Managing The Lifecycle Of Physical Security Systems

A practical guide for enterprise security teams to plan, deploy and manage security systems with confidence

Jon Polly, PSP, IC3PM
David Santiago, CSP, PSP

siteowl®

Contents

About the Authors

Jon Polly
(PSP, IC3PM)

Jon Polly is the Chief Solutions Officer for ProTecht Solutions Partners, a security consulting and project management company.

An industry veteran, Jon has designed security systems and managed projects for city-wide surveillance and transportation camera projects in Raleigh and Charlotte, N.C.; Charleston, S.C.; and Washington, D.C.

Jon is certified is certified as a Physical Security Professional (PSP) through ASIS International, and in Critical Chain Project Management (IC3PM) by the International Supply Chain Education Alliance (ISCEA).

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.

1. Introduction

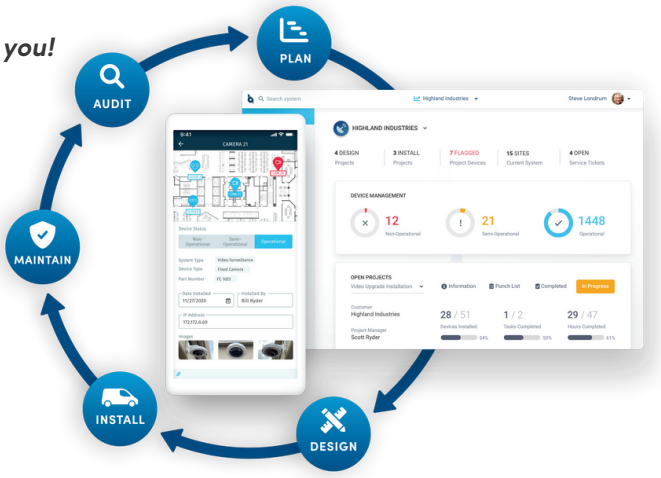
What is Lifecycle Management?

Lifecycle management is the process of determining the lifespan of a physical security product or solution and planning the steps to take when it is time to retire the solution and/or its products. But it doesn't just stop there. Lifecycle management is also about preparing for how to replace or update managed security systems without disrupting or negatively impacting businesses' day-to-day operations.

The process of lifecycle management is complex and challenging for any security director and his/her team. Frequently, we hear security directors or their teams tell us "We don't know what we have, we don't know what our warranty status is, we have all these spreadsheets but really no central place where all this information is stored and managed."

Sound familiar? If you said yes, then this ebook is for you!

The key to confidently managing the lifecycle of physical security systems, is a combination of knowledge, visibility, and the ability to make timely, data-driven decisions. To accomplish this, you need actionable information, a robust platform that manages all this information, and strong processes.



From frustration to confidence

Meet SiteOwl, the world's first real-time lifecycle cloud-based platform that's transforming the way security directors manage physical security systems. This ebook, written by two accomplished physical security professionals, will arm you with the information you need to answer critical questions that you may already ask yourself regularly, such as:

- Do I have a comprehensive inventory of all my security assets?
- Which of my devices needs upgrading? And when?
- Are my vendors doing what they're supposed to do?
- How can I keep track of multiple projects efficiently?

As a security professional, you know firsthand that in today's digital world you can't afford the risks that come with low visibility, siloed information, and poor system performance. The good news is this: with the right systems and tools you can take control and get the most out of your security investments.

We hope this ebook will help you streamline your processes and optimize your physical security systems.

Let the journey begin!

2. Knowing what you have

You can't protect what you don't know you have

It is best to complete a thorough security inventory audit before considering a system overhaul.

Having an accurate asset inventory ensures your company can keep track of the type and age of hardware in use. In doing so, you gain greater insight into your system's design and discover ways to improve security without making extensive updates.

Inventorying physical security assets

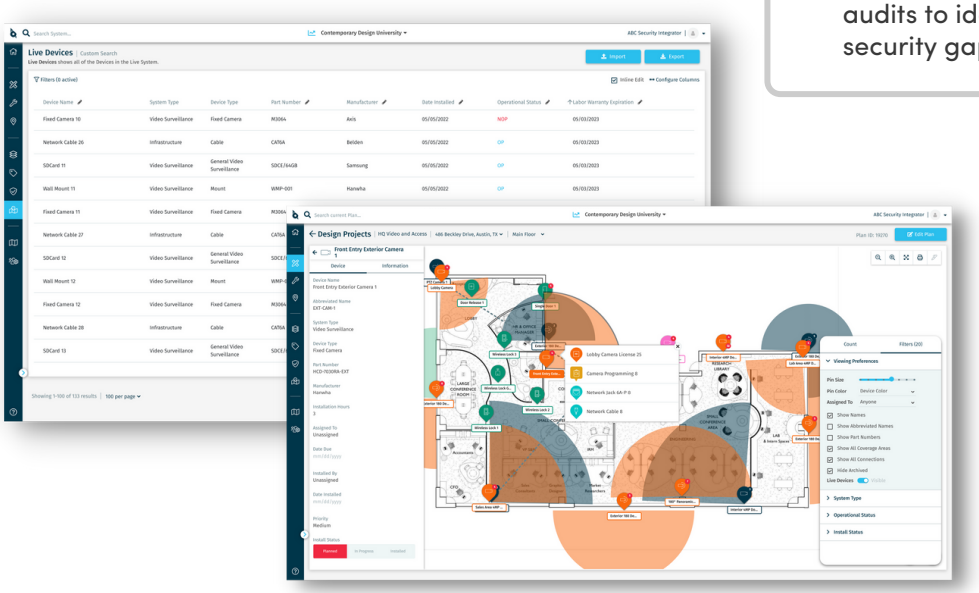
Asset inventory is a foundational element of your security program that can ultimately improve your security posture. It helps you mitigate risk and ensure business operations run smoothly. Many security professionals think an asset inventory can be as simple as an Excel spreadsheet.

