Building a Robust Physical Security Team

A guide for enterprise security leaders to maximize efficiency and value.

siteowl®

TABLE OF CONTENTS

INTRODUCTION

Welcome to Building a Robust Physical Security Team: A Guide for Enterprises.

In the rapidly evolving security landscape, the importance of a well-structured and capable physical security team cannot be overstated. Even as cybersecurity continues to be a top priority for businesses, the reality is without a robust physical security infrastructure, it's nearly impossible to protect a company from the myriad of risks that can threaten its operations and reputation.

Enterprises, big and small, face a number of security challenges that require a proactive and comprehensive approach to safeguard their assets, employees, and operations.

- 88% of U.S. businesses now experience more physical security threats.
- 75% of companies consider physical security as one of their top priorities.
- 85% of cyber security breaches involved a human element; this includes exposure to insider threats and physical breaches.

Who is this guide for?

This guide is for enterprise security leaders that want to leverage the latest technology and best practices to build a robust physical security team for their enterprise. No shortcuts, no quick fixes, no magic bullets. This guide will take you through the process of building a robust physical security team from the ground up.

What is covered in this guide?

This ebook offers insights and strategies to create a resilient physical security team that protects your enterprise.

SECTION 1	Enterprise Physical Security 101,' lays the foundation, addressing the critical aspects of assessing your current security posture, defining the team's scope, and integrating key stakeholders.
SECTION 2	'Best Practices for Building a Robust Physical Security Team,' delves into essential team capabilities, physical security systems, and adopting a lifecycle framework for continuous improvement.
SECTION 3	The Future of Physical Security Teams,' explores emerging challenges, technological opportunities, and creating a secure environment for thriving business operations.

We've also created SiteOwl Insights packed with actionable tips to help you build a robust physical security team that prioritizes lifecycle management so that you can get the most out of your physical security investments.

Let's go!

SECTION 1

Enterprise Physical Security 101

1.1 Assess your physical security posture

Your physical security posture is the overall state of your security measures and their effectiveness. As an enterprise security leader, you know firsthand that without a strong security posture, your organization is vulnerable to a wide range of risks including:

- **Unauthorized access**

  This includes unauthorized individuals gaining access to your organization's premises, facilities, or systems. According to the Ponemon Institute's 2020 Report, 10% of malicious breaches are caused by a physical security compromise. The report also states that it takes 223 days to identify a physical breach and 69 days to contain it.

- **Physical damage**

  Physical security encompasses protection against damage to an organization's property, equipment, or data resulting from fire, theft, vandalism, or other physical threats. While cybersecurity threats are often highlighted, statistics show that 60% of companies have encountered a physical security breach in the last five years, emphasizing the significance of addressing physical security risks alongside cybersecurity measures to safeguard organizations effectively.

- **Business disruption**

  Any event that disrupts an organization's normal operations, such as power outages, cyberattacks, or natural disasters, falls under the scope of physical security concerns. In a recent 2022 State of Protective Intelligence Report, 88% of business and security leaders acknowledged a rise in physical threats targeting their enterprise organizations.

- **Reputational damage**

  Physical security concerns encompass potential damages to an organization's reputation resulting from security breaches, data leaks, or incidents.

CONDUCTING A PHYSICAL SECURITY ASSESSMENT

Assessing your physical security posture is important to identify any weaknesses, and help you prioritize your security investments.
Another way to think about the assessment is to consider how much risk you are willing to accept. Ask yourself the following questions:

- What are the critical assets that need to be protected?
- What are the current security measures in place to protect these assets?
- Are there any gaps in the current security measures?
- Are the physical security systems being properly maintained?
- What are the most important security investments that need to be made?
- What's my budget for physical security?

Business continuity is central to these concerns, with 69% of security executives emphasizing that a fatality due to missed physical threats could lead to irrecoverable financial and reputational consequences.

Methods for assessing your physical security posture

Depending on your industry and risk profile, there are many ways to assess your security posture. For example, in the manufacturing sector, security teams tend to focus on the risk of theft, cargo tampering, and facility damage. Whereas in the financial sector protecting data centers and securing the premises against intrusion is more of a priority.

Regardless of your industry, your security posture is a reflection of your organization's ability to identify, assess, and mitigate risks. Here are some of the most common methods used to assess security posture:

- **Conducting a risk assessment**

  A risk assessment is a systematic process of evaluating the likelihood and severity of an event occurring and its potential impact on your organization.

- **Conducting a vulnerability assessment**

  A vulnerability assessment evaluates your physical security infrastructure to identify weaknesses in your physical security system.

- **Performing a threat and vulnerability analysis**

  A threat and vulnerability analysis evaluates the potential threats that could affect your organization and the vulnerabilities that could allow an attacker to exploit those threats.

INSIGHT # 1

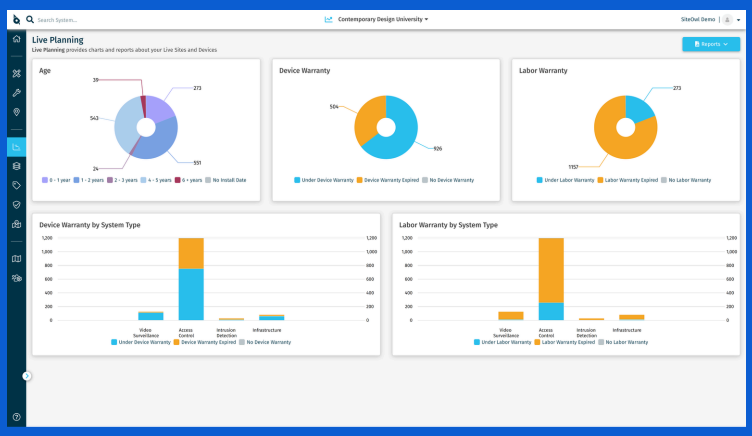
Physical Security Lifecycle Assessment

Traditional security assessments that measure risk assessment or vulnerability remain useful, but they often overlook the importance of lifecycle management.

Physical security systems without lifecycle management are subject to risk and inefficiency that are magnified over time.

Take the SiteOwl Physical Security Lifecycle Assessment to learn how to mitigate security risks and identify optimization opportunities.

SiteOwl enables security directors to improve budgeting, planning, and risk management with access to device-level service and warranty information to plan changes, upgrades, and budgets.



1.2 Establish an operating framework for your team

Knowing your physical security strengths and weaknesses is a solid first step, but without a defined strategy, it's difficult to build a robust physical security team.

