Securing Your Manufacturing Facility: A Guide for Physical Security Teams

Expert Strategies and Proven Techniques for Successful Security System Implementation and Maintenance

David Santiago, CSP, PSP

sitedowl®

Contents

About the Author

David A. Santiago
(CSP, PSP)

David Santiago is a military veteran with extensive experience in security operations (SecOps) and risk management.

As a security director, David led teams in high-risk environments and worked with security professionals at the highest levels of the government, including the U.S. State Department.

Today, David uses his experience and passion for security to educate others about the importance of physical security and the ongoing cyber-physical convergence.

Introduction

This Essential Guide to Physical Security Systems for Manufacturing Facilities is a useful resource for security leaders who want to modernize their security systems in a manufacturing environment.

Physical security is the first layer of protection against any physical or cyber threat. Over 85% of cyber security breaches in the past few years involved a human element. Understandably, many security professionals in the manufacturing industry are looking for practical solutions to manage their security infrastructure efficiently.

Who is this guide for?

The guide is designed for those who oversee or are involved in physical security for manufacturing facilities. It provides a detailed overview of the industry's current state, along with essential factors to consider when implementing a security system. The guide also highlights the advantages of using cloud-based systems for managing the lifecycle of physical security systems.

What is covered in this guide?

Physical security is changing as technology improves and leaders turn to cloud-based solutions for managing security systems. Although the industry has been slow to embrace new technology, the cloud is making it easier for leaders to modernize their security systems.

The guide includes a detailed look at the current state of the industry, key considerations for implementing a physical security system, and other core topics such as:

- The manufacturing risk landscape
- How to operate security systems in a cloud-first world
- Overcoming challenges in the manufacturing industry
- Physical Security Lifecycle Management Framework
- How to move away from legacy systems to a cloud-based solution.
- Future of Physical Security in Manufacturing Facilities

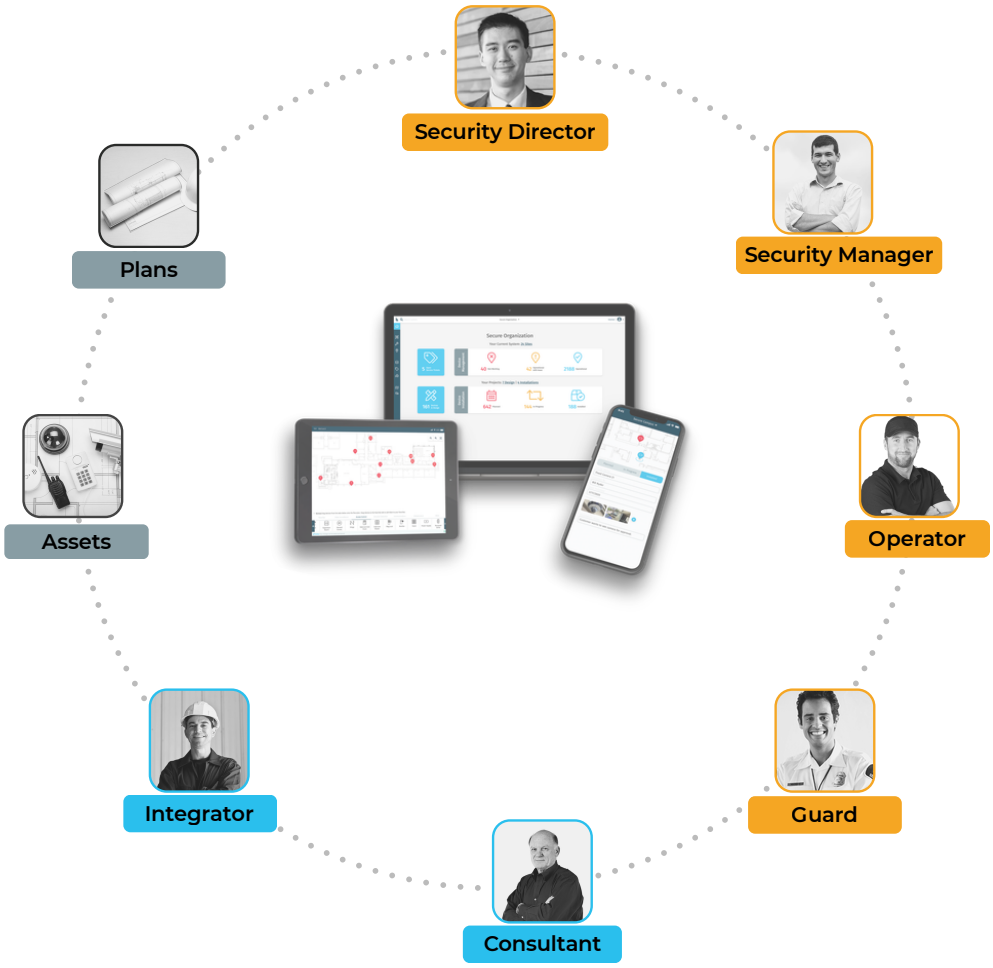
Throughout the guide, you'll find a number of relevant and helpful resources that will help you start thinking about your physical security infrastructure's lifecycle roadmap. In addition, to help you along the way, we've added a number of links to whitepapers, case studies, and other valuable insights from industry leaders and security experts.

