OPERATIONAL **SECURITY** TECHNOLOGY

Principles, Challenges and How to Achieve Mission-Critical Outcomes Leveraging OST

SIA
SECURITY INDUSTRY ASSOCIATION

ALLEGION™ M.C. DEAN BUILDING INTELLIGENCE ONVIF® wesco

About the Authors

John Deskurakis currently leads security at Daikin Applied Americas, where he serves as chief information security officer (CISO) and deputy chief information officer (deputy CIO). His mission is to transform all elements of security into an integrated and frictionless model that can accelerate business capabilities and ensure resilience. Deskurakis was previously a chief security officer for multiple global conglomerate technology manufacturers, such as Carrier and Johnson Controls, where he directly supported a wide range of multinational businesses and subsidiaries, including LenelS2, Edwards, Kidde, Tyco, Software House, Exacq, Illustra, American Dynamics, Simplex, Grinnell and more. Prior to that, he led secure research and development efforts bolstering a range of complex defense programs at Raytheon. Deskurakis has also served as a managing partner at CybrDesk, a security technology provider and consultancy. He is an expert on a range of security topics, with considerable focus on IT, operational technology and security technologies.

With multiple degrees, including a Master of Science in cybersecurity from the Johns Hopkins University Whiting School of Engineering, a Bachelor of Science in computer science and a Bachelor of Science in information systems from the University of South Florida, he is active in his community and academia and trade organizations. Deskurakis has served as the board chair of Security Industry Association's Cybersecurity Advisory Board, a board member of the International Society of Automation (ISA) Global Cybersecurity Alliance, a board member of the ISA Security Compliance Institute, a board member of the Real Estate Cybersecurity Consortium and a technical panelist for the UL-2900-1 Standard for Software Cybersecurity for Network-Connectable Products.

Chris Lynch is a software engineer and security architect, specializing in system integration and design for security strategies in operational technologies and industrial control systems. His focus is currently the application of proactive strategies to design and deliver complex operational technologies within industrial manufacturing. A graduate of the University of South Florida, with a degree in cybersecurity, Lynch is an avid fisherman, system developer, security researcher, technology enthusiast and contributor to technology publications.

Table of Contents

Appendices & References

PRODUCED WITH GENEROUS SUPPORT FROM

ALLEGION
M.C. DEAN BUILDING INTELLIGENCE
ONVIF®
wesco

SIA extends its appreciation to the leadership and employees of Allegion, M.C. Dean, ONVIF and Wesco for their underwriting of this report and their service and guidance as part of the steering committee of this report.

Abstract

It is unlikely controversial to suggest that most businesses are considerably dependent upon technology to negligibly function. We look to technological methods to build foundations and improve our delivery. The capabilities provided by these means can create an edge or help achieve competitive advantages. And while reliance upon mechanization and automation has become a common approach to improve effectiveness, achieve consistency, deliver value and scale operational efficiency, results tend to vary wildly. When it comes to selecting, integrating, implementing and maturing the technologies that are intended to operationalize and maintain our core business functions, most organizations are fundamentally unequal.

In the security industry, achieving excellence within our operational technical stack is an important objective to help ensure mission success. We tend to deploy and rely upon some unique systems to do the job of security. There can be considerable challenges that are often misunderstood or overlooked when it comes to our security software and hardware. These tools can help us succeed but can also ensure we fail. Deeper understanding of these technologies can ensure greater situational awareness and mitigate the probability of common mistakes and gaps.

In an increasingly complex operational space where threats are continually evolving, it is easy to become enthusiastic about the promise of advanced and emerging security technologies. But that sort of zeal must be tempered by the reality that there is more opportunity for miscues, missteps and malfunctions than there are for simple plug-and-play happy-path advancements. Clear understanding of the principles, challenges and purpose-built solutions will better ensure achieving mission-critical outcomes while leveraging operational security technologies to defend and provide seamless continuity for your business.

In this paper, we will explore some of the prominent operational security technology (OST) types and their corresponding challenges and discuss strategies to better ensure optimal delivery and best operational practices. The discussion and topics covered are most relevant to the security industry professional, as well as the security industry technology consumer within the small to medium-sized business range.

Bearing

Global market demand for operational technology (OT) has evolved substantially in recent years. With a projected compound annual growth rate (CAGR) of 10% from 2024 to 2030, this market trend is expected to continue for years to come.[1] Some of the key drivers for the momentum are predictable but worth pointing out. While businesses value efficiency improvements and attempt to lower operational costs, the complexity of systems, customer demands and competitive requirements are evolving.[2] These realities, coupled with the rapid adoption of new and emerging technologies like artificial intelligence (AI) and machine learning, are driving a wave of modernization.[2] Although on-premises versions of OT systems tend to be most common, the demand for alternative cloud-based solutions is growing significantly because they can lower physical barriers and provide greater flexibility and scalability.[1] One of the larger vertical segments of the OT market is the building management system (BMS) space, and this is germane to the security industry. Over the next five years, OT market growth within the BMS segment is projected to be the fastest growing, with a CAGR of 15.2%.[1]

Security industry professionals are accustomed to the notion of having to protect places, people and important resources, such as certain types of OT. And in this respect, there is a general familiarity within the industry when we envision a range of OT types, especially those considered to be part of critical infrastructure. OT components can also be a vital focus of many security plans and sometimes are even thought to be the very crown jewels of a business.

The convergence OT and information technology (IT) has been a popular topic of conversation in recent years. But what sometimes gets overlooked is the relation of both to physical security. A comprehensive security strategy depends greatly upon collaboration from various stakeholders, and technical alignment and integration in certain key domains.[3] IT, OT and (physical and cyber) security capabilities, for example, should synergize. In practice, however, while physical access to many of the technologies connecting devices within a typical business environment are usually under the purview of physical security, the three domains rarely understand each other.[3]

There is yet another angle. The outcomes and outputs provided by many OT elements are rather important to the day-to-day objectives of security personnel. While it may not seem obvious, the average OT ecosystem can significantly impact the considerable responsibilities of the security mission. Not only are our security tools and technologies of the trade connected to and reliant upon OT devices, but some of the security software and hardware we utilize daily can be considered operational technology in its own right. The OT coin is indeed two-sided in security. An understanding of some of the principles and challenges related to the types of OT we rely upon daily as security professionals can make a significant difference when we are faced with increasing complexity and evolving threats. Coupled with zero-failure expectations while ensuring mission-critical outcomes, OT is significantly important to the security industry.

1 Operational Technology Market Trends. Accessed on: Oct. 26, 2024. [Online]. Available: https://www.grandviewresearch.com/industry-analysis/operational-technology-market-report (Grand View Research, 2024)
2 Operational Technology Market Size and Forecast. Accessed on: Oct. 26, 2024. [Online]. Available: https://www.verifiedmarketresearch.com/product/operational-technology-market (Verified Market Research, 2024)
3 7 Steps to Align IT, OT and Physical Security. Accessed on: Oct. 26, 2024. [Online]. Available: https://www.iansresearch.com/resources/all-blogs/post/security-blog/2022/11/29/7-steps-to-align-it-ot-and-physical-security. (IANS 2022)

Simplification

To begin to understand a thing, we must start by specifying what we are talking about. Defining what operational technology is, does and is not can be a challenge. It will often become the source of enthusiastic debate, especially among technical operators from different industries, disciplines and domains. It is important, at a minimum, to agree about some of the foundational concepts and definitions before diving into any technical discussion. But how do we get there?

If we carefully consider the root cause of these types of polite disagreements, we may quickly realize that OT tends to exist at convergence points and will often intersect an array of assorted utilitarian needs, requirements and functions. And at these intersections, context, purpose and details will often vary. Therefore, human interpretation will be influenced by a diversity of detached experiences and resultant points of view. Definitions will naturally become divergent.

This is an important consideration because although we ubiquitously hear the term "operational technology" and know it plays a large role in our daily lives, we don't often recognize our individualized way of thinking about it. This common lack of self-awareness of thought may be the source of the friction we experience when we realize we are not aligned with our colleagues on the basics of concepts and definitions within OT discussions and other topics like it. How then do we synergize our foundations so that we may focus upon exploration and identification of the challenges and opportunities that will lead us to greater outcomes? Quite simply, we agree on scope, and we purpose-fit a definition so we may build healthy discussions accordingly.

If we begin by sourcing general definitions of OT, we will find that it is often thought about as purely industrial in context. For example, Cisco says that "OT is for connecting, monitoring, managing, and securing an organization's industrial operations. Businesses engaged in activities such as manufacturing, mining, oil and gas, utilities, and transportation, among many others, rely heavily on OT."[4] While that is true, there are other points of view and other "true" definitions.

Some will say OT is specifically hardware. But others would debate that. For example, Gartner suggests OT is "hardware and software that detects or causes a change, through the direct monitoring and/or control of industrial equipment, assets, processes and events."[5] This also seems true, but is a broader interpretation and may not translate exactly to Cisco's. Then again, maybe it does. Define "industrial equipment." Everything is perspective dependent, of course.

RedHat says that while "OT systems are primarily used to interact with the physical world, IT systems are primarily used to solve business problems for end users."[6] Although the first part of the sentence arguably captures the essence of what virtually any OT does, the second part can probably be disputed given some additional context. For example, industrial control systems such as programmable logic controllers also solve business problems, enable automation and provide value for end users. They also happen to be capable of interaction with the physical world. They are industrial controllers. This definition can be confusing and would require an indisputable definition of "business problem." What is clear is that opinions vary. And while some would argue all three mean the same thing, others

4 How Do OT and IT Differ? Accessed on: Oct. 27, 2024. [Online]. Available: https://www.cisco.com/c/en/us/solutions/internet-of-things/what-is-ot-vs-it.html (Cisco)
5 Operational Technology (OT). Accessed on: Oct. 27, 2024. [Online]. Available: https://www.gartner.com/en/information-technology/glossary/operational-technology-ot (Gartner)
6 What is operational technology? Accessed on: Oct. 27, 2024. [Online]. Available: https://www.redhat.com/en/topics/edge-computing/what-is-ot (Red Hat, 2022)

would not. All points of view provide value when we begin to focus on the problem statements and solutions related to OT.

Although defining OT can be subjective, conditional and even context dependent, the conditions that drive relative understanding are typically connected to our own unique industry, practices, needs and/or intended usage. The various points of view that sometimes form divergent definitions also can drift together to form a solid basis of understanding and a generalized view of OT. With careful consideration, we may realize that most of the seemingly conflicting definitions are all correct, given the proper context. Divergent opinions should therefore all be treated as valuable inputs to a greater understanding.

For the purposes of this discussion, it is not necessary to define what OT means to everyone, any situation and every application. The full array of OT topics would be too broad and largely unrelatable to our respective security mission. What is essential is narrowing scope so we may develop some specificity within our problem space.

