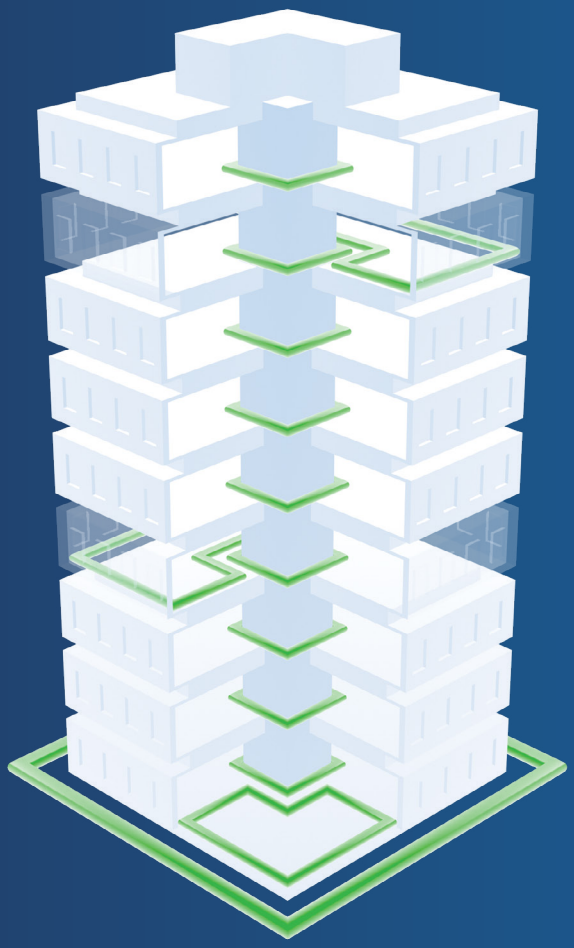
ANIXTER

GLOBAL TECHNOLOGY BRIEFING

RISK MANAGEMENT BEST PRACTICES

FIVE LAYERS OF PHYSICAL SECURITY



INTRODUCTION

A successful organization manages risk throughout its various divisions—everything from finance to human resources to facilities. Managing risk is also a central component of smart building design, where the right approach can holistically address physical and cyber challenges, reducing the risk of breach and increasing your peace of mind.

Without a solid foundation of a safe and secure environment for employees and visitors, organizations cannot devote the amount of energy and attention required to handle their important everyday challenges.

Commercial spaces, and the organizations that occupy them, exist for a particular purpose. Safe and secure environments enable an organization to focus and ultimately achieve that purpose.

Proactive vs. Reactive Security

The future of commercial security will see a split between practicing reactive security and proactive security. Proactive security anticipates risk and finds solutions while the threat is still manageable. Reactive security is costly, both in terms of the potential for tragedy and the potential for debilitating financial costs. Case in point, in the U.S. alone, workplace violence, just one of many elements of risk management, accounts for an annual price tag of $5 billion.

The National Crime Prevention Institute identifies three steps to move towards a proactive security approach:

- A vulnerability assessment to identify the deficiencies and excesses in the security process
- A cost/benefit analysis to determine if recommendations are affordable, feasible and practical
- A test of the system to confirm that everything is working properly and determine if changes need to be made to achieve the desired level of security

Sources: Booz Allen Hamilton, “The Role of Buildings in Mass Shootings” in Buildings.com. 2014.
Marianna Perry, National Crime Prevention Institute (NCPI),
“Proactive vs. Reactive Security” in Buildings.com. 2010.

CONSIDERATIONS

From Analog to IP Video Surveillance

A prominent trend in the security industry is an evolutionary shift from the traditional analog-based video surveillance technology first deployed in the 1950s to newer network-based digital systems. This migration provides many functional and financial benefits to companies who need to provide better protection for people and assets.

Video monitoring, recording and analysis can be made available to responsible parties, wherever and whenever needed, thanks to advances in microprocessors and other computer technologies. High-quality cameras may now be plugged in wherever there's a suitable port, enjoying the flexibility and manageability of today's telephone and computer systems. Live and recorded video can be accessed from network attached PCs across local area networks (LANs) or the Internet using familiar network technologies such as Ethernet and Internet Protocol (IP).

Investment vs. Risk: Striking a Balance

Physical security deployments are significant investments with the majority of costs incurred upfront. Once installed, these security systems are often considered adequate, receiving little to no maintenance post installation. However, processes become outdated while those with malicious intent become more sophisticated. By building a scalable interoperable security solution, proactive updates and upgrades are simpler, quicker and more cost-effective than complete system revisions, helping you effectively balance the costs of maintaining a robust physical security system with reduced risk of attack and breach.

Steps You Must Take

1. Create a Battle Plan

What are the plans and procedures to defend against threats that are increasing in sophistication and complexity?

2. Invest the Time to Stay Informed

Being properly plugged in with the commercial building security world should be a priority for an organization. Join some of the active, vibrant communities of security professionals, who share updates on the latest threats and ways to overcome them. Attend industry conferences and join, participate, listen, learn and share.