We've also created SiteOwl Insights to help you optimize the way you manage and maintain your physical security infrastructure.

Let's go!

About SiteOwl

SiteOwl's cloud-based platform helps manufacturing security professionals streamline and optimize their physical security systems. By offering real-time visibility, accurate device information, critical lifecycle management data, and robust installation project management capabilities, SiteOwl changes the way security professionals manage the lifecycle of their physical security infrastructure.



Securely Navigating the Future

A Look at the Changing Security Landscape in Manufacturing

Manufacturing facilities are vulnerable to various security threats such as theft, sabotage, violence, vandalism, and cyber-physical attacks, making physical security a top priority.

While cybersecurity breaches are frequently reported, physical security is just as important for the protection of people and assets. For instance, a security flaw in access controls, like unauthorized access to facilities or system permissions, could enable someone to use a USB device or other removable hardware to introduce a virus or malware into your network.

"A physical attack was the main method in 54% of all data breaches.."
(ENISA Threat Landscape 2020 – Physical Threats)

On February 5, 2021, unidentified cyber actors obtained unauthorized access to the supervisory control and data acquisition (SCADA) system at a U.S. drinking water treatment facility. The unidentified actors used the SCADA system's software to increase the amount of sodium hydroxide, also known as lye, a caustic chemical, as part of the water treatment process.

Thankfully, water treatment plant personnel immediately noticed the change in dosing amounts and corrected the issue before it caused an environmental incident. Still, the incident highlighted the importance of physical security, the importance of lifecycle management, and the need for a holistic approach to industrial security.

The Security Landscape is Changing

As the manufacturing industry continues to embrace modern technology and automation, it finds itself confronted with an evolving security landscape. The rapid development of the Internet of Things (IoT) and the increasing reliance on physical security systems have exposed manufacturers to new challenges including:

- Supply Chain Interruption
- Cyber-Physical hybrid attacks
- Digitization of manufacturing operations

Prioritizing Physical Security: A Must for Manufacturers

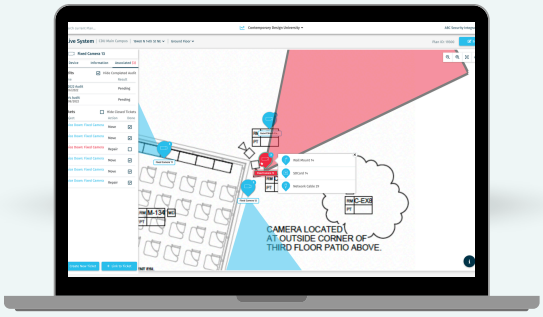
Physical security risks are amplified when manufacturing facilities fail to conduct regular physical security risk assessments, adopt proactive policies and procedures, and implement appropriate physical security technology.

To help safeguard physical and human assets, production plants and other vulnerable operations require an integrated security system that brings together multiple security technologies. These technologies must be able to communicate in real-time, share data, and integrate with existing operational systems.

Above all, physical security systems must operate optimally at all times and adapt to changing threats. This requires a robust lifecycle management solution to ensure that security systems remain effective.

In the following sections, we'll look at how manufacturing facilities can manage their physical security systems and achieve high levels of operational effectiveness through lifecycle management.

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.



Insight #1

Maximize the information on devices!

Physical security optimization focuses on maximizing the effectiveness of security measures within a given environment. A centralized platform enables security administrators to:

- Maximize security system visibility to respond to incidents proactively.
- Maximize accessible data to make smart decisions.
- Maximize insights into asset inventory for lifecycle management.
- Maximize data into asset inventory for lower costs.
- Maximize equipment utilization and uptime.

By maximizing the capabilities of your current security systems, you can achieve greater results with less effort, and the good news is that there is a simple solution to do this.

Protecting Your Manufacturing Facility

The Importance of Physical Security

"75% of companies consider physical security as one of their top priorities."- Gartner

Physical security is important for protecting manufacturing facilities from security risks like theft, sabotage, violence, and cyber-attacks. Installing access control systems, video surveillance, and other security measures can help detect and prevent potential threats. This minimizes the risk of security breaches, protecting employees, assets, and reputation while also ensuring the safety and security of employees and assets.