We should therefore start by reminding ourselves that we operate within a specific horizontal industry – and that is security. Considering our unique focus and responsibilities, it would be wise to limit our range of discussion by thinking about OT as it relates to us. Moreover, rather than thinking about OT in the context of what we might protect, we should apply a little pragmatism in our temperament by focusing on the technologies that help us operate as security professionals. What is our version of OT? Is there security OT? Refining the field in this way helps us better ensure precision, relatability and a robust conversation. It is also practical!

With that in mind, we will develop a definition for operational security technology. Consider it a subset of OT, with many of the same qualities to ensure relative operational success within our distinctive field. We will define OST as the underlying technical elements that enable us to do our work as security professionals. It's not necessarily industrial machinery, but it can be. OST are the technologies that help us scale, automate and ensure successful security outcomes. All are leveraged to support and deliver the principal mission of physical security. OST are therefore technologies that, in some way, connect us with the physical world we are attempting to protect and help manage security problems.

Recall our discussion of subjectivity. Within our narrowed scope, we might slightly adjust some of the prevailing definitions of OT previously reviewed, flavored with security. We could imagine Cisco might now say "OST is for connecting, monitoring, managing and delivering an organization's security operations." Perhaps Gartner says, "OST is hardware and software that detects or causes a change through the direct monitoring and/or control of security equipment, assets, processes and/or events." RedHat may tell us that "OST systems are primarily used to interact with the security perimeter and primarily used to solve security problems for end users."

It is interesting to note that when we limit our scope and infuse some domain-specific context, suddenly the somewhat different sounding points of view and varied definitions start to find convergence and alignment. Applying our own industry-specific conditionals, we forge ahead.

Magnification

The actual complexity of our refined scope should not be underestimated. There are many types of OST that may be connected, integrated and automated in different ways within the security world. These systems are relied upon to help ensure specific physical and operational security requirements. They are leveraged to solve important business and end-user problems. OST are counted on to help us achieve mission-critical outcomes. Technologies like physical access control systems (PACS), surveillance systems, detection devices, perimeter and environmental controls, and security management solutions, among others, can help to ensure our duties as security professionals are easier to support and delivered in a consistent and thorough manner.

However, for as many problems as OST can manage, mitigate and solve, they may also be replete with complexity and pitfalls that can introduce distractions and white noise and even detract from the value they are intended to provide. Complex OST solutions can deliver many benefits but are not always simple to field and maintain. Implementation, integration and ongoing life cycle maintenance is not so simple in many cases and must be planned for and handled judiciously. Without proactivity, a deep understanding of the problem statements, domain expertise and a systemic strategy, OST synthesis and coordination can become the fulltime focus, supplanting our customary "day job" within security operations. The interruptions alone can become detrimental to the core mission and impact the very security posture OST are intended to enhance.

What is worse, many technology-related disruptions only surface after we realize we have not selected the right OST to fit our unique needs. Requirements can be illusive. Technology selection can be hit and miss and costly when imprudent choices are made. Given we have planned well and made wise OST selection decisions, simple integration defects can cause security gaps and synchronization failures between physical and digital security elements. These misses can result in vulnerabilities and inconsistent

outcomes. When multiple complex technologies that had been designed by different original equipment manufacturers (OEMs) are sewn together to create integrated capabilities within a mesh security stack, stakeholders tend to blindly expect the new unified system will inherently perform well. We take for granted it will connect users to more information and ensure better results. But reality tends to be different. Almost half of PACS administrators in a recent survey reported that improving user convenience is difficult, while about a quarter of respondents stated that one of their top three challenges was integrating their security systems with other enterprise systems.[7] This is relational.

OST must operate within a larger ecosystem of technologies that are not necessarily part of the security mission. Most elements, OST or otherwise, have not usually been designed to work together and are not even commonly architected in the same era. Modern technologies are regularly connected to legacy components with a range of incongruent performance capabilities, resource requirements and divergent limitations. When we begin connecting these dissimilar systems, the hope of consistent outcomes and clean interoperability is frequently presumed but rarely realistic without considerable technical domain knowledge, planning and effort. Sometimes, one or more subsystems just will not work with the rest. Unfortunately, assuming the worst outcome of interoperability is the more prudent presumption.

When we consider integration, we must also keep interoperability in mind. Connecting systems together is complicated enough, but now we must think one level deeper and contemplate the prospect of these systems exchanging information and then doing something of value with that data. We must also ensure that separate systems in the same environment can operate as designed in concurrency without impacting one another. Understanding what will happen upstream and downstream is opaque. Interoperability issues and incompatibility between systems intended to function as a unified supersystem can result in inefficiencies, security gaps and decreased oversight. This can cost stakeholders a lot of wasted time and money.

Consider the possible direct impacts of interoperability failures on the security mission. If your various systems don't easily integrate, it may also be worth exploring whether a smart facility management platform could reduce interoperability barriers and provide a more robust security posture. Reduced automation and mechanization will typically result in increased manual activities and stretched human workloads.[8] Overstrained security operators are more prone to making mistakes or failing to identify security gaps.[9] Disparate systems tend to be characterized by data silos, which can cause delays, misunderstandings, reduced response times or failure to identify threats.[10]

Let us consider for a moment video system integration. According to Leo Levit, chairman of the Open Network Video Interface Forum (ONVIF), "if systems connect but can't share and use data properly, it leads to problems like inefficiency or security risk. ONVIF protocols help disparate components to work together more smoothly, preventing data problems that cause delays and missed threats. The cost of interoperability failure isn't just financial — when automation fails it directly impacts the human operators who become overburdened by manual processes. ONVIF's commitment to standardization addresses both the technical and operational aspects of this challenge."

7 Physical access control: Survey reveals new deployment trends, L. Merredew. Accessed on: Nov. 2, 2024. [Online]. Available: https://www.securitymagazine.com/articles/98710-physical-access-control-survey-reveals-new-deployment-trends. (Security Magazine, 2022)
8 How outdated automation leads to more manual effort — and what you can do about it, N. Kinson. Accessed on: Nov. 3, 2024. [Online]. Available: https://www.redwood.com/article/how-outdated-automation-leads-to-more-manual-effort-and-what-you-can-do-about-it (Redwood, 2022)
9 Why Overworked Employees Are Security Risks, D. Kelley. Accessed on: Nov. 3, 2024. [Online]. Available: https://securityintelligence.com/security-risk-staffing-it-teams-overworked-employees (Security Intelligence, 2014)
10 Safety and Security Systems Interoperability, Pkimluker. Accessed on: Nov. 9, 2024. [Online]. Available: https://www.clr2wrk.com/safety-and-security-systems-interoperability (Clear 2 Work, 2022)

Many other challenges must be considered before introducing new OST solutions, including operational constraints, ease of use, regulatory requirements and logistical demands, as well as efficiency and scalability concerns. There are user requirements, business models and delivery obligations that may not align well with the technical solutions being delivered into our environment. To further complicate matters, one's technology OEM may be in the process of modernizing systems you leverage in a way that could become disruptive for your environment.

Perhaps, for example, the OEM of your PACS solution is transforming the locally hosted on-premises software you know and love to a new cloud-based SaaS offering. It may sound wonderful, more modern, universally accessible and scalable, but it may also be incongruent to your environment and the realities of local support capabilities. The new advancement may just be difficult or even impossible for current staff to manage. If you are working with a technology dealer or integrator, do not assume they will be maintaining your cloud instances the offering requires. Be aware, system and functional requirements are not always made crystal clear.

Emerging technologies are not always well aligned to the rest of the security stack and building technology ecosystem where your OST lives. New innovations may present new risks and pitfalls that we aren't yet ready to manage or aware of. It is crucial to understand all aspects of the OST you will rely upon. From selection to integration, implementation, maintenance, upgrades, cutovers and lifecycle support, all facets must match your own needs and capabilities.

A great many things can go wrong. Start with a strategy that includes prudent consideration of business essentials and outcomes. Plan for continual evaluation, analysis and testing. While some of the most obvious and complicated core challenges related to OST can be found under the hood and within the realm of integration, interoperability and performance, there are other pitfalls that may not be as predictable. Strategic vendor partnerships and trusted domain expertise are a must.

Identification

Setting aside for a moment the bigger picture of ecosystem realities and operational challenges, we move into the T portion of OST as our next click down. We focus now upon the technology elements that enable operations in the security world. Despite our circumscribed scope of discussion, a wide range of component types, systems and subsystems must be considered when we think about OST. If we limit ourselves only to the basics that must connect and operate well within a unified security ecosystem, such as PACS, BMS, surveillance and monitoring components, sensors, alarms, fire and safety equipment, cyber tools, IT systems and cloud-based systems, we may begin to appreciate mastering all is not a simple prospect. These assorted OST elements are not simple and tend to require differentiated support. Security system components tend not to be elementary plug-and-play technologies. They are not always compatible with each other. Professional support is often required and always recommended.

To better conceptualize the scale and scope of the OST space, it is helpful to develop a broad-based visual, outlining some of the key types of technologies. While this is certainly not an exhaustive compilation of all OST, it provides an understanding of the wide range of different system elements one is likely to encounter within the common security stack. There is much to think about when we start digging into OST. We will define and clarify the major category types presented below. As we dive deeper into some of the component elements within the five columns of Table 1 – Common Operational Security Technology, our goal is to develop a better general understanding or challenges in order to illuminate best practices, strategy and planning.

Table 1 – Common Operational Security Technology (OST), by Category

Physical Access Control Systems (PACS)	Surveillance Systems	Detection Systems (Alarms & Sensors)	Perimeter & Environmental Security	Security Management
Keycard systems	Closed Circuit TV	Anomalous Pattern Detection	Building Mgmt. Systems (BMS)	Physical Security Operations Center
Biometric systems	IR Cameras	Smart Alarms	Power and Comms Backup Systems	Remote Monitoring
PIN Code Access	Pan-Tilt-Zoom Cameras	Radar and LiDAR	Barriers and Bollards	Video Analytics Technology
Identity & Access Management (IAM)	Thermal Imaging Cameras	Geofencing Technology	Fencing Solutions	Incident Reporting Systems
Multi-Factor Authentication (MFA)	Body Cameras	Seismic Sensors	Barbed and Razor Wire	Mass Notification Systems
Interlocking Doors	Pattern Recognition Technology	Panic Devices	Gate Technologies	Guard Tower Systems
Turnstile Systems	Facial Recognition Cameras	Smoke & Gas Detectors	Vehicle Access Control	Communication Devices
Smart Locks	Motion Activated Cameras	Water, Temp, Heat & Humidity Detectors	Turnstiles	PA Systems
Mobile Access Control Systems	License Plate Recognition Systems	Motion, Vibration and Tamper Sensors	Mantraps and Security Vestibules	Fire Detection and Suppression Systems
Security Gates	Remote Video Monitoring Systems	Acoustic Monitoring	Security Booths	Emergency Exit Systems
Visitor Management Systems	Cloud Surveillance and Storage Systems	Drone Detection Systems	Lighting, Signage and Physical Deterrents	Integrated Security Platforms
RFID Tags	Video Analytics	Magnetic Sensors	Storm Shutters and Resistant Windows	Internet of Things (IoT) Security Devices
Credential Management SW	Network Video Recorders	Glass Break and Pressure Sensors	Drainage and Flood Barriers	Cybersecurity Capabilities
Identity Recognition Systems	Drones and Robots	Microwave Field Detectors	Containment Systems	GPS Tracking

Physical Access Control Systems (PACS)

When discussing OST, it is almost inevitable to start with PACS at the forefront of the conversation. It is after all, the front line of most organizational physical defenses. These systems generally serve as the protective gateway, defending valued assets and providing authorized admission. They ensure only sanctioned parties have access to critical resources. To clarify, a PACS is an electronic or digital system that grants physical access to authorized individuals by confirming identities, leveraging key cards, mobile credentials, biometrics and other factors of authentication.[11] Table 2 provides a great overview of some of the major components found within the common PACS deployment.