1.2.1 Select a physical security team model that works for your organization

With IT and cybersecurity teams taking on an ever-increasing role in protecting physical assets, organizations use different models to accomplish their physical security objectives.
There are three predominant models that are commonly adopted in organizations.

a. The siloed model

In this model, the IT and cybersecurity teams are responsible for protecting the organization's digital assets, while the physical security team is responsible for protecting the organization's physical assets. This model can be effective if the two teams are well-coordinated, but it can also lead to gaps in security if the teams are not working together effectively.

Pros of the siloed model	Cons of the siloed model
Specialization Each team can focus on their specific expertise, leading to a deeper understanding and proficiency in their respective domains. This specialization can result in better management of digital and physical assets.	**Limited collaboration** Lack of effective collaboration between the IT, cybersecurity, and physical security teams can lead to communication gaps and hinder a holistic approach to security. It may result in missed opportunities to identify and address potential threats that span both digital and physical realms.
Efficiency When well-coordinated, the siloed model can allow each team to operate efficiently within its scope. It avoids potential conflicts of interest and ensures that both teams can prioritize their tasks without overlapping responsibilities.	**Inadequate threat response** In the absence of integrated communication, the siloed model may lead to delayed or inadequate responses to security incidents that require a joint effort from both teams. This can expose the organization to increased risk and potential damages.
Clear responsibilities With clearly defined roles, there is less ambiguity regarding each team's responsibilities. This can promote accountability and streamline decision-making processes	**Increased vulnerabilities** Isolated teams may overlook potential attack vectors that combine digital and physical elements. Hackers can exploit weaknesses at the intersection of digital and physical security, creating a larger attack surface for threats to penetrate.

Overall, while the siloed model can work effectively under certain conditions, it requires strong coordination and communication between the IT, cybersecurity, and physical security teams to minimize potential security gaps and maximize the organization's overall security posture.

b. The integrated model

In this model, the IT and cybersecurity teams work together with the physical security team to protect all of the organization's assets, both digital and physical. This model is generally more effective than the siloed model, but can be more complex to implement and manage.

Pros of the integrated model	Cons of the integrated model
Holistic approach The integrated model enables a comprehensive and holistic approach to security, as all teams collaborate to protect both digital and physical assets. This alignment helps identify and address threats that may originate from different areas, providing a more robust security posture.	**Complexity** Implementing and managing an integrated model can be more complex than the siloed model. It requires clear communication, collaboration, and potentially adjustments to existing workflows and processes.
Efficient resource allocation By working together, teams can optimize resource allocation and avoid redundancies. This streamlined approach allows for better utilization of budgets and personnel, ensuring that security efforts are aligned with organizational priorities.	**Interdepartmental challenges** n the absence of integrated communication, the siloed model may lead to delayed or inadequate responses to security incidents that require a joint effort from both teams. This can expose the organization to increased risk and potential damages.
Cross-domain threat mitigation The integrated model allows for better coordination in addressing threats that span multiple domains. For example, a cyber threat might lead to physical security implications, and the integrated model ensures a unified response to mitigate the risk effectively.	**Resource and training requirements** The integrated model may necessitate additional resources and training to ensure that all teams are well-equipped to handle both digital and physical security aspects effectively.

Despite its challenges, the integrated model has the potential to provide a more robust security posture, with increased synergy among teams and a better ability to respond to emerging threats that affect the organization in various ways. Successful implementation requires strong leadership support, effective communication, and a commitment to fostering collaboration among teams.

c. The outsourced model

In this model, the organization outsources its physical security to a third-party provider. This model can be a good option for organizations that do not have the resources or expertise to manage their own physical security.

Organizations considering the outsourced model should conduct thorough due diligence to select a reputable and reliable security provider. A well-structured service level agreement (SLA) should define roles, responsibilities, and performance expectations to ensure a successful and secure outsourcing partnership.

Pros of the outsourced model	Cons of the outsourced model
Access to expertise By outsourcing physical security to a specialized third-party provider, organizations gain access to a team of professionals with expertise in various aspects of security.	**Loss of direct control** Outsourcing physical security means giving up direct control over security operations. Organizations may have limited oversight on day-to-day activities, which could lead to concerns about responsiveness or compliance with security protocols.
Cost-effective For organizations with limited resources, outsourcing can be a cost-effective solution. Hiring and maintaining an in-house security team can be expensive, while outsourcing allows for a more flexible and scalable approach to security.	**Security integration challenges** Integrating outsourced security operations with internal processes and culture can be challenging. Misalignment in values and practices may create friction and affect the overall effectiveness of security measures.
Focus on core competencies By entrusting physical security to a dedicated provider, organizations can focus on their core business activities without diverting resources to manage security operations.	**Data privacy and confidentiality risks** Sharing sensitive information with a third-party security provider could pose data privacy and confidentiality risks if not managed properly. Ensuring robust data protection measures is crucial in such arrangements.

The best model for your organization will depend on your specific needs and circumstances, but what's most important is that you identify the model that works best for you and then implement it effectively.

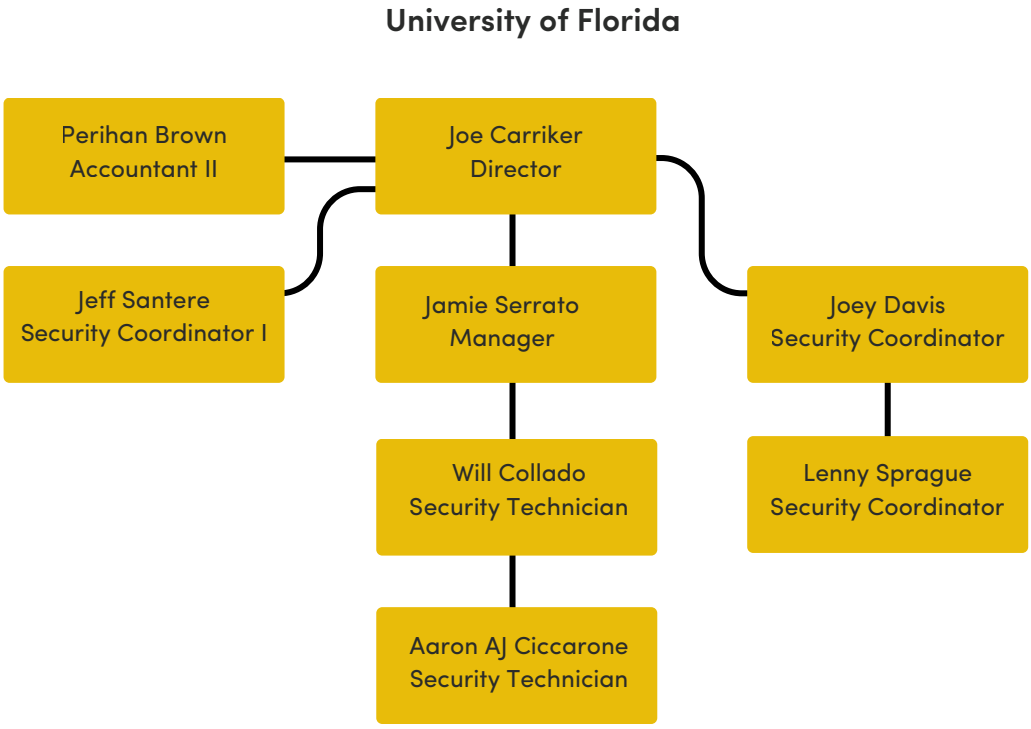
Regardless of the model you choose or are already using, it's important to develop a clear security strategy that includes defined roles and responsibilities for all security team members.