3. Complete Organizational Commitment, Including the Budget

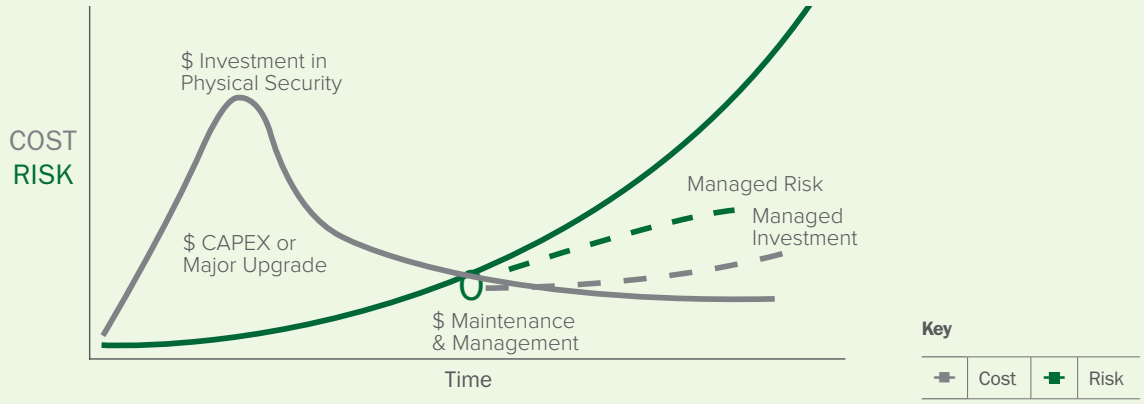
From the boardroom to the front lines, an organization must have complete buy-in and commitment to the level of security it requires. To stay ahead of the risk factors, the strategy must be to exceed the requirements, not to simply accomplish the minimum.

Maintaining Sound Policies and Procedures

It is critical to maintain and follow sound policies and procedures. This is part of an overall security plan that balances best practices with a willingness to evolve to properly defend against new threats.

- A policy document is a living, breathing thing. Policies are not static. Policies should be frequently reviewed and updated.
- Security protocols should be understood by all and followed closely.
- Complacency must be avoided throughout the organization.
- Logical security and physical security policies are interrelated and support one another. The logical security strategy should have a physical component to it.

Investment vs. Risk

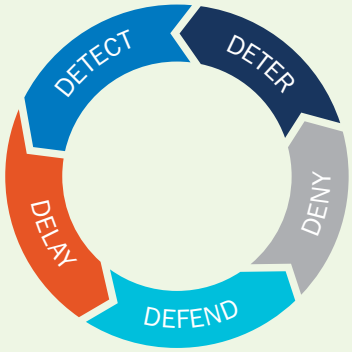


Prevention, Detection, Response

While it may not be possible to ensure complete protection at all times, employing an approach that responds to each stage of a threat is crucial in mitigating serious harm. It is important to consider your approach to the "Five Ds" of protection in a commercial setting:

- Deter
- Detect
- Delay
- Defend
- Deny

Defense in Depth: "Five Ds" of Protection



A layered approach to security for critical infrastructures

The Necessity of Interoperability

The entire ecosystem that serves the commercial building security market is continuing to evolve to provide more interoperable solutions that will eventually support standards based open architectures. However, today there are still disparate systems that do not integrate with one another. This creates security gaps that are an impediment to the mission of keeping people and facilities safe.

Commercial security has made great interoperability progress by developing network-based solutions that have the same communication protocols.

Formerly, manufacturers built proprietary systems without regard to integration with other systems or manufacturers. Today they are opening up their application programming interfaces (API) to allow integration with many other security subsystems. There is still one host system, usually the access control system, which releases their API so other subsystems can integrate to it. This requires the manufacturers to work together to keep everyone updated on new software and firmware upgrades and hardware enhancements.

Clearly, the future of commercial building security will include smart security systems that have standards-based open architecture environments with a multifaceted, layered approach, allowing components from multiple manufacturers to work as one seamless interoperable system. This will enable a scalable, flexible, long-term security solution and put the end user in control. The length of time it takes to get to a true standards-based open architecture is dependent on the end user's requirements for such a solution.

Safety-Critical Is Security-Critical

According to Gartner, there are three core lessons for organizations seeking to create a safe and secure experience for their customers, employees and partners.

1. Safety and security planning and governance must be aligned to account for security's impact on safety technologies and services.
2. Cyber-physical security practice can be enhanced by embracing some safety cultural principles, behaviors and attitudes.
3. Focus on the cyber-physical security lessons being learned today in the convergence of IT/OT and the deployment of security for the Internet of Things.

Source: Earl Perkins, Gartner. The Marriage of Cybersecurity and Safety for Organizations.

Cyber Security and Automation

With the massive benefits for a company from automation within a commercial building, it is important to consider the potential threats as well, and develop a proactive strategy to address building automation systems, safety systems and critical environmental technology from a security perspective.

