dangers including theft and vandalism. Accidents and accidental damage also fall under the umbrella of events that may be covered by a physical security plan.

So, what do physical security systems and plans entail? On the surface, physical security measures include locks, gates, video security cameras and security guards. Although these are excellent strategies, there are deeper layers that you should take into account when creating a physical security plan.

An effective plan should include equipment and technology, and can work alongside these areas:

- Training: Ensure your staff has the proper knowledge in implementing your physical security strategy.
- Site design and layout: Equipment and physical security components should be strategically placed to complement the design and layout of your facility.
- Emergency response readiness: Staff in your facility should be trained on what to do during certain situations and emergencies.
- Access control: Understand how you will assign access to your staff and limit access for restricted spaces.
- Environmental components: Create safety measures to mitigate damage from intentional or unforeseen natural disasters that may happen.



KEY PHYSICAL SECURITY MEASURES

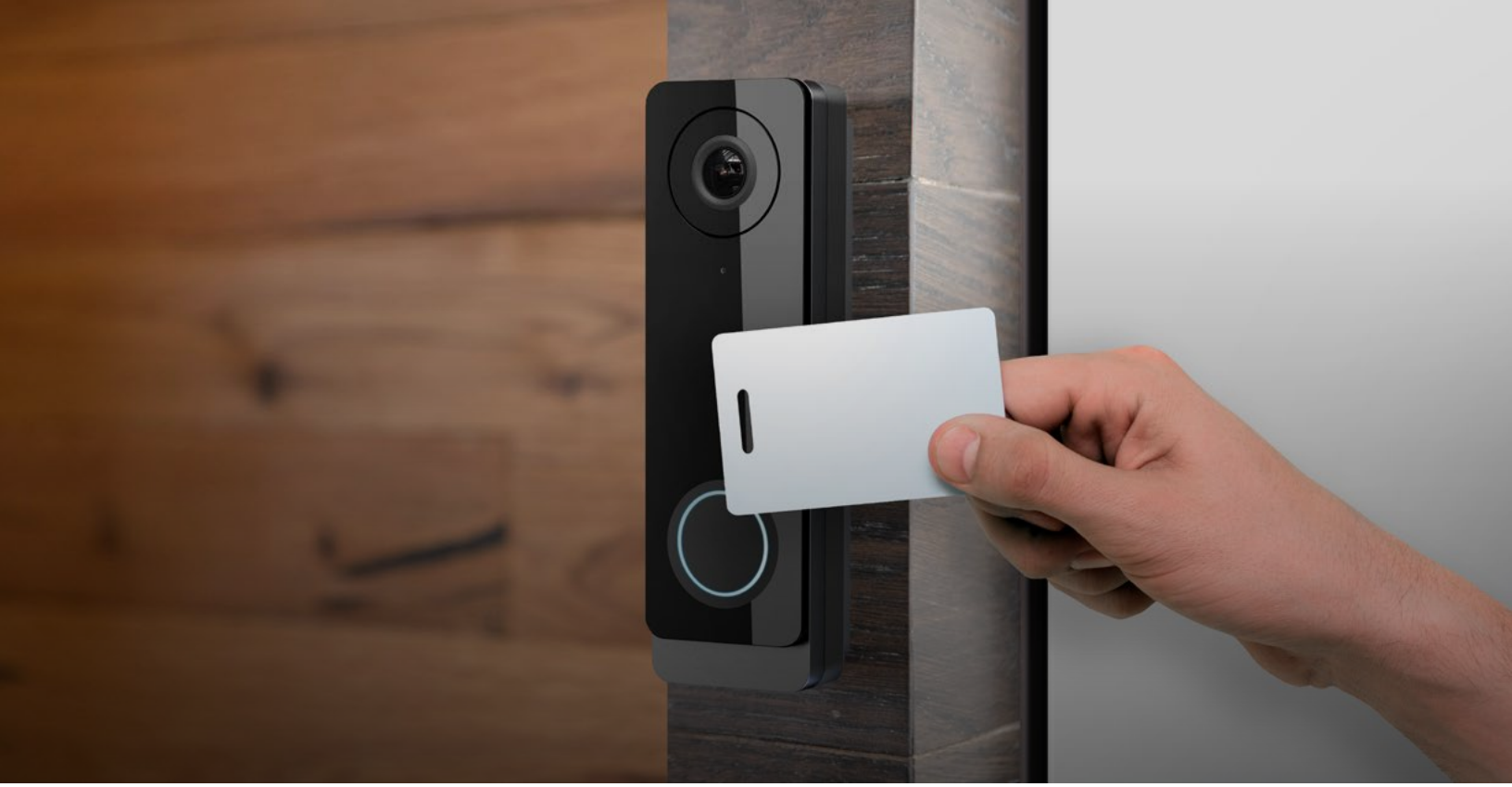
When it comes to preventing different types of physical security threats in any facility, there are many types of innovations that you can use, from encrypted access cards and security cameras to mobile credentials and temperature sensors. But before you use any of these systems, it's important to understand the different elements that can contribute to your overall plan.