The truth is to get the most value from your security assets, you must be able to track and analyze issues such as physical location, maintenance requirements, depreciation, performance, and eventual asset disposal. In short, you need efficient full-lifecycle management to standardize and optimize your security assets and infrastructure.

BEST PRACTICE SPOTLIGHT

Platforms such as SiteOwl allow end users to access their security systems information in ways never before possible. For example, users can:

- track and manage all physical security system devices across multiple locations from a single interface
- collaborate directly with their integrator on new system designs, manage repairs and maintenance requests, and
- rapidly perform system-wide audits to identify and repair security gaps.



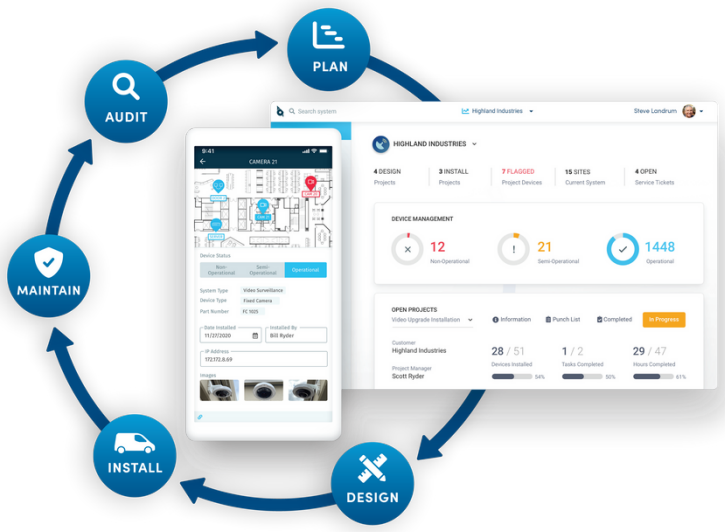
Ditching disparate systems

Designing and managing security systems seamlessly is a top challenge for every security director. But as your organization grows, employee headcount rises, and new locations are added, new systems can be introduced without regard to how they work with what is already in place. This results in disparate systems creating a multitude of challenges, including:

- Inaccurate system information
- Lack of standardized security system management practices
- Increased effort to maintain due to lack of interoperability
- Inadequate information for internal reporting and system management

Integration of disparate systems is essential

A disparate system is often characterized as an information silo because of the data system's isolation from or incompatibility with any other data systems. Physical security software tools such as SiteOwl enable you to manage and visualize disparate systems and functions that handle security and surveillance on a digital floorplan, allowing you to get the most out of your security investment.



BEST PRACTICE SPOTLIGHT

When all elements of a physical security system work together in a unified way, they not only secure a business but yield actionable business intelligence that can be leveraged and combined with operational data to improve efficiency.

Unification brings together all security system components seamlessly in a centralized platform with one user interface in a way that can vastly improve physical security management.

While security integrators have developed a variety of methods to unify physical security solutions, these, by and large, remain a set of disparate systems with limited communication and interoperability among them.

3. Designing the right solution

How do you determine what you need?

Before implementing physical security measures in your building or workplace, it's important to determine the vulnerabilities of your current physical security measures. While each organization has unique priorities, challenges, and budget constraints, all can benefit from a detailed physical security assessment to evaluate current measures and identify potential gaps.

Physical security vulnerability assessment

A comprehensive security vulnerability assessment is essential before designing or upgrading your physical security system. Without that information, you risk wasting valuable resources on unnecessary protection measures.

Physical vulnerabilities can include physical elements of your building and procedural gaps for responding to physical threats. In terms of physical security systems, the main areas you should evaluate are

- electronic security systems, including video surveillance and access control systems,
- building management, and life safety equipment, including panic buttons, motion detectors, sensors, and building safety equipment.

BEST PRACTICE SPOTLIGHT

Physical security planning: access control, surveillance, and security testing are a physical security plan's three most crucial elements.

Once those elements are in place, you want a platform to keep up with critical maintenance and upkeep so that you know when equipment fails, warranties are about to expire, and who to contact when something goes wrong.