Data breaches to obtain credit card information are the most common and publicized cyber threat, though other potential dangers include the following:

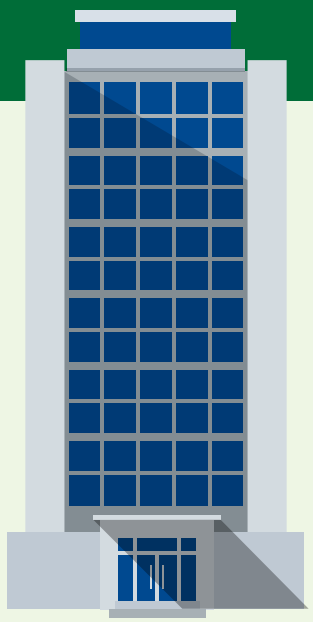
1. Shutting down heating or cooling for sensitive locations such as pharmaceutical or food processing plants
2. Manipulating cooling settings on an HVAC system in a corporate building, creating significant business disruption and lost productivity
3. Shutting down cooling or power management functions for a data center, destroying IT equipment and taking business critical applications offline
4. Gaining unauthorized access to an Internet-connected physical security system to enable kinetic attacks

The cyber-related threats pose increased economic burden on an organization if not handled proactively. The United States Department of Defense recently developed the Unified Facilities Criteria, which states:

"While the inclusion of cyber security during the design and construction of control systems will increase the cost of both design and construction, it is more cost-effective to implement these security controls starting at design than to implement them on a designed and installed system. Historically, control systems have not included these cyber security requirements, so the addition of these cyber security requirements will increase both cost and security. The increase in cost will be lower than the increase in cost of applying these requirements after design."

Source: Johnson Controls and Booz Allen Hamilton Inc., CyberSmart Buildings: Securing Your Investments in Connectivity and Automation. February 2017.

876,000
number of IP-enabled management-level HVAC controllers in **2015**



1,100,000
number of IP-enabled management-level HVAC controllers in **2018**

- **95%** of building systems that are connected to the Internet have insecure connections
- **65%** of vendors have remote access to building systems
- **85%** have no vendor access policy
- **92%** of building system computers are running outdated, insecure, unpatched software
- **40%** of building control and monitoring systems have a potential backdoor to the Corporate Network

695,000
the number of attacks on SCADA systems doubled from 2013 to 2014

69,666
known vulnerabilities reported by NIST in the National Vulnerability Database

9,400
new vulnerabilities found in 2014 alone, 2/3 were related to network attacks

Note: Statistics represent U.S. only.

Source: Intelligent Buildings, CyberSafe. 2016.

CHALLENGES

Challenge I:
Providing a Safe Workplace

Employees today expect at a minimum to be provided with a safe working environment. This is essential not just in attracting and retaining key talent, but also allows staff to focus on daily tasks, which can improve business productivity.

The challenge for employers is to leverage technology and policies to protect against internal and external threats.

Additional trends include the following:

- Violence is becoming more common in today's workplace, representing billions of dollars in liability around the world.
- The prevalence of smart devices is a major cause of theft in the workplace. At risk is not only sensitive personal information but also any company data stored on these mobile devices.
- Cyber threats are a reality for all businesses, not just large corporations.

Key Commercial Building Risk Trends

WORKPLACE VIOLENCE

Annual estimated price tag of $5B in the U.S. alone

Source: Booz Allen Hamilton

VISITOR SAFETY

Commercial security will see a split between practicing reactive security and proactive security

Source: Security Magazine

MOBILE DEVICE THEFT

60% of IT admins reported a lost or stolen smart phone in the last year

Source: lookout.com

CYBER THREATS

It's not a matter of IF a company is hacked, it's only a matter of WHEN

Source: OccamSec

Challenge II: Preventing Theft

Trust is crucial to growth within a successful organization. An approach that relies on a reactive response to theft can easily erode this trust.

Employers have the responsibility to protect both personal and business assets.

The challenge is to maintain privacy while also monitoring for potential criminal activity.

Variance in Valuables Adds Complexity

Certain technologies and policies can assist in theft prevention of personal items like phones and purses. Very different kinds of technology can be more effective in theft prevention of company consumables, which includes everything from office and janitorial supplies to kitchenware.

This challenge is also informed by considering what the building is used for, when it is used and particularly who will be using it.

Challenge III: Achieving Regulatory Compliance

Regulatory compliance can be complex in a commercial setting, involving accessibility, energy use, data management and physical design.

Organizations must consider how to meet audit requirements to comply with various regulations. Depending on the industry and its objectives, this may include SOX, HIPAA, PCI-DSS, OSHA and ADA, among others.

OSHA
The OSH Act created the Occupational Safety and Health Administration (OSHA), which sets and enforces protective workplace safety and health standards. OSHA also provides information, training and assistance to employers and employees.

OSHA standards for commercial buildings include:

1910.36a	Exit routes must be permanent
1910.36a2	Exits must be separated by fire-resistant materials
1910.36a3	Exits must be a self-closing and latching fire door
1910.36b	Adequate number of exit routes required
1910.36c1	Exits must discharge to a refuge area
1910.36d	Exit doors must be unlocked from the inside
1910.36e2	Doors must swing in direction of egress
1910.36f	Capacity of an exit route
1910.36g	Exit route height and width requirements
1926.34a	Obstructed means of egress
1926.34b	Clearly marked exit signs
1926.34c	Continual maintenance of egress pathways
1926.35a	Written emergency action plans
1926.35b1	Emergency escape procedures and routes
1926.35b2	Emergency critical operations procedures
1926.35b3	Emergency mustering procedures

ADA
The Americans with Disabilities Act (ADA) defines and enforces requirements for all new commercial building construction and alterations. Its purpose is to remove accessibility barriers in all state and local government buildings as well as public accommodations, transportation and commercial facilities.

NFPA
The National Fire Protection Association (NFPA) develops and publishes more than 300 consensus codes and standards intended to eliminate death, injury, property and economic loss due to fire, electrical and related hazards. NFPA codes and standards, administered by more than 250 Technical Committees comprising nearly 9,000 volunteer committee member seats, are adopted and used throughout the world.