When creating a physical security strategy, you need to have all your security measures complementing one another. This means that you need to use different types of physical security measures in a layered approach to ensure that you're protected from every angle.

So, what is good practice for physical security? Here are the most common elements in an effective physical security plan:

- **Deterrence:** This type of physical security technology focuses on keeping unwanted people, vehicles or animals away from a certain area. Deterrence can encompass various equipment such as signage, security cameras and access control systems. It also includes physical barriers such as doors, locks and walls. It is essentially any security systems or equipment that can help deter intruders from entering sensitive areas.
- **Detection:** Deterrents can only do so much. If you want to fully protect your facility, you need to have devices that can identify potential intruders and ways to alert the correct authorities. Some technologies you can use for physical security detection measures are sensors, alarms and automatic notifications.
- **Delay:** Several physical security controls are created to slow intruders down when breaking into a facility. Simple security measures such as additional doors, locks and security guards can help delay incidents. More advanced physical security technology, such as key cards and mobile credentials, can make it more difficult for unauthorized users trying to enter a building. With this technology in place, it's easy to mitigate a breach before too much damage is caused.
- **Response:** Once a breach or intrusion happens, you must also have a response strategy in place, such as building lockdowns or automatically notifying emergency services.

Successful and effective plans should include these technologies to ensure that a facility can prevent physical threats and take necessary action if a security breach occurs.



COMPONENTS OF PHYSICAL SECURITY CONTROLS AND SYSTEMS

Physical security controls fall into three main areas of concern: access control, surveillance and testing. How well these security components function can make or break your physical security program. Their performance can also indicate how well your plan was implemented, where to improve and what to maintain.

Access Control

The most effective way to maximize your physical security controls is by limiting and controlling who can access your commercial premises. This physical security component involves the means of restricting the exposure of specific assets and areas to authorized staff only. Companies can use physical security components like keypads, ID badges, biometric logins and security guards to limit access for unauthorized individuals.

So, how does access control work? The first line of defense of physical security is its architecture. This includes walls, gates, doors and guards that are strategically placed to deter criminal entry. In some locations, barbed wires, additional locks, visible security signs and equipment can help reduce attempts to enter a facility.

There are also more advanced access control measures that use a technology-supported approach to tighten up building security. One example of physical security is using proximity ID badges. Instead of just a plastic ID badge, employees are issued key cards that use NFC or RFID technology to authenticate identity when entering various locations in the building.

Apart from employees, companies can also provide visitor access cards to easily control which areas your visitors can access in your facility. Some companies use mobile authenticators instead of ID cards to validate identities to enter a building. These ID scanners and authenticators will act as obstacles for anyone without authorization, making it more challenging for attackers to gain access to certain assets and information on your premises.

Enabling multi-factor authentication (MFA) increases the time it takes for intruders to carry out any criminal offense they have in mind. This physical security best practice requires users to present at least two authorized credentials, such as typing in a PIN code and scanning an ID badge. The more strategically placed obstacles are in place, the more time companies can buy to act on threats and mitigate them.

Additionally, access control can do much more than restricting unauthorized access. Physical barriers like walls and fences can help protect buildings from natural and environmental disasters including landslides and floods. Obviously, these risks depend on the location, but organizations must always consider threats like this when investing in physical security systems.

