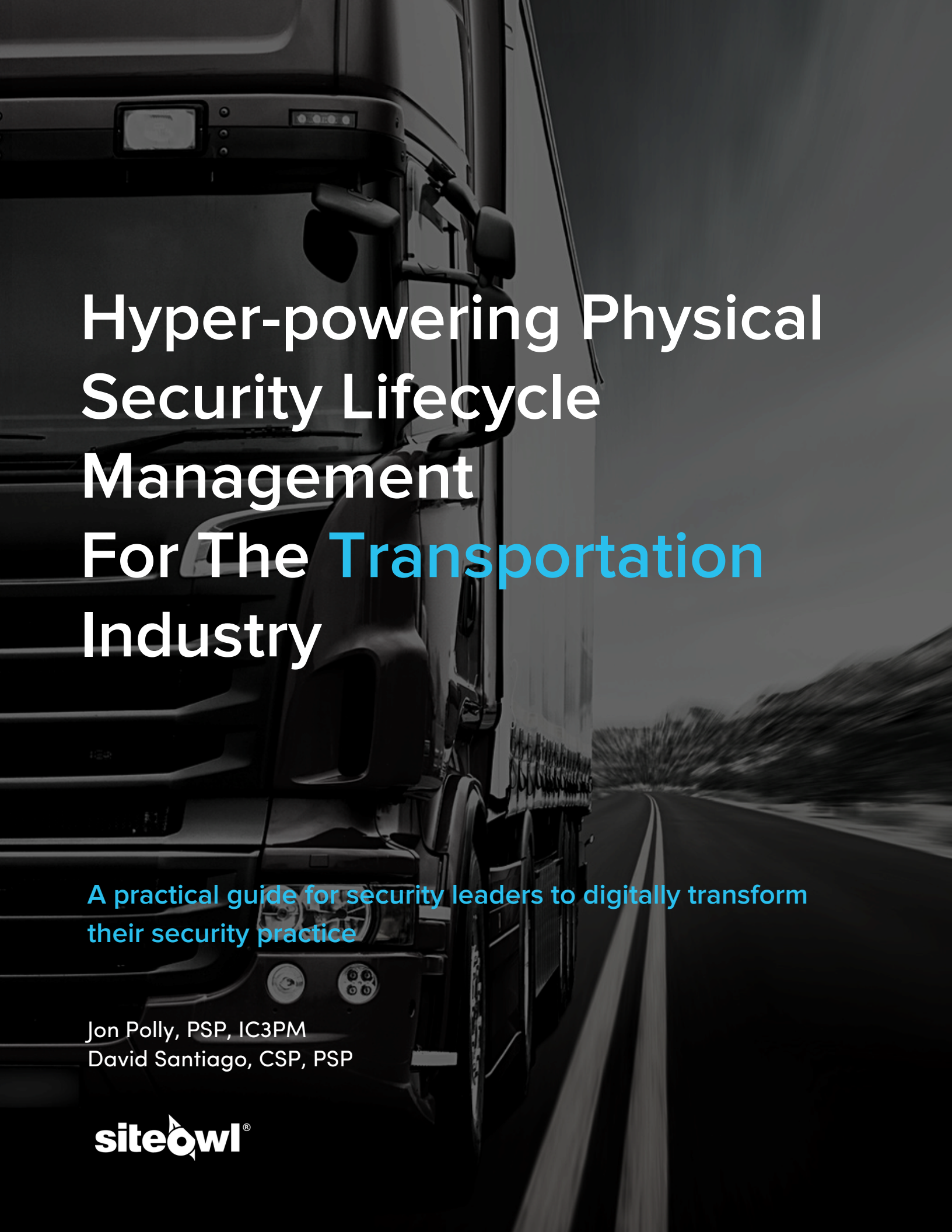


Hyper-powering Physical Security Lifecycle Management For The Transportation Industry

A practical guide for security leaders to digitally transform their security practice

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.

Introduction

Digital Transformation is changing everything, and the transportation industry is no exception. With the fast adoption of new technologies, such as the Internet of Things (IoT) and the rise of cloud computing, the transportation industry has seen many changes over the last decade. However, the digital transformation of the industry is still in its early stages.