Code examples include:

101 NFPA 101 is the Life Safety Code that is the most widely used source for strategies to protect people based on building construction, protection, and occupancy. Its purpose is to minimize the effects of fire and related hazards. It is the only document that covers life safety in both new and existing structures. It includes provisions for all types of occupancies, with requirements for egress, features of fire protection, sprinkler systems, alarms, emergency lighting, smoke barriers, and special hazard protection.

80 NFPA 80 addresses general requirements and provisions for care and maintenance of fire doors and other opening protectives including swinging doors, horizontally sliding doors, vertically sliding fire doors, rolling steel doors, fire shutters, service counter fire doors, hoistway doors for elevators and dumbwaiters, chute doors, access doors, fire windows, glass block assemblies, fire dampers and fabric fire safety curtains.

72 Rules cover the application, installation, location, performance, inspection, testing and maintenance of fire alarm systems, supervising station alarm systems, public emergency alarm reporting systems, fire warning equipment and emergency communications systems (ECS), and their components. Provisions are expressed in prescriptive requirements with performance-based design methods and risk analysis requirements provided and essential for the proper design and integration of mass notification systems.

Challenge IV: Preventing Cyber Threats

When a single data breach can cost the average company $4 million, preventing cyber threats in an IoT environment is crucial to managing risk and reputation.

This may be the biggest challenge for businesses today due to the vulnerability of the increasing number of networked devices and sensors. Even in existing buildings, there are likely multiple systems connected to the outside world via an Internet connection. They may have been put in by a system supplier to provide remote monitoring to reduce the cost of an operations service contract, or they may require connectivity to a cloud service. There are many opportunities to use the experience of the IT world to mitigate the risk of these connected systems using best practices on policies, monitoring and hardware.

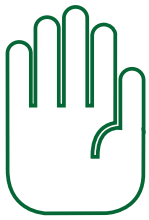
It's essential to consider best practices to prevent hacking of IP devices that reside on your network. For example, cameras and similar devices typically hold predefined security measures that always should be changed. A best practice would be to customize the settings to match the requirements for the rest of all IT infrastructure.

The reality of BYOD (Bring Your Own Device) environments creates additional challenges, as a person bringing multiple devices into a building is essentially bringing multiple new doors that could be opened for a costly breach.

In the future, smart buildings will provide an open architecture where sophisticated security technologies and protocols will combat new and evolving threats.

Source; IBM, Cost of Data Breach Study. 2015.

Challenge V: Limiting Physical Building and Network Accessibility



Directing the flow of traffic among employees and visitors is essential to providing a safe environment, made all the more challenging with the goal to provide seamless and secure network access.

This comes down to an ability to authenticate the identity of who is accessing the building and the network.

Today, advancing technologies and malicious strategies require another question to be considered—how do you ensure the person using the credential is in fact the person assigned to that credential?

The Key Is Biometrics

Access control credentials only identify the credential, not the person who is holding it. Biometrics positively authenticate an individual by identifying their measurable physiological traits, such as fingerprints, iris patterns and facial or hand geometry, before granting access to a restricted area. Biometrics has two modes: verification and identification.

VERIFICATION

Verification uses a one-to-one comparison and requires a secondary credential. In this case, the biometric element simply confirms that the person using that credential is the individual to whom it was issued as well as holds the authority to enter. One-to-one verification can be achieved by storing biometric templates in the reader database or storing the biometric template on a credential. Storing the biometric template on a credential maintains privacy regulations that prevent storage of biometric data; it also serves as dual authentication. Triple authentication includes a pin code along with the credential and biometrics. The user enters their pin code to recall their template in the reader to be matched to their live biometrics. Storing a biometric template on a credential works well but if the end user is seeking to eliminate credentials, then this method will not be ideal.

IDENTIFICATION

Identification is the process of determining that the person requesting access is who they say they are. This involves matching the biometric characteristic to a template called up from a central database. Biometric identification uses a one-to-many comparison in order to ascertain whether a given user is authorized for entry. The biometric characteristic alone is used, and is compared to all templates in the database until a match is found or the data is rejected as unidentified. Since the stored template and the live biometric are converted to an encrypted algorithm, matching occurs instantaneously.

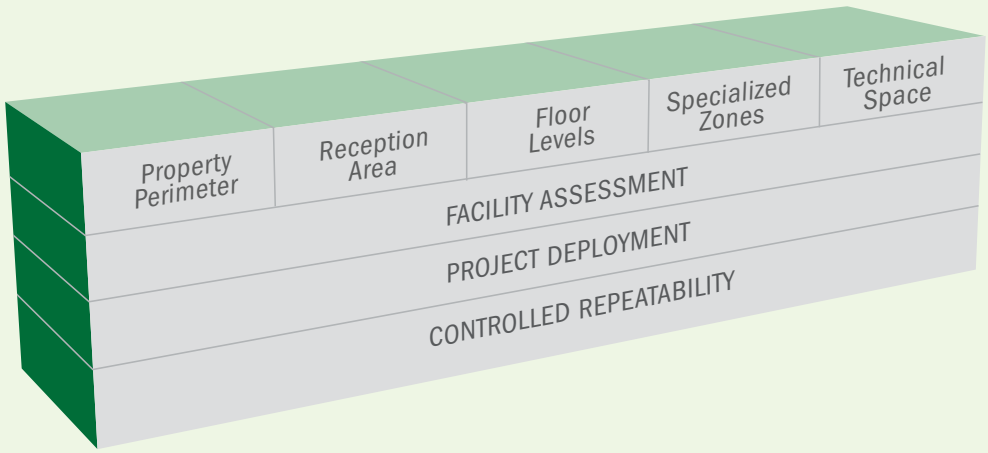
SOLUTIONS

The Anixter Approach

Five Layers of Physical Security

In today's world, there is a strong emphasis on providing a secure and safe environment for a modern workforce. Reducing risk and increasing peace of mind allows staff to focus on the task at hand. Anixter's layered physical security approach provides you with the ability to deter, detect, delay, defend and deny at every layer of your commercial building.