Here are ten prioritized physical security requirements:

- Identifying and controlling individuals who enter and exit the facility
- Tracking movements of building occupants and assets
- Controlling access to restricted areas
- Tracking and locating equipment, products, and other resources
- Tracking the location of personnel on site in the event of an incident
- Integrating control and security systems for greater speed and efficiency
- Protecting process systems from potential intrusion
- Responding quickly to alarms and events
- Lifecycle management of security systems
- Maintaining security awareness and training of personnel

Effective Physical Security Measures

Every industry is at risk for threats in various ways, and the manufacturing industry is no exception. The most effective physical security measures for manufacturing facilities encompass a holistic approach that optimizes security technology and fosters a security-conscious culture among employees.

Security directors, facility managers, and coordinators can use various physical security solutions to address the challenges of securing manufacturing facilities. These solutions include but are not limited to the following:

1. VIDEO SURVEILLANCE

Surveillance cameras play a significant role in bolstering security measures for manufacturing facilities. By strategically installing cameras, companies can continually monitor activity within the premises, identify potential threats, and respond in a timely manner.

Video surveillance can improve physical security in a manufacturing facility in several ways -

- Deterrence: The presence of cameras can serve as a deterrent to potential intruders, as they are less likely to attempt to breach the facility if they know they are being monitored.

- Detection: Video surveillance cameras can detect security threats in real-time, allowing security personnel to respond quickly and effectively to potential security breaches.

- Investigation: In the event of a security breach, video surveillance footage can provide valuable evidence that can help identify the perpetrator and aid in investigations and prosecutions.

- Monitoring: Video surveillance cameras can be used to monitor sensitive areas of the facility, such as equipment rooms, loading docks, and inventory storage areas, to ensure that only authorized personnel have access.

- Auditing: Video surveillance footage can be used to audit facility processes, ensuring that employees are following security protocols and procedures.

Overall, video surveillance can be an effective tool for improving physical security in a manufacturing facility, providing an additional layer of protection and enabling security personnel to detect, respond to, and prevent potential security threats.

2. ACCESS CONTROL

Implementing a robust access control system in manufacturing facilities is crucial to ensuring both the safety and security of employees, as well as the protection of valuable equipment and proprietary information. These systems may utilize a combination of physical barriers, identification methods, and advanced technology to monitor and regulate entry and exit points throughout the facility.

Access control can improve physical security in a manufacturing facility in several ways:

- Restricted Access: Access control systems can be used to restrict access to sensitive areas of the facility, ensuring that only authorized personnel have access. This can help prevent theft, sabotage, and other security breaches.

- Monitoring: Access control systems can provide a record of who has accessed sensitive areas of the facility and when, allowing security personnel to monitor for unusual or suspicious activity.

- Integration: Access control systems can be integrated with other security systems, such as video surveillance, to provide a more comprehensive security solution.

- Multi-Factor Authentication: Access control systems can use multi-factor authentication, such as key cards and biometric identification, to ensure that only authorized personnel are granted access.

- Customization: Access control systems can be customized to fit the unique needs of the facility, allowing for greater control over who has access to certain areas and when.

3. INTRUSION DETECTION

Intrusion detection systems are helpful for physical security because they provide an additional layer of protection and enable security personnel to detect and respond quickly to potential security threats. This can help prevent or minimize the potential damage from security breaches and keep employees, assets, and information safe.

Intrusion detection systems can improve physical security in a manufacturing facility in several ways:

- Early Detection: Intrusion detection systems can detect potential security breaches at an early stage, enabling security personnel to respond quickly and prevent or minimize the potential damage.
- Alerts and Notifications: Intrusion detection systems can generate alerts and notifications to alert security personnel to a potential security breach, allowing them to take appropriate action.
- Integration: Intrusion detection systems can be integrated with other security measures, such as video surveillance, to provide a more comprehensive security solution.
- Deterrence: The presence of intrusion detection systems can act as a deterrent to potential intruders, as they are less likely to attempt to breach the facility if they know they are being monitored.

4. LAYERS OF DEFENSE

In physical security, layers of defense" refers to the practice of implementing multiple security measures in order to create multiple barriers for potential security threats. These security measures may include things like access control systems, video surveillance, perimeter security, intrusion detection systems, and security personnel.

By layering multiple security measures, the goal is to create a more comprehensive and robust security posture that is better able to deter, detect, and respond to potential security breaches or threats. The idea is that if one layer of defense is breached or fails, there are additional layers in place to prevent the security threat from advancing further into the facility or causing significant damage.