While card-based access control systems tend to be one of the most common types of PACS solutions utilized by organizations today, modern security strategies are evolving and the complexity is growing.[12] For example, in many operations physical security and cybersecurity strategies are converging, resulting in PACS more regularly becoming integrated with the logical access control systems (LACS).[13] LACS are customarily leveraged to manage and standardize user access to computer networks, systems and data. And there is a utilitarian motivation for this. Simply put, much of the data available within either system is useful to both. So why not share?

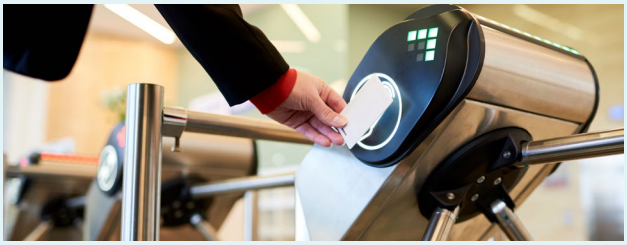
Table 2 – Common PACS Components

Component	Description
Access point	Entrance point or physical barrier where an individual interacts with the PACS. For example, access points include turnstiles, gates and locking doors.
Credential reader and keypad	The reader provides power to and reads data from a physical credential. It also sends this data to a control panel to authenticate the credential and request access authorization. Depending on the facility's unique policies, individuals may need to enter a PIN into the keypad or a biometric.
Biometric reader	Captures biometric data (such as the fingerprint, facial image or iris scan) and verifies it against the known or stored credential biometric data.
Control panel	Receives the credential data the reader sends and verifies its presence in the credential holder data repository. It then makes an access decision and transmits authorization data to the access control server and access point.
Access control server	Grants authorization to individuals requesting access (for example, presenting an access card credential to a reader). It also registers and enrolls individuals, enrolls and validates credentials and logs system events.
Credential holder data repository	Contains individual identity data and physical access privileges. Control panels use this authoritative data to validate credential data.
Auxiliary Systems	Organizations may integrate the PACS with additional facility monitoring systems, such as surveillance, fire alarm and evacuation systems.

Source: http://www.idmanagement.gov/university/pacs

11 Physical Access Control Systems 101. Accessed on: Jan. 22. 2025. [Online]. Available: https://www.idmanagement.gov/university/pacs/ (Oidmanagement.gov, 2023)
12 10 Types of physical access control systems, OLOID Desk. Accessed on: Jan. 22. 2025. [Online]. Available: https://www.oloid.ai/blog/10-types-of-physical-access-control-system (Oloid, 2023)
13 Integration of IAM with Physical Access Control Systems, D. Simmons. Accessed on: Jan. 22. 2025. [Online]. Available: https://techvisionresearch.com/wp-content/uploads/2020/03/PACS-LACS-20200310-excerpt-final.pd (TechVision Research, 2020)

LACS tend to be more commonly associated with IT-centric identity and access management (IAM) deployments. But in a converging world, more systems will be integrated across increasingly blurred lines of technology silos. According to Gartner, "security and IAM leaders will take an increasing role in selecting, implementing and operating new PACS technologies."[14] IT, OT and operational convergence creates efficiencies.



Physical Access Control Systems

- Keycard Systems
- Biometric Systems
- PIN Code Access
- Identity and Access Management
- Multifactor Authentication
- Interlocking Doors
- Turnstile Systems
- Smart Locks
- Mobile Access Control Systems
- Security Gates
- Visitor Management Systems
- RFID Tags
- Credential Management SW
- Identity Recognition Systems

The world is changing. But what about organizations that lack extensive security teams, and the array of functional leaders who Gartner tells us are now starting to work together? Small and medium-sized businesses (SMBs), for example, tend to rely upon limited internal resources, augmented by vendor partner relationships to ensure the security mission is well supported. In these cases, complexity can actually increase. Standard approaches designed for large corporations will miss the mark for SMBs. This is where a deep understanding of one's own unique needs and requirements and the right alliances become crucial.

For the SMB leader, the following will outline a starting point thought experiment (using PACS as the case study) to begin exploration and help avoid common pitfalls. Finding the right path for individual success varies.

1. **Meat and potatoes.** Seek the solutions and technologies that best fit your specific needs. Emerging technologies and fad solutions are not always suitable. Simple requirements can be managed simply. Build a solid foundation of the basics, and fine tune from there. Build to suit, aligning to your prioritized needs and operating model. Be able to answer this question, "What problem(s) am I trying to solve?" Then identify the solution.
2. **Cloudy forecast.** OEMs are increasingly introducing cloud-based PACS solutions with the intent of marketing scalability advantages and presenting a do-it-yourself alternative to SMBs. While these options may be right for you, there are questions:
    a. **Cost –** Hosting technology in the cloud is not always as inexpensive as it may seem. There can be savings, sure. But are there hidden operational, support and domain expertise expenses? Determine the total cost of ownership (TCO) early.
    b. **Expertise** – Most SMBs lack the personnel required to implement, integrate and support cloud hosted systems in perpetuity. It is never as simple as advertised. Ensure you are situationally aware of what it takes to play in this space.
    c. **Compliance and Security** – Protecting hosted data isn't a given, and your cloud vendor is only responsible to a point. As the instance owner, you will maintain many security responsibilities independently.

14 Technology Insight for Physical Access Control Systems. Accessed on: Jan. 22. 2025. [Online]. Available: https://www.gartner.com/en/documents/3451120 (Gartner, 2016)

Ensuring compliance with industry-specific regulations related to data will be an added layer of required complexity.

d. **Performance** – Maintaining high performance after cloud migration is not always seamless and simple. Much will depend upon your unique system constraints, user and support requirements and needs of your business.

e. **Vendor Lock-In** – Once you become reliant upon a cloud provider, it can become difficult or expensive to migrate away or make substantive changes. Make sure you understand what an exit plan might look like, just in case.

f. **Future-Proofing** – when implementing cloud-based solutions, SMBs should ensure scalability and growth considerations. For example, can network infrastructure handle the likelihood of increased traffic of tomorrow?

3. **If it sounds too good to be true...** Before assuming a PACS solution is as simple as DIY, make sure you know what you are getting into. Even if you are seeking third party support, do some homework independently. Consider many of the challenges outlined within this document, review the resources provided in the appendices, and always consult with a trusted professional or vendor partner.

4. **Preparation.** Whether working with a trusted integration partner, attempting to update or introducing new PACS in a DIY fashion, there are some key planning actions that should be considered. The following preparatory advice is based upon guidance from idmanagement.gov and has been refined for our purposes and scope of discussion.[11]

a. Identify your stakeholders at the beginning and designate a PACS project leader.

b. Designate staff to fill key roles where possible. As needed, leverage trusted partners to serve as architects, engineers, integrators, testers and operators.

c. Engage technology and security domain experts early. CISOs and CIOs are your friend. Call them in.

d. Require the creation, maintenance and availability of an integrated master schedule for the life of your project. This document should include project phases, tasks, resources and dependencies. Responsible parties should be designated.

e. Establish a PACS life cycle management plan to help estimate hardware and software upgrades over the systems operational life cycle. Think TCO.

f. Build the cost of software licensing and system sustainment into your project budget. Identify all related system upkeep costs as an annualized TCO.

g. Work with site or facility technicians and engineers to identify constraints specific to your target space. These constraints may be a limiting factor in tech selection.

h. Plan standardized site-specific deployment strategies.

i. Remember that legacy system elements, such as credential readers, may not support new modes of operation required for compliance standards.

j. Use legacy credentials and non-compliant modes of operation only in

a migration strategy, not as the end state. Final state plans must standardize on compliance.

k. Retire and phase out secondary, legacy credentials.

l. Use your organization's LACS-based identity management system as the authoritative source for all user records in the PACS, if possible.

m. Some PACS allows the assignment of user access levels at the time of credential registration. Plan the method of assignment before provisioning/registration.

n. Use a risk-based approach when selecting appropriate authentication mechanisms for physical access to buildings and facilities.

o. Remember that access points should not rely solely on an authentication mechanism that requires optional card features. These features might not be available on all user-population cards.

p. Design and configure PACS to meet the target environment's needs. For example, do not require multifactor authentication (MFA) when only one factor is needed.

q. PKI is the foundation for high-assurance PACS implementations. Plan for it.

r. There is always more. Consult a professional and continually seek improvement.

5. **Operationalizing OST**. The job doesn't end after you have proactively planned for a new system implementation and successfully integrated and deployed. Operationalizing your PACS OST is another task that requires a great deal of consideration. The following advice is based upon guidance provided by idmanagement.gov and has been refined for our purposes and scope of discussion.[11]

a. Mission success requires people, process and tools. Now that you have the tools, make sure the right people and purpose-built processes are in place. Ensure your approach fits your business needs and is robust and continually improving.

b. Things will go wrong. Define clear processes and procedures for resolving business and user requirements, as well as system bugs and incidents. For example, defective credential readers may surface. An employee's access card may be lost or become inoperable. Have plans to solve inevitable problems.

c. Be sure to identify key support personnel and expected levels of support.

d. Perform regular system maintenance and patching of the PACS components.

e. Establish clear procedures for testing upgrades before widespread deployment. Develop roll-back procedures whenever upgrading or moving to new versions.

f. Ensure PACS is configured and maintained to operate in compliant states. Regularly review compliance, policy and governance requirements.

g. Work with your IT and cybersecurity professionals to ensure PACS is regularly patched, updated, secure and operating efficiently.

h. Ensure an appropriate identity and access management plan is in place, maintained and reviewed regularly. Make sure system identities are managed in accordance with industry standards and business requirements.

i. Remove all personally identifiable information from PACS endpoints to protect privacy.

j. Audit system functionality regularly. For example, verify that access points are challenging the correct number and type of authentication factors. Consider using test credentials that have expired or been revoked to ensure correct operation.

The fundamental takeaway is quite simple: While PACS solutions may seem simple on the surface, they are far from it. Did we say this was simple? PACS connect to many things, from the front door of a building to elevators and critical company resources. Getting these systems stood up and working well can be an arduous journey. There is an array of obstacles that exist within many stovepipes. Knowing them well will help ensure operational success.