When considering your physical security risk assessment, it's always best to be proactive vs. reactive when it comes to keeping people safe. A risk assessment gives you a fair chance to cover the gaps in your security, and protect yourself, your employees, and your business before something happens.

Keeping things scalable

Every organization wants to grow and evolve, but factoring in security to your company's business goals, alongside all the other challenges that come with operating in today's business climate, isn't always straightforward. Indeed for some, it may even be a major barrier to evolving for some.

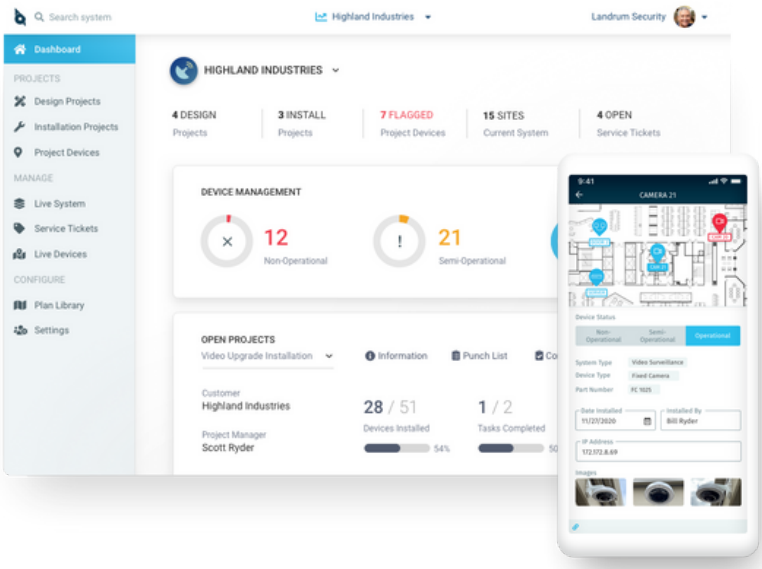
The good news is that you no longer need to choose between security and scalability. Thanks to technology advancements and lifecycle management platforms, you can now implement convenient, scalable, and secure solutions.

Scalable Security Systems

One of the biggest challenges security directors face when scaling their security system is a lack of standardization and management practices. While the scale and sophistication of your controls and monitoring will vary depending on location and need, best practices can be applied across the board to ensure a robust physical security posture.

A cloud-based lifecycle management platform makes it easier for you to scale up or implement new technology. Three key features that will enable you to scale your physical security system include :

- Comprehensive system dashboard so you can assess your entire security system performance from anywhere.
- Complete asset information to maintain detailed device-level data, including warranty expiration, pictures, and much more.
- Ease of access so that information is available at your fingertips anywhere and at anytime.



BEST PRACTICE SPOTLIGHT

Scaling your access control system

A scalable system does not require the abandonment of any equipment to grow in scale. The organization may purchase a larger ACS license, but they do not have to waste capital investment to expand their system.

To accomplish this, you need access to device-level service and warranty information to plan changes, upgrades, and budgets.

Accurate system information allows you to make data-driven decisions and fiscally responsible security investments.

4. Creating the right processes and systems

Building a culture that focuses on keeping information current

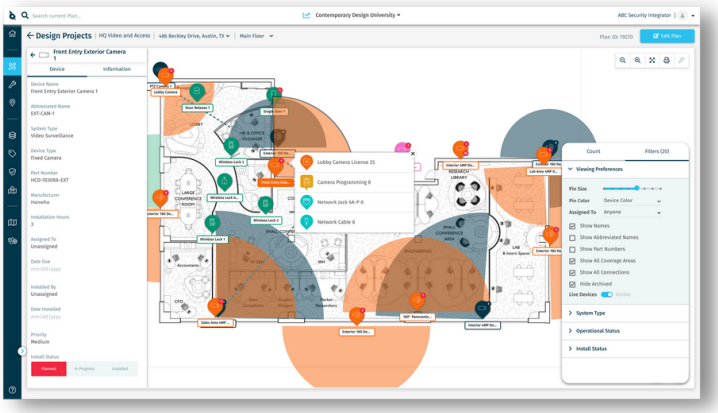
Everyone in your organization contributes to your security culture. No amount of investment in physical security will be effective without the right security culture.

Building a culture that prioritizes physical security requires accurate information to monitor both ongoing service/ maintenance work, as well as adds, moves, changes to the existing system. In order to accomplish this important mission, you need to be able to:

- Conduct system-wide audits to identify and fix security gaps.
- Continually optimize your security inventory and physical security infrastructure.
- Require accountability across all service and installation projects

Keeping information current

Security directors use lifecycle management platforms to obtain complete system visibility with real-time activity tracking.



BEST PRACTICE SPOTLIGHT

Physical asset management- Imagine having to control your asset lifecycle management by hand for each security camera or access card reader in your company. Assets will undoubtedly fall through the cracks. That's why you need a centralized platform that allows you to monitor your assets and conduct audits systematically.