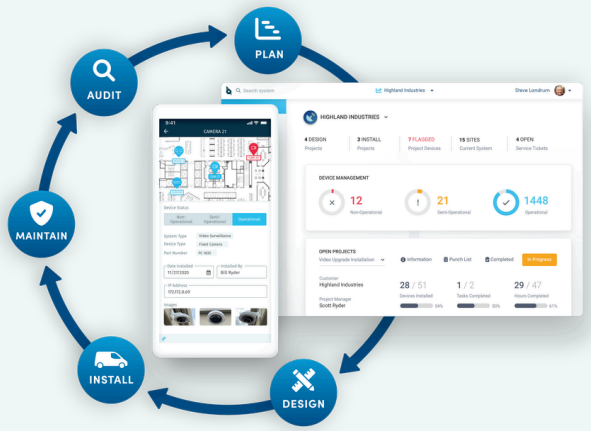
5. REMOTE MONITORING

Remote monitoring can be an effective tool for improving physical security measures in a manufacturing facility, providing an additional layer of protection and peace of mind for facility managers and security personnel.

This allows security personnel to monitor the facility and respond to security events from a remote location, helping ensure a timely response to security threats, even if security personnel are not physically present on site.

Remote monitoring can improve physical security measures in a manufacturing facility in several ways -

- Firstly, it allows security personnel to keep an eye on the facility even when they are not physically present on site. This means that they can respond quickly to security threats as they arise, potentially preventing them from escalating and causing damage or disruption to the facility.
- Secondly, remote monitoring can provide a cost-effective alternative to having security personnel on site around the clock. This can be especially beneficial for smaller manufacturing facilities that may not have the resources to hire and maintain a full-time security team.
- Thirdly, remote monitoring can be used in conjunction with other security measures such as video surveillance and access control systems. By integrating these systems with remote monitoring, security personnel can be alerted to potential security breaches and respond accordingly, even if they are not physically present on site.



Platforms like SiteOwl help security team get much needed visiblity and accessibility to key security system information when they need it. Paper-based plans and spreadsheets are cumbersome and hard to keep up-to-date.

A proactive approach to physical security

Regular reviews and updates are necessary to maintain the effectiveness of physical security systems and adapt to emerging risks. A comprehensive and proactive approach to physical security can help minimize disruptions, protect assets, and ensure a secure environment for the workforce.

Insight #2

Video Surveillance Management

Most manufacturing facilities have video surveillance systems, but without proper lifecycle management, security teams are not able to:

- Monitor ongoing service issues, and conduct system-wide audits to identify and fix security gaps and vulnerabilities.
- Stay on top of ongoing security system deployments.
- Monitor ongoing system operations and maintenance activities in real-time.

With SiteOwl, system administrators can proactively monitor security devices to identify and address potential issues before they become full-blown outages. In addition, adopting a lifecycle management strategy can help organizations make informed decisions about upgrading or replacing equipment, improving planning and budgeting, and reducing the risk of system failures and downtime.

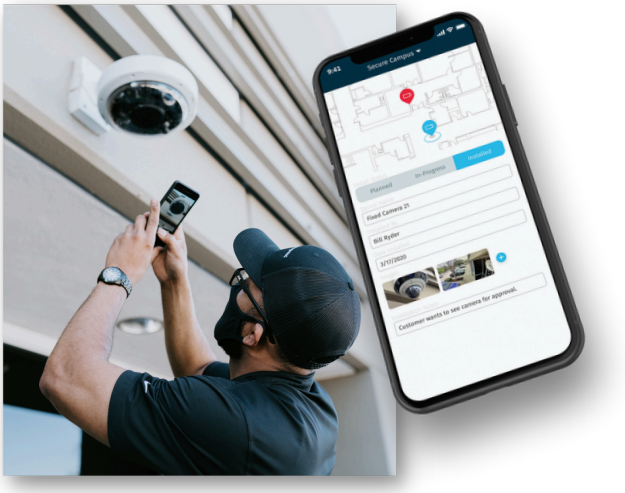
Navigating a Cloud-First World

How Cloud Technology is Reshaping Physical Security in Manufacturing Facilities

Physical security is important for protecting manufacturing facilities from security risks like theft, sabotage, violence, and cyber-attacks. Installing access control systems, video surveillance, and other security measures can help detect and prevent potential threats. This minimizes the risk of security breaches, protecting employees, assets, and reputation while also ensuring the safety and security of employees and assets.

"Cloud adoption has risen rapidly over the past ten years, with 92% of enterprise business strategies now relying on the cloud" - IDG Survey

With the advent of cloud computing, the transformation of physical security has reached new heights, impacting areas that we have yet to comprehend fully. Cloud adoption has risen rapidly especially in the manufacturing industry with 87% of manufacturers relying on the cloud.