1.2.2 Define the roles and responsibilities for each team member

While we cover roles in more detail in Section 2, here are some key roles within the security team that you should consider defining. One person may perform more than one role in smaller organizations.

- Security leadership & management
- Physical security manager
- IT & Cybersecurity liaison
- Security guards or officers
- Access control specialists
- Security technology specialists
- Emergency response
- Security training & awareness
- Incident response
- Security technicians
- Security project manager
- Vendor manager

Ultimately, you want to build an organization structure that is effective, efficient and scalable. We've provided an example of the security team's organizational structure below.



1.2.3 Develop or revise your security plan

Creating or revising a security plan involves a systematic approach to address all areas of physical security in your organization. After conducting an assessment of your organization's security needs, you'll want to determine the scope and focus of your plan.

Some organizations choose to develop a single plan that encompasses all aspects of security, while others focus on one or more specific areas.

Your security plan should be tailored to your organization, based on

- The size of your organization
- The type of activities you conduct
- The location of your facilities, and
- The level of security you need to maintain

Regardless of the scope, you'll want to include the following elements

- **Security Policies and Procedures**

  Develop detailed security policies and procedures that cover all areas of physical security. This should include access control protocols, visitor management, emergency response procedures, incident reporting, and more.

- **Physical Security Equipment**

  Identify and deploy appropriate physical security equipment such as alarms, locks, access control systems, and perimeter barriers based on the risk assessment.

- **Security Training and Awareness**

  Conduct regular security training sessions for all employees to educate them about security best practices and their roles in maintaining a secure environment.

- **Vendor Management(if applicable)**

  If security services are outsourced to a third-party provider, define the responsibilities, expectations, and performance standards for the vendor

- **Compliance and Regulations**

  Ensure that the security plan complies with relevant industry regulations and legal requirements.

1.2.3 Inventory your physical security assets

You can't manage what you don't know you have, so obtaining an accurate inventory of your physical security assets is crucial to establishing a solid physical security program.
Physical security systems are typically spread across multiple locations, so conducting a full inventory of all your assets can be hard. Having a central platform to track, manage, and maintain your assets, such as SiteOwl, can help you streamline the process.

But the value of an accurate inventory goes beyond just knowing where everything is. An inventory is a starting point for creating a solid physical security program that provides protection, reduces risk, and delivers a positive return on investment.

Here are some key benefits of maintaining an accurate inventory of physical security assets:

- **Risk Assessment and Mitigation**

  Having a complete inventory allows security professionals to identify critical assets, assess their vulnerability to potential threats, and prioritize risk mitigation efforts accordingly.

- **Resource Allocation**

  Knowing the exact number and location of security assets enables efficient allocation of resources and budgets. It helps avoid unnecessary expenses on redundant or underutilized equipment.

INSIGHT # 2

Inventorying physical security assets

The SiteOwl platform offers unprecedented access to security systems information for end users. With SiteOwl you can:

- Efficiently track and manage all your physical security devices across multiple locations from a single interface.
- Collaborate directly with integrators on new system designs.
- Handle repairs and maintenance requests
- Conduct system-wide audits to identify and fix security gaps quickly.

- **Incident Response**

  In the event of a security incident, an accurate inventory allows for a swift response by quickly identifying affected assets and potential points of entry or breach.

- **Maintenance and Upgrades**

  Regular maintenance and upgrades of security assets are essential to ensure their effectiveness. An inventory helps track maintenance schedules, identify outdated equipment, and plan for necessary upgrades.

- **Compliance and Audits**

  Many industries and organizations have specific security regulations to comply with. An accurate inventory aids in demonstrating compliance during audits and ensures that the security program meets industry standards.

- **Security Training**

  Understanding the types and locations of security assets helps in customizing trainingprograms for security personnel and other employees to effectively utilize and support these assets.

- **Loss Prevention**

  An inventory enables organizations to track assets and prevent loss due to theft or misplacement.

1.3 Identify key internal stakeholders and make them part of the team

Building a robust physical security team goes beyond just hiring skilled professionals; it involves collaboration and support from key stakeholders within your organization. In this chapter, we explore the critical process of identifying and involving key stakeholders who play a pivotal role in shaping the success of your security efforts.

Mapping the stakeholder landscape

Mapping the stakeholder landscape within your organization involves identifying individuals or groups that directly or indirectly influence security decisions and are vested in the outcomes.
Let's identify top stakeholders and see how they can help shape your security strategy

- **C-suite executives**

  Top-level executives, such as the CEO, CFO, and COO, who have overall responsibility for the organization's success and are concerned with risk management, business continuity, and protecting the company's reputation.

SELLING PHYSICAL SECURITY SYSTEMS TO THE C-SUITE CAN BE A CHALLENGE...

Historically, physical security has been seen as a cost center or a necessary evil that is not a priority for the C-Suite. However, with technological advances and increasing adoption of digital transformation, this perspective is beginning to change as executives become more aware of the value unlocked by data-driven insights.

In fact, the physical security market is anticipated to reach USD 278.1 billion by 2032, expanding at a CAGR of 7.9% between 2023 and 2032.

With SiteOwl, physical security data can be structured and easily shared with other departments. This is a game changer for physical security professionals and can significantly improve security outcomes and business results.