Lifecycle management platforms like SiteOwl enable security professionals to manage their system planning, design, installation and service from one centralized location, while providing system-wide visibility. Often, these platforms also have reporting capabilities that help security professionals to plan security investments.

With SiteOwl, you can manage the information behind every element of your access control, video surveillance, and intrusion detection systems — all from a single location.

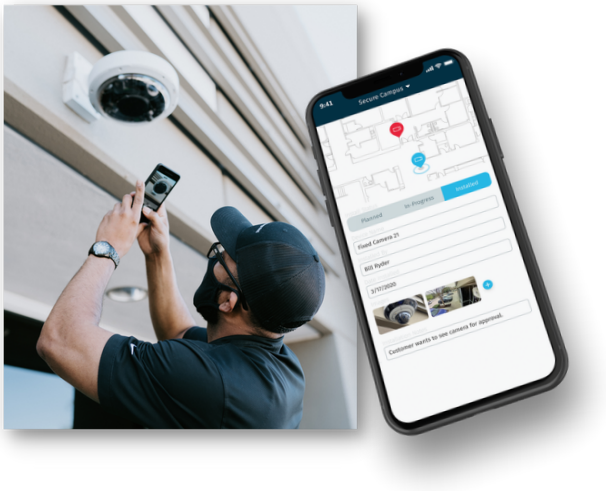
Digitizing your current systems and processes

While most industries have fully embraced the digital revolution, the physical security industry was forced to scale rapidly without the technology to support them for a long time.

Digital transformation is about ensuring all aspects of your physical security system are on the same page. It requires developing solutions that can actively deal with outside and internal threats simultaneously. To accomplish this you need to visualize your data and have access to critical system information from anywhere.

Digital transformation

The same type of scale other industries have seen with digitization, including cyber security, can be realized in the physical security sector. Streamlining processes are far easier to achieve than you might think, mainly thanks to lifecycle management platforms that automate systems designed specifically for the security industry.



BEST PRACTICE SPOTLIGHT

Most physical security system bids and designs are still completed using pen and paper. When you use a platform with digital tools, you'll be able to create detailed designs and convert them to comprehensive installation projects without any information loss. Additionally, you'll be able to keep your team, vendors, and key stakeholders all on the same page.

A digital approach to physical security can help you improve the effectiveness and efficiency of your security program by streamlining:

- Workflow technologies and automation to detect, investigate and remediate routine responses;
- Connected (IoT) sensors and video analytics to identify threats faster;
- Real-time communication and collaboration

5. Working with the right vendor

Knowing what type of vendor you need

The traditional Security Director is an accomplished law enforcement or military veteran with the ability to manage people. But do they know security technology? Most would admit not. So they need a strategic vendor partner to help them define the security technology. Depending on the size of the project, this could be a security consultant or a security integrator.

Selecting the right vendor requires doing some research to ensure the vendor knows what they are talking about and has direct access to the technology vendors. The right resource will have a reputation to back them up.

The security market is filled with noise and glamour, fast-talking salespeople, and marketing hype. Finding the right vendor will help guide and deliver interconnected subsystems of technology that work together to meet the needs the Security Director is facing.

A strategic vendor partner will be with the Security Director for the long haul, introducing new technologies that work within the existing ecosystem to improve efficiency or mitigate risks.

BEST PRACTICE SPOTLIGHT

Security integrators seek to set themselves apart from the competition by emphasizing what makes their service unique, but at the end of the day, you must choose the integrator that provides the best value for your company.

Differentiation is a subjective matter and each organization has its own set of challenges and requirements but here are four differentiating factors to consider:

- Reputation - In most cases, a stellar reputation can be a trusted indicator that a vendor is reliable, trustworthy, and operates as a professional business
- Products and technologies supported - You want to work with integrators that support the same solution set that your organization needs
- Partnership - Integrators that look at their relationship with you as transactional are less likely to be successful partners in the long run
- Price - Your goal should be to work with a vendor that offers fair and transparent pricing so that you understand the true operational costs of managing your system

Collaborating with your vendor(s)

Partnering with a strategic vendor partner should happen before a project even takes place. Ideally, this would occur with a technology roadmap being created around the technology ecosystem currently in place. At the onset of a project, a strategic partner should be involved. This can help with design to define the technology ecosystem, is it being expanded, or replaced?

Security technology and subsequent services affect more than just the Security Department. With the right strategic vendor partner security technology can be planned to bring business intelligence to the organization, increasing employee engagement or customer experiences.

Early involvement in a project will provide time to work through any concerns and shortfalls. The strategic vendor partner can help guide the organization to new technologies to increase efficiencies and reduce risks, or simply to generate useful data that was not previously available.