Physical security is increasingly driven by digital technology, and as a security leader, you must understand how digital technologies can help you increase operational efficiency and improve safety.

The proliferation of security devices, coupled with cloud computing, has created a sea of opportunities for transportation business owners, managers, and executives to improve the security and safety of sites, equipment, and employees.

While transportation agencies have started embracing new technologies to improve their operations, many adopt a reactive approach to physical security by only implementing new measures after an incident.

A reactive approach to physical security includes

- Installing/upgrading a video surveillance system after a break-in or vandalism.
- Installing or updating an access control system after an incident.
- Adopting IoT and connected vehicle technologies after a fatal incident.

Sadly the list goes on, but it doesn't have to be this way. Instead, transportation agencies can proactively embrace new technologies to keep pace with evolving physical security threats while maintaining a strong focus on safety and security.

This ebook will provide you with an overview of the digital transformation that is happening in the transportation industry and how to take advantage of the digital tools available to address your current physical security challenges and best prepare for the future.

About SiteOwl:

SiteOwl is a unified digital platform that transportation security teams and their security integrators can use to manage their physical security lifecycle from a central platform.

With SiteOwl, security leaders can unlock a number of key benefits including

- System-wide visibility from a central platform that’s accessible from anywhere
- Increased collaboration across internal security teams and external vendors
- Real-time access to operational data, including designs, projects, maintenance and auditsEffective planning & budgeting

Buckle up and let the journey begin!

Digital Transformation 101

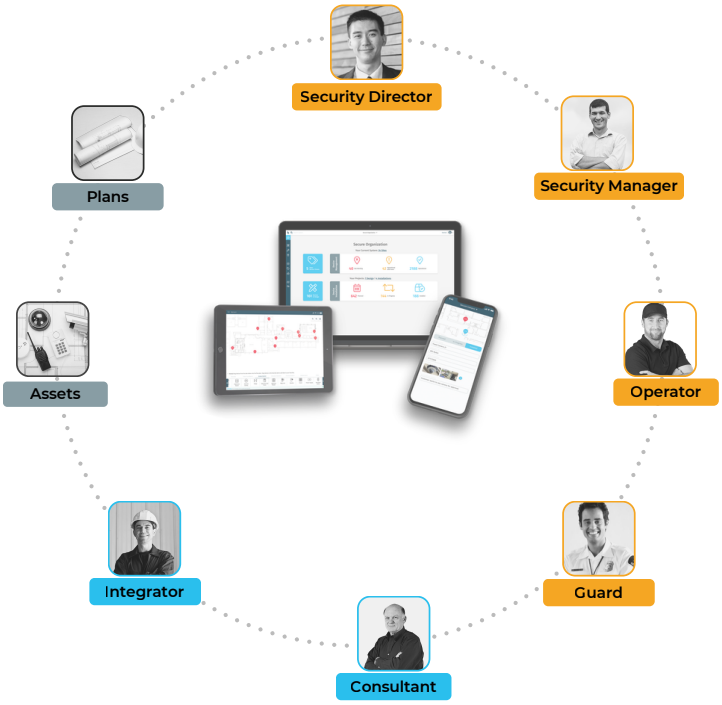
Digital Transformation is the integration of digital technology to change, optimize and streamline how an organization operates and delivers value.

Within the subject of digital transformation, are two terms that are used often; "digitization" and "digitalization".

Digitization is the process of making analog information digital. Digitization is a straightforward process. Every time you turn a piece of paper into a digital format, you digitize it.

Digitalization, on the other hand, is when you move existing processes to digital technologies.

Many physical security teams in the transportation sector still use legacy methods to track and manage their systems. Whether using a notepad to document information or a spreadsheet to manage assets, there are more effective ways to manage a robust security system.



Insight #1

Envisioning the future...

Transportation management in 2030 will look dramatically different than it does today. Advanced technologies will continue to develop and provide greater capabilities for managers to improve operations and reduce costs. In addition, as the marketplace continues to mature, more companies will be using technology to protect and manage their assets.