- **Facility managers**

  As a security leader, you need facility managers on your side. They're responsible for overseeing the physical infrastructure and facilities, including buildings, offices, and warehouses. They play a key role in implementing security measures within the premises.

  Physical security systems connected with building automation tools provide even greater protection and efficiency for building operations. Security systems that collect data about building usage and occupancy can feed automated building systems, such as elevator dispatch, lighting, fire, or HVAC operations, to streamline processes or schedule optimal maintenance.

- **Human Resources department**

  HR and security go together like access control and employee badges. HR professionals oversee employee onboarding, training, and personnel management. They work closely with the security department in areas like access control, background checks, and security awareness training.

- **IT and Information Security teams**

  Regardless of your physical security team's organizational structure, IT and information security teams are key partners in protecting your organization. They provide the critical infrastructure and technology that keep your systems running and secure. According to the Cybersecurity and Infrastructure Security Agency (CISA), "Organizations with converged cybersecurity and physical security functions are more resilient and better prepared to identify, prevent, mitigate, and respond to threats." Convergence also encourages information sharing and developing unified security policies across security divisions.

- **Finance department**

  No budget, no robust physical security team, it's a simple equation. The finance team is involved in budgeting and resource allocation for security initiatives and is interested in ensuring cost-effective security solutions.

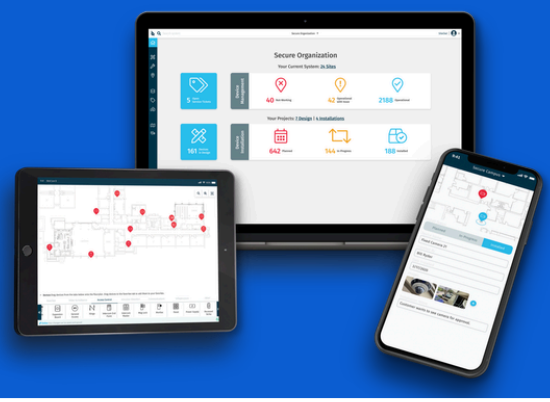
INSIGHT # 3

Get Leadership buy-in with the right information

Collaborating with internal stakeholders is essential for the success of your physical security department. To accomplish this you need actionable insights, consolidated reports, and the ability to share information with stakeholders in real-time.

SiteOwl's platform empowers your security team with data-driven insights that can be easily shared with the right stakeholders at the right time. With the power of SiteOwl, you'll be able to make data-driven decisions with confidence!

With SiteOwl, you get system-wide insights that enable fiscal accountability and cost-effective solutions. By having real-time information about device level service and warranty information to plan changes, upgrades, and budgets, you can easily win the approval of the finance team.



1.4 External stakeholders can help you connect the dots

External vendors are another important group of stakeholders that you want on your side. They provide specialized products, services, and expertise that will contribute to your overall security posture. Security consultants bring specialized knowledge and experience, offering expert advice and conducting risk assessments to address specific security challenges. Industries that have a higher risk profile, such as oil and gas, manufacturing, and financial services, are more likely to require the assistance of a security consultancy firm.
In addition to security consultants, some common external vendors that collaborate with a physical security department include:

- **Physical security integrators**

  Physical security integrators offer specialized services to help organizations design, install, and integrate various security technologies into a cohesive and effective system. Here's a list of some of the services that physical security integrators provide:

  - Security system design
  - Access control integration
  - Video surveillance integration
  - Perimeter security integration
  - Alarm monitoring and response
  - Visitor management solutions
  - Building management systems
  - Security system upgrades and expansions

Many physical security integrators use SiteOwl to manage physical security installations and provide better service to their customers. From designing a security system to managing installation and service, SiteOwl is the first unified platform for physical security integrators.

- **Security guard and patrol services**

  Security companies may provide trained security personnel for on-site patrols, access control, and incident response, particularly for large facilities or high-risk areas. Security guard companies are no longer limited to the use of traditional guardhouses. With the use of modern technology, guards can now be equipped with mobile devices that allow them to track their patrol routes, monitor alarms, and record their activities.

- **Audit and Compliance Firms**

  These vendors conduct security audits and assessments to evaluate the organization's compliance with security standards, regulations, and industry best practices.

Connecting the dots across physical security technologies

Collaboration with these external vendors is crucial for the physical security department to leverage specialized expertise, cutting-edge technologies, and industry best practices. Building strong relationships with vendors ensures that the organization receives optimal support and solutions to maintain a robust security environment.

Engaging with industry associations and networks allows access to best practices and benchmarks, fostering knowledge exchange with peers. Regulatory and compliance bodies provide guidance on adhering to security-related regulations and standards, ensuring legal compliance.

By leveraging the support and expertise of these external stakeholders, a security director gains access to a broader range of resources and insights. This collaborative approach strengthens the organization's security posture, ensuring a safer environment for employees, customers, and assets.

SECTION 2

Best practices - Building a robust physical security team

2.1 Physical security team capabilities & roles

Physical security teams are quickly becoming hybrid teams of physical security specialists, IT professionals, and an arsenal of technological tools. This evolution is driven by the increasing complexity and sophistication of security threats in today's digital age.

As organizations rely more on technology for their day-to-day operations, the need for a holistic approach to security has become paramount. Physical security specialists now work hand-in-hand with IT professionals to integrate physical and digital security measures, leveraging the power of technology to detect, prevent, and respond to incidents effectively.

The Physical Security Team plays a vital role in this endeavor, with their capabilities and roles strengthening the overall security posture. Since no two organizations are identical, physical security teams are not one-size-fits-all.

Let's look at some key roles that make up a robust physical security team:

Director of Physical Security

The Director of Physical Security is responsible for managing the organization's entire physical security program. They have the authority and oversight to ensure that all aspects of security, including access control, surveillance, and perimeter protection, are effectively implemented and maintained.
One of the key responsibilities of the Director of Physical Security is to develop and enforce security policies, strategies, and budgets. They collaborate with various stakeholders to craft comprehensive security plans that align with the organization's goals and risk profile.

As a high-level security professional, the Director of Physical Security reports directly to top-level management and stakeholders. They provide regular updates and insights on the security program's performance and effectiveness and ensure that decision-makers are well-informed about security matters and can make informed choices to enhance the organization's overall security posture.

Physical Security Manager

The Physical Security Manager holds a critical position within the organization's security structure. Reporting directly to the Director of Physical Security, they are entrusted with overseeing the day-to-day operations of the Physical Security Team. In this role, the manager ensures that all security measures, including access control, surveillance systems, and security personnel, are effectively managed and maintained to safeguard the organization's assets and personnel.

