QUICK START GUIDE

Quick Start Guide to Physical Security

CompTIA

Introduction: Six Steps for Building a Robust Physical Security Practice

Business owners are often concerned over the protection of their networks, data, employees and visitors and, of course, their assets. Ensuring a safe and secure workplace is an important responsibility, not something they would just hand off to anyone. They look to those they not only trust, but who have the necessary skills to support their physical security systems and strategies – a prime opportunity for capable and knowledgeable solution providers.

Physical security is that often-hidden and somewhat forgotten, yet an extremely crucial part of the business infrastructure. And like many of today's solutions, the assessment and planning processes that occur beforehand are as important as the technology decisions they make. The top priority is to address each customer's specific organization needs and, when done properly, solution providers should experience exponential growth in their physical security practice revenue and profitability.

The opportunity is considerable. Like many of today's technology solutions, physical security has become an essential component of many businesses, with considerable value regardless of organizational size or vertical market. They are commonly found (or hidden, in many cases) in banks, retail stores, colleges and libraries, as well as in the corridors of virtually every office building and parking facility today. They have become such a commonplace fixture in the workplace that few people even seem to notice them anymore. Look around – that's opportunity.

While the market demand for video surveillance continues to grow at a rapid pace, traditional physical security methods are undergoing a transformation. Legacy analog devices are being replaced or incorporated into the latest IP-based digital technologies. Many companies are taking it slow, employing a hybrid platform strategy to make the transition more cost-effective. It also allows businesses to leverage the best features of both systems while building out their solutions.

That evolution is in full swing, creating new opportunities for providers who are willing to make the commitment – and the right investments. With other physical security-related technologies making similar analog-to-digital conversions (including access control, intrusion detection, fire detection and alarms, just to name a few), many channel organizations should find themselves well-positioned to profit from this "IT evolution." That is, if they have the skills and knowledge that business customers want…and need.

What does it take to build a profitable and customer-valued offering? This CompTIA Quick Start Guide, Six Steps for Building a Robust Physical Security Practice, details a number of industry "best practices" to help solution providers evaluate the opportunities and put the right pieces in place.

The Digital Revolution Creates a Channel Play for Physical Security

Transformation and market demand. Those are two key reasons physical security has become a more lucrative option for solution providers. Whether driven by new regulatory compliance measures or an interest in greater employee protection, businesses are more interested in surveillance and access controls than ever before.

In fact, the global market for these technologies projected to reach more than $100 Billion by 2020 with very strong annual growth (9.98% CAGR) according to a recent report from research firm MarketsandMarkets. Who better to connect the latest physical security technologies into a business' infrastructure than a skilled professional who already supports the network?

Consider the key elements that make up these solutions:

- Access Control
- Video Surveillance
- Perimeter Intrusion Detection
- Screening and Scanning
- Image data compression and analytics
- Data storage and backup

In general, solution providers are network specialists. That can be a significant advantage with the growth of Digital Security and Surveillance (DSS), but analog still controls a significant amount of the physical security space. Many businesses have made significant investments in their legacy infrastructure and, in some cases, continue to do so.

While the interoperability of IP-based technologies gives providers and end users a wide array of options when building security solutions, for many customers a "rip and replace" strategy may not be the best approach. Previous investments, budget constraints and organizational objectives all come into play.

Hybrid physical security systems, combining digital solutions with existing analog infrastructure, are proving to be ideal compromises or, in some cases, preferred options. Those who are most successful understand how to assess the unique needs of each business. They incorporate existing infrastructure into their solutions and develop transition plans that strategically replace previous technological investments.

Solution providers looking to build physical security practices need to understand that technological expertise is only part of the equation (the rest will be covered later).

PHYSICAL SECURITY PLATFORMS

Traditional surveillance used proprietary analog solutions based on legacy Closed Circuit Television (CCTV) technology. These legacy systems are typically sold in fixed-size ranges

that are tied to the number of cameras being deployed. Analog cameras require their own separate cables for video, control and power, adding cost and complexity to the installs.

These legacy surveillance systems – also referred to as CCTV (closed-circuit television) systems – include analog cameras wired into a DVR (Digital Video Recorder) using coaxial cables. A video monitor connects to the DVR so observers can watch the protected area. The recordings have transitioned from video tape to hard disk-based file storage over the last several years, but the units have not changed substantially.