The preparation and operational guidance provided in this section can be generalized and retrofitted to almost any OST deployment. The key lesson to understand is any successful OST implementation requires this level of strategic thinking. PACS is a great example for this exercise because it is so ubiquitously found within the average security stack. For your PACS, always expect to need to solve for complicated problems, and be well prepared within areas such as technology selection, integration, interoperability, identity management, credential and access management, cybersecurity, performance, reliability, scalability, regulatory compliance, user training and, of course, cost. But wait, there's more! Our best practices guidance provided within Appendix B offers a starting point for strategic thinking as well as technology acquisition planning. As always, it's wise to consult with a trusted security industry professional, such as a technology dealer, distributor and/or integrator. Develop a great supply chain and use it.

Surveillance Systems

Surveillance Systems

- Video Security Systems
- IR Cameras
- Pan-Tilt-Zoom Cameras
- Thermal Imaging Cameras
- Body Cameras
- Pattern Recognition Technology
- Facial Recognition Cameras
- Motion Activated Cameras
- License Plate Recognition Systems
- Remote Video Monitoring Systems
- Cloud Surveillance and Storage Systems
- Video Analytics
- Network Video Recorders
- Drones and Robots

Surveillance systems are an indispensable resource for monitoring and identifying potential threats. Enabling an organization to observe, deter, and react to potential problems in real time by utilizing technologies such as purpose-fit cameras, network video recording systems or remote monitoring is fundamental. Having eyes in the sky is an obvious proactive step in the process of maturing a physical security posture. Moreover, technology is maturing and evolving, so much so that we're starting to observe robots and drones more commonly as part of the surveillance footprint.[15]

When implementation of surveillance systems is discussed, video storage must also be part of the conversation. Short-term and archival storage of video data is usually a required element of the system, and big data storage can present some

15 Domestic Drones. Accessed on: Jan. 22. 2025. [Online]. Available: https://www.aclu.org/issues/privacy-technology/surveillance-technologies/domestic-drones (ACLU, 2025)

challenges.[16] There may be compatibility and accessibility issues whenever we talk about data. Beyond concerns connected to large volumes of data, we must also consider compliance requirements, such as privacy, and reliability problems, such as power and network connectivity.

Let us not forget that any time the data topic surfaces, so too will security's first cousin, cybersecurity. That network we were just evaluating for dependability will now need another set of eyes performing analysis and testing. Available and operational are not the same things as secure.

Having data and usability of data are not the same thing either. Quick and reliable access to historic footage is crucial, both for investigative and forensic needs. Role-based access to video data, pattern identification and occasional evidence sourcing for legal and compliance purposes allows organizations to have eyes on their entire facility and future viability. Never assume your valuable surveillance data has been operationalized and is already providing value to your business. Implementing the right system to match your needs and deliver value is not so simple, but certainly achievable.

Let's say we have achieved that. Are we done yet? No. Simply installing a great surveillance system at a building is not always a valuable outcome in and of itself. Having a real capability still requires a bit more. What about the right strategy? Are your cameras in the right spots? It is crucial to identify the prime targets of surveillance. What are your facility's access points and crucial assets? Are they mapped in your plan? Do you have a plan? Do you have growth strategies for your sites that are congruent with a technology plan to support them? Deploying scalable surveillance systems that align to organizational development requirements helps to provide physical security continuity of critical infrastructure as responsibilities inevitably evolve.

But wait, there's more! Our important outcomes are not facilitated by merely fielding the right technologies, the right way with the right strategy. A true capability requires the right combination of technology, process and people to be effective and provide value.

The first thing we tend to think about when we ponder surveillance is someone sitting behind a monitor, making observations in real time. And that is a basic requirement, of course. And this is. Obviously why we came to it last.

The effectiveness of the surveillance system is not only determined by its underlying technology, but also by the accessibility of the system by the people who are accountable and responsible to provide security outcomes. Without the personnel who are appropriately trained to view and respond to security threats, the system will only collect data that may never be utilized. The combination of technology and human interaction is critical for a robust physical security posture. Have your great systems been operationalized appropriately for human use? Can the system proactively identify potential threats, and provide alerts to security personnel, if needed? Are the systems effective, and do they match your business and team needs?

16 Designing Physical Security Monitoring for Water Quality Surveillance and Response Systems. Accessed Jan. 24, 2025. [Online]. Available: https://www.epa.gov/sites/default/files/2017-11/documents/esm_design_guidance_2017-11-02.pdf (EPA, 2017)

Detection Systems: Alarms and Sensors

Detection Systems (Alarms and Sensors)

- Anomalous Pattern Detection
- Smart Alarms
- Radar and LiDAR
- Geofencing Technology
- Seismic Sensors
- Panic Devices
- Smoke and Gas Detectors
- Water, Temperature, Heat and Humidity Detectors
- Motion, Vibration and Tamper Sensors
- Acoustic Monitoring
- Drone Detection Systems
- Magnetic Sensors
- Glass Break and Pressure Sensors
- Microwave Field Detectors

When we think about detection systems, for the purposes of this discussion we are sticking to the narrowed scope of our conversation, aligned to our OST model. We are focusing upon alarms and sensors for the most part. These are the essential but often forgotten appliances and devices that are strategically leveraged within zones of protection to identify potential threats, risks, and breaches. When something gets a bit too toasty, our heat detectors feel it. If something starts moving through a protected field, a motion sensor sees it. Pressure sensors provide a sense of touch, smoke detectors can virtually smell smoke and the signs of fire, while our glass break sensors allow us to hear something that may help us keep the zone secure.

Think of your detection system as the sensory network of the physical security ecosystem – the parts that bring our capabilities to life. Small but mighty, our alarms and sensors are a key to mission success. When our detection elements are properly orchestrated within an appropriate defensive mesh, we can gain a holistic understanding of the security landscape and develop effective strategies that better mitigate risks.[17]

From a technical design point of view, these types of technologies share some similarities with IoT) devices, but to be clear, they are not exactly the same. Both tend to share parallels in cloud and edge computing integration strategies, real-time monitoring and communications, event-based triggers and remote accessibility. Where they are dissimilar is important to understand. Generally speaking, security detection components serve a unique functional purpose and may be characterized by different network dependencies, as well as limited automation and scalability capabilities when compared to common IoT devices. We also tend to want to make our security sensors and alarms a lot less universally accessible to people or parallel systems that do not serve a purpose in the security mission. Understanding what components work and do not, and where and why, within our operational infrastructure will help ensure the right decisions are made during tech selection, implementation, maintenance, upgrades and improvement.

When we think about operational challenges connected to detection devices, false alarms tend to most commonly surface. From a technical perspective, think of this as a misfire. If it happens infrequently, we have an annoyance or small distraction. If it becomes more frequent, it may transform into white noise that can elevate the probability of security risks, incidents, or gaps in defenses. From a human perspective, think about it as the sensor that keeps crying wolf. False alarms result in complacency and conditioning of personnel to ignore what eventually is a true alarm; one that may run the risk of going unanswered.[18]

17 7 environmental components to take in consideration during a physical security audit. Accessed Jan. 25, 2025[Online]. Available: https://www.security101.com/blog/7-environmental-components-to-take-in-consideration-during-a-physical-security-audit (Security 101, 2025)

18 False Fire Alarms. Accessed Jan. 27h 2025 [Online]. Available: https://www.firehouse.com/home/news/10545242/false-fire-alarms (Fire-

There are many causes, but some of the most common are human error, integration and deployment issues, poorly positioned sensors, outdated technology, system failures, power outages and a lack of appropriate maintenance.[19] Working with qualified security integration professionals can help avoid many of these types of pitfalls. Regular maintenance and testing of your security edge devices is required, but often deprioritized. Much can go wrong over time, and most of these system elements have a finite operational life. Establishing failover, redundancy and backup system capabilities is advisable.

Where practicable, it is best to select advanced technologies capable of reducing the white noise of false alarms. High-cost systems driven by smart features and custom integrations can often be a barrier to entry for many organizations, especially SMBs. To balance cost constraints, prioritize high-risk areas found in an initial physical mapping of company infrastructure. Not every sensor must be the same. Uniformity of components isn't an outcome. Painting with a broad brush from the macro level is unnecessary when one is keenly aware of their micro needs and requirements.

Although detection systems are often used to protect from human risks, they are also leveraged to protect various facilities from environmental threats. Fire, wind and water can cause as much or more damage than any other threat to a company's infrastructure. Weather conditions such as strong winds can create false alarms for motion sensors, disrupt placement or even destroy poorly placed components.[20] It is important to design the OST mesh ecosystem with resilience against unique external threats, while maintaining the capabilities necessary to accurately alert the intended receiver. Sensor placement isn't as simple as it may seem. As the front line of our physical security sensory intake framework, OST detection systems play a unique and critical role in the overall mission. A lot rides on getting this part right. Leave nothing to chance.

house, 1996)

19 3 tips to help reduce the risk of false alarms. Accessed Jan. 27, 2025 [Online]. Available: https://www.adtsecurity.com.au/blog/security-tips-community/risk-of-false-alarms (ADT, 2025)

20 7 Ways to Prevent False Alarms with Your Security System. Accessed January 27th 2025 [Online]. Available: https://adssecurity.com/prevent-false-alarms-with-your-security-system (Vector Security, 2021)

Perimeter and Environmental Security (PES)

Perimeter and Environmental Security

- BMS
- Power and Communications Backup Systems
- Barriers and Bollards
- Fencing Solutions
- Barbed and Razor Wire
- Gate Technologies
- Vehicle Access Control
- Turnstiles
- Mantraps and Security Vestibules
- Security Booths
- Lighting, Signage and Physical Deterrents
- Storm Shutters and Resistant Windows
- Drainage and Flood Barriers
- Containment Systems

Creating a physical perimeter around a facility gives outsiders a sense of what is public and what is private. Effective perimeters protect against intrusions, vandalism and unauthorized access for unapproved visitors. Deploying low-tech solutions like fencing and barriers provides a material deterrent, enabling an organization with additional layered defensive measures to protect facilities. Perimeter security can include intrusion detection systems, reinforced walls, gates or entry management systems. Arguably, it can include a lot of other things that we have already talked about, such as PACS, surveillance technologies and sensors. While true, we are narrowing the focus in this section specifically to just the types of elements found on Table 1, under the PES column.

When evaluating the various PES types of components, the focus is physical and technological barriers that delay, prevent, or constrain unauthorized access. While these devices play a crucial role in the physical security defensive ecosystem, we must ask if they generally fit within our general definition of OST. Specifically, does OST imply *only* digital or electronic technologies? Recall, we defined OST as:

> The underlying technical elements that enable us to do our work as security professionals; technologies leveraged to help us support, automate, scale and deliver the principal mission of physical security; OST help manage security problems and connect us with the physical world we are attempting to protect.