BEST PRACTICE SPOTLIGHT

SiteOwl allows end-users and their security vendors to collaborate in ways never before seen in the industry. Using SiteOwl, security teams can :

- partner with their vendors to build rich digitial designs easily and quickly, while taking into account existing infrastructure information
- get real-time updates of installation progess from the field
- stay up-to-date on any ongoing maintenance, projects, system audits and much more

Collaboration tools, like SiteOwl, can improve communication between the Security Department, construction teams, and strategic vendor partners. Collaboration can help remove confusion around project status and provide additional tools for the organization

6. Managing the project

Managing the resources

The project team is supposed to be a cohesive unit with a singular mindset to achieve a successful project. The problem is many times a project team has never worked together. Initially, there will be some difficulties when any new team member is added. Once the team starts to find cohesion, the project is often already underway.

The Right Tools

There are multiple project management methodologies and project management tools to go with each. However, many security integrators do not have basic project management tools, causing a project team to immediately struggle with how to functionally manage a project. Project Management tools, like SiteOwl, can help integrators and organizations collaborate on projects, provide a standardized experience and deliver them successfully; projects that are on time, on budget, and at the highest quality.

BEST PRACTICE SPOTLIGHT

Modern turnkey project management solutions either lack the features integrators need in order to focus on project design and cost savings, or they can't scale in a way that integrators can track progress and deliver results in an effective way. SiteOwl allows you to:

- Stay on top of ongoing security system deployments and maintenance work in real-time
- Drive team and integrator accountability across all service and installation work performed
- Conduct system-wide audits to identify and fix security gaps

Managing the Project Resources

The project manager and the project team as a whole need to know what resources are to be utilized on a project, and when those resources are available. Failure to manage resources appropriately is one of the easiest ways to delay a project. Resources have to be accurately accounted for when the project is laid, on something like a Kanban board. If resources are accurately allocated, the project will stay on track. Deviation requires additional management by the project manager and ultimately the project team.

The project sign-off

The project sign-off is one of the most overlooked documents in project management. Typically, most project managers will speak to the project champion who will confirm the project was successfully implemented. The project manager then contacts finance to invoice the organization for any remaining balance to the purchase order. It is a glorified gentlemen's agreement that leaves all parties involved liable for issues.

The Project Sign-Off Document

The project sign-off document is a simple one-page document that should at the very minimum reference a project name or number, the contract name or date signed, the delivered bill of materials (BOM), and a place for both the project manager and the project champion to sign and date.

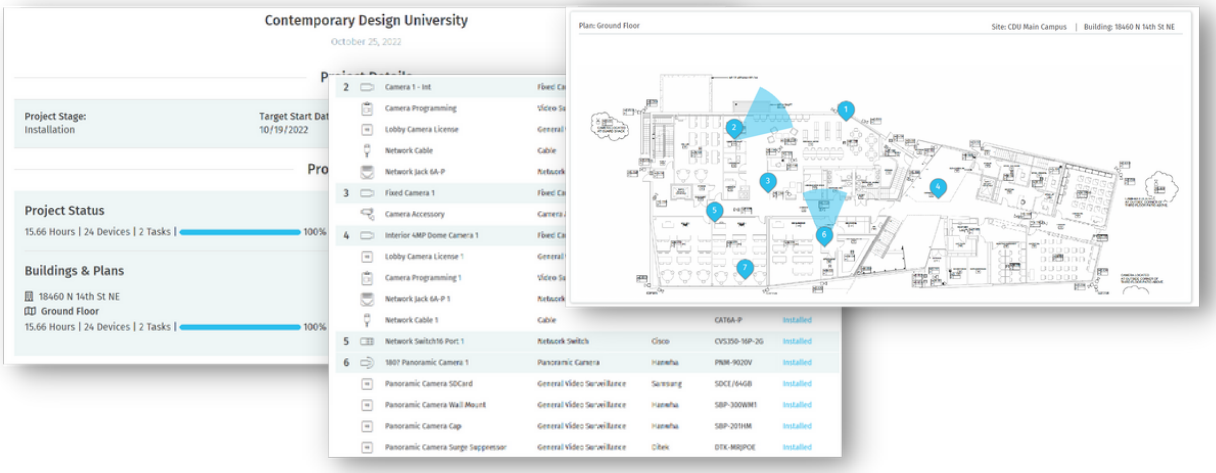
What this accomplishes is that both parties have an accurate account of equipment that was commissioned, and is now active in the project champion's organization. By signing the document, it is a legally binding document to state what day the project was accepted as complete. This date is now the official warranty date that the security integrator will use to base all warranty work for a one year period on.

The detailed BOM will define what equipment was covered for the one year warranty, and will serve as the basis for any ongoing service level agreements (SLAs) as to what equipment is to be covered under the SLA. The SLA will typically be based on a percentage of the commissioned BOM.

BEST PRACTICE SPOTLIGHT

SiteOwl empowers you with accountability tools to ensure your installs, upgrades, and moves are successful. With security management platforms like SiteOwl security directors can coordinate with technicians to:

- Review images
- Read progress reports in real-time
- Sign off on work product and share detailed information



Organizations and Security Integrators many times find themselves at odds over when the project is complete. The sign-off document removes all doubts.