DSS systems are much more flexible and readily scaled to meet the changing needs of business customers. A virtually unlimited number of cameras can be deployed through numerous buildings by leveraging existing computer networks. System limitations fall into two categories: (1) bandwidth and (2) physical security management application restrictions.

Advances in DSS camera technology continue to increase its advantages over legacy analog systems. The latest offerings are higher definition and offer improved coverage, digital zoom, remote monitoring and on-camera image processing. Many of these features and advances are not available on analog cameras– a major driver in the digital transformation.

IP Advantages over Analog Technology

	Analog Technology	IP-Based Technology	IP Benefit
Installation	Separate cabling requirements for video, control, power	One IP cable delivers video, control, power	Simplified installation, leverages your current IP infrastructure
Resolution	Max 704x480 (4CIF)	HDTV (720p/1080p) 5MP (2560x1920)	Highly scalable, flexible architecture. HD video capabilities improve coverage, accuracy Many new features/functionality compared to analog.
Scalability	Complex cabling requirements, vendor lock-in with proprietary systems	Simple cabling into existing network infrastructure, open standards based HW	DSS systems can be easily expanded as needs increase. Open standards give providers a variety of vendor options.
Security	No encryption or authentication	Encryption and multi-level access control	Your data is secure and safe from outside manipulation
Cost	Lower cost cameras, but potentially higher labor and HW costs	Advantages in cost of installation, economies of scale for larger systems	As DSS systems scale, they provide a lower total cost of ownership with more advanced capabilities

The structure of a digital surveillance system differs in several ways from their analog counterparts. With smaller systems, the topology of each is quite similar. IP-enabled cameras communicate with an NVR (Network Video Recorder) using a LAN (local area network) connection. VMS (Video Management Software) on the NVR controls where captured footage is stored/saved internally and/or offloaded onto a network attached storage (NAS) device. The NVR provides end users with camera monitoring capabilities and allows them to control various aspects of the system.

The primary difference with digital platforms is that everything is connected to the IP standard network, while a separate coaxial cable is required to manage analog systems. Many digital cameras are PoE (Power over Ethernet) capable, which eliminates the need for separate electric cords.

A number of the available NVRs also have a limited number of analog inputs that allow customers to plug in some of their legacy cameras (analog). These devices are typically referred to as "hybrid" NVRs.

For larger systems, or systems requiring advanced capabilities, the NVR is often replaced with a more powerful standalone video server running an independent VMS package. Legacy analog cameras can still be integrated into the system using video encoders to translate the analog streams to IP protocol. And the VMS controls all aspects of the system including client PC monitoring and storage of video to network based storage devices.

These types of systems can scale to thousands of cameras across multiple campuses, with monitoring from unlimited remote locations and device types. They are also able to support some of the more advanced analytics features described in the accompanying sidebar.

Security Surveillance Solutions Comparison

	Analog CCTV Systems	Hybrid Analog + Digital Systems	Digital, IP-based Systems
Descriptions	Analog cameras send CCTV signals to a DVR (which uses disc-based storage)	Uses a DVR that can also accept analog video. Allows digital and analog cameras to use a single platform	Uses industry standard IP protocol to connect devices to the LAN. Smaller installations can use a dedicated NVR to capture and transmit video. Larger installations send video to a PC server and use VMS software to monitor and record.
Advantages	Mature technology. Low-cost equipment available from a wide range of vendors.	Leverages and preserves previous investments. Offers some digital features.	Highly flexible, scalable architecture. HD video capabilities, improved coverage and accuracy.
Disadvantages	Hard to scale Limited features/ functionality Lower resolutions Distance limitations	Hard to scale. Features/functionality, resolutions and distance limitations based on legacy technology	Newer technologies not compatible with existing analog systems. Cost premium over analog cameras.