What to do

Make a list of the top 5 most exciting technology innovations you see coming to the transportation industry in the next 5-7 years. Examples include machine learning, autonomous vehicles, automated freight ship-loading, and offloading.

SiteOwl makes it easy for you to stay ahead of the digital curve by providing solutions that help you manage your physical security systems in the cloud, while bringing security teams, vendors, digital floorplans and security assets together into one platform, effectively digitizing and digitializing your security practice.

Examples of Digital Transformation in Transportation & Logistics

PROCESS TRANSFORMATION

Digital transformation requires that organizations make fundamental changes to how they do things. These changes can be large and systemic but also small and incremental. The best transformation initiatives involve a combination of both approaches. For example, a company that wants to change how it processes orders and payments may use cloud computing to eliminate paper forms and manual paperwork processing

OPERATIONAL TRANSFORMATION

Digital transformation initiatives usually involve a company's operations. For example, a company might decide to digitize all its physical security systems so that the employees can monitor the security of their facilities remotely. In addition, the company would use software to manage the systems instead of visiting the facilities in person.

CULTURAL TRANSFORMATION

Teamwork makes the (digital) dream work. Digital transformation requires an environment of trust and collaboration. It's not a matter of simply handing off the responsibilities to a team of people who will go to work and get things done. A culture of digital transformation requires everyone to have a stake in the outcome and the tools they need to succeed, with multiple moving parts to manage and numerous risks to manage.

Digital Transformation Outlook

Every industry, from banking to retail, is impacted by digitization. But, in some ways, the transportation industry is different because it is central to many other sectors and critical to the global economy.

Providing safe and efficient transportation services depends on the ability to manage complex operations at scale. Increasing technological innovation, urbanization, and the growing expectation of consumers are pressuring transportation companies to prioritize the modernization of their operations.

According to a Forbes Insights report, 65% of logistics, supply chain, and transportation executives recognize the importance of digital transformation and plan to make it a top priority for years to come.

- 87% of business leaders think that digital transformation will disrupt their industry.
- The top benefits of adopting a digital model are it improves operational efficiency (40%), allows for faster time to market (36%), and helps meet customer expectations (35%).
- The Worldwide Digital Transformation Spending in Logistics Industry is Projected to Reach $75.5 Billion by 2026
- 86% of companies believe that cloud technology is critical to digital transformation.

Digitization Challenges in Transportation

Digital technologies and solutions will transform the transportation industry in the coming years, but not all organizations are prepared to take advantage of these new opportunities.

Similar to many industries that the digital economy has disrupted, the transportation sector is experiencing rapid change and evolution. New business models, disruptive technologies, and shifting consumer preferences are all changing the transportation sector. The challenge is harnessing these changes and taking advantage of them to build new, more efficient systems.

Insight #2

Embracing change...

Transportation agencies, companies, and owner-operators that embrace digital solutions can get the most out of their security investments by using digital tools and applications that make their operations more efficient, connected, and responsive.

What to do

Document your current processes to determine where digitizing could increase efficiency and justify implementation. Choosing a single process, such as how you manage security projects or service and installation quality, can help you find a starting point.

Three Barriers to Digitization

1. OUTDATED MODELS

Traditionally, the transportation sector has resisted change mainly due to concerns about safety and the impact of innovation on traditional business models. However, the landscape has changed significantly over the past few years. Digital technologies have become available at low costs and in low quantities. With the advent of 5G networks and the availability of affordable sensors, these technologies can potentially be transformative for the transportation sector.