It's clear that cloud-based physical security will continue to grow in importance, particularly when used in conjunction with increased automation and adoption of management technologies. While this trend will affect every aspect of physical security, here are a few areas where cloud-based physical security solutions will have a significant impact:

ACCESS CONTROL

Adopting cloud solutions can provide real-time monitoring of access control systems, allowing security personnel to quickly respond to security breaches. They can also provide greater flexibility in managing access control systems, enabling remote management of access permissions.

VIDEO SURVEILLANCE

Cloud-based solutions can provide secure and efficient storage of video surveillance footage, enabling quick and easy access to footage from anywhere with an internet connection. It can also leverage artificial intelligence and machine learning to analyze footage and detect unusual or suspicious behavior.

INCIDENT MANAGEMENT

Using the cloud for incident management can help physical security teams to quickly respond to incidents and track them in real-time.

INCIDENT MANAGEMENT

Using the cloud for incident management can help physical security teams to quickly respond to incidents and track them in real-time.

LIFECYCLE MANAGEMENT

Ultimately, physical security systems require lifecycle management to ensure optimal performance regardless of how they are deployed. They should be maintained and updated regularly to ensure their integrity and functionality. Cloud-based platforms are the most viable option for organizations looking to maintain a strong security posture while digitally transforming their physical security systems.

Cloud-based Physical Security is the Future Present

As cloud computing continues to evolve, organizations must prioritize the seamless integration of these advancements into their existing security strategies.

"Around 54% of businesses intended to switch to cloud-based access control by 2022." - HID Global

Cloud-based physical security is becoming increasingly important, especially in lifecycle management for physical security systems. This allows for the continuous improvement of security measures, ensuring that organizations stay up-to-date with the latest protective technologies. This proactive approach can reduce vulnerabilities and strengthen the overall security infrastructure.

Cloud-Based Security Systems: Benefits for Manufacturing

Using cloud-based security systems has many benefits including -

LOWER COST

Cloud-based physical security systems don't need as much on-site hardware and software, so they're cheaper to set up. Instead, organizations pay a monthly fee to access the cloud-based security system, which can be more cost-effective in the long run.

SCALABILITY

These systems can easily be expanded or reduced depending on the organization's needs. This is great for businesses that have changing security requirements, like seasonal operations.

Insight #3

Physical Security Embraces Cloud-Based Technology

Physical security has evolved significantly in recent years, shifting its focus to the digital realm. The increased reliance on cloud-based technology has revolutionized how organizations manage their security infrastructure. Traditionally, physical security professionals have relied on on-premise solutions and legacy tools to manage their security infrastructure with limited success.

SiteOwl solves numerous pain points by providing cloud-based management, intuitive visual design, and updated project workflows to an industry long overdue for an overhaul.

REMOTE ACCESS

Security personnel can monitor and manage security events from anywhere with an internet connection. This makes it easier to keep an eye on things and respond to any issues that arise.

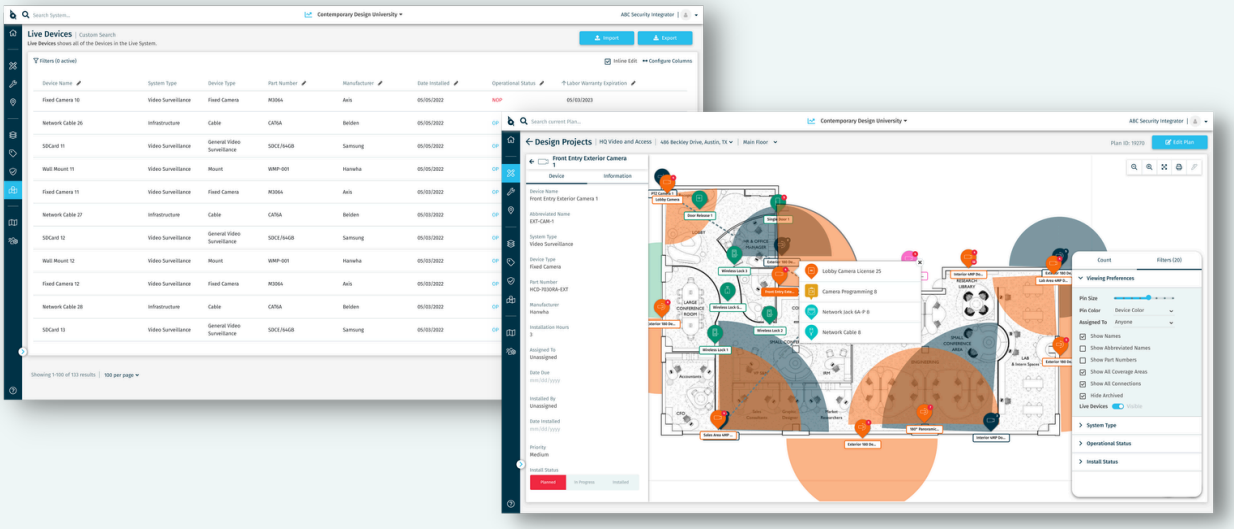
FLEXIBILITY

Cloud-based systems offer a wide range of security applications like access control, video surveillance, and intrusion detection. Organizations can choose which features they need and easily add or remove them as their needs change.