As a key liaison between different departments and stakeholders, the Physical Security Manager is vital in promoting collaboration and communication. They work closely with other teams to align security initiatives with the organization's overall goals and priorities. Through their expertise and leadership, the Physical Security Manager contributes significantly to creating a safe and secure environment for the organization and its stakeholders.

Security Operations Center (SOC) Manager

The Security Operations Center (SOC) Manager plays a pivotal role in ensuring the efficient functioning of the Security Operations Center, if applicable. They are responsible for monitoring and coordinating surveillance systems, alarms, and incident response activities to address security threats and breaches swiftly. In addition to overseeing the SOC's day-to-day operations, the manager leads and manages the SOC personnel, ensuring they are well-trained and equipped to handle security incidents effectively. By optimizing the use of resources and personnel, the SOC Manager plays a vital part in maintaining a vigilant and responsive security posture for the organization.

Physical Security Coordinator

The Physical Security Coordinator serves as a crucial link between various security functions within the organization, ensuring the seamless implementation and coordination of physical security measures. Their role involves overseeing the day-to-day operations of security systems, such as access control, video surveillance, and alarms, to maintain a safe and secure environment. The coordinator collaborates with different departments to align security strategies with organizational goals, conducts risk assessments, and develops security protocols and procedures. They also handle incident responses, investigate security breaches, and provide timely reporting to management. Through their vigilant efforts, the Physical Security Coordinator is pivotal in enhancing the organization's security posture and safeguarding its assets, employees, and stakeholders.

Security Patrol Officers

Security Patrol Officers are vital members of the organization's security team, responsible for conducting regular patrols of the premises to monitor and safeguard the property. With a keen eye for detecting potential security risks, these officers quickly respond to incidents, emergencies, or security breaches that may arise. Their prompt actions and decisive handling of situations help minimize potential damages and ensure the safety of individuals and assets on the premises. Additionally, Security Patrol Officers play a crucial role in providing a visible security presence, serving as a strong deterrent to potential threats and criminal activities. Through their vigilance and dedication, they contribute significantly to creating a safe and secure environment for all within the organization's premises.

Security Training and Awareness Specialist

The Security Training and Awareness Specialist is a key player in promoting a security-conscious culture within the organization. They are responsible for developing and delivering comprehensive security training programs to educate employees about security best practices and protocols. Through engaging and informative sessions, they ensure that all staff members are well-informed about security risks and how to mitigate them effectively. Additionally, the specialist conducts awareness campaigns to reinforce key security messages and encourage proactive participation in maintaining a secure environment. Their efforts are vital in empowering employees with the knowledge and skills needed to protect the organization from potential threats and security breaches.

Enterprise Security Team Building is all about collaboration!

This is a basic representation of an Enterprise Physical Security Team. Depending on the organization's size and complexity, there may be additional roles and personnel to cover specific security needs. Collaboration with other departments like IT, HR, and Facilities is crucial for a comprehensive security approach.

2.2 Physical security systems and processes

"Strength is not just in walls and locks; it lies in the unwavering dedication to protecting what truly matters." - Unknown

At its core, Physical Security is a collection of systems and processes designed to protect your assets and ensure operational continuity.

If you've followed the previous chapters, you have a solid foundation for building a robust physical security team. With these foundational elements in place, you can now focus on the specific physical security systems and processes that will provide the necessary level of protection for your organization.

The challenge now is to build a comprehensive lifecycle management program to keep your systems, processes, and personnel operating at peak efficiency.

Critical Physical security systems and best practices

Essential physical security systems are vital to a comprehensive security strategy crafted to safeguard assets, personnel, and facilities. These systems come in a diverse range and can be customized to suit an organization's unique requirements.

Let's review three critical physical security systems and best practices:

INSIGHT # 4

Spreadsheets don't work

Imagine having to use spreadsheets to track

- The location of every device
- Age of system/devices
- Service history
- Device failure history
- Warranty Expiration
- Device attributes such as IP address, part number, coverage area/angle, devices connections etc.

Security leaders choose SiteOwl because they know that a comprehensive physical security plan combines both technology and security operations to reduce risk and protect people, assets, and facilities.

"Across every site and location, I can see everything I need to know - here on my phone."

Program Manager, **Major Regional Hospital**

Perimeter security

Perimeter security systems are designed to protect the outer boundaries of a facility, such as fences, gates, barriers, and bollards. They help prevent unauthorized access and can deter potential intruders from attempting to breach the premises.

Best practices:

- **Layered approach**
  Adopt a layered approach to perimeter security. Utilize multiple security measures, such as fences, gates, bollards, and surveillance cameras, to create multiple barriers that deter potential intruders and provide early detection.
- **Lighting and visibility**
  Ensure proper lighting around the perimeter to deter unauthorized access during nighttime. Well-lit areas increase visibility for surveillance cameras and security personnel, reducing blind spots and enhancing overall security.
- **Regular maintenance and testing**
  Regularly inspect and maintain perimeter security devices and equipment. Test the functionality of gates, fences, and sensors to identify and address any issues promptly. Conduct routine tests to verify that the entire perimeter security system is operational and effective.

Access control

Access control is a fundamental security measure that regulates who can enter specific areas within a facility. It typically involves using identification methods such as keycards, biometric scanners, or PIN codes to grant or deny access. Access control systems help prevent unauthorized entry and can track individuals' movements for security and auditing purposes.

Best practices:

- **Centralized management**
  Use a centralized management system to oversee access control across the organization. Centralized management allows for better control, monitoring, and auditing of access permissions and events.
- **User training and awareness**
  Train employees on access control best practices and security protocols. Employees should understand the importance of protecting access credentials and be aware of potential social engineering tactics that could compromise the system.
- **Auditing and monitoring**
  Conduct regular audits and monitoring of access control logs and events to detect any unusual activities or potential security breaches. Promptly investigate and address any suspicious incidents.