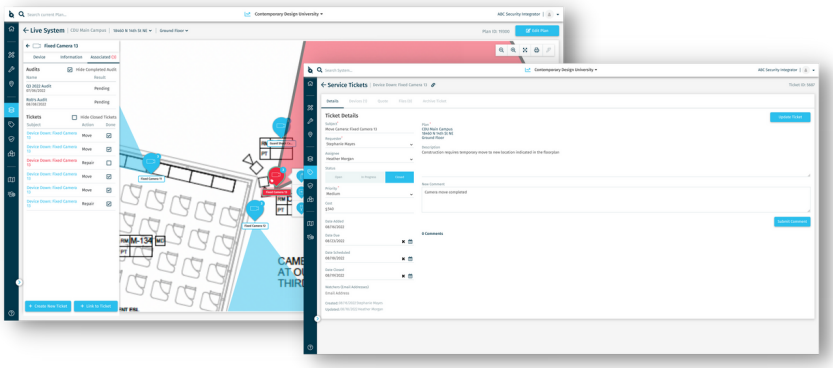
7. Making fiscally sound security investments

Making budget planning a data-driven process

The yearly budget is due next month, and there is a frantic search to determine how much was spent this past year on security technology services and additions. This may mean calling finance to track invoices, delving into a spreadsheet nightmare, or quickly calling the strategic vendor partner vendor for some advice. What if that information was readily available at the click of a button?

Strenghthening your planning using the right data

In the past, security technology was deployed based on choke points, Crime Prevention Through Environmental Design (CPTED), best practices, and aesthetics. While those are still very valid design elements, now there is the addition of incorporating a data-driven approach. Choke points and best practices are often built on previously available data.



BEST PRACTICE SPOTLIGHT

Many security integrators are siloed when it comes to sharing information. As a result, security directors and end users are often left out of the loop. SiteOwl allows you to place all project information in a single location.

- Security Designs
- Floor Plans
- Parts Lists
- Daily Job Reports
- Service Tickets
- Meeting Notes
- Equipment Schedules
- Quality Control Images
- Scope of Work Documentation

and much more!

For example, a common assumption is that if a security device is placed at a specific location, the threat is mitigated because it deters incidents fom occuring in the first place and even if one does occur, data will be captured of the incident. The data behind that is no different, than say, the use of analytic data to determine the flow of people. Why put a general access card reader on a door no one ever walks through? Data can provide detailed budget planning data based on trends and use patterns.

Quantifying the return on your security investment

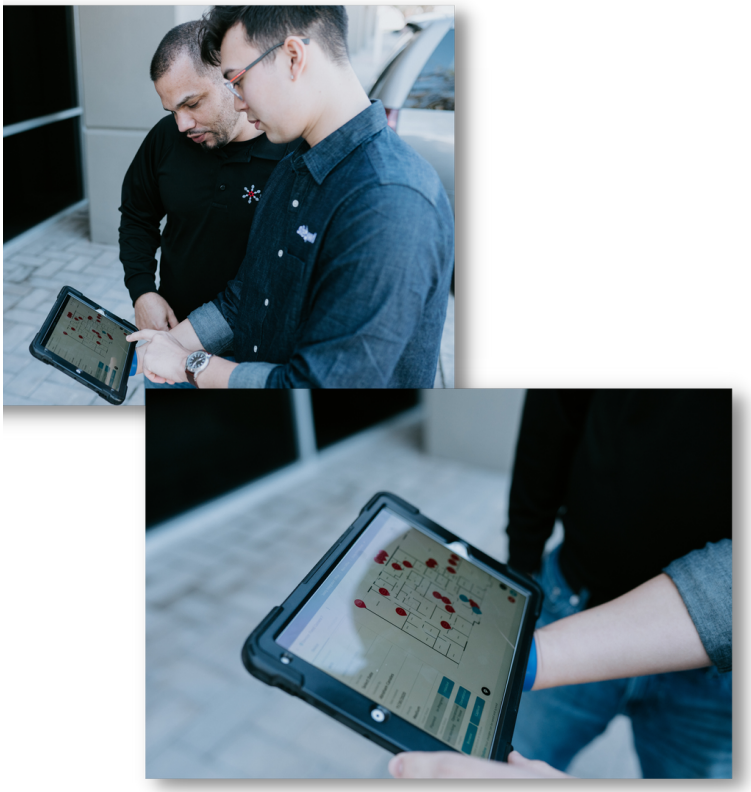
Let's be honest. The security department of an organization typically has the least amount of influence and the least amount of budget of most of the business units. Most organizations treat the Security Department as an insurance policy, the last stand in the event of a tragic event; and many times they are not wrong. Traditionally, money spent with security has seen very little Return on Investment (ROI), and has been measured qualitatively in Fear, Uncertainty, and Doubt.

So how does an organization quantify the ROI of its security investment; people, processes, and technology? The best ROI is zero incidents at the least amount of spend but in reality that may be unattainable.