AUTOMATIC UPDATES

Cloud solutions offer automatic software updates, eliminating the need for on-site maintenance and reducing the risk of security vulnerabilities.
Data Backup. With automatic data backup, security data is always available in case of a disaster or system failure.

Platforms like SiteOwl help security directors and their teams effectively plan, design, install, manage and audit their physical security infrastructure from a single interface, building comprehensive system intelligence that is centralized and accessiible from anywhere.



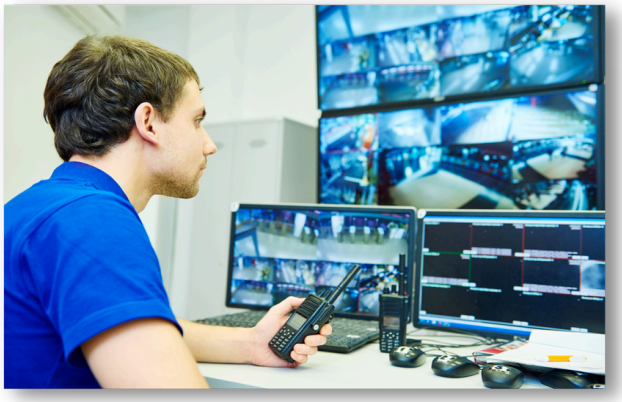
Tackling the Challenges of Physical Security

How Lifecycle Management can transform security system management

The manufacturing industry has unique challenges, mainly due to the size of the facilities that need to be protected and the volume of people and assets that are constantly in motion. Many manufacturing facilities use physical security systems that were designed decades ago and are now either outdated or improperly maintained.

"88% of U.S. businesses now experience more physical security threats..." - 2022 CSO Survey

At the same time, new technologies, such as Internet of Things (IoT) devices and artificial intelligence (AI), are revolutionizing manufacturing facilities' operations. While these technologies are enabling manufacturers to streamline operations, they are also raising new challenges.



Security Lifecycle Management 101

Lifecycle management is an often overlooked, but integral, part of physical security. Physical security systems must be constantly monitored and maintained to ensure that they function as intended and provide the level of protection required by an organization.

Physical security lifecycle management is the process of planning, implementing, maintaining, and upgrading physical security measures to protect an organization's assets and personnel. This includes assessing risks, designing security systems, implementing controls, monitoring and testing the systems, and continuously improving the security posture.

The goal of physical security lifecycle management is to ensure that an organization's physical security measures are effective, efficient, and aligned with the organization's overall security strategy. Some of the challenges impacting both the effectiveness of security systems and the focus of enterprise security teams are:

- Incomplete system information – not knowing what you have.
- Lack of visibility across the age of the components of the security system.
- Inconsistent tools to manage ongoing service and installation quality.
- Difficulty identifying trends in physical security systems.
- Lack of standardized processes and procedures.

Without a well-defined lifecycle management process in place, security teams are left with no way to know the full lifecycle of their security systems or even if they are working correctly.

STEP 1: PLAN

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

Planning includes:

- Determining people, environment and assets that need protecting
- Understanding any regulatory requirements security systems must comply with
- Building a strategy and budget for closing the gap between what you have and what you need

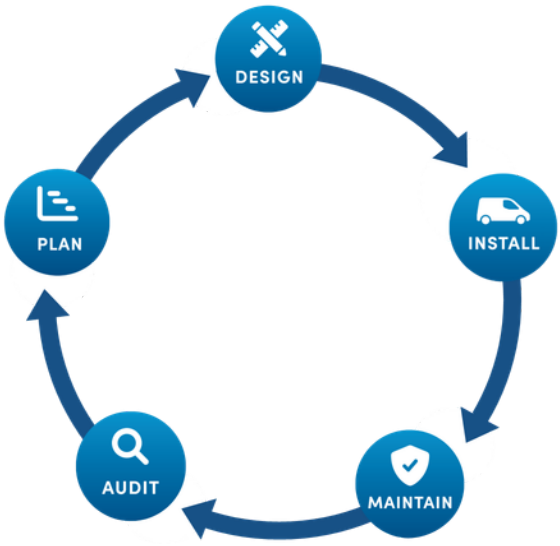
STEP 2: DESIGN

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 with their security integrators, consultants, and other vendors.