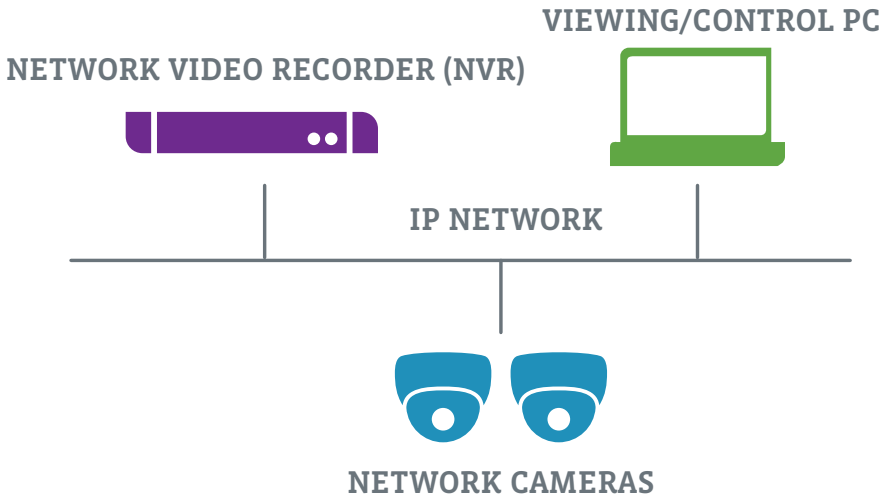

Figure 1: Topology utilizing a Network Video Recorder (NVR)

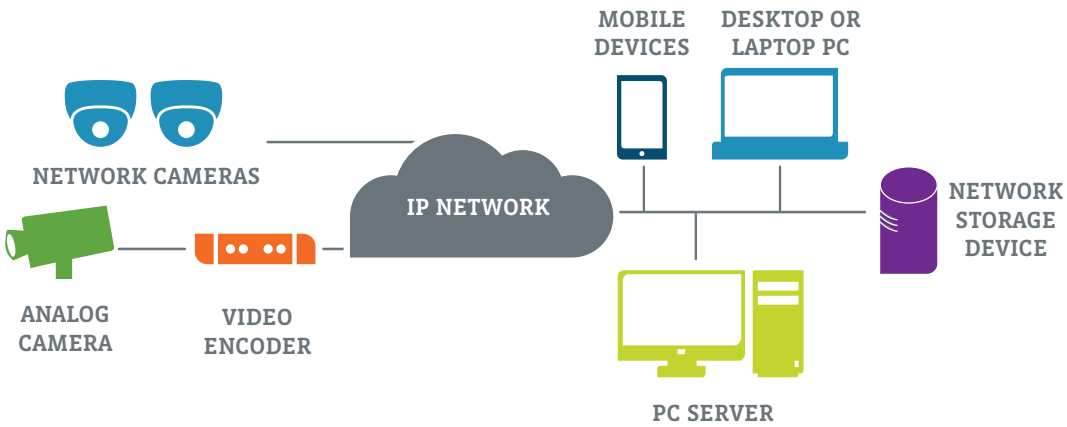

Figure 2: IP-based video server topology

Video Analytics: Create Real Customer Value

By some estimates there are more than 30 million cameras in the world capturing more than 250 billion hours of raw video footage each year. That is a staggering amount of information! Much like the early days of the Internet, before the rise of search engines, the sheer volume of data is simply overwhelming for businesses to grasp. But many are learning that by harnessing and leveraging that information, they can improve their operations or meet specific compliance requirements. Solution providers who can help their customers better organize and make sense of all their surveillance footage have a unique opportunity to drive more installs and increase their sales opportunities. That's where video analytics comes in.

These solutions, often referred to as Video Content Analysis (VCA), are used to scrutinize large amounts of captured video data – either in real time or from storage. They allow organizations to extract useful business or security-related details that can be utilized in a couple ways:

1. **Enhanced security** – By implementing security functions such as virtual trip wires, facial recognition and license plate detection – video analytics can be used to make an environment more secure and aid in ongoing criminal investigations. This information can help investigators zero in on critical footage or related content without having to sort through thousands of hours of video. For example, once they identify a suspect's face or license plate number, the analytical solution can quickly sort through and identify other footage that contains the same person or vehicle. That saves the investigators countless hours and a tremendous amount of frustration.
2. **Business decision process** – In addition to providing enhanced security and aiding in criminal investigations, video analytics is making a valuable contribution to the business decision-making process. Some commercially available analytics solutions can utilize network video cameras to obtain accurate customer counts and monitor store traffic flow and patterns. They can measure customer or employee "dwell time" at key locations such as checkouts, and analyze customer queues and waiting line patterns. This intelligence can help businesses improve staffing and resource level planning, allow them to optimize store layouts, and make other crucial operational decisions.