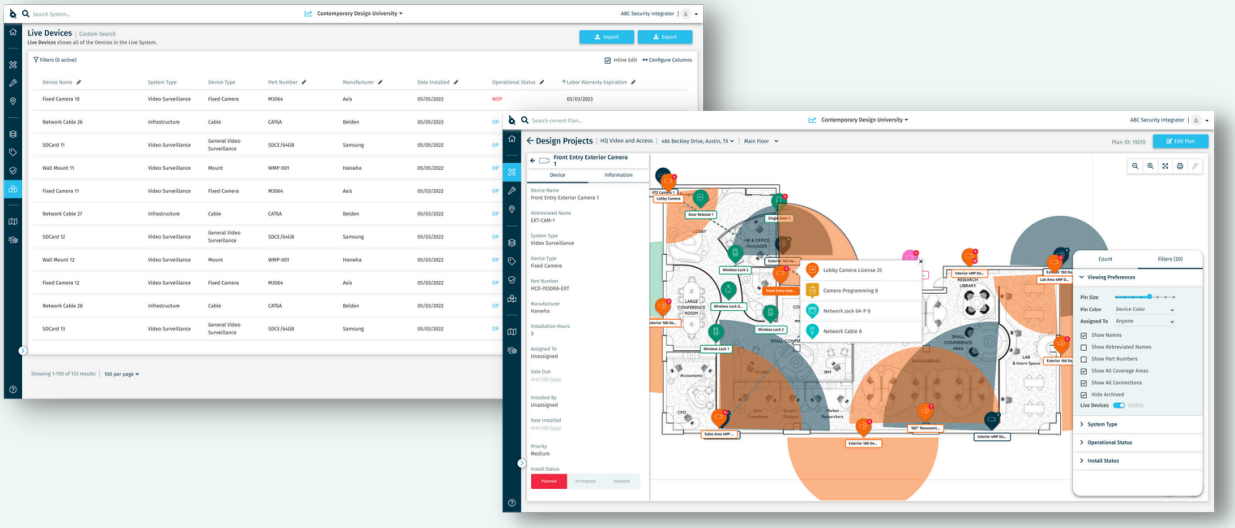
2. LACK OF STANDARDIZED SYSTEM MANAGEMENT PRACTICES

The transportation sector is experiencing a major transition in the way it operates. New and disruptive business models are emerging at a rapid pace, and the lack of standardized system management practices is slowing down much-needed innovation.

3. LACK OF VISIBILITY

It is difficult for stakeholders to track and evaluate the benefits and costs of emerging security technologies in the transportation sector. While the digital environment is primed for IoT implementation, it is challenging to identify the benefits if an organization does not have the ability to make data-driven decisions based on actionable insights.

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.



Getting Started

When it comes to implementing digital solutions in the transportation and logistics sector, a one size fits all approach will not work. Instead, you must determine your organization's unique needs and identify effective ways that don't compromise efficiency or security.

Implementation Challenges

Ironically, most of the challenges companies face in implementing digital solutions are not technical in nature. Rather, they are associated with the culture and philosophy of the company. In other words, the real challenge in implementing digital solutions lies in the company's ability to change "the way things have always been done."

Digital implementations backed by cloud-based platforms have taken the trucking industry to the next level of efficiency and effectiveness. But, implementing digital solutions can be a daunting task for many companies, especially in the case of large organizations.

Companies may be reluctant to change their working methods because it is a complex undertaking.

In order to determine the best digital solution for your company, you must assess the current state of your fleet's digital transformation profile, define a clear vision, get buy-in and the support of leadership.

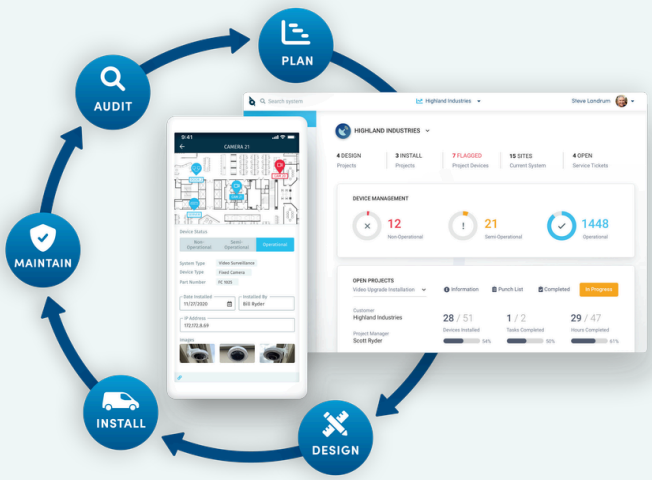
Insight #3

Visibility is critical...