For the purposes of this discussion, we will assert it does. Our attention will remain on the electronic and digitally connected portions of the OST domain – that is, the technical elements. While solutions like barbed wire, simple fencing and barriers play an important role in security, narrowing our discussion keeps the narrative consistent and focused. Moreover, this subsection of Table 1 can be a bit of a gray area of the discussion, debatable and subjective to one's own specific point of view.

On that note, we will start with one of those disputable points – that is, the building management system (BMS) being categorized as an element of PES. Some may argue BMS is more appropriately aligned to our next section, the security management category of Table 1. But our contention is the primary mission of a BMS is managing heating, ventilation and air conditioning; energy; and lighting systems within a building.[21] The key focus of BMS is related to management of the environmental controls within a commercial space. BMS is a tool and also an operational technology. Over the years, BMS systems have evolved to play an important role in the security mission by helping to integrate, automate and scale an array of physical security, fire and life safety system components within a

21 What is a Building Management System? Accessed Feb. 10, 2025 [Online]. Available: https://www.cim.io/blog/what-is-a-building-management-system (CIM, 2025)

commercial building space.[22] In this way, BMS are leveraged to deliver OST capabilities to support the greater building environment. Therefore, we submit that BMS is an element of our PES because it enables us to do our work as security professionals and is leveraged to help us support, automate, scale and deliver the principal mission of physical security. It also happens to be an important key enabling technology for security as it provides a conduit, or a highway system to the entire environment designated for protection.[21]

Many times, however, facilities owners, SMB leaders and physical security technicians aren't accustomed to working with BMS and find themselves surprised by some of the nuance.[23] For example, it is not uncommon to find that BMS platforms can be highly challenging when it comes to integration. BMS can be characterized by proprietary components and protocols that do not easily connect to your OST. There is commonly legacy technology to deal with, compatibility issues and even scalability limitations. There can be cybersecurity and compliance issues related to frequently leveraged and insecure BMS protocols like BACnet and Modbus. The challenges are not unsolvable, and the advantages of leveraging BMS to better deliver and consistently support security outcomes are worth the investment in terms of long-term savings.

Evolving complexity of data and information into more easily consumable solutions is highly desirable whenever possible. It may be wise to consider capabilities that can integrate all your BMS platforms into an easily accessible 'single pane of glass.' This provides operators insight into all their systems, simply and immediately. Jay Williams, Vice President of Network Infrastructure Sales at Wesco, says "we're finding that as the number of OSTs and other platforms continues to grow, organizations are looking for solutions that can help them connect, collect, analyze and act on those disparate data streams - all from a single screen."

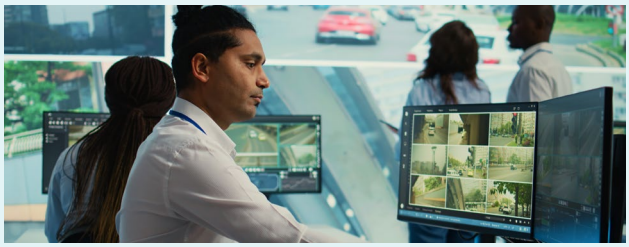
Providing a stable environment for an organization's facilities can lead to an increase in productivity. It's also a success driver for primary OST, like PACS, surveillance systems and sensors. Consider lighting for a moment. It may not seem like an OST component to many. But it certainly plays several essential roles. Think of lighting as a secondary OST for a moment, that is required for security personnel to be effective as individuals and may also be necessary to ensure the effectiveness of many video surveillance systems.[24] There is a third example of lighting's security utility. Creating a constant illuminated environment will support the security mission directly by deterring potential criminal threats. Keeping a protected space looking busy, active and alive can create a less intriguing target for potential attackers.

PES elements play a critical role within the overall security maturity posture of a site. Understanding and identifying what they are is often illusive for the SMB and for larger businesses as well. One doesn't think about how communications, power systems and building automation is intrinsically connected to the security mission, until something goes wrong. Having the right plan starts with seeing the entire field of battle. And when automated gating technologies and security booths are digitally connected to your greater security ecosystem, all the same thinking, strategy and planning previously discussed will apply to your PES elements as well. Functional requirements development, technology selection, implementation, integration and life cycle support and maintenance considerations will

22 How Integrating Security Systems With BMS Can Help Elevate Commercial Property Security. Accessed Feb. 10, 2025 [Online]. Available: https://stealthmonitoring.com/crime-prevention/how-integrating-security-systems-with-bms-can-help-elevate-commercial-property-security (Stealth Monitoring, 2025)
23 The challenge of securing building management systems, E. Ben-Meir. Accessed Feb. 3, 2025 [Online]. Available: https://www.techtarget.com/iotagenda/blog/IoT-Agenda/The-Challenge-Of-Securing-Building-Management-Systems (TechTarget, 2019)
24 Lighting the Way to a Smarter, Safer City. Accessed on Jan. 31, 2025 [Online]. Available: https://www.securityindustry.org/2018/09/14/lighting-the-way-to-a-smarter-safer-city/ (SIA, 2018)

also need to be deliberated as they apply to these nuanced elements of the security maturity journey too. Once again, things are not always as easy as they first may seem, and it is therefore wise to consult with a trusted security industry professional, such as a technology dealer, distributor and/or integrator.

Security Management



Security Management

- Physical Security Operations Center
- Remote Monitoring
- Video Analytics Technology
- Incident Reporting Systems
- Mass Notification Systems
- Guard Tower Systems
- Communication Devices
- PA Systems
- Fire Detection & Suppression Systems
- Emergency Exit Systems
- Integrated Security Platforms
- IoT Security Devices
- Cybersecurity Capabilities
- GPS Tracking

Security Management encompasses a wide range of OST intended to connect, protect and optimize. Important outcomes revolve around enabling organizations provision of a centralized real-time threat management function, coupled with broad-based support and response. The common theme here is scalability. Administration of complex integrated OST can often require an array of skilled workers are fielded to understand, optimize and operationalize an assortment of technologies, data and high-pressure situations. Finding ways to automate some of that work is highly regarded. The creation of a physical security operations center (PSOC) is a primary example of one strategy large corporations employ to protect facilities at scale.

PSOCs give organizations the ability to consolidate large data sets streaming in from a network of OST devices and deliver a single pane of glass approach to more economically and consistently and efficiently manage threats.

But often, when people consider the idea of a PSOC, or hear the words "security operation center," they envision a massive room with screens all over the walls, like it's NASA Mission Control. They imagine computer towers the size of an SUV, and desks lined up in dark rooms, with security operators filling every seat, rapidly attempting to solve complex problems, and communicating with shadowy figures like Jack Bauer. For the average SMB, the idea of a PSOC may sound like a bit of a stretch. But it's not.

Think of it as just software, because that is really all it takes. Anyone with an appetite for security coupled with budget limitations and a laptop has a viable path on this journey.[25] Everything needed for the standard PSOC can be acquired for as little as a few hundred dollars per month in total licensing fees. Some of the basic software-based elements include:

- Command center and incident response software
- Electronic access control and authentication software
- Surveillance and video management software
- Alarm and intrusion detection management software

Sure, that may sound like a lot of sophisticated

25 Best Physical Security Software. Accessed on Feb. 1, 2025 [Online]. Available: https://www.softwareworld.co/physical-security-software/ (SoftwareWorld, 2025)

things. But this isn't as inaccessible as it may seem. The good news is you probably already have most of the parts. For example, many of the prominent electronic access control systems, which are a foundational element of your PACS stack, include electronic access control and authentication software. Sounds obvious, right? Surveillance and video management software is most likely part of your network video recording system. And even if you lack these elements, this is not a difficult climb.

The key to the PSOC journey is democratization of data. Integration with BMS will help enable richer centralized capabilities. The fundamental takeaway is this is a possible outcome for the SMB. Other lightweight and inexpensive solutions, such as mobile monitoring applications that can be delivered to a smart phone, will help provide greater levels of scalability, effectiveness and supportability for the facilities leader on a budget. PSOC strategies and competencies are not the exclusive domain of the corporate one percent crowd. There are solutions for most budgets.

Security management steers us toward a single common outcome: understanding and managing the bigger picture. This category of OST represents the elements that consume and functionalize large datasets, creates mass awareness, value, and delivers broad-based comprehensive outcomes. Cybersecurity capabilities are an example, and an integral ingredient of the bigger picture. We like to say that it is a first cousin of physical security. Facilities and building systems aren't secure when they are not cybersecure. As a wise person once said, be proactive and engage technology and security domain experts early. CISOs and CIOs are your friend.

These are the high impact OST elements, in terms of results. Mass notification systems ensure stakeholders can relay and receive critical alerts when needed, at scale. Organizations with the capacity to direct and steer large crowds effectively have an advantage in crisis management and everyday operations. Rapid data exchange, connectivity and integration with other critical elements of the security ecosystem, such as life safety, fire systems, security components and other primary OST, add efficiency and reduces risk.[26]

There are diverse applications and purposes when we think about security management OST components. If expand our scope of thought to all the various types of OST, and then integrate each, creating interdependent spokes within a security machine, a PSOC might be thought of as the hub. That's what makes it useful, and this is the true value of security management thinking. For as much complexity as each element of the security ecosystem may present, tying everything together in order to deliver a centralized platform is achievable, but not so simple.

As is the case with all subsections of our OST big picture, security management technologies require a lot of thought, deliberation and planning. And while some technology vendors may suggest DIY options for the SMB, we will reiterate that things are not as simple as they may seem. Consolidating all the complexities of your OST systems with the right strategies and technologies to suit your individualized business priorities and needs is an achievable end-state goal. Achieving scalability and delivering high value with limited resources can be done with a great understanding of the technical options, the right planning, domain knowledge, integration, person power and ongoing maintenance and support. Security management is about keeping your mission capabilities effective and sustainable. Doing this is worth doing it right, and none of the many challenges are insurmountable. Develop your plan, leverage your resources and partnerships and execute well. Always remember the job of security and OST development is not a finite state. Threats will evolve, and so must your strategy.

26 The Benefits of Fire, Life Safety and Security Integration, T. Giannini. Accessed on February 4, 2025 [Online]. Available: https://www.buildings.com/industry-news/article/10189775/the-benefits-of-fire-life-safety-and-security-integration (Buildings, 2012)

Conclusion

Great things happen when stakeholders are communicating well and understanding each other. Whether you are a security industry insider, professional, technician or integrator, or are in the supply chain, or happen to be a leader at a SMB with an OST appetite, mutual understanding of the operational space, challenges and relative ability to facilitate, deliver, consume and support will be everything. Buying expensive tools in the OST domain is not a solution to a problem. It simply takes more.

Every first-time climber or adventurer requires a capable guide. If you are a SMB consumer of OST, it is always unwise to start this daring expedition without the prudent advice of your trusted security industry professional, technology dealer, distributor and/or integrator. Sometimes the goal of economy is achieved by making the right early choices and wise investments that result in life cycle cost savings. Long-term thinking can prove to be less disruptive to your business and more sustainable and result in better security outcomes. It all comes down to the right plan.