The latest NVR appliances typically include basic Video Content Analytics capabilities, as do many standalone VMS packages. A number of vendors specialize in expanding the analytics capacity of these systems and offer training programs to their channel partners. This is a real opportunity

area for solution providers, offering a value add that many of their businesses customers could benefit from. Not only can they address their clients' physical security concerns, but these advanced analytical capabilities allow them to highlight trends in their businesses.

With that information in hand, customers can bolster their defenses and strengthen their marketing and sales strategies– leading to a safer workplace and increased revenue opportunities.

Solution providers who are capable at designing, implementing and managing these advanced analytical solutions will have a distinct advantage over those offering physical security services alone. With more complex technologies, compliance concerns and general business needs, organizations are relying more on skilled outsource partners to help them handle it all.

The Digital Transformation May Take Time

As compelling as the advantages are for DSS, the changeover has not happened quickly – and it still has a long way to go. A major reason for such a slow transition (more than ten years, and counting) is businesses' continued reliance on security dealers for systems and support services. That community has a long history with legacy analog solutions and is deeply invested in maintaining that infrastructure. Dealers understand how to market, sell, and service that equipment and, while digital surveillance may be hold some interest, it's not a core competency for most–, at least not yet.

Security dealers seldom have much experience with internet services, servers, storage, and networking, and making that transition is neither quick nor easy. Add to this the fact that – as is the case with most technology innovations – legacy analog solutions still enjoy somewhat of a cost advantage over the new digital platforms. The largest differential is with cameras. The analog versions are readily available from a number of vendors at a very low price point.

If advanced security or analytics capabilities are not required – the lower cost analog solution may be "good enough." DSS may be a tough sell for the cost-conscious business owner. But the price gap is closing quickly and digital-based video cameras are expected to be on par with analog devices within the next several years.

Even though the benefits of DSS far outweigh the legacy equipment, some buyers will require highly compelling reasons to discard their existing sys-

tems. A hybrid approach may work well for those customers, allowing them to integrate the latest digital technologies with their existing infrastructure–a conservative option that leverages past, current and future investments.

The DSS market provides a compelling growth opportunity for solution providers who are looking to leverage their existing competencies in networking, storage, managed services and cloud computing. Physical security presents an opportunity to grow "wallet share" and "mindshare" with existing customers who are almost certainly buying security solutions today. A physical security offering also allows providers to attract new clients and expand into new and more lucrative markets (i.e. financial, education, healthcare).

When surveillance technologies are incorporated into useful business solutions, providers can boost their recurring services revenue, traditional product sales and their support contract options. For example, by leveraging cloud-based storage, they can backup digital content files into a safe and secure location for their clients. They can employ managed services to ensure their customers' security systems are up and running at all times. And, with high-resolution digital video capabilities, providers can sell incremental analytics services including identification, situation awareness, behavior analysis, traffic flow and other advanced capabilities.

The key to success in DSS is to offer a comprehensive portfolio of solutions and support options. Not just the cameras, recorders, storage, networking, and infrastructure solutions required to effectively manage these systems – but the core IT offerings every business customer needs. Physical security practices allow providers to expand their vertical expertise and spark deeper conversations, the discussions that lead to more long-term business opportunities.

Terms and Associations for Physical Security Pros

ABCHS (American Board for Certification in Homeland Security): members include active and retired military, law enforcement and security experts, first responders, and others dedicated to national security

Codec: a device or computer program for encoding or decoding a digital data stream or signal

DVR (Digital Video Recorder): device used to capture and store video from analog cameras (includes hard drive)

Hybrid DVR: Digital video recorder that can also accept analog video inputs

NVR (Network Video Recorder): used to record digital video streams coming in on the IP network to local or network storage

ONVIF (Open Network Video Interface Forum): an organization focused on developing a global standard for the interface of DSS products and access control

PSIA (Physical Security Interoperability Alliance): an organization whose mission includes the development and promotion of standards for video analytics, recording, and content management

VCA: Video Content Analysis enables capabilities such as virtual tripwires, left-baggage detection, wrong-way lane detectors, people counting systems

VMS: Video Management Software provides for system control and configuration, viewing of content, and video analytics

Six Steps for Building a Valued Physical Security Practice

Based on the research and required skill sets, surveillance and access control technologies represent a real business opportunity for the channel. Demand for physical security systems, especially the latest digital solutions, is growing in the business community. Regardless of vertical or organization size, these technologies fit perfectly in the general solution provider portfolio of service offerings, the perfect complement to network and managed services support. With that in mind, how can a solution provider determine if a physical security practice makes sense for his or her particular business? These six steps will help them evaluate the opportunity and start building a viable strategy:

STEP 1. RESEARCH YOUR OPPORTUNITIES

As solution providers should do with every major business investment, spend time assessing the sales potential for physical security solutions in their particular markets. Are current clients already employing systems? If so, identify the company providing and supporting their platforms as well as the specific technologies they are utilizing. Does the existing system solve their current and future business needs? Perform a basic assessment of their infrastructure, including the number of analog and digital cameras, access controls and whether they're employing DVRs or NVRs.