Video surveillance

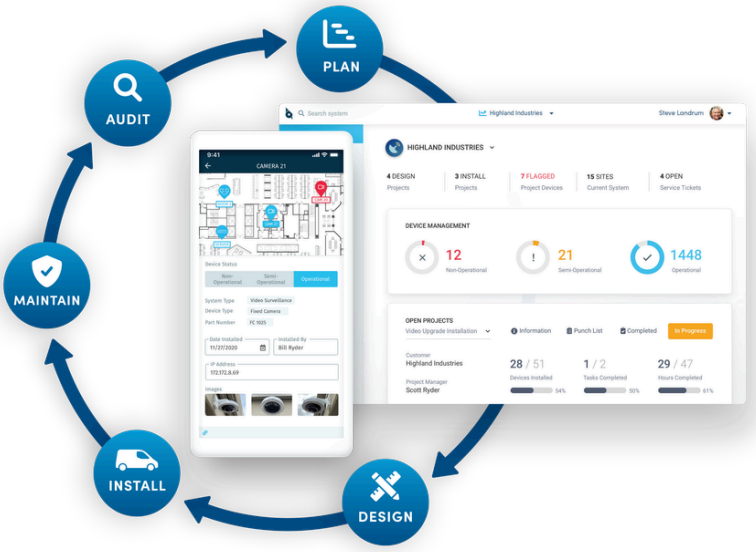
Video surveillance involves the use of cameras to monitor and record activities within and around a facility. These systems act as a deterrent to potential intruders and provide valuable evidence in the event of security incidents. Modern video surveillance systems often incorporate advanced features such as motion detection, night vision, and remote monitoring.

Best practices:

- **Optimal camera placement**
  Strategically position cameras to cover critical areas, entry points, and high-risk zones, ensuring maximum coverage and clear visibility.
- **Secure data storage**
  Safeguard recorded footage with secure data storage solutions, utilizing encryption and access controls to prevent unauthorized access to video archives.
- **Auditing and monitoring**
  Comply with relevant privacy laws and regulations when deploying video surveillance systems, and clearly communicate the presence of cameras to individuals within the monitored areas.

Managing physical security systems

Managing physical security systems is labor-intensive. Despite advancements in technology, many security teams still rely on paper-based systems or outdated tools like spreadsheets to manage their physical security infrastructure. These legacy methods can be time-consuming, prone to errors, and lack the efficiency and capabilities offered by modern security management solutions. Embracing technology-driven platforms can greatly enhance the effectiveness and responsiveness of security operations, leading to a more robust and proactive security posture.



Consistent and scalable security system practices, standardized across vendors

SiteOwl enables physical security teams to develop consistent and scalable security system practices, standardized across vendors, through its comprehensive platform and powerful features.

Here's how SiteOwl achieves this:

- **Centralized Project Management**

  SiteOwl provides a centralized platform for managing all security projects, allowing security team members to have a unified view of ongoing projects.

- **Standardized Vendor Onboarding**

  With SiteOwl, security teams can establish standardized vendor onboarding processes. This includes predefined requirements, documentation, and protocols that vendors must adhere to, ensuring consistent practices from the start of each project.

- **Uniform Workflows and Templates**

  Predefined workflows and templates for security projects, allowing the security director to establish consistent processes across all projects. These templates help streamline project management and ensure that best practices are followed consistently.

- **Collaboration and Communication**

  Seamless communication and collaboration between the security director, the security team, and the vendors. This helps align security strategies and practices, fostering consistency throughout the project lifecycle.

- **Standardized Documentation**

  Ensures that all project-related documentation, such as blueprints, schematics, reports, and contracts, are uniformly organized and accessible. This standardized documentation enhances project transparency and simplifies data analysis.

  And much more!

2.3 Adopt a Physical Security Lifecycle Framework

A physical security program without a central lifecycle framework is like a car with no steering wheel. You may have a state of the art security infrastructure, but without a central framework, your team won't be able to keep the whole program in sync. It involves the continuous monitoring, maintenance, and updating of security infrastructure to ensure its effectiveness over time. By implementing a comprehensive lifecycle management program, organizations can proactively address vulnerabilities, resolve issues promptly, and stay ahead of emerging threats. This approach not only enhances the overall security posture but also helps maximize the return on investment in security technologies.

The previous chapters covered the basics to help you establish a solid physical security strategy in place, now it's time to bring it all together and establish a holistic lifecycle framework.

Why do security teams struggle with effective lifecycle management?

Lifecycle management provides a structured and strategic approach to ensuring the effectiveness of your security measures. Think about it this way: Would you rather react to a security incident after it has occurred, or be proactive and prevent it before it happens?

Most security teams would choose to be proactive, but in reality, they adopt a reactive approach to physical security by default.

The biggest reason many security teams struggle to effectively stay on top of their security systems is the lack of tools that can consolidate and centralize their security system information.

A vast majority of security teams use legacy, disconnected tools and systems that AREN'T scalable or purpose-built for security infrastructure management.

Paper-based floor plans

- Hard to consolidate information
- Poor tool for record keeping
- Doesn't track warranty, service and audit information

Spreadsheets

- No visual context
- Error prone
- Hard to manage large security infrastructure

CAD Drawings

- Static, isn't a real-time record of system information
- Primarily used for designs and as-builts
- Can't be used to manage service

Generic Project Management Software

- Doesn't work well for security projects
- Primarily used for installation
- Hard for field staff to provide real-time updates

Lifecycle Management Phases

The physical security lifecycle has five distinct phases. We cover them in more detail in the following pages.

Lifecycle Management Phases

The physical security lifecycle has five distinct phases. We cover them in more detail in the following pages.

The five phases of Physical Security Lifecycle Management

Plan

Planning is the process of assessing and identifying your organization's security requirements and then building a solid plan to help your team meet them.

Planning Includes:

- Determining people, environment and assets that need protecting.
- Understanding any regulatory requirements your security system must comply with.
- Inventorying your current physical security devices in your infrastructure, their lifespan, warranty status, service history and other information.
- Reviewing any recent security audit outcomes to determine gaps.
- Building a strategy and budget for closing the gap between what you have and what you need.

Design

Designing is a multi-stage process using the information gathered in the planning step to build a security solution that the organization needs. Enterprise security teams often do this in partnership with their security integrators, consultants and other vendors.

As an organization expands, so does the number of physical assets it has. New locations, equipment, and buildings are common to any growing company. Still, as the number of connected devices continues to grow, the design process must take into consideration the following:

- The number of systems your organization has (e.g Video Surveillance, Access Control, Intrusion Detection, Critical Communication and other technologies).
- What is best suited for the environment and organization's needs?
- What is needed to ensure they work together effectively?
- Whether they comply with any applicable laws and regulations.
- How well the system design aligns with the overall security strategy.

Install

When installing a new physical security system or upgrading an existing one, there are a number of decisions that must be made. For instance:

- Should the organization work with a security integrator to install the system or self-install?
- Who will manage the project?
- How will progress be reported?
- Who will sign off?
- How will the quality of work be evaluated?
- How will the team ensure that the project is completed on time and under budget?