If you are a security industry professional who is charged with the mission of being that trusted guide in the OST journey, understanding the needs of your customer, the real desired outcomes and the full life cycle requirements is as important as technical domain expertise. Mutual understanding of what victory looks like, what it takes to get there and what problems we are trying to solve will help ensure mutual success.

Whether rolling out a particular OST for the first time, migrating to new or improving old, the important questions should revolve around outcomes, strategy, planning, tool selection and the details of integration, delivery and life cycle support. All parties require awareness, but unfortunately, they often don't have it. Many businesses and organizations will prioritize implementing the new system to solve the problem of the day, while neglecting to plan for long-term maintenance and life cycle support.[27] Getting this right is everyone's responsibility.

It is not uncommon to make the mistake of believing that acquiring the shiny new OST solution is the destination, rather than just the start of the journey. It is human nature to assume the rest of the job will become easy to figure out once we have the tools that can effectively operationalize our mission requirements. A capability requires more than just the underlying technology. Owning lawn equipment doesn't mean the lawn looks beautiful. An OST will seldom provide value independently. More is required and the right recipe for success varies at every business.

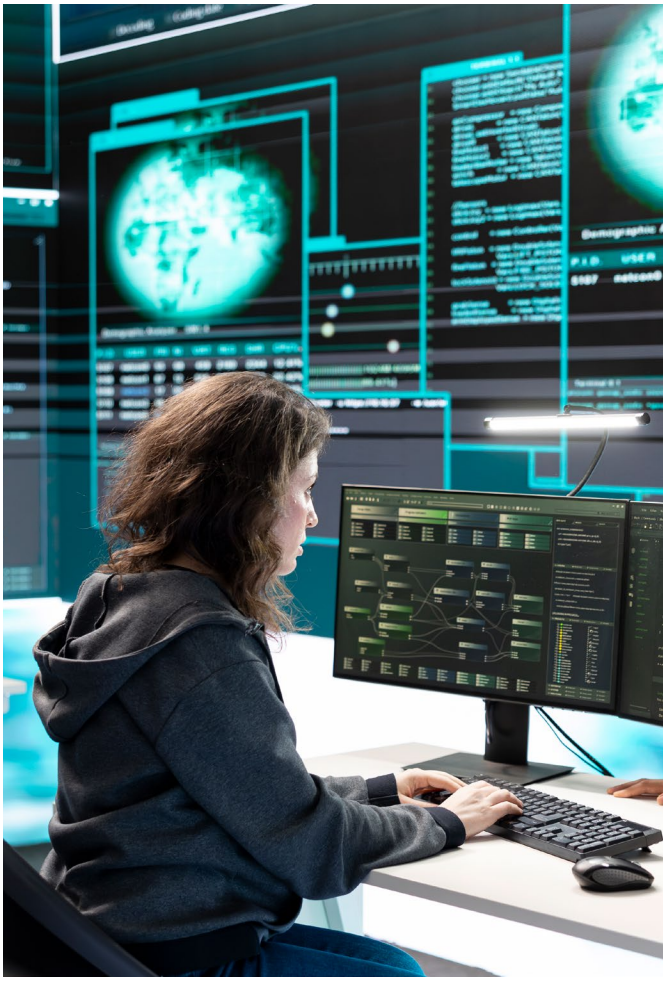
Analysis, evaluation and preparation are integral at the onset of any project focused upon instituting or improving security capabilities. Commissioning new or maintaining existing OST requires more than OEM and vendor promises. Many of these technologies are complicated to integrate and maintain. An internal resourcing and support plan is essential for success. Strong third-party partnerships are advantageous. There will always be needs for improvement, progress and advancement when leveraging OST that is intended to solve human or physical problems. Be proactive and have a plan.

Considering the reality that security operational needs and requirements tend not to be static and continue to evolve,[28] we must recognize that our OST

27 PwC's 2024 Digital Trends in Operations Survey – Why significant business outcomes are still difficult to achieve – and what you can do. Accessed on: Nov. 9, 2024. [Online]. Available: https://www.pwc.com/us/en/services/consulting/business-transformation/digital-supply-chain-survey.html (PwC, 2024)

28 Risk is Dynamic, So Physical Risk Assessment Should Be Continuous, D. Young, M. Martin. Accessed on: Dec. 1, 2024. [Online]. Available: https://www.asisonline.org/security-management-magazine/articles/2023/11/dynamic-risk-assessment/continuous-physical-risk-assessment (ASIS, 2023)

elements require continuous attention and dynamic support. As advancements such as AI and machine learning continue to evolve, and new technologies emerge, so too will the associated risks and attention we will have to apply to our mission critical OST.[29] Sometimes advancements, such as a new cloud delivery of traditionally on-premises security technologies, can introduce pitfalls and support gaps that your OEM may have failed to prepare you for. Our institutional OST infrastructure and ecosystem must be designed to scale to our individualized needs.



Recognizing who we are and where we operate will help safeguard against problematic OST implementations. Fundamental questions should be answered before charging into the fray to solve the problem of the day and committing to a sizable capital expenditure, without understanding the bigger picture, hidden costs and potentially considerable operational costs to come. Things change. Can your institutional approach become dynamic or are you operating within a static environment that shifts slowly? The usual story many security operators tell is they lack the time to drive improvements but tend to be aware of the gaps.[30]

Right-sizing, aligning and improving one's security tech stack requires a strict focus on operational outcomes and the discipline and objectiveness to constantly look for opportunities. Communicating the benefits and value of security initiatives effectively to the decision-makers holding the purse strings and authority to act can be an artform. But the necessary ingredients are usually connected to data, context and alignment to the goals of the organization, business or institution. OST improvement or introduction should be handled carefully and planned in accordance with the bigger picture and a deep understanding of the full set of prevailing factors.

The OST domain is a complex web of challenges and pitfalls, but none are insurmountable and the security outcomes at the end of the journey are well worth the investments necessary. Protecting people, property and valuable resources is a noble pursuit. But it isn't easy. By working together, and sharing our valuable experiences and domain expertise, we can ensure mutual success by collaboratively strategizing and resolving the challenges to better ensure optimal delivery and best operational practices.

29 The 15 Biggest Risks Of Artificial Intelligence, B. Marr. Accessed on: Dec. 1, 2024. [Online]. Available: https://www.forbes.com/sites/bernardmarr/2023/06/02/the-15-biggest-risks-of-artificial-intelligence (Forbes, 2023)
30 8 challenges every security operations center faces, J. Burke. Accessed on: Dec. 1, 2024. [Online]. Available: https://www.techtarget.com/searchsecurity/tip/8-challenges-every-security-operations-center-faces (TechTarget, 2020)

APPENDICES

This collection of reference materials provides guidance on many best practices that could be leveraged for strategic planning related to OST. This content is offered as a guide to begin further exploration of the topics in this paper.

The content provided in these appendices (A, B and C) is based solely on the authors' research, personal knowledge and experience. Much of this section's content is drawn from common industry standards and publicly available sources. It is intended for informational purposes only and should not be construed as comprehensive or definitive advice. While every effort has been made to ensure the accuracy of the information, the authors cannot guarantee that all potential solutions or scenarios have been covered. Use of the information provided is at your own discretion and risk. SIA, the authors and any associated parties deny any liability for damages or losses incurred as a result of the application or reliance on the content contained herein. It is recommended that you seek professional guidance tailored to your specific situation.

APPENDIX A

Prominent Reference Material Relating to OST and Physical Security

NIST SP 800-82r3
This document provides guidance on how to secure operational technology while addressing their unique performance, reliability, and safety requirements. OT includes programmable systems and devices that interact with the physical environment or manage devices that do.

NIST 800-12 Chapter 15
This chapter discusses the benefits of physical security measures and presents an overview of common physical and environmental security controls.

CISA Physical Security
The Cybersecurity and Infrastructure Security Agency provides access to tools and resources that support physical security and resilience. It coordinates with stakeholders and experts to provide recommendations on protective measures for organizations of all sizes.

North American Electric Reliability Corporation (NERC)Security Integration
This document provides information on securing the electricity grid during rapid grid transformation, focusing on cybersecurity efforts for distributed energy resources (DERs) and DER aggregators.

Data Center Physical Security Guidelines
This document outlines best practices for securing data centers and physical infrastructure that store, process and transmit sensitive data.

National Center for Education Statistics
This resource covers security measures for educational institutions, outlining protocols to secure student data, IT systems and campus facilities against threats.

Principles of operational technology cyber security
This document presents six principles to guide OT decision-makers in ensuring cybersecurity decisions do not negatively impact OT environments.

Best Practices for Planning and Managing Physical Security Resources: An Interagency Security Committee Guide
An Interagency Security Committee guide providing strategies for physical security resource allocation, risk assessment and investment in security infrastructure.

Protect the Physical Security of Your Digital Devices
A CISA guide outlining the steps to secure mobile devices, laptops, and other digital assets from theft, unauthorized access and tampering.

OSY/OCIO Security Awareness Tips
This document provides security awareness training and best practices to prevent unauthorized access, insider threats and breaches.

Cybersecurity Best Practices
A CISA framework combining cybersecurity and physical security best practices, including password management, multifactor authentication and security audits.

Using Operational Security (OPSEC) to Support a Cyber Security Culture in Control Systems Environments
Guidance for integrating OPSEC principles into cybersecurity policies within critical control systems, such as power grids and industrial automation.

DoD Operations Security
The U.S. Department of Defense provides OPSEC strategies covering risk management, sensitive data protection and military security protocols.

Introduction to Physical Security Student Guide
A guide covering fundamental physical security measures, including perimeter defense, access control systems and emergency response planning.

Physical Security Assessment Standards and Best Practices Tennessee Higher Education Campuses
Security measures designed to protect higher education institutions, ensuring campus safety, emergency preparedness and risk mitigation.

HHS Cybersecurity Program
A program from the U.S. Department of Health and Human Services providing best practices for securing electronic health records, medical devices and hospital networks.

Physical Security Guideline for the Electricity Sector
A NERC guideline on securing power plants, substations and energy control centers from unauthorized access and cyber threats.

Data Center Physical Security Guidelines
A guide covering the best practices for physical security of data centers. The Open Compute Project gives a technical overview that offers guidance for single servers all the way up to multi-building campuses.

Global Information Assurance Certification Paper
A white paper on best practices for physical security, including risk assessment, security audits and incident response planning.

United States Department of Labor Cybersecurity Program Best Practices
This document offers best practices for data protection, physical security of IT assets and insider threat mitigation for government agencies and private companies.

Physical Security Measures Overview – National Center for School Safety
A planning document for school security, including emergency preparedness, security infrastructure, and protective measures for students and faculty.

Physical Security Design Manual for VA Mission-Critical Facilities
A Department of Veterans Affairs publication on securing mission-critical government facilities, including security strategies for hospitals, data centers and offices.