There are three key factors that will help solution providers determine if they have a real opportunity to sell physical security to existing customers: recent investments, legacy infrastructure, and business goals. While the first two seem quite similar, some business clients may be reluctant to replace their older systems if they appear to be in good working order and there is no logical business need for replacing them. That's why it's so important to ask customers what they like and dislike about their existing physical security solutions. Are there features they need or are they looking for certain upgrades in the future?

This is also a good time to take a deeper dive into the technologies, skills, and competencies required to be successful in this space. Many of the aptitudes needed here may already be covered and any training investments will likely complement their existing services portfolios. Network, server, and storage could be current areas of strength. Video formats and standards, camera and access control technologies and installation will likely be new, requiring training and educational investments.

Once providers complete their research and gain a higher understanding of the opportunities, an initial financial analysis should be conducted to determine the potential impact this type of practice could have on the bottom line. The results of that process should help determine if a physical security practice makes good business sense, and whether they should move forward with the remaining steps.

STEP 2. IDENTIFY SOLUTION AND SERVICE OFFERINGS

Once a solution provider has completed the research step and decided that the DSS opportunity is attractive enough to move forward, it's time to identify the specific solution set and service offerings the firm needs to develop and offer its own customers. Turnkey systems provide a quick and easy entry into the space, though they may be limited in capacity or scalability. These areas typically self-contained NVRs that integrate a video server and storage with video management software (VMS). An alternative approach is to provide a customized DSS system tailored to meet the needs of each individual customer's facilities and business needs.

A best practice for evaluating those options is to engage in discussions with the vendors of the equipment you're interested in selling and supporting. Review their documentation, training processes, and partner and customer success stories. Be sure to evaluate the vendors on their physical security offerings and feature sets, as well as their technical, sales, and marketing support.

Finally, consider what service offerings you could logically attach to surveillance and access control solutions. Depending on vertical expertise and skill sets, that may include physical security assessments, installation, monitoring services, periodic camera cleaning and maintenance and advanced video analytics. Many of these could be bundled into a recurring revenue service to better

Expert Recommendations

1. **Think Long-Term:** make a commitment to your physical security customers. Build a solid reputation and expand your offerings.
2. **Attend Industry Events:** immerse your team in physical security knowledge, training and peer discussions. Vendor and distributor conferences offer opportunities to learn best practices, explore the latest technologies and discuss business concerns and opportunities.
3. **Develop Strong Vendor Relationships:** work closely with suppliers, especially when launching a new practice. Leverage training and support programs, as well as sales and marketing resources.
4. **Stay Positive:** don't criticize your prospects' previous physical security investments or other providers they have worked with. Focus on the working parts of their existing infrastructure and, whenever possible, incorporate them in proposed new solutions.
5. **Get Certified:** the best way to build a solid reputation in the physical security space is through technical and solution expertise. Learn as much as possible about designing, installing and supporting these systems if you want to succeed.
6. **Join Associated Groups:** affiliate with like-minded physical security professionals and build your business' credibility. There are several to choose from, so ask vendors and peers which are most relevant in your region (noted in another sidebar).
7. **Support Your Community:** get involved in local activities and take a genuine interest in law enforcement. Join the area Crime Stoppers effort or offer to teach seniors about home security. If possible, ask to do a "ride-along" with local police to learn about criminal activities in your community and to gain valuable best practices to better protect your business clients.

support your customers' needs (and to build a more profitable DSS business).

STEP 3. EVALUATE AND CLOSE POTENTIAL KNOWLEDGE AND SKILLS GAPS – HIRE, TRAIN AND PARTNER

Once the solutions, services, and vendor options have been evaluated, it's time to review internal resources. First off, providers need to identify and close any potential skill gaps that could hinder the launch and long-term success of their DSS practices. As is always the case, there are three primary methods for addressing this issue: 1) train existing staff on these solutions, 2) hire new staff members with those particular talents or 3) partner with other solution providers or experts with those skills.