In addition to micro-segmentation of logical security, our approach provides commercial building managers with a clear set of guidelines and best practices for macro-level security implementation.



Best Practice I:
Property Perimeter

Establish a physical defense around the property perimeter and building exterior doors to deter external threats.

Considerations

When protecting the property perimeter, it is important to consider:

- ☐ How do you manage vehicle and pedestrian entrances and exits during and after business hours?
- ☐ How do you monitor and control parking facilities?
- ☐ What methods do you use to prevent unauthorized access to the building?
- ☐ How do keep the building accessible to the handicapped and emergency personnel?

Recommended Solutions

Parking Lots and Parking Structures
Access to medium security commercial building parking areas can be managed with unattended drop-arm gates and UHF readers with window tags that allow for extended read ranges. Readers can be configured as standalone systems or connected into the building's access control system. Drop-arm gates with self-service ticket dispensers control access to visitor parking. IP intercoms with or without video integration are used for authorization before entering the parking area.

High security commercial buildings typically have guard shacks and rolling gates to control traffic, while active vehicle barriers and ram-resistant cable barriers prevent vehicles from penetrating the property perimeter.

Parking Structure Emergency Communications Systems
Emergency call stations, identified by high-visibility colored lighting, allow for contact directly to emergency personnel. Integrated video enables security personnel to see what is happening. The stations are connected to the building's VoIP phone system and can even roll over to smartphones.

RISK MANAGEMENT BEST PRACTICES

Building Perimeter
Fixed bollards or heavy cement planters prevent vehicles from breaching the building perimeter. Bollards can be manually retractable to allow for maintenance vehicles.

Loading Docks
Loading dock doors are vulnerable to unauthorized access and should be locked and monitored. Wide dynamic range (WDR) cameras are appropriate due to the fluctuation in light levels. Door prop alarms can prevent doors from being left unsecured, while intercoms with or without integrated video allow authorized couriers into the building for deliveries.

Lobby Entry Doors
Access control with automatically scheduled unlock and lock times allow the doors to be open during business hours but locked to the general public after hours. The First Person In (FPI) function prevents the doors from unlocking until the first tenant enters, which is important on snow days or holidays for example. Access control is used after business hours to allow tenants in and record their entry. Often the same access control system manages both the building perimeter and the tenant suites, so tenants can use one credential for both.

Stairwells and Emergency Exits
To control pedestrian access, all secondary doors and stairwell exits should be exit only with night latch function hardware that is locked from the outside or with no exterior hardware at all. These doors should have exit devices on them for unimpeded egress and door closers to close and relock after exiting. They should also be monitored and/or alarmed to prevent them from being propped open.

Key Control
A patented restricted key system prevents unauthorized key duplication of the master keys and suite keys while providing building management, maintenance and cleaning crews access throughout the building. Doors with electronic access control should have a mechanical key bypass and lockdown capability for emergencies.

Handicap Access
The Americans with Disabilities Act (ADA) requires that all commercial building provide unimpeded access for handicapped persons. Automatic door operators using a chain drive motor can open heavy lobby doors upon the push of a wired or wireless handicap button.

Video Surveillance
To monitor the exterior of the building with changing levels of light, wide dynamic range (WDR) cameras are effective. High-resolution, multi-sensor panoramic cameras can monitor critical areas and entranceways. Video surveillance can be sent to mobile devices, such as smartphones or tablets, to enable security personnel to monitor the video on the go. Video analytics enhances efficiency by creating automated parameters that filter out normal motion events and detect events that security should review. License plate recognition (LPR) software can be used to monitor traffic and access to specific parking areas on the property.

Emergency Key Boxes
Required for most commercial buildings, these are mounted on the exterior of the building near the main lobby doors. Master keys are stored inside for emergency first responders. Access is restricted to police and fire rescue personnel.

Emergency Voice Systems (EVS)/Mass Notification
Located in a security command center or in the reception area of the building, emergency voice systems can allow emergency personnel to reach all building occupants with specific instructions for evacuation or shelter in place situations. Advanced features can send alerts to digital signage, desktop computers and VoIP phones. Phone, text or email alerts can also be sent to individuals.

Best Practice II:
Reception Area

Control access beyond the lobby area and access to tenant or office spaces on higher floors within the building.

Considerations

When protecting the reception area, it is important to consider:

- ☐ What role does reception play in enforcing your security policy?
- ☐ How do you manage visitors and contractors?
- ☐ Does your building contain multiple tenants?
- ☐ Are there restricted floors within the building?