As an organization expands, so does its number of physical assets. 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 an 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
- How well the system design aligns with the overall security strategy.

A robust security design effectively protects people, assets, and environments, is cost-effective, and will last a while without a complete overhaul.



Physical Security Lifecycle Management

STEP 3: INSTALL

When installing a new physical security system or upgrading an existing one, several decisions are necessary for responses to answers the following questions:

- 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 the project is completed on time and under budget?

STEP 4: 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, plan for repairs or replacements, and reduce the likelihood of a security event resulting from faulty or malfunctioning equipment.

Maintenance includes activities such as:

- Cleaning and refocusing lenses, housing, and verifying camera placements
- Inspecting power supply and network connections
- Checking wiring and cable harnesses for wear and tear
- Cleaning of control components and ensuring control equipment is operational
- Updating firmware and software
- Testing alarms and communication systems
- Reporting any anomalies or variations

STEP 5: 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.

Insight #4

Spreadsheets Don't Work for Physical Security

Spreadsheets are good for many things but they're NOT:

- Designed to manage physical security systems. They lack the purpose-built design required to manage complex security systems effectively.
- They're not built to scale. Spreadsheets are also inflexible, making them unsuitable for scaling up or integrating new security systems.

Just imagine having to use spreadsheets to:

- The exact location of every security 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.

Getting started with a Lifecycle Assessment

Implementing a Lifecycle Management practice requires planning and rigor. The first step is often to assess the current state of the physical security infrastructure. A security system lifecycle assessment is an effective way for manufacturing organizations to identify potential risks and vulnerabilities affecting their security systems.

This includes evaluating the current state of their security systems, finding gaps in their security infrastructure, and taking steps to fix them.

An assessment can help manufacturing security leaders to

- Understand the current state of their physical security system lifecycle practices.
- Identify ways to make better use of resources.
- Discover areas where security operations can be improved.
- Establish more efficient ways of working with integrators.
- Analyze ways to lower costs and increase efficiencies.
- Identify opportunities for risk reduction.

Managing the Security System Lifecycle

Physical security lifecycle management in the manufacturing industry provides several benefits. Firstly, it improves the overall security posture by ensuring that security measures are up-to-date and tailored to meet the specific needs of the organization. This helps to save costs as potential security threats can be identified and addressed before they become costly security incidents.

Secondly, it ensures compliance with relevant regulations, standards, and best practices.

Thirdly, it helps to better manage risks associated with physical security by conducting regular risk assessments and addressing potential security threats. Lastly, effective physical security measures and systems enable manufacturing organizations to operate more efficiently by minimizing disruptions and downtime caused by security incidents.

But many security teams use tools such as pen and paper, Auto CAD or Visio drawings and spreadsheets to track their system information.

The simple truth is that legacy pen and paper, or spreadsheets, while practical, aren't scalable. Security systems can number thousands of devices across video, access control, intrusion detection and much more. Keeping track of new designs on AutoCAD or Visio, and tracking asset information on spreadsheets is ineffective. Fortunately, the security system lifecycle can be effectively managed through digital transformation.

Insight #5

A digital approach to physical security lifecycle management

A digital approach to physical security lifecycle management is a game changer for manufacturing enterprises wanting to maximize their security investments.

With a centralized platform, manufacturing security teams can:

- Consolidate, track and manage all physical security devices across multiple locations with a single interface.
- Obtain Project Status Reports and updates from anywhere.
- Stay on top of ongoing security system deployments and maintenance work in real-time.
- Conduct System Audit and Maintenance Tracking
- Monitor ongoing service issues and conduct system-wide audits to identify and fix security gaps.

With SiteOwl, you can accomplish all these and more without leaving the office while reducing operational inefficiencies and costs. Now that's a win/win!

Security teams that invest in a comprehensive lifecycle management platform like SiteOwl can centralize system information, including designs, installation projects and maintenance, while at the same time, staying on top of warranties, moves, adds and changes and much more. What's more, all this information is readily available on digital floorplans that continue to aggregate system changes over time.

Security team challenges	How SiteOwl solves them
Lack of visibility of systems and devices	Robust real-time reporting to facilitate coordination, commissioning and programming.
Lack of standardized security system management practices	Consistent and scalable security system practices, standardized across vendors.
Inadequate information for internal reporting, auditing, and compliance	Centralized system of record with auditing, warranty and lifecycle management.
Using legacy tools such as spreadsheets to monitor and manage security systems.	Data-driven decision making with consolidated system reporting

Leveraging Actionable Intelligence for Improved Physical Security

Why Data-Driven Insights are Essential for Manufacturing Facilities

Manufacturing leadership teams need to make tough decisions on how to allocate their security budget to safeguard their business. A crucial aspect of implementing effective physical security systems is making budget planning a data-driven process. By utilizing accurate data and analytics, decision-makers can allocate resources efficiently and ensure optimal system performance. This proactive approach addresses potential vulnerabilities and maintains the highest level of security.