Some of the more common gaps IT firms may find include:

- **Security practices and policy:** Before starting a physical security practice, solution providers must understand standard best practices, as well as laws and regulations for all the jurisdictions they work in (customer locations as well). Federal, state, and local governments may each have their own regulations – especially as it relates to video surveillance – so you need to research these carefully and ensure your company is prepared to meet all known requirements. In some states, counties or cities, licenses may also be required to sell and install security equipment.
- **Video and camera technology:** Solution providers have to have a solid understanding of video technologies– both analog and digital – including formats, codecs, and streaming and storage protocols. You need to know how the cameras operate, their inner workings and maintenance requirements. Providers must be able to properly specify, place, install, and configure cameras based on resolution needs, required coverage, operating environment, and lighting conditions. Each is critical to the performance of the security solution. Many vendors provide the appropriate education and certification programs that give their partners the foundation they need to get started, as do several of the distributors with physical security divisions. Some even offer the design and system configuration assistance providers often need, especially when just starting out. Ask peers and industry experts for recommendations and spend some time evaluating the available programs.
- **Video Management Software (VMS) knowledge:** In the end, the applications and their capabilities define the physical security solution and its business value to your customers. All technical, sales, and marketing personnel have to fully understand the features, functions, interfaces, and technical capabilities of the chosen system. The experience is essentially what your team will be selling and supporting. Many of the leading VMS vendors offer extensive training and certifications that will boost your company's expertise. Providers who take advantage of these programs will build their industry knowledge and increase their credibility with end customers.
- **Job estimating and bidding:** Positioning a VMS solution for a particular business is an essential element of closing the sale, but accurately estimating and bidding the job often determines whether or not the project will be profitable. This can be a risky proposition for most solution providers, likely one of the toughest gaps they'll have to bridge. The challenge here is that many of the potential problems when estimating physical security projects are "construction trade" issues, not technology related. Imagine installing 25 cameras across a campus with some mounted outdoors on high poles that must be securely set in the ground and others fixed in high rafters and placed on mounts drilled in exterior concrete walls. Some of that equipment might require underground cabling or unique channeling. Most are activities IT solution providers rarely, if ever, have to deal with. Consider how much time, money, planning, approvals,

safety, equipment, and insurance are required to complete this type of project. Those are just a few reasons providers often partner with construction or cabling contractors with proven expertise in these areas. Want to ensure potential alliances and projects are both successful? Include the job estimating and bidding process in partner project agreements, in addition to the details and requirements for installation.

STEP 4. DEVELOP A MARKETING PLAN

A great starting point for building a physical security practice is to start with existing clients who are already consuming these services. They also make a good initial target audience for your DSS marketing plan. While these customers may be fairly familiar with your IT services, be sure to remember they will need a proper introduction to your latest security offerings. Some may already have a security provide, so you have to be prepared to deliver a more compelling value proposition. What benefits would they receive transitioning from their old analog systems to the latest in digital technologies?

In other words, the value propositions you promote must extend beyond simply adding a physical security platform. Focus on the business benefits of an IP-based DSS solution and your company's ability to support their comprehensive technology needs. For example, develop a value proposition based on the improved coverage and accuracy of HD video, showing customers and prospects how it can reduce both their risks and costs. Similarly, highlight the use of advanced video analytics to drive improved business intelligence, if it makes sense for your clients and markets. Consider promoting the profitability angle as well, showing how the "business intelligence" capabilities of these advanced solutions could boost their bottom lines.

To attract new customers, develop a plan that builds your company's credibility as an expert in DSS. You might start an online marketing campaign, buying search terms and developing a blog that covers key issues SMB organizations face related to physical security area. Spread the word, tell your community why DSS technologies are solid business investments and why their particular companies could benefit from their installation. Don't forget to highlight your new practice and expertise on your own website, as well as in your sales and marketing collateral.

Finally, look to leverage your chosen distributors and vendors for incentive and funding programs, marketing assets, and co-marketing materials that can be utilized in your own marketing campaigns. Explore all the resources at your disposal and make good use of no or low-cost materials.