Visibility is critical when it comes to managing security systems and devices. Transportation agencies and organizations must ensure at least a minimum level of visibility across their physical security systems to effectively protect their operations, people and assets.

What to do

Conducting a physical security audit either in-house or with the help of a security professional/integrator can help you identify vulnerabilities in your system and provide a roadmap for effective ways to digitally transform the delivery and management of your security infrastructure.



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.

Three Key Steps to Consider Prior to Digitization

In order to determine the best digital solution for your company, you must assess the current state of your fleet's digital transformation profile, define a clear vision, get buy-in and the support of leadership.

ASSESS YOUR CURRENT STATE

You need to understand the current state of your company's digital transformation profile before you begin implementing a digital transformation strategy. This includes evaluating the strengths and weaknesses of your current security infrastructure and seurity practices.

DEFINE A CLEAR VISION

Before implementing any digital transformation strategy, you must define your company's vision and goals. Your digital transformation strategy should be aligned with the overall business strategy. The concept should be realistic and attainable and guide your company's digital transformation.

OBTAIN BUY-IN AND SUPPORT

Digital transformation is a company-wide endeavor that requires the full support of executives. If your company lacks a digital transformation champion at the top, you may be setting yourself up for failure. Make sure that your executives are actively involved in the digital transformation initiative and understand the benefits of a digital transformation strategy.

Insight #4

Building a business case...

Building a business case for your digital strategy can be challenging, but with the right tools and some planning, it can be done! Get senior management support and buy-in by highlighting digital opportunities that will positively impact operations, mapping the internal stakeholders and the critical factors for success.

What to do

Review a success story on how an organization implemented digital transformation and created a culture of innovation. Take notes and include your thoughts on the organization's challenges and barriers and how they overcame them.

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 existing measures and identify potential gaps.

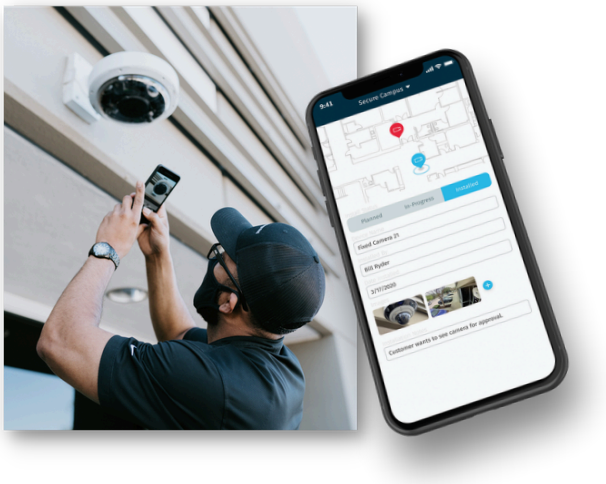
Physical Security Vulnerability Assessment

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 gaps in procedures that should be in place to respond 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.

When considering your physical security risk assessment, it's always best to be proactive vs. reactive. 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.



Insight #5

Physical security planning...

Physical security planning for warehouses, distribution centers, and logistics facilities require three essential components: perimeter fencing, access control, and surveillance.

Perimeter fencing should be strong, uncompromising, and not easily scaled or cut through. Access control must be foolproof, with no way for unauthorized personnel to gain entry.

Finally, once a given facility is secure, surveillance can be either passive or active.

Regardless, it would be best if you had a central platform to manage all security-related information and coordinate all the components that make up a security system.

Keeping Things Scalable

The digital future in transport and logistics will evolve towards digital models that enable a seamless and integrated journey. Any physical product and its digital counterpart will co-exist in the physical and digital space, with real-time information flowing seamlessly between them. This wave of digital innovation will redefine the industry, and change the face of transport and logistics in the coming years. It will also usher in a new era of demand for innovative logistics solutions such as:

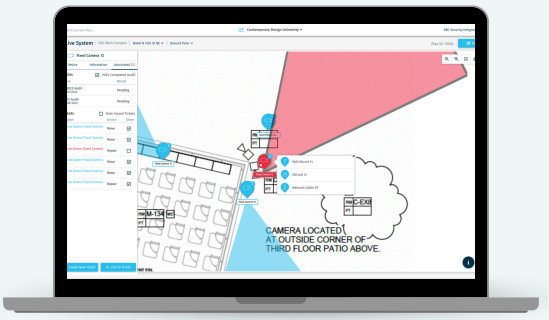
- On-demand warehouse
- Autonomous trucks
- Machine learning optimization
- Predictive maintenance
- And countless other digital innovations!