Physical Security Program: Access To DoD Installations
A DoD security guide outlining physical security access control policies for military installations, focusing on credentialing, restricted zones and emergency response.

APPENDIX B

OST Best Practices

The information in this section should be used as reference material that provides some generalized best practices guidance relating to operational technology in the physical security domain. Please review Appendix A for some prominent source material in this space to develop a deeper understanding.

Select Strategic Thoughts for Acquiring or Updating OST Systems

Technology Selection

- Define Clear Objectives – Identify specific problems the OST needs to solve before evaluating options.
- Use a Requirements Matrix – Create a checklist of functional and nonfunctional requirements tied to business goals.
- Stakeholder Alignment – Conduct workshops all stakeholders to ensure consensus.
- Business Impact Analysis – Evaluate how the OST aligns with key performance indicators.
- Technology Shortlisting Framework – Develop a scoring system based on critical features, scalability and cost-effectiveness.
- Consult Industry Experts – Engage consultants or industry partners.
- Pilot Testing – Run proof-of-concept tests to compare different solutions in real-world scenarios.
- Customer Reviews and Case Studies – Look at real user feedback and industry adoption rates to filter out hype-driven products. Ask for customer references from OEMs.
- TCO Analysis – Include licensing, training, maintenance and upgrade costs in budget planning.
- Opt for Scalable Solutions – Choose modular or cloud-based technologies that grow with business needs.
- Return on Investment Forecasting – Compare potential efficiency gains against upfront investment to justify costs.
- Leverage Subscription Models (SaaS) – Reduce capital expenditures by opting for pay-as-you-go pricing models.
- Choose Open Standards – Prioritize solutions that support widely accepted industry standards
    - Example: SIA Open Supervised Device Protocol (OSDP) and ONVIF can ensure a balance of security and interoperability. Avoid proprietary protocols.
- Middleware Solutions – Implement API gateways or middleware platforms to connect incompatible systems.
- Cloud-Based Integration Platforms – Use cloud-native technologies that offer flexible integration with other services, when and where it makes sense.
- Vendor Evaluation – Confirm integration capabilities before purchase and test interoperability in a sandbox environment.
- Adopt Modular Architectures – Select solutions that allow easy expansion or customization.
- Cloud-Native and Microservices-Based Solutions – Ensure the chosen technology supports elastic scaling.
- Consider Vendor Road Maps – Assess the long-term viability of a technology by reviewing the vendor's innovation pipeline.
- Hybrid Models – Use a combination of on-premises and cloud solutions to balance control and scalability, when and where it makes sense.
- Security-First Approach – Assess encryption, authentication mechanisms and compliance certifications (for example, ISO 27001, SOC2, GDPR).
- Third-Party Security Audits – Conduct

penetration testing and risk assessments before deployment.
- Role-Based Access Control (RBAC) – Implement fine-grained access permissions to minimize security risks.
- Compliance Checklists – Ensure alignment with industry standards.
- User-Centric Design – Select technology with intuitive user interface/user experience to reduce the learning curve.
- Choose Open-Source or Open-Standard Technologies – Avoid vendor lock-in by selecting interoperable solutions.
- Multivendor Strategy – Avoid reliance on a single provider by diversifying technology suppliers.
- Service-Level Agreements (SLAs) – Negotiate flexible contracts with vendors to ensure continued support.
- Exit Strategy Planning – Establish a migration plan for data and applications
- Benchmark Testing – Conduct stress tests and performance evaluations before full deployment.
- Cloud Redundancy and Failover Strategies – Ensure availability through redundant cloud instances.
- Service Uptime Guarantees – Choose vendors with high SLAs (99.99% or higher uptime commitments).
- Agile Decision-Making Framework – Use methodologies like RACI to clarify decision roles.
- Set Clear Timelines – Define decision deadlines to avoid prolonged evaluations.
- Risk vs. Reward Analysis – Use weighted scoring models to evaluate options objectively.
- Pilot Programs – Deploy small-scale tests before full commitment to mitigate risks.

Cost

- Prioritize High-Risk Areas – Start by upgrading OST in the most sensitive locations before expanding systemwide.
- Life Cycle Cost Analysis – Evaluate the total cost of ownership over time to avoid hidden expenses.
- Grants and Incentives – Explore government or industry grants that support physical security improvements.

Integration and Interoperability

- Open Standards – Choose OST that support open protocols such as SIA OSDP to ensure a balance of security and interoperability. Avoid proprietary protocols.
- API-Based Systems – Select OST with robust APIs that allow integration with third-party security platforms.
- Middleware – Deploy middleware to act as a bridge between legacy and modern security infrastructure.
- Cloud-Based Systems – Using cloud-based security solutions can streamline integration across multiple systems and locations. But be sure a SaaS Solution fits your needs, and you can support its deployment.

Reliability

- Offline Mode Support – Deploy OST that allow doors and access points to function in offline mode if the network goes down.
- Backup Power Solutions – Ensure OST has an uninterruptible power supply to maintain operations during outages.
- Redundant Architecture – Implement failover servers and decentralized access control decision making to prevent downtime.
- Regular Maintenance and Testing – Schedule system health checks and preventive maintenance to identify potential issues before failures occur.

Regulatory Compliance

- Implement Compliance-Aware OST – Use systems that support role-based access, audit logging and compliance reporting.
- Data Retention Policies – Ensure access logs are stored securely and comply with industry-specific retention requirements.

- Access Review Audits – Conduct periodic access audits to ensure that only authorized individuals have access to sensitive areas.
- Secure User Data Handling – Follow best practices for storing and processing personal data related to access control.

Identity and Credential Management

- Adopt Multifactor Authentication – Combine RFID cards with biometrics (fingerprint, facial recognition) or mobile authentication for stronger security.
- Use Smart Credentials – Implement encrypted smart cards, mobile-based credentials or blockchain-based identity management.
- Automate Access Revocation – Integrate OST with HR systems to automatically revoke access upon employee departure.
- Biometric Authentication – Deploy biometric access systems for high-security areas to eliminate risks from lost or cloned cards.

Cybersecurity

- End-to-End Encryption – Ensure that all OST data, including credentials and logs, are encrypted (AES-256 encryption or better is recommended).
- MFA – Use MFA for OST management interfaces and critical security functions.
- Regular Patching and Firmware Updates – Keep all OST devices up to date with security patches to close vulnerabilities.
- Network Segmentation – Isolate OST from general IT networks to prevent lateral movement in case of a cyberattack.
- Penetration Testing and Security Audits – Regularly test OST for vulnerabilities and conduct third-party security audits.

Performance

- Cloud-Based and SaaS OST – Implement a cloud-based OST where it makes sense for seamless scalability across multiple locations.
- Load Balancing and Redundancy – Deploy scalable server architectures with redundancy to handle increased demand.
- Edge Computing – Use intelligent edge controllers to process access control decisions locally and reduce dependency on central servers.
- RBAC – Implement hierarchical permissions to simplify management as the system scales.

Training

- User-Friendly Interfaces – Choose OST solutions with intuitive user interfaces to reduce training complexity.
- Security Awareness Programs – Conduct ongoing training sessions for employees on best practices for access control.
- Mobile and Remote Access Management – Offer mobile-based access solutions for convenient and secure authentication.
- Gamification & Incentives – Use security training programs with rewards to encourage compliance and awareness.

Big Picture Thinking: Devising Strategy Connected to OST Systems

Identify Assets

Identifying important assets that require the need for security is the first stage in safeguarding an organization. These resources often consist of operational technology systems, employees, sensitive data and physical infrastructure. Security teams can effectively manage resources and prioritize protection activities when they have a clear understanding of what is valuable within an organization. Organizations can start to lay the groundwork for their security strategy and guarantee that the most precious resources are protected to the highest degree by outlining all their important operational assets. This step also entails determining dependencies, classifying assets according to their significance, and understanding how security threats might affect operational continuity.

Assess Risk
Organizations must use risk assessments and security audits to analyze potential threats and vulnerabilities after assets have been identified. This entails examining internal risks including insider threats, policy and compliance and structural flaws. In addition, organizations must identify external threats like invasions, cyberattacks, and theft. Organizations can focus their security plans by using the information from a comprehensive risk assessment driven by the severity of various security vulnerabilities. Organizations may stay ahead of developing threats and modify their security measures accordingly by regularly conducting risk assessments as seen fit. This ensures that vulnerabilities are identified, fixed and tested before they are exploited by threat actors.

Control Access
A fundamental security safeguard is access control. Access control ensures that only people with permission may interact with locations, operational assets or sensitive data. Security measures like visitor management systems, biometric scanners, key cards, multifactor authentication and role-based access controls should be put in place by organizations. These precautions lower the possibility of insider threats, physical breaches and illegal access. Effective access control not only protects private zones but also makes it possible for security controls to monitor people's movements and activities inside an organization's facilities. Organizations can identify irregularities and security regulations with the aid of routine audits and access log monitoring.

Monitor Activity
Security systems are continuously monitored to guarantee that any suspicious activity is promptly identified and dealt with before it gets out of hand. To provide ongoing facility monitoring, organizations should implement intrusion detection technology, motion detectors, alarm systems and CCTV cameras. Confidential regions, such as high-risk zones, sensitive areas and access points, should be under constant surveillance. Organizations can improve the efficiency of their security measures rapidly by combining automated surveillance with real-time human oversight.

Secure Perimeter
The first line of defense against attacks and unlawful access from external threats is a well-secured and defined perimeter. To prevent and redirect unwanted incursions, organizations should provide robust physical barriers including security checkpoints, reinforced doors, fencing and controlled entrance points. Securing pedestrian and vehicle access is another aspect of effective perimeter security, which makes sure that only individuals with permission can enter anywhere near restricted areas. Creating an atmosphere of security will deter unwanted external threats. Improving perimeter security by minimizing blind spots and deterring intruders can be accomplished through lighting, signs, and environmental design. In addition to safeguarding assets, a secure perimeter adds another line of defense that complements internal security protocols.

Develop Response
Organizations are better equipped to respond swiftly and efficiently in the event of emergencies, disasters or security breaches when they have a clear response strategy in place. Specific procedures for dealing with various risks, including physical incursions, cyberattacks, natural catastrophes and internal attacks, should be outlined in incident response plans. Incident response plans should encompass all duties allocated to personnel to extinguish any and all threats. To guarantee the success of a response plan, organizations should set up clear communication procedures, assign response teams and hold frequent emergency drills within their organization. Making sure employees are well informed during an emergency is crucial to the safety of an organization's employees. An effective response strategy reduces the effects of

security events, safeguards employees and property and guarantees that interruptions are managed effectively. Organizations can enhance their capacity to handle security incidents and quickly recover from possible threats by regularly revising and testing their response plans.