Maintain

Physical security systems such as video surveillance, access control and intrusion detection require regular maintenance. This helps security teams keep their systems up to date and plan for repairs or replacements, and reduce the likelihood of a security event that resulted from faulty or malfunctioning equipment.
Maintenance includes activities such as:

- Cleaning and refocusing lenses, housing and verifying camera placements.
- Checking wiring and cable harnesses for wear and tear.
- Cleaning of control components and ensuring control equipment is operational.
- Testing alarms and communication systems
- Reporting any anomalies or variations.

Audit

Auditing is a crucial part of physical security lifecycle management, and it allows security teams to ascertain if current security systems and measures are fit-for-purpose.
Physical security systems audits help organizations assess and evaluate the current state of their physical security infrastructure as well as:

- Identify security gaps and loopholes in the current physical security infrastructure.
- Present suggestions for improvements or solutions to address identified gaps.
- Assess the level of effective compliance with physical security standards and regulations.
- Identify systems that may need to be retired or replaced.
- Provide the information needed to plan and budget for security investments.

2.4 Evaluate Your Security Team's Performance

Evaluating and improving your physical security team's performance is crucial to maintaining a high level of security effectiveness.

By regularly evaluating the performance metrics below, organizations can identify areas for improvement, optimize their physical security systems, and ensure a robust and reliable security infrastructure to protect their assets and personnel effectively.

Performance Measures

Establish clear and measurable performance criteria for the security team. This can include response times, incident resolution rates, and adherence to standard operating procedures. Regularly review these metrics to assess the team's performance objectively.

- **Incident Response Time**
  Measure the average time it takes for the security team to respond to incidents or security breaches. A shorter response time indicates a more proactive and efficient team.

- **Incident Resolution Rate**
  Track the percentage of security incidents that are successfully resolved by the security team. A high resolution rate demonstrates the team's effectiveness in handling security challenges.

- **Security Audit Scores**
  Assess the results of security audits and inspections to evaluate the team's adherence to security protocols, policies, and industry best practices.

- **Training and Certification Completion**
  Keep track of the percentage of team members who have completed required security training and certifications. Ensuring that the team is well-trained enhances their competency in handling security incidents.

- **Employee Feedback**
  Seek feedback from employees and stakeholders on the security team's performance and responsiveness. Positive feedback indicates a strong security culture and effective communication.

- **Downtime Percentage**
  Measure the amount of time the security systems are offline or not functioning as intended. A low downtime percentage indicates that the systems are reliable and available when needed.

INSIGHT # 5

SiteOwl's Physical Security Lifecycle Management Framework

SiteOwl's Physical Security Lifecycle Management Framework helps companies manage all aspects of their physical security infrastructure from a single platform.

- **Centralized Management**
  Enables better oversight and coordination of security initiatives.

- **Data-Driven Insights**
  Allows organizations to make informed decisions and optimize security measures.

- **Scalability**
  Standardized practices make it easier to replicate successful security implementations across multiple locations or properties.

- **Response Time**
  Track the time it takes for the security systems to detect and respond to security events, such as alarms or breaches. A shorter response time ensures timely alerts and quicker actions.
- **False Alarm Rate**
  Monitor the frequency of false alarms triggered by security sensors or cameras. A low false alarm rate reduces unnecessary disruptions and ensures that the team responds to genuine security threats.

INSIGHT # 6

Stay on the leading edge with SiteOwl

Security teams are now faced with the challenge of keeping up with the latest physical security solutions. This can be a daunting task, especially with inaccurate inventory and a lack of visibility into the status of a security system. SiteOwl's centralized platform solves many of these challenges.

Challenge	Solution
Incomplete and/or inaccurate system information	Data-driven decision making with consolidated system reporting
Lack of standardized security system management practices	Consistent and scalable security system practices, standardized across vendors
Inability to accurately forecast and plan budgets	System performance visiblity enables fiscally responsible security investments

SECTION 3

The Future of Physical Security Teams

3.1 Future Physical Security Challenges & Opportunities

The physical security landscape is constantly evolving, presenting both challenges and opportunities for security leaders that want to optimize their security posture, streamline processes, and address the challenges of the future.

As we venture into the future, new technologies, changing threats, and global events create a dynamic environment that demands innovative approaches to security. In this context, understanding and addressing the future physical security challenges and opportunities become paramount for maintaining a robust security posture.

Overarching Challenges & Opportunities

- **Rising Technological Advancements**

  Advancements in technology offer promising opportunities for enhancing physical security measures. The integration of Artificial Intelligence (AI), Internet of Things (IoT), and cloud computing has the potential to revolutionize security systems, enabling real-time data analysis and predictive threat detection. While these innovations offer unprecedented capabilities, they also introduce challenges such as cybersecurity risks and the need for skilled personnel to manage and maintain these complex systems.

- **Cyber-Physical Security Convergence**

  The future of physical security will undoubtedly witness an increased convergence of cyber and physical threats. As digital and physical worlds intertwine, cyber-attacks can have significant physical implications, and physical breaches can lead to severe data compromises. Securing these interconnected systems necessitates a holistic approach that addresses both digital and physical vulnerabilities. Organizations must bridge the gap between their IT and physical security teams to collaborate and implement comprehensive strategies for cyber-physical security.

- **Global and Hybrid Threats**

  In an interconnected world, physical security challenges extend beyond traditional boundaries. Global events, such as pandemics and geopolitical tensions, can disrupt supply chains, workforce mobility, and business operations. Additionally, the rise of hybrid threats, involving a combination of physical and cyber elements, poses complex security challenges. Organizations must proactively adapt to these evolving threats and embrace agile security measures that can withstand unexpected disruptions while maintaining a strong security stance.

INSIGHT # 7

Future proof your physical security investments

Future-proofing your physical security investments is essential to ensure that your security measures remain effective and relevant in the face of evolving threats and technology.

Scalability is important for future-proofing physical security investments because it enables organizations to adapt and expand their security measures to meet changing needs and requirements over time.

SiteOwl's standardized and centralized approach allows for seamless scalability across projects and locations. As your organization grows or security needs evolve, SiteOwl can accommodate expanding requirements without compromising efficiency or performance.

Ongoing challenges...