The Formula for Return on Investment (ROI) is

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

The easy part is the Cost of Investment; this could include the whole budget or portions such as salaries and system cost. The challenge with quantifying an ROI is calculating an accurate return. The cost of an incident would be a negative (-) amount while prevented incidents a positive (+) assumed amount.



Historical Reduction

One way to measure ROI is to review the number of incidents responded to over the lifetime of the investment. Has that number gone down? As people, processes, or technology were implemented, does the number of incidents reflect the changes?

Current Value

When the system was put in, was the intent to have the people, processes, and technology siloed to just focus on the security of the building? If so, the ROI is going to be significantly less than if those elements of security are used to create efficiencies across the organization. When another business unit is able to reduce costs 5x or 10x because of data shared, the ROI increases exponentially.

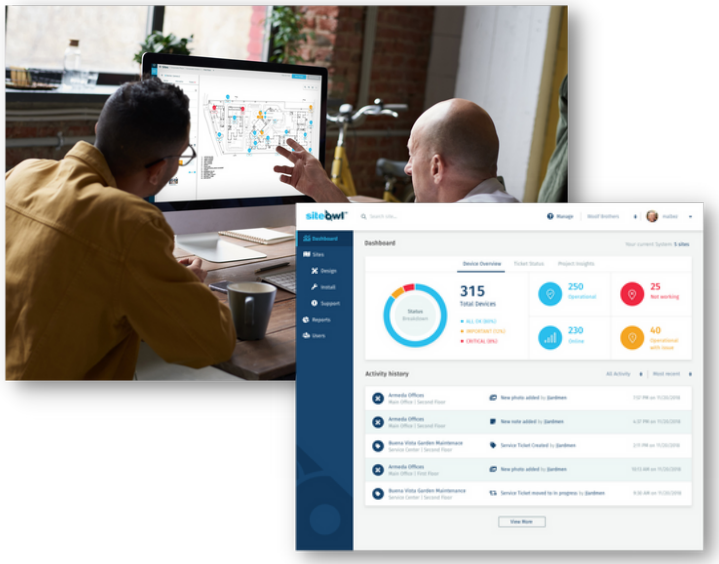
8. Letting the numbers speak for themselves

Making data the core of your decision-making

Today there is more data being generated than could ever be fully used. So what data is useful? Traditionally camera systems have been implemented with a 30-day retention period, while most organizations respond to incidents within 3 days, the rest of the video fills up hard drives that no one ever looks at.

The same is true for access control alarms and alarm systems; when an alarm system triggers, security responds and mitigates the alarm; but when nuisance alarms occur (random data being generated because of a failure) they are cleared out quickly and frequently ignored.

Useful data and how the data can be used by the organization to increase efficiencies, reduce risks, and drive employee engagement and customer experiences should be the primary focus for decision-making.



BEST PRACTICE SPOTLIGHT

By using the concepts built into the fabric of SiteOwl, security directors can

- Identify failure trends in specific model numbers across the enterprise
- Proactively plan for upgrades and replacements based on installation and/or warranty dates
- Build and implement consistent and scalable security system practices, standardized across vendors
- Make fiscally responsible security investments

In the previous example, does the security technology simply record data; video, card swipes, etc.; or does it intelligently record valuable data that reduces search times and increases business intelligence by solving problems? Can it be used to be a solution not only for the Security Department, but also to solve problems for other business units?

At SiteOwl, data generated is used to increase efficiencies for security integrators, while also solving problems across the organization.

Managing the lifecycle of your assets

The organization has bought a security system, assets with warranties and fixed costs. What now? In the past, many companies have relied solely on Service Level Agreements (SLAs) provided by both technology manufacturers and security integrators. But many of these are done wrong.

The Proper SLA

A proper SLA is a partnership between the organization and the security integrator. It should include a preventative maintenance aspect, be reasonably time-bound, and fiscally responsible.

Preventative Maintenance

The SLA should have at minimum a biannual functionality test of the covered system. The system test should include each sensor type in real-world use. All batteries should be tested with a proper meter. Camera domes should be cleaned inside and out with appropriate cleaning materials to ensure the view is clear, removing dirt or bugs from the camera.