Surveillance tools and technology

When it comes to prevention and post-incident recovery, surveillance is the most critical component of physical security. It refers to the staff, resources and technology used by organizations to monitor the activity of different areas of the facilities. This includes video cameras, sensors, guards and automatic notification systems.

One of the most commonly used types of physical security technology for this component is security cameras or closed circuit television (CCTV) cameras. These devices continuously record the activity of a given area, allowing you to see what's happening at a particular location in real time, or record it for later viewing.

Some security cameras come with built-in analytics that can detect and classify objects intelligently, notifying you if there is something unusual going on. When you choose video equipment for your facility, make sure to enlist the help of a security camera installer who can carefully assess every entry point, checking for any blindspots that can be exploited.

A security camera installer will also ensure that your video cameras are strategically placed in locations that require constant monitoring and protection.

Importance of video cameras for physical security

When criminal activity happens, you need evidence to prove the event occurred. Often, video security gives the proof you need. Most cameras allow for constant recording in a particular area, with some that have night vision capabilities to see through darker environments. If something suspicious happens at your facility, you can use these recordings as evidence.

In addition, some monitoring devices offer an automatic notification feature, which provides you with instant alerts for physical security threats such as intrusion detection. Advanced video cameras and management software often have real-time monitoring, allowing you to see in-action breaches as they unfold. This can give you an idea of how to mitigate them as quickly as possible.

Physical security systems testing

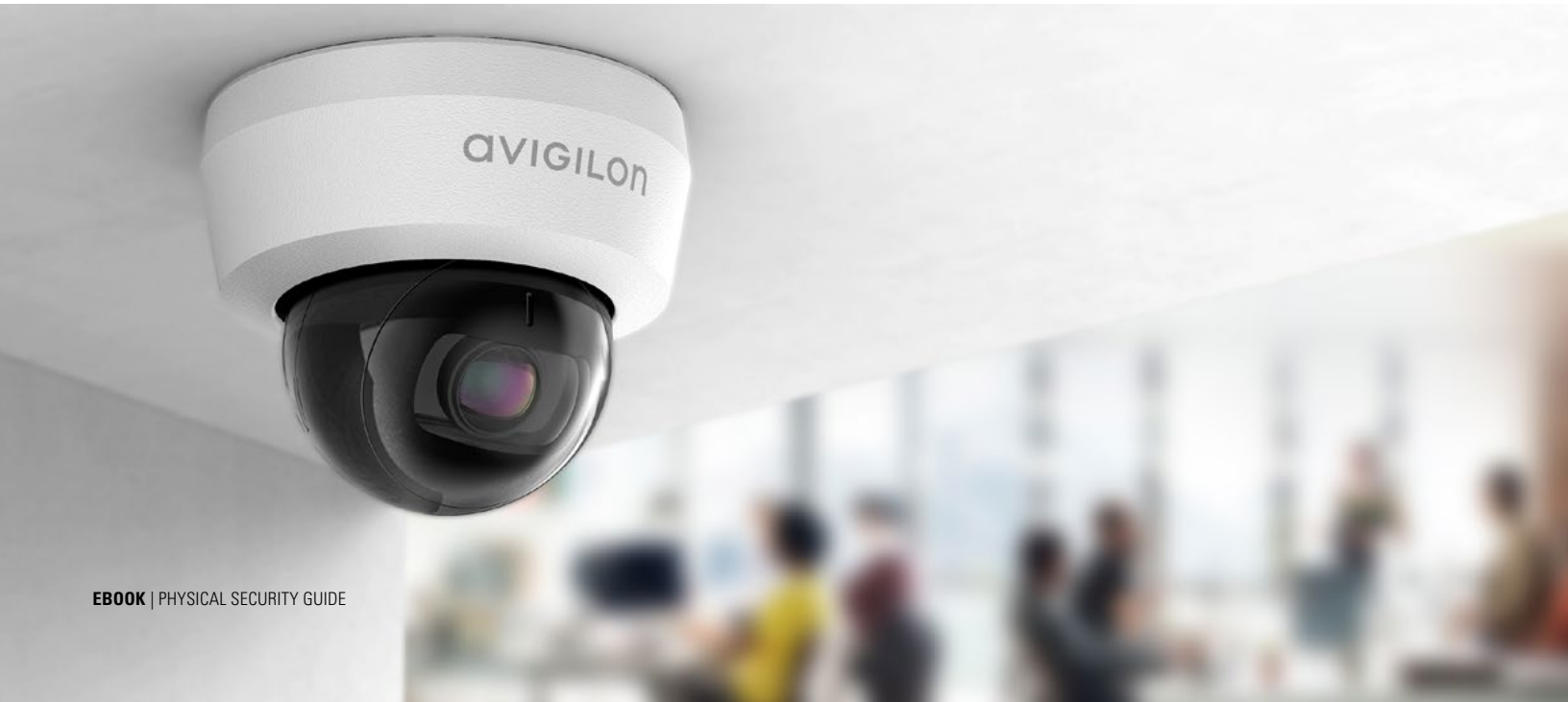
Access control and monitoring are preventative physical security measures. Often, business owners are not able to measure the effectiveness of their building's physical security until an incident occurs. To mitigate damages before they occur, it is advised to conduct testing as a physical security best practice. This physical security component checks how well your organization identifies, responds to and contains a security threat.