Several reports, including a 2021 study conducted by IBM, forecast that digitalization will drive the trucking business by 2030. In order for transportation companies to adapt to the changes ahead they will need to leverage technology and make an effort to change the way they operate.

Scalability will be one of the biggest challenges that the trucking industry will face as they make the digital leap. Companies that want to reduce costs and improve efficiency must ensure scalability in all layers of their solution architecture.

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.

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 #6

Scalable physical security implementation...

One of the biggest challenges transportation and logistics leaders face when scaling their systems 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 enabling 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 any time.

Implementing The Right Processes And Systems

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 ensures all aspects of your physical security system are on the same page. It requires developing solutions that can simultaneously deal with outside and internal threats. 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 is far easier to achieve than you think, mainly thanks to lifecycle management platforms that automate systems designed specifically for the security industry.

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

When it comes to digitizing your physical security systems, it makes sense to digitize processes clogged with paper. Document your current maintenance processes to determine where digitizing could increase efficiency and justify implementation.

Digitizing Your Current Systems And Processes

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.

Insight #7

Digital approach...

Choosing 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 processes, such as how you keep track of equipment warranties and maintenance schedules, will help you identify gaps in your current system and allow you to evaluate your options for digitizing it.

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.

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?

These are questions that transportation agencies and operators need to be asking as they plan for the future. After all, the digital transformation of transportation is just getting started.

Data-driven Planning

Picture this: The yearly budget is due, 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?

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 built on previous data that says if a security device is placed at a location, data will be captured of an incident or because the security device is there, the threat is mitigated.

Their data behind that is no different than say the use of analytic data to determine the flow of people. Data can provide detailed budget planning data based on trends and use patterns.Why put a general access card reader on a door no one ever walks through?

Insight #8

Using Data to increase efficiencies...

Incomplete and or inaccurate system information is one of the main obstacles to digital transformation. Data-driven decision-making (DDDM) is the process of using data or facts to inform decisions rather than just relying on intuition, observation, or guesswork.

With SiteOwl, system owners can confidently make data-driven decisions thanks to reliable and accurate insights into the condition of their security devices.

Data can be generated not only for the safety and security of an organization but also to help the other business units understand their struggles.

Data-generating devices, such as security cameras, can be valuable tools to provide information to business units like HR or Marketing. An example would be to institute a stair-walking health plan, participants may receive an award, but HR can leverage a reduction in health insurance premiums because the cameras validated the program.

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.

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

A 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 hour 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

A 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.

Insight #10

Using Data to increase efficiencies...

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

Cloud platforms like SiteOwl allow security leaders and their vendors to track warranty, device history, service tickets, audits and much more.

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? Many 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 glamor, 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.

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 always be to work with a vendor that offers fair and transparent pricing so you understand the true operational costs of managing your system.

Insight #9

Centralizing system information...

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!

Quantifying the ROI of 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? Quantify is to provide a numerical value to the ROI, with zero incidents at the least amount of spend being the perfect ROI. Let's look at a couple of ways here.

Formula

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.

Conclusion

The transportation industry is experiencing major changes driven by technology and information.

Physical security has always been a concern, but now the focus is shifting from securing physical assets to securing data, but the security paradigm remains the same. The challenge is how to secure data while maintaining business operations and the ability to adapt to an ever-changing landscape of threats.

Transportation security leaders face multiple challenges today. In addition to the many physical threats, transportation and logistics sites face increased criminal activity, theft, and loss.

As a transportation security leader, your job is to keep your business operating and ensure the safety of your people and your assets. 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 time has come for the physical security industry to embrace digital transformation.

The transportation 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.

Request a demo today!

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

siteowl®