Data-driven budget planning eliminates guesswork and enables leaders to make informed decisions backed by evidence, contributing to enhanced protection of manufacturing facilities. Many manufacturers use multi-year budgets for planning their physical security infrastructure. This tool can be used alongside a strategic plan to help organizations map out long-term goals and the tools and processes required to achieve them.

While each organization has unique priorities, challenges, and budget constraints, successful multi-year budgets have some common characteristics, especially when it comes to planning and providing a framework for leadership to make more informed decisions.

Quantifying the return on your security investment

Evaluating and quantifying the return on investment (ROI) for physical security planning in manufacturing facilities is crucial for informed decision-making. A well-implemented security system helps minimize disruptions, protect valuable assets, and ensure a safe working environment, directly impacting the overall operational efficiency.

By measuring key performance indicators (KPIs) such as incident response time, asset loss reduction, and system uptime, leaders can assess the effectiveness of their security investment. Understanding the ROI will enable manufacturers to make data-driven decisions, optimize their security budgets, and continuously improve their physical security strategy.

Calculating Physical Security ROI

A well-calculated ROI enables organizations to maximize their profits while ensuring their employees' and assets' safety and well-being. So how can manufacturers quantify the ROI for security investments?

A standard formula for ROI is:

ROI % = (Return - Cost of Investment) / Cost of Investment x 100

In theory, physical security technology ROI is a straightforward calculation: net gain/cost multiplied by 100. In practice, the analysis is often more complicated because not all contributors to the investment and return translate directly to a dollar amount.

But here's the challenge: Investment is not simply the sticker price of a given technology component or line items on an invoice.

Instead, organizations should calculate the investment in terms of the total cost of ownership. Here are examples of the costs you should include when calculating your investment in security technologies:

- Subscription and user license fees
- Training and support
- Integration with other technologies
- Hardware purchases
- And the big mysterious one: INEFFICIENCIES.

Unfortunately, inefficiencies often scale automatically, so when a basic task is time-consuming, error-prone, or otherwise inefficient, the impact compounds over time. Even additional mouse clicks add up over time.

Here are some questions to identify inefficiencies: Does the technology create more or fewer steps for team members to perform their basic duties? Are there redundant processes that could/should be automated?

Ultimately, sharp manufacturing security leaders articulate and demonstrate ROI by connecting security investments to specific organizational objectives. They position security as a business enabler through which important priorities are safely achieved. Of course, these priorities may vary by the organization's size and location, and other factors. Still, they should always be driven by accurate data and a clear understanding of the organization's risks.

Conclusion

Future of Physical Security Systems in Manufacturing

The future of physical security systems in manufacturing is poised for significant advancements as technology evolves and threats become increasingly complex. Integrated solutions combining video surveillance, access control, and security analytics will play a crucial role in bolstering the safety and efficiency of manufacturing plants.

Manufacturers will thrive in the 21st century by embracing digitization and leveraging technology to design, manage, and maintain their physical security infrastructure.

Optimizing physical security to thrive in a connected world requires a strategic approach that leverages technology and fosters collaboration among stakeholders. By integrating advanced security solutions that enable:

- System-wide visibility
- Real-time Project Status
- Effective planning & budgeting
- Collaboration across teams
- System Audit and Maintenance

With the rise of the Internet of Things (IoT) and advancements in artificial intelligence (AI), smart security systems can identify and respond to potential risks with greater accuracy and speed. Collaboration between stakeholders and investment in these cutting-edge technologies will be essential for ensuring a secure and resilient manufacturing sector for years to come.

As much as technology has transformed the manufacturing sector, the future of physical security systems in manufacturing hinges on how manufacturers respond to technological shifts and integrate them into their existing security systems. As such, lifecycle management is critical for ensuring the future viability of physical security systems in manufacturing.

The lifecycle management discussed in this guide, along with the actionable tips to optimize a physical security program, provides the foundation for manufacturing security leaders to evaluate and ultimately optimize their physical security program.

Still, they're only the tip of the physical security iceberg.

SiteOwl is well-positioned to support manufacturers as they digitize their physical security systems to leverage the power of IoT, AI, and other technologies to transform their operations.

Join us at an upcoming conference or visit us online at www.getsiteowl.com for more information about the physical security digital transformation.

Learn more about SiteOwl at
www.getsiteowl.com / inquiries@getsiteowl.com / 888-748-3695.

siteowl®