Testing requires educating employees, often through training and written communication. Cameras and technologies can do a lot, but businesses will be better protected if employees are knowledgeable about the company's security measures and what to do in the event of a physical security threat. This particularly applies to natural disasters such as fire and earthquakes, but is equally important in identifying physical security risks such as tailgating or other suspicious activities.

Importance of testing for physical security

Testing allows business owners or security personnel to understand how well their security system works and which areas to improve. If you conduct mock physical security breaches, you can see how well your employees perform in various scenarios. This gives you an idea of how your security measures are performing and if there are other vulnerabilities you need to protect.

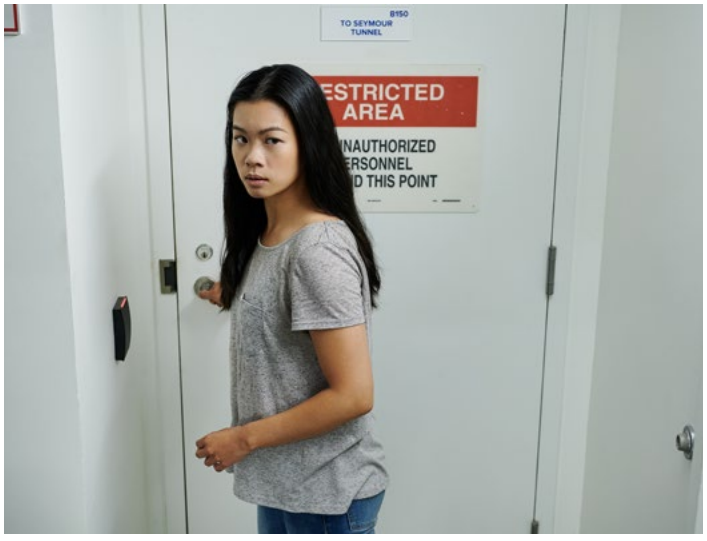
At the same time, educating employees about physical security policies and protocols can make them feel safer at work. If employees are made aware of the systems in place to detect criminal activity, it helps to deter any physical threat activity, such as fraudulent behavior or employee theft.



EXAMPLES OF PHYSICAL SECURITY IMPLEMENTATION

Perimeter security

This is one of the most common physical security examples we see today. Perimeter security is straightforward. It involves creating physical barriers that protect your facility from intruders. This includes fences, gates, barbed wire and security guards. This type of physical security is also your first line of defense to deter intruders from getting into your facility.



Environmental elements

The layout and landscaping on your property can help control the flow of traffic on the premises and deter unwanted activity. For example, high hedges around the perimeter, motion-activated lighting and maintained walking paths make it easier to spot anyone who looks suspicious lurking around the building exterior.

Secure credentials for authorized individuals

Requiring every authorized individual to have access credentials is among the top security best practices to implement in your building. There are many types of systems, and each can be used depending on the threat level or importance of an area, including:

- Key cards or ID badges
- Key fob system
- Biometric readers
- Keypad locks
- Mobile-based credentials

These physical security devices ensure that each user can easily access the building when needed. They also give businesses better insight into daily traffic, failed access attempts and potential physical security threats.