STEP 5. PREPARE AND UNLEASH THE SALES TEAM

In parallel with the development of the new practice's marketing plan, solution providers should also be readying their customer engagement strategies. A successful DSS solution launch requires careful preparation of everyone in the organization – especially for those charged with selling it to customers and prospects. Your physical security success lies with the sales team. They make the connection and create the dialogue that, if the alignment is right, get businesses to sign on the dotted-line.

In the physical security field, which requires training, certifications and sales tools that enable your team to easily demonstrate the value of DSS solutions to customers. Develop sales presentations and collateral around their particular offerings, as well as demo and trial programs that help close deals.

Each sales professional should be prepared to discuss the analog to digital transition and how that might fit each customer's business needs. Some may desire a gradual conversion to DSS solutions, utilizing as much of their past investments as possible while gaining some of the features and capabilities they need from the new platforms. The hybrid model is an attractive option for potential customers, and your sales team will play a crucial role in "connecting the dots" based on

each prospect's unique value need. That process starts with discussions around business goals and past investments in their physical security infrastructure, and continues along until your team delivers a plan that makes the best financial and operational sense for the customers.

Sales teams have to think of every new engagement as a service opportunity. Should the solution include maintenance, storage, and analytics add-on services? If it creates value and ensures a more successful customer experience, the answer should be a resounding "yes!" The win-win scenario is just as applicable in physical security as it is with other IT solutions.

The final step of building a physical security strategy is reviewing and possibly amending compensation plans. Are your existing incentives going to help or hurt your DSS solution goals? Depending on the mix of expected product resale and services revenue, the compensation plan may need to be adjusted. Run the numbers and get feedback from the sales team. Are they excited about the opportunity to sell physical security? Will the incentive package hurt or help sales of your other IT solutions? Check with vendors and peers for recommendations and be willing to amend your plan along the way, if needed.

STEP 6. SCALE AND ENHANCE

Once steps 1-5 have been completed, you should be ready to launch your DSS business. Start rolling out the marketing campaign to existing customers and elicit their feedback. Engage a few clients at a time and start a "beta program" with the initial group. That will help your team gain experience in critical system design, project estimation, installation and configuration.

Once those projects are complete, assess whether they were as profitable as planned. Take into account that the processes were being developed with the initial group, so future installs should require less time and effort as the team hits its stride. Be sure to document all installation procedures (or at least those that will be repeated in the future) for training and process improvement purposes. That also gives your team the ability to adjust pricing for future DSS system bids – helping to ensure those projects and the business unit remain profitable.

References

MarketsandMarkets, Physical Security Market by System (Access Control, IP Video Surveillance Software, Locks, PSIM, PID), Services (System Integration, Maintenance & Support, and Designing & Consulting), Vertical, and Region - Global Forecast to 2020.

http://www.marketsandmarkets.com/Market-Reports/physical-security-market-1014.html?gclid=CM3Typfn6csCFVGAaQodWeoIHg

SOLUTION CONSULTANT/CONTRIBUTOR:

Jason Destein CHS IV, CNTA Advanced Solutions - Physical Security Partner Technical Enablement Ingram Micro

About CompTIA

CompTIA is the voice of the world's information technology (IT) industry. As a non-profit trade association advancing the global interests of IT professionals and companies, we focus our programs on four main areas: education, certification, advocacy and philanthropy. Our purpose is to:

- Educating the IT channel with our educational resources that are comprised of: instructor-led courses, online guides, webinars, market research, business mentoring, open forums, networking events, as well as helping our members advance their level of professionalism and grow their businesses.
- Certifying the IT workforce as we are the leading provider of technology-neutral and vendor-neutral IT certifications, with more than 1.4 million certification holders worldwide.
- Advocating on behalf of the IT industry. In Washington, D.C., we bring the power of small and medium IT businesses to bear as a united voice in helping our members navigate regulations that may affect their businesses.
- Giving back through philanthropy, our foundation enables disadvantaged populations to gain the skills needed for employment in the IT industry.

Our vision of the IT landscape is informed by more than 25 years of global perspective and more than 2,800 members with more than 2,000 business partners spanning the entire IT channel. We are driven by our members and led by an elected board of industry professionals.

All proceeds are directly reinvested in programs that benefit our valued members and the industry as a whole. Headquartered outside of Chicago, we have offices across the United States; as well as Australia, Canada, China, Germany, India, Japan, South Africa, and the United Kingdom.

For more information, visit CompTIA.org.

CompTIA

CompTIA.org