Recommended Solutions

Electronic Visitor Management

Electronic visitor management systems enable preregistration of visitors and contractors. Visitors can use a kiosk to accept company policies, NDAs or other criteria, and badges can be printed as temporary credentials. Coupled with an employee/tenant badging system, this creates an environment of alertness as visitors are identified and deterred from entering restricted areas. Electronic records are kept to quickly reregister return visitors, flag barred visitors and account for visitors in case of emergencies.

Glass and Optical Turnstiles

Turnstiles restrict unauthorized personnel from going past the lobby. Glass turnstiles use a physical glass barrier that is waist or full height, while optical turnstiles may have only an arm to restrict access. Both use beam optics to verify that only one person is going through the turnstile with the card read.

Credentials
Depending on the building's security requirements, credentials to operate turnstiles can range from low-security temporary barcodes to permanent card badges to advanced biometric readers.

Video Management System
Video surveillance in the reception area monitors and records during business hours as well as afterhours. The video management system (VMS) can be integrated with the access control system to provide a visual record of activity. Choosing a VMS is critical, as all video surveillance footage is viewed and extracted through the VMS. VMS software must meet the facility's current and growth needs, allowing for management of not just video surveillance but other linked operational technology systems.

Video Analytics
Analytics can monitor pedestrian traffic flow, detect people entering through an exit and identify parcels left in the reception area. The video monitoring station in the lobby should be optimized to support processing of the video footage.

Best Practice III:
Floor Levels

Manage floor access to office/tenant areas and building operations rooms.

Considerations

When protecting restricted floor levels, it is important to consider:

- ☐ How do you manage floor access through elevators and stairwells?
- ☐ How do you keep tenant spaces secure while allowing building services to have full access?
- ☐ How do you maintain a clear stairwell egress and ingress path during building emergencies?

Recommended Solutions

Visitor Management
In a multi-tenant building, visitor management systems can be deployed at the suite level with basic features. Requirements may only include onsite registration, visitor badge printing and electronic visitor records.

Mechanical Access Control
Tenants in most cases only require mechanical keys to enter their suite. Their keys do not operate in other tenant spaces or utility and janitorial rooms. Master keys can gain access to tenant and utility spaces on all floors, or the key system can be designed with individual floor masters.

Electronic Access Control
Building electronic access control systems can be partitioned so that the individual departments or tenants can only view and manage their individual areas or suites. However, the property manager has the ability to manage the complete system. This allows the tenant to use the same credential to access the parking area, building entry and their own space.

Elevators
Card readers in elevator cabs allow access to individual floors based on access control permissions. Usually only tenants have credentials that operate readers in the cabs.

Stairwells
Stairwells need to be locked from the stairwell side, but upon alarm activation, the doors must unlock on both sides on all floors to allow free ingress and egress for evacuation and emergency personnel. Stairwell doors must also close and latch every time to prevent fire from spreading through the stairwells. Specialized “high-rise” locks are required that are dual failsafe. These can be energized to lock under normal access conditions and unlock under emergency conditions. Building access control systems can connect into the high-rise locks and have readers in the stairwells for access.

Elevator Video and Communications
Cameras in vandal-resistant enclosures monitor events in the individual elevator cabs. Video transmission can be done through the elevator cable bundle or wirelessly with a transmitter on the top of the cab and a receiver at the top of the elevator shaft. Emergency intercoms are required in all elevator cabs for two-way communication to emergency personnel.

Video Surveillance
Doors that access floors and suite entrances should deploy video surveillance to record all access and egress events. Set to record on motion, video surveillance can be standalone or integrated with an electronic access control system for video verification. Lower resolution (720p) can be used in small spaces.

Best Practice IV:
Department Zones

Secure assets and comply with privacy regulations with attention to specialized departmental zones.

Considerations

When protecting department zones, it is important to consider:

- ☐ What are your key business areas you need to protect?
- ☐ How do you secure departmental assets and records?
- ☐ How do you comply with privacy regulations?

Recommended Solutions

Electronic Access Control
Electronic access control can prevent unauthorized personnel from entering restricted departments, such as human resources, legal or finance. If a suite already has electronic access control integrated into the building, then adding access control to a department entrance is done through the existing system. Otherwise, standalone battery-powered access control locks can be installed on the door.

Mechanical Key Bypass
Access controlled doors should always have a mechanical key bypass, and keys should be restricted to prevent unauthorized duplication and use.

RISK MANAGEMENT BEST PRACTICES

Company Records Protection
External file cabinet locking bars attached to existing file cabinets allow extra security for critical files and records. This can help you maintain compliance with company policy or regulations requiring higher security methods or dual control practices. Additionally, fireproof file cabinets and records safes can be used to protect critical documents from fire and theft.

Mechanical Key Management
Key management boxes are used to organize keys to doors, file cabinets and desks, while electronic key records management keeps track of what the keys operate and who they are issued to.

Video Surveillance
Careful consideration should be taken when actively monitoring employees in work areas, as this has an adverse effect on morale. In work areas, video surveillance can be deployed to monitor critical assets and records—for example, monetary collection and handling.

Corporate Day Lockers
With more employees working remotely and using shared resources, day lockers can optimize work space for multiple users by allowing employees to store their personal items at the end of a day's work.

Workplace Asset Management
In higher security applications, passive RFID is used to ensure company assets remain in the building. High-value assets use active RFID tags to be able to track their location in real time.

Best Practice V:
Technical Space

Protect networking infrastructure, IT servers and data storage in technical areas.