Restricted access areas

This physical security example shows how measures can be implemented for restricted areas, such as a server room or area with expensive equipment. Areas like this can only be accessed by a small subset of the staff, which requires additional access credentials, such as MFA, unique PINs or biometric credentials. If anything goes missing or is damaged in the room, it narrows down who can be held accountable.

Additional monitoring security components, such as video cameras or a staffed guard, can further deter unauthorized activity in restricted spaces.

Logs and audit trails

Another way to secure a facility is through detailed logging. Instead of just limiting access, this physical security method keeps a record of which credentials are used, as well as where and when the activity occurred. This doesn't only deter unauthorized users, but also allows you to create a forensic-friendly data environment essential for physical security management and maintenance.

For example, records of multiple failed login attempts or attempted access using a lost card would be easier to spot with detailed activity logs. If there's a security breach, you can quickly identify weaknesses in your system through audit trails.

Monitoring systems

Most organizations have surveillance in place to protect a facility. This allows them to detect intruders right away that may have bypassed other security measures, like perimeter security. Some systems can also detect natural disasters and issue warnings. These systems can include motion detectors, security cameras and fire alarms. In some situations, having these devices record activities is enough. However, other facilities require a surveillance system to be actively managed by a guard or personnel.

Staff members

Often, business owners will need personnel to enforce physical security measures, and hiring security staff can help address issues as they arise. There are some staff members or security personnel that are explicitly hired to implement security plans, while others are only encouraged to take an active role when an emergency happens.

For instance, security guards and receptionists can act as gatekeepers, only giving access to those who are authorized. Patrols, on the other hand, can monitor a section of a facility at certain hours of the day. However, staff members shouldn't be the only physical security measure implemented in an organization. Security teams or other staff should be supplemented with other technologies and components to ensure that every ground that needs protection is covered.

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 all the potential risks in your building and design security plans to mitigate the potential for criminal activity.

Common threats to physical security

In the digital era we live in, the number of threats is alarmingly increasing, with many originating from cyberspace. From data breaches to hacking, the focus of many organizations has shifted, with greater focus on security solutions for physical security that also protect digital assets.

There are common threats to physical security. These threats can be targeted not only at the assets on your premises but also at your digital and human resources. Physical security threats can be natural or man-made, so it's vital that your strategy addresses both vulnerabilities. Threats can also be categorized based on the place of origin of the attacks:

Internal threats

This type of physical security threat comes from within your organization. Internal physical security risks are more challenging to contain than external threats as they are tougher to predict. They can be accidental or malicious in nature. Examples of such risks include:

- Employees committing theft or causing property damage
- Careless staff members leaving restricted areas open
- Mistakes made by your security team
- Faulty infrastructure or hazardous work conditions

In fact, internal theft from employees is estimated to top $50 billion each year for U.S. businesses. Therefore, you need to have security measures in place to keep internal members from being tempted to act maliciously. This can include RFID-enabled access devices and video security systems to protect critical areas of your facility.

Internal threats can also come from non-human sources such as fires due to faulty wiring, mishandled equipment, and more. Because these types of threats are harder to predict, it's best to identify any areas of your facility that are more exposed to this type of danger and take proactive steps to mitigate this physical security risk. A proper emergency preparedness and response plan is also a critical physical security measure for these types of scenarios.

External threats

As its name implies, this type of threat originates from outside your organization. This can include attacks from outside parties with malicious intent and natural disasters. External physical security threats can also include:

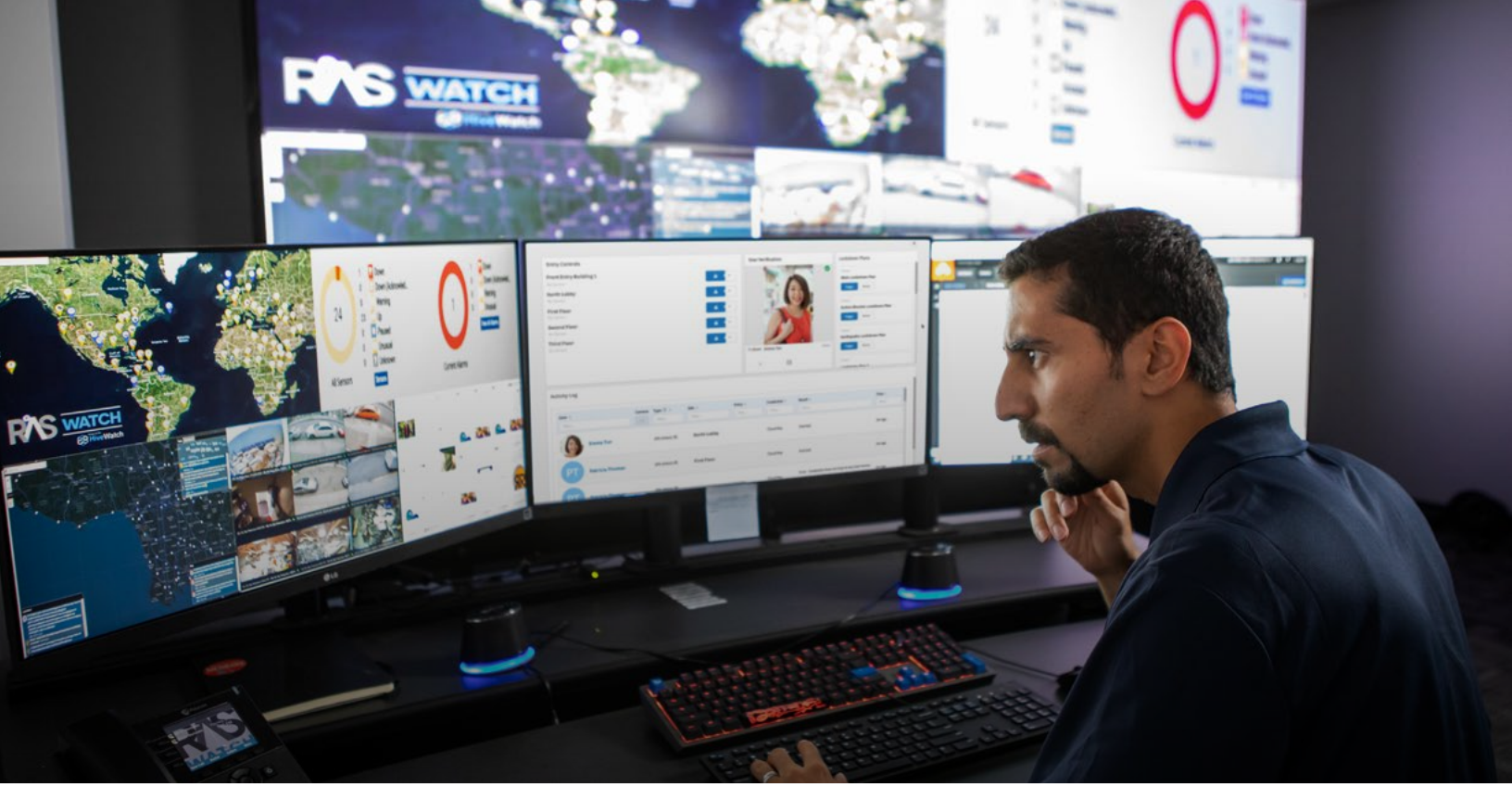
- Forced entry or break-ins
- Vandalism and property damage
- Unauthorized entry for persons outside your staff or approved visitor list

In the United States alone, theft from commercial properties accounted for more than 37 percent of all burglary crimes in 2019, according to data from the FBI. Most of the time, this type of crime is perpetrated by external actors. However, internal actors can also participate in such events, sometimes unknowingly by letting a tailgater into a building or leaving a door propped open by accident.

Natural threats

These physical security threats constitute damage caused by natural causes like floods, earthquakes, lightning strikes and other unpredictable natural disasters. In this situation, the physical security risk lies in the fact that such an event can cause extreme damage to your assets and endanger employees.

More than the loss of hardware, the loss of years of critical business data and investment, as well as injuries to your employees can have a severe blow to your business operation. This is why it is crucial that physical security strategies include proper training and communication for emergency procedures across every industry and property type.