Train Personnel

The effectiveness of security response depends on the individuals in charge of carrying them out. Frequent awareness and training courses will assist staff members and security teams in understanding their responsibilities for preserving a safe workplace. Workers should receive training on cybersecurity best practices, emergency protocols, access control guidelines and other security measures that best protect organizational assets. To get ready for real-world threats, security teams should participate in scenario-based training. Repetitive training reenforces duties and expectations of employees that are managing the outcome of security events. An organization's security efficacy is escalated, and the chance of error is greatly decreased when there is a security-aware culture surrounding an organization.

Build to Suit Organizational Needs

There are countless resources advising companies they need this or that. OST are only operationally beneficial if they fit the unique operational needs of an organization or business. A fast-food restaurant does not need a bank vault, rather a lock box for daily transactions is probably required. This isn't to say a bank vault won't protect the items inside, but it would be impractical, costly and unnecessary for the restaurant's daily operations. Finding what fits a company's needs does not need to be a difficult task. The key is assessing the risks associated around operational needs, prioritizing one of those, and selecting technologies that efficiently streamline security throughout an organization. After identifying the security goals of an organization, decide what technologies fit best with each objective. For instance, a surveillance system is not intended to stop or alert unauthorized visitors from entering premises, but a physical access control system is. Perhaps you need both, but maybe you do not. Build to suit.

Scalability is Key

Scalability in OST implementation is crucial when maintaining long-term security solutions. If the goal of the organization is operational growth, the physical security posture must also be able to grow. By adding modular, automated, compliant technologies, organizations will have the ability to grow their physical security posture in parallel with the growth of their operations and related needs. For instance, a SMB with one or two locations may only need a small investment in OST, but as that organization upgrades or acquires locations, they may require a larger investment. Prioritizing scalability will allow for the safeguarding of assets combined with the reduced long-term costs and complexities of OST upgrades.

Functionality First

When it comes to OST, functionality comes first. "The key is that the function is being performed. How it is done is secondary--and completely up to the organization and its unique requirements."[31] Security is not a "one package fits all" domain. Implementing minimal but functional OST may be deterrent enough for many organizations. For instance, a small business or startup might have highly restrictive budget constraints with respect to security. Without a budget for a designated security team or complex systems, that organization may be justified in approaching their physical security with a simple surveillance system, alarms and locked doors. Tilting the spectrum of security from simple to complex should happen once a thorough risk assessment justifies the need for advanced measures. This idea seems to bring us back to our original concept and ties the circle back to building to suit.

31 Protecting Your System: Physical Security. Accessed Jan 29, 2025[Online]. Available: https://nces.ed.gov/pubs98/safetech/chapter5.asp

APPENDIX C

Key Takeaways

1) OT tends to exist at convergence points and will often intersect an array of assorted utilitarian needs, requirements and functions. And at these intersections, context, purpose and details will often vary. Therefore, human interpretation will be influenced by a diversity of detached experiences and resultant points of view. All provide value.
2) OST are the underlying technical elements that enable us to do our work as security professionals; technologies leveraged to help us support, automate, scale and deliver the principal mission of physical security; OST help manage security problems and connect us with the physical world we are attempting to protect.
3) An understanding of some of the principles and challenges related to the OST we rely upon daily as security professionals can make a significant difference when we are faced with increasing complexity and evolving threats. Coupled with zero-failure expectations while ensuring mission-critical outcomes, OST is significantly important to the security industry.
4) Complex OST solutions can deliver many benefits but are not always simple to field and maintain. Implementation, integration and ongoing life cycle maintenance is not so simple in many cases and must be planned for and handled judiciously. Have a plan.
5) The OST domain is a complex web of challenges and pitfalls, but none are insurmountable and the security outcomes at the end of the journey are well worth the investments necessary. Protecting people, property and valuable resources is a noble pursuit. But it isn't easy. By working together and sharing our valuable experiences and domain expertise, we can ensure mutual success by collaboratively strategizing and resolving the challenges to better ensure optimal delivery and best operational practices.

References

1. Operational Technology Market Trends. Accessed on: Oct. 26, 2024. [Online]. Available: https://www.grandviewresearch.com/industry-analysis/operational-technology-market-report (Grand View Research, 2024)
2. Operational Technology Market Size And Forecast. Accessed on: Oct. 26, 2024. [Online]. Available: https://www.verifiedmarketresearch.com/product/operational-technology-market (Verified Market Research, 2024)
3. 7 Steps to Align IT, OT and Physical Security. Accessed on: Oct. 26, 2024. [Online]. Available: https://www.iansresearch.com/resources/all-blogs/post/security-blog/2022/11/29/7-steps-to-align-it-ot-and-physical-security. (IANS 2022)
4. How Do OT and IT Differ? Accessed on: Oct. 27, 2024. [Online]. Available: https://www.cisco.com/c/en/us/solutions/internet-of-things/what-is-ot-vs-it.html (Cisco)
5. Operational Technology (OT). Accessed on: Oct. 27, 2024. [Online]. Available: https://www.gartner.com/en/information-technology/glossary/operational-technology-ot (Gartner)
6. What is operational technology? Accessed on: Oct. 27, 2024. [Online]. Available: https://www.redhat.com/en/topics/edge-computing/what-is-ot (Red Hat, 2022)
7. Physical access control: Survey reveals new deployment trends, L. Merredew. Accessed on: Nov. 2, 2024. [Online]. Available: https://www.securitymagazine.com/articles/98710-physical-access-control-survey-reveals-new-deployment-trends. (Security Magazine, 2022)
8. How outdated automation leads to more manual effort — and what you can do about it, N. Kinson. Accessed on: Nov. 3, 2024. [Online]. Available: https://www.redwood.com/article/how-outdated-automation-leads-to-more-manual-effort-and-what-you-can-do-about-it (Redwood, 2022)
9. Why Overworked Employees Are Security Risks, D. Kelley. Accessed on: Nov. 3, 2024. [Online]. Available: https://securityintelligence.com/security-risk-staffing-it-teams-overworked-employees (Security Intelligence, 2014)
10. Safety and Security Systems Interoperability, Pkimluker. Accessed on: Nov. 9, 2024. [Online]. Available: https://www.clr2wrk.com/safety-and-security-systems-interoperability (Clear 2 Work, 2022)
11. Physical Access Control Systems 101. Accessed on: Jan. 22. 2025. [Online]. Available: https://www.idmanagement.gov/university/pacs/ (Oidmanagement.gov, 2023)
12. 10 Types of physical access control systems, OLOID Desk. Accessed on: Jan. 22. 2025. [Online]. Available: https://www.oloid.ai/blog/10-types-of-physical-access-control-system (Oloid, 2023)
13. Integration of IAM with Physical Access Control Systems, D. Simmons. Accessed on: Jan. 22. 2025. [Online]. Available: https://techvisionresearch.com/wp-content/uploads/2020/03/PACS-LACS-20200310-excerpt-final.pd (TechVision Research, 2020)
14. Technology Insight for Physical Access Control Systems. Accessed on: Jan. 22. 2025. [Online]. Available: https://www.gartner.com/en/documents/3451120 (Gartner, 2016)
15. Domestic Drones. Accessed on: Jan. 22. 2025. [Online]. Available: https://www.aclu.org/issues/privacy-technology/surveillance-technologies/domestic-drones (ACLU, 2025)
16. Designing Physical Security Monitoring for Water Quality Surveillance and Response Systems. Accessed Jan. 24, 2025. [Online]. Available: https://www.epa.gov/sites/default/files/2017-11/documents/esm_design_guidance_2017-11-02.pdf (EPA, 2017)
17. 7 environmental components to take in consideration during a physical security

audit. Accessed Jan. 25, 2025[Online]. Available: https://www.security101.com/blog/7-environmental-components-to-take-in-consideration-during-a-physical-security-audit (Security 101, 2025)
18. False Fire Alarms. Accessed Jan. 27, 2025 [Online]. Available: https://www.firehouse.com/home/news/10545242/false-fire-alarms (Firehouse, 1996)
19. 3 tips to help reduce the risk of false alarms. Accessed Jan. 27, 2025 [Online]. Available: https://www.adtsecurity.com.au/blog/security-tips-community/risk-of-false-alarms (ADT, 2025)
20. 7 Ways to Prevent False Alarms with Your Security System. Accessed Jan. 27, 2025 [Online]. Available: https://adssecurity.com/prevent-false-alarms-with-your-security-system (Vector Security, 2021)
21. What is a Building Management System? Accessed Feb. 10, 2025 [Online]. Available: https://www.cim.io/blog/what-is-a-building-management-system (CIM, 2025)
22. How Integrating Security Systems With BMS Can Help Elevate Commercial Property Security. Accessed Feb. 10, 2025 [Online]. Available: https://stealthmonitoring.com/crime-prevention/how-integrating-security-systems-with-bms-can-help-elevate-commercial-property-security (Stealth Monitoring, 2025)
23. The challenge of securing building management systems, E. Ben-Meir. Accessed Feb. 3, 2025 [Online]. Available: https://www.techtarget.com/iotagenda/blog/IoT-Agenda/The-Challenge-Of-Securing-Building-Management-Systems (TechTarget, 2019)
24. Lighting the Way to a Smarter, Safer City. Accessed on Jan. 31, 2025 [Online]. Available: https://www.securityindustry.org/2018/09/14/lighting-the-way-to-a-smarter-safer-city/ (SIA, 2018)
25. Best Physical Security Software. Accessed on Feb. 1, 2025 [Online]. Available: https://www.softwareworld.co/physical-security-software/ (SoftwareWorld, 2025)
26. The Benefits of Fire, Life Safety and Security Integration, T. Giannini. Accessed on Feb. 4, 2025 [Online]. Available: https://www.buildings.com/industry-news/article/10189775/the-benefits-of-fire-life-safety-and-security-integration (Buildings, 2012)
27. PwC's 2024 Digital Trends in Operations Survey – Why significant business outcomes are still difficult to achieve – and what you can do. Accessed on: Nov. 9, 2024. [Online]. Available: https://www.pwc.com/us/en/services/consulting/business-transformation/digital-supply-chain-survey.html (PwC, 2024)
28. Risk is Dynamic, So Physical Risk Assessment Should Be Continuous, D. Young, M. Martin. Accessed on: Dec. 1, 2024. [Online]. Available: https://www.asisonline.org/security-management-magazine/articles/2023/11/dynamic-risk-assessment/continuous-physical-risk-assessment (ASIS, 2023)
29. The 15 Biggest Risks Of Artificial Intelligence, B. Marr. Accessed on: Dec. 1, 2024. [Online]. Available: https://www.forbes.com/sites/bernardmarr/2023/06/02/the-15-biggest-risks-of-artificial-intelligence (Forbes, 2023)
30. 8 challenges every security operations center faces, J. Burke. Accessed on: Dec. 1, 2024. [Online]. Available: https://www.techtarget.com/searchsecurity/tip/8-challenges-every-security-operations-center-faces (Tech Target, 2020)

**PRODUCED WITH GENER-
OUS SUPPORT FROM**

securityindustry.org