While rising technological advancements, security convergence and hybrid threats will continue to challenge businesses, additional ongoing challenges will keep security leaders on their toes. In the next decade, security leaders will have to embrace digitization to stay ahead of emerging threats and leverage cutting-edge technologies to enhance their security operations.

Current physical security challenges

IoT Security

As the adoption of IoT devices grows, ensuring the security of interconnected devices becomes critical to prevent potential breaches and unauthorized access.

Maintenance and monitoring

Regardless of the rate at which technology advances, security teams will continue to face the challenge of ensuring that their security systems are properly maintained and monitored to prevent potential breaches and unauthorized access.

Sustainability and environmental impact

As organizations aim for environmentally responsible practices, finding sustainable and energy-efficient security solutions becomes essential to reduce the environmental impact

By staying ahead of emerging threats and leveraging cutting-edge technologies, businesses can create a secure environment that fosters growth and resilience in the face of a rapidly changing world.

3.2 Leverage Technology for Enhanced Security

Technology has become a crucial component in enhancing physical security effectiveness across a wide range of industries.

Numerous sectors are leveraging innovative solutions to create safer environments for their assets, personnel, and customers. For instance, in the retail industry, advanced video surveillance systems with facial recognition and people counting capabilities are employed to monitor store activities, prevent shoplifting, and enhance customer safety. Additionally, IoT-based solutions are utilized for inventory tracking and access control to restricted areas, ensuring a comprehensive security approach.

In healthcare, access control systems with biometric authentication secure sensitive areas such as patient rooms and medication storage. Video monitoring systems are used to ensure patient safety and monitor high-traffic areas to prevent unauthorized access. Similarly, the banking and finance industry heavily invests in security technology, implementing biometric authentication at ATMs, facial recognition for access control, and advanced alarm systems to protect their assets and data against theft and fraud.

SiteOwl for enhanced physical security management

SiteOwl was designed to help forward thinking security professionals address the challenges of managing their physical security infrastructure. Gone are the days of relying on spreadsheets and paper reports to manage your physical security infrastructure. With SiteOwl, you can manage your physical security infrastructure from a central platform without the need to install and configure multiple software applications or rely on complicated spreadsheets.

Today, large organizations have thousands of physical security devices across tens to hundreds of buildings. Enterprise security teams must overcome a series of hurdles as these systems require continual changes to meet business needs.

- **Traditional collaboration methods don't work**

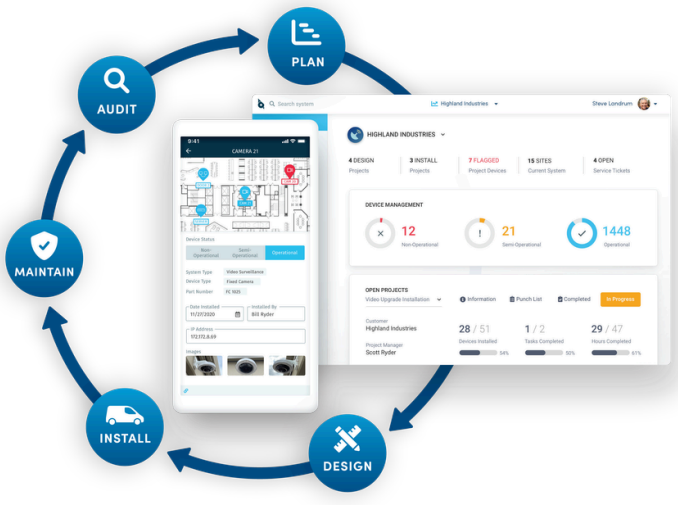
  They disjointed and do not streamline collaboration between the security team, stakeholders, facilities, IT and security vendors. These manual processes also make vendor oversight at geographically dispersed locations difficult.

- **Legacy data management doesn't scale**

  iSecurity teams organize information using spreadsheets, printed plans and siloed information that don't connect to lifecycle workflows. Maintaining an accurate picture of deployed equipment is time-consuming and impractical, increasing organizational costs and security risks.

- **Siloed communication increases risk**

  Teams rely on phone calls, meetings, and expensive site visits. Without centralized and shared knowledge, teams are routinely not on the same page, impacting speed and quality.



Build and manage security systems with confidence

System-wise visibility
Get the whole picture - all locations, devices, issues and activities.

Single source of truth
Centralized system of record for all design, installation and maintenance.

Collaboration across teams
Keep security teams and vendors aligned throughout the system lifecycle.

Effective planning & budgeting
Leverage data-driven insights to make cost-effective security investments.

Manage designs & projects
Create digital designs on the fly and track installation progress in real-time.

Purpose-built for security
Suite of role-based apps built for enterprise security and integrators.

"We're upgrading our analog cameras to IP at every one of our branches. I don't know how we would accomplish a project this large in a manageable amount of time without SiteOwl."

Security Director, **Multi-State Bank**

CONCLUSION

Thriving in a Secure Environment

The future of physical security teams is set to be more collaborative, mobile, and technologically advanced than ever before. Security teams will thrive in the 21st century by embracing digitization and leveraging technology to design, manage, and maintain their physical security infrastructure.

Collaboration will become a cornerstone of the modern security landscape, as security teams collaborate seamlessly with other departments, stakeholders, and external partners. This approach will foster a holistic understanding of security risks and enable security teams to proactively address system issues with minimal disruption to operations.

Mobility will revolutionize how security teams operate, allowing them to stay agile and responsive. With mobile devices and applications, security personnel will have real-time access to critical information and incidents, enabling quicker decision-making and more effective incident response.

Technological advancements will be at the forefront of the future security landscape. Artificial intelligence, machine learning, and video analytics will play vital roles in enhancing threat detection, automating routine tasks, and providing valuable insights from vast amounts of data.

As the world becomes increasingly digital, physical security teams must adapt and embrace technology to stay ahead of evolving threats. Embracing collaboration, mobility, and technological advancements, security teams will not only thrive in the 21st century but also play a pivotal role in creating safer environments for organizations, communities, and society at large.

The future is bright for physical security teams that embrace innovation and SiteOwl is here to help usher in a new era of comprehensive security solutions.

Join us at an upcoming conference or visit us online at www.getsiteowl.com for more information about how you can digitally transform the management of your physical security systems and take your security program to the next level!

About SiteOwl

SiteOwl is the only physical security system lifecycle management platform that brings enterprise security teams, their security vendors, and assets together on one unified platform.

The solution's suite of applications connect real-time data and workflows, specific to the physical security industry, to drive collaboration, visibility and efficiency.

To learn more, please visit getsiteowl.com.