WHY CYBER AND PHYSICAL SECURITY CONVERGENCE MATTERS

For digital infrastructure, cybersecurity plays an integral part in its safe operation. However, data systems can still be breached via a physical security threat. This is one reason many businesses today are turning toward cyber and physical security convergence for more proactive protection.

Cyber and physical converged security 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. This type of security strategy safeguards essential business data, critical and confidential information, as well as hardware, personnel and other tangible structures.

With more devices connected to internal networks than ever before, approaching cybersecurity with physical security measures in mind helps create a well-rounded strategy that covers your business from multiple angles and removes redundancies across your security teams.

PHYSICAL SECURITY BEST PRACTICES

So, what physical security measures should you have in place to keep your facility secure? What components of physical security should you give more attention to?

There is no one-size-fits-all physical security solution. Every organization has different needs, but there are common measures that, when adjusted to fit your situation, can help protect your organization from physical attacks.

Investing in security personnel

One of the best deterrents against possible attacks is visible security, and this is what investing in security personnel can guarantee. For example, you can hire extra security guards or change the existing patrol routes to cover more ground. Consider manning important entrances and exits, which can help ensure that no unauthorized entries or exits happen.

Having security personnel can also give your employees peace of mind and dissuade those with malicious intent from working against your business. However, having security guards doesn't automatically guarantee protection and safety. You also need to ensure that your security team understands your organizational requirements and is trained in the physical security measures your business is implementing. They should also have state-of-the-art equipment that they carry on their duty that can help deter and delay intruders. Security staff should also know how to respond appropriately in different security situations.

Using monitoring systems

Security guards can be effective in deterring and delaying intruders, but they can only detect threats within their proximity. This is where monitoring systems come into play. This type of physical security system can help you know what's happening in various areas of your facilities at the same time while preventing potential dangers. However, not all monitoring solutions are right for every property, and many factors contribute to their effectiveness.

Security cameras should be strategically placed in locations that can offer maximum visibility over your premises. These video recordings can act as evidence when a breach occurs, and cameras equipped with AI analytics can help security teams know where to focus in critical moments.

An automated alert system can notify the right person immediately in case of unauthorized access or suspicious movements in a particular area of your facility. This allows immediate response to threats to help lessen any damage.

Sensors can also help provide better situational awareness. Some examples of the physical security component include smoke sensors, temperature sensors, water or leak sensors and occupancy counting devices.

Some systems also allow security team leaders to check the location of their guards through GPS. This allows a quick response and delegation when an incident occurs, as leaders know who to call within the location of the incident.

Limiting facility access

Accessibility is an important factor to consider when it comes to security. Easy access to your facility makes it easier for malicious actors to compromise your assets. An effective way to stop this from happening is by restricting access to your facility.

How you will restrict access to your property depends on what you want to protect and the risks you want to minimize. In areas that need less security, a guard will suffice. Some situations may call for visitors to verify their identity and for guards to conduct security checks when entering and leaving the building. However, in areas where maximum physical security should be implemented, more advanced access control like biometric readers and coded locks should be in place.

Educating your employees

Even with the most advanced security systems and trained guards implemented in a facility, it is crucial that employees are made aware of physical security protocols, particularly when it comes to natural disasters and physical intrusion.

To guarantee that employees are prepared, make sure that they are well-trained to handle physical security threats. When they know the standard operating procedure, they can contribute to protecting an organization's assets. Additionally, educating employees can give them a peace of mind in knowing that they are protected when breaches and emergencies occur.

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 posturing:

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 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.

Final thoughts on physical security plans, systems and solutions

Every business is unique, and so are its physical security requirements. There is no one-size-fits-all approach that can protect all aspects of your business, so it's critical to ensure that your physical security plan is customized to your organization and facility. Understanding what physical security is, as well as what robust physical security standards are, is a good start.

As physical and digital worlds continuously overlap, you need a trusted partner that helps you navigate both. Conduct a thorough risk assessment and consult with a professional to get the most out of your physical security systems and technology.

MOTOROLA SOLUTIONS

AVIGILON™

Motorola Solutions, Inc. 500 West Monroe Street, Chicago, IL 60661 U.S.A. **motorolasolutions.com**