Considerations

When protecting technical spaces, it is important to consider:

- ☐ How do you secure IT equipment?
- ☐ What is your procedure for server room access?
- ☐ How do you manage contractor access to data suites and cabinets?
- ☐ How are you maintaining compliance with SOX and PCI-DSS?
- ☐ How do you ensure the environmental requirements are being met inside the technical spaces?

Recommended Solutions

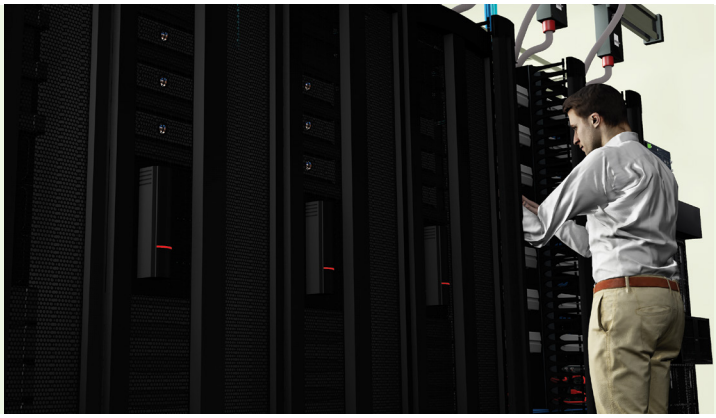
Data Centers

Standard data center security protocols apply for tenant data centers. Electronic access control with biometric readers can positively authenticate authorized users before access is granted, while man traps with anti-tailgating systems verify that only one person is entering the data center per valid credential. Free egress through both doors of the man trap is required to comply with life safety regulations.

Computer Rooms

In multi-tenant buildings, a small room within the tenant suite usually holds the IT equipment and servers, often on racks rather than in data cabinets. The level of security at this entry point is reflected by the risk or compromise of the information on the servers in the room. Access to the computer room may be restricted by any of the following methods:

- A restricted key system that has a master key level or is keyed different from all other locks in the suite
- A single-code mechanical push button lock that provides 24/7 access but no access records



- A battery-powered standalone lock with multiple codes that has no access records but can be put into a lockout mode that requires a specified manager code to access or activate/deactivate
- A battery-powered standalone lock with multiple codes and/or credentials plus time zone restrictions and access records
- Hard-wired networked access control with real-time monitoring and video integration, providing the ability to retrieve access records, change user permissions from anywhere in the network and implement dual custody access, dual authentication and biometric credential security

Data Cabinet Security

Keeping records of who entered a data cabinet and when is critical to maintaining company and regulatory compliance. Electronic access control at the data cabinet level captures all access records in addition to regulating who has access. It can even restrict contractors' access to specific days and times. In higher security applications, biometric readers at the cabinet can positively authenticate the individual before allowing access to the cabinet.

Electronic Key Management

For smaller data centers or computer rooms, electronic access control may not be cost effective. Electronic key management boxes secure the data cabinet keys in the cabinet. Only authorized persons can open the cabinet and can remove only the keys that they are authorized to use. The key management box records who removed the key, what time it was removed and what time it was returned. Access records are stored in the box and can be downloaded onto a flash drive for analysis.

Video Surveillance

Video surveillance provides a visual record of who has accessed the data center and data cabinets. Since IT spaces typically feature low light due to limited human presence, surveillance cameras should be able to capture usable images in low light conditions. Corridor format cameras focus on the space between rows of cabinets.

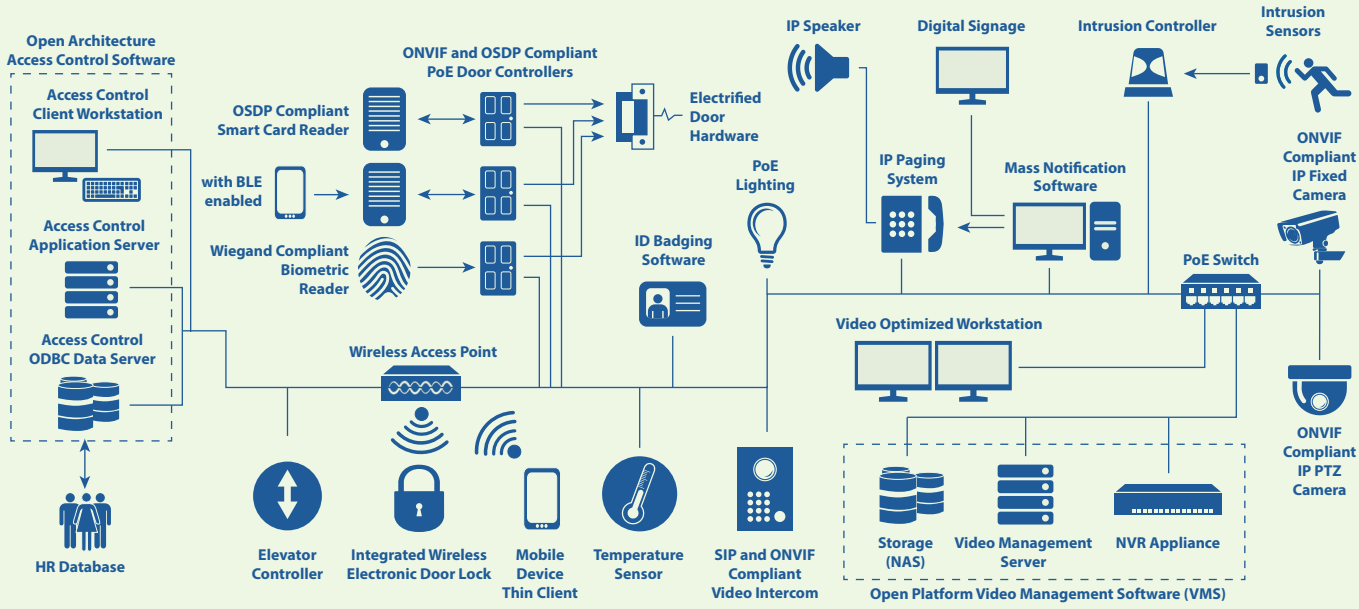
Additionally, the IT space is where the video is being stored. The switches, servers, and storage for video surveillance need to be optimized for that application, and the devices need to meet specific criteria to continuously perform their functions in a secure manner.