Reasonably Time Bound

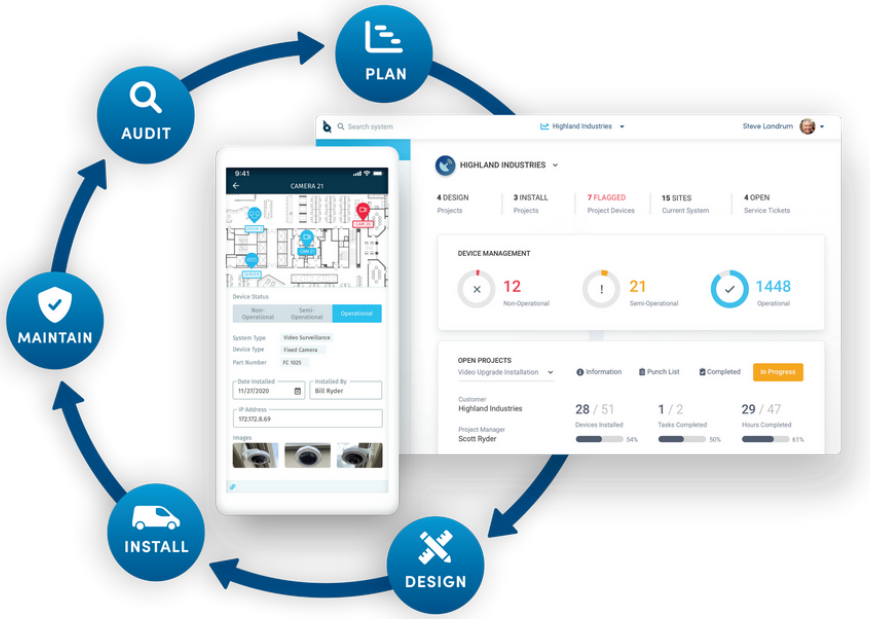
An SLA should have a time requirement. Depending on severity, this could be set out initially in the SLA. Priority calls may be given a 4 hours response while routine calls may be the next business day. A reasonable amount of time for a technician should be applied to each call.

Fiscally Responsible

An SLA should be provided to the organization based on the total system value, not installed value. The SLA should be reasonable based on response time and equipment RMA. As many of the technology manufacturers extend warranties to 3-5 years, many offering advanced RMAs, the SLA should reflect those warranties.

Lifecycle Management at your Fingertips

SiteOwl offers the organization and the security integrator tools to manage the lifecycle of all commissioned equipment. Organizations can seamlessly communicate service requests and know product warranties at the tip of their fingers, accurately budgeting for replacements in following years and planning out future budgets based on technology service calls and warranty expiration dates.

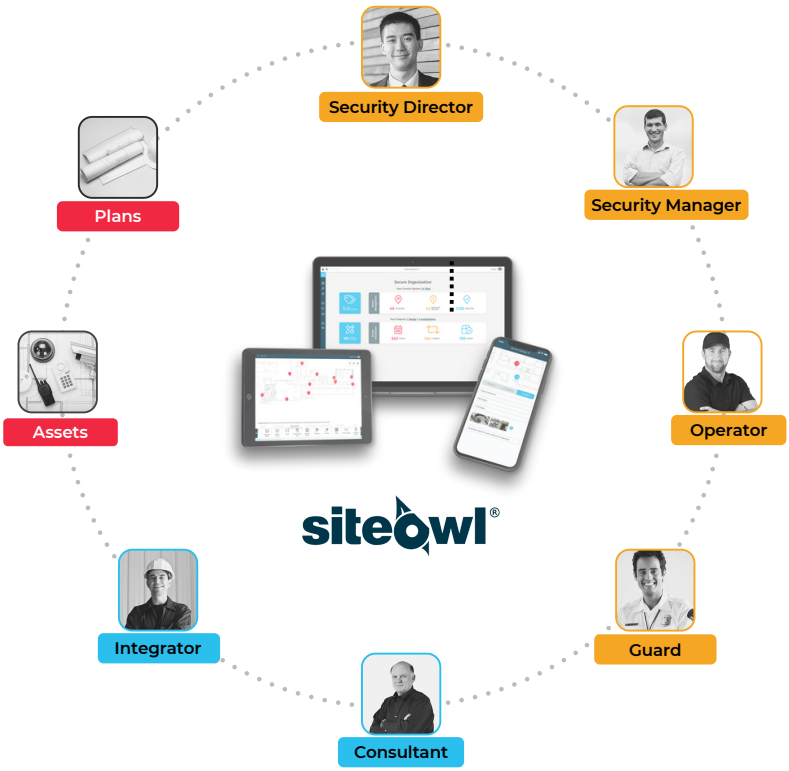


9. Conclusion

Elevating your playbook for an enhanced security program

As a security director, you have a tough job. Keeping safety measures in place without jeopardizing your organization's operational efficiency is no easy task. You must regularly assess the threat landscape, make adjustments, and ensure your security measures remain effective.
Many factors prevent or slow your organization's ability to implement a solid cyber-physical convergence framework. Some of the leading challenges include:

- Lack of standardized security system management practices (you don't know where to start...)
- Inability to accurately forecast and plan budgets (you want to start but are not sure you have the resources...)
- Incomplete and/or inaccurate security system information (you lack the data to make a case to your leadership team..)



The physical security industry is embracing digital transformation

The security industry is facing a huge digital disruption, and to be successful, you need to embrace digital transformation. Maintaining the status quo will only increase your risks and prevent your organization from capitalizing on a valuable opportunity.

Organizations are complex ecosystems. When people, processes, and technologies are connected and working together across an organization, it improves business performance. For companies early in their expansion or those looking to create an enhanced security program the solution lies with digitization, smart integration, and effective lifecycle management that enables you to digitally transform the delivery and management of your security infrastructure.

SiteOwl is an award-winning platform transforming how enterprise security teams and their integrators manage the lifecycle of their physical security systems.

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

siteowl