Environmental Monitoring

Ensuring the IT equipment is running within a defined temperature range could also be part of the risk management process. Monitoring temperature, power and potential water leakage inside these spaces is a recommended best practice for all communications room spaces.

Open Architecture Security Solution

The concept of open architecture security systems suggest flexibility with best-of-breed options and the latest technology. This view represents the challenge of these technologies working together.



TECHNOLOGY SUMMARY

Technology Solutions

The chart below details the technology solutions that can support a layered security approach in a commercial building.

TECHNOLOGY	Property Perimeter	Reception Area	Floor Level	Specialized Zones	Technical Space
Emergency call boxes	✓				
Access control		✓	✓	✓	✓
Intrusion detection	✓	✓	✓	✓	✓
Fire detection and suppression		✓	✓	✓	✓
Visitor management software	✓	✓	✓		
Mass notification	✓	✓	✓	✓	✓
Surveillance solutions	✓	✓	✓	✓	✓
Server storage and workstations					✓
Video management software					✓
Content analytics					✓

Anixter's Technology Support Services can offer further insight to your specific application. For more information, contact your local Anixter representative.

anixter.com/commercialbuilding

SUPPLY CHAIN SOLUTIONS

As you develop a smart building roadmap, it's also important to consider the physical migration from the existing environment to the building's future state. This entails identifying the challenges and risks during the installation phases of technology deployment. Coordination between material deployment and installation schedules can have an impact on the productivity, efficiency and connectivity of work environments.

Properly coordinated deployments allow for tangible savings in time, reduced installation costs and increased efficiencies, all while reducing the risks of lost productivity associated with the physical migration of the building environment.

Challenge	Service	Save Time	Reduce Costs	Increase Efficiency	Mitigate Risk
Coordinating the deployment of the right system components that corresponds with the integrator installation schedule	Deployment and technical services	✓	✓	✓	✓
Confirming all system components work properly as an integrated solution	Interoperability testing		✓	✓	✓
Video camera deployment and on-going maintenance	IP addressing and serial number tracking	✓	✓	✓	
Coordinating installations by kitting similar solution components	Custom part number for each unique configuration	✓	✓	✓	✓
Managing integrator SLAs and maintenance agreements	Life cycle management, asset management and managing maintenance costs and upgrades		✓		✓

For more information, contact your local Anixter representative.

anixter.com/services

ANIXTER

SPONSORED BY ANIXTER'S TECHNOLOGY ALLIANCE PARTNERS℠

Anixter's Technology Alliance Partners provide solutions designed to connect the world's most important systems. Our partners help organizations operate more efficiently and securely while maximizing value.

Allied Telesis · Life Is On APC by Schneider Electric · ATLONA a Panduit company · AVAYA · AXIS COMMUNICATIONS

BARCO · BELDEN SENDING ALL THE RIGHT SIGNALS · Berk-Tek A NEXANS COMPANY · BOSCH Invented for life · Cambium Networks · Comba

CHATSWORTH PRODUCTS · COMMSCOPE · CORNING · EnGenius · FLUKE networks · General Cable A Brand of Prysmian Group

legrand AV · legrand Cablofil · LEVITON · LG Life's Good · milestone · NEC

Nexans · OBERON · PANDUIT · Polycom · Prysmian Group · RUCKUS

sera4 · Signify the meaning of light · Specified Technologies STI Inc. THE FIRESTOP AUTHORITY · SUPERIOR ESSEX · TRIPP·LITE · VERTIV

GLOBAL REACH. LOCAL ADVANTAGE.

With Anixter, you get a true local partner around the world. No other distributor of our kind can claim an in-country presence in approximately 50 countries and in over 300 cities.

We do business in more than 35 currencies and 30 languages, which means we are uniquely positioned to help facilitate your project in the local environment, reduce risks and keep costs down.

- FOUNDED 1957
- OVER 9,400 EMPLOYEES
- OVER $8.8 BILLION IN SALES
- APPROXIMATELY 50 COUNTRIES
- IN OVER 300 CITIES
- OVER 100,000 CUSTOMERS
- NEARLY 600,000 PRODUCTS
- OVER $1 BILLION INVENTORY
- FORTUNE 500 COMPANY
- STOCK SYMBOL AXE

About Anixter: anixter.com/aboutus
Legal Statement: anixter.com/legalstatement

Anixter Inc. World Headquarters
2301 Patriot Boulevard
Glenview, Illinois 60026
1.224.521.8000