WHITE PAPER

The Paybacks of Carefully Planned Security Technology Implementation

By Brock Josephson, PSP

When done right, enhanced electronic security can lead to increased operational efficiencies and reduced insurance premiums. This explains the surge in investment in advanced electronic security systems. Yet, adopting the technologies that provide security and operational benefits can be overwhelming.

Choosing the Right Technology

In many ways, the electronic security industry is like the .com companies of the 1990's. In the last 10 years the world has been flooded with more security technology than ever before. According to an IHS Market video surveillance report, the number of professional surveillance cameras shipped has increased by 10 times between 2006 and 2016 from 9.9 million in 2006 to over 106 million in 2016 and is expected to reach 160 million annually by 2020. Other security related products have seen similar growth.

Like with the .com boom, sadly many of the companies in the market today promise technologies that do not perform as advertised and will likely not be around 10 years from now. Investing in the right security technologies can bring significant security, operational and financial benefits to the organization. Investing in the wrong technologies can result in wasted capital, frustrated stakeholders and managers, and increased security vulnerabilities.

Developing an effective technology strategy prior to the procurement and deployment of electronic security systems is key to avoid these negative outcomes. Proper planning prior to design or deployment of the technology is necessary and must consider the following:

- **Develop** clear and measurable performance metrics for each security system
- **Identify** technologies that meet performance metrics (on paper) and shortlisting a viable number of testable options.
- **Test** potential technologies for performance, robustness and ability to integrate into your security system.
- **Prepare** the system deployment, maintenance and training.

Before we dive into these planning milestones, it is worth exploring how the planning phase fits into the larger project picture:

Phases of a Security Enhancement Project:

- Identify the Security Need
- Project Planning
- System Design
- Training and Implementation
- Assessment
- Maintenance

If the project planning is done correctly, then you set the course for a successful overall enhancement project.

Development of Performance Metrics

Once the decision is made to increase the electronic security, there is a tendency to start researching viable technologies immediately — but don't do it! Like any good realtor would tell you, don't go house shopping until you know what you want and what you can afford (and really need), otherwise you're likely to end up with a flashy house that is too expensive and doesn't meet your needs.

In much the same way there are a lot of technologies out there that look very enticing but could become very costly and restrict your ability to implement other technologies in the future. Before you start looking at solutions, it's smart to develop a list of metrics to score potential solutions.

Performance metrics can generally be broken down into one of seven categories:

- **Functionality** – These identify how the system will function and typically carry the most weight in the decision-making process. These can include metrics such as device range, rate, speed, coverage and capacity.
- **Environmental** – These identify how the system holds up to the elements and typically includes metrics such as ingress protection (IP) ratings, temperature ratings and vandal resistance.
- **Usability** – This include metrics such as ease of installation, ability to integrate with other systems, etc.
- **Communication** – This includes metrics such as supported communication protocols, data encryption standards, bandwidth and storage used.
- **Costing** – This includes purchase price, installation cost, ongoing maintenance, training and total cost of ownership.
- **Viability** – This includes metrics such as manufacturer's years in business, minimum number of units deployed in similar environments and minimum technology readiness level.
- **Business Value Add** - Are there any value adds beyond security to consider, such as increased operational effectiveness, decreased insurance premiums or increased customer satisfaction.

Performance metrics should be developed with feedback from as many stakeholders as possible. Stakeholders will vary from organization to organization, but typical roles include: systems and security operators, operations, information technology, compliance, law enforcement liaisons, engineering and executive leadership.

All these stakeholders to do not necessarily need to be involved in the day-to-day execution of the project; however, soliciting these stakeholders for feedback on system criteria they would like to see will help an organization obtain buy-in on the project. It may also be possible to earn some goodwill by providing a benefit beyond security to some of the stakeholders.

The more each metric can be understood and quantified relevant to the individual stakeholders, the better. This will better inform decisions on which technologies to implement and how to implement them to maximize system effectiveness across the entire organization.

Business Value Add

Without fail, each organization deals with stakeholders who are generally resistant to increased security measures. This resistance is generally not unfounded as security can sometimes create burdens such as decreased operational effectiveness, increased costs and no additional revenue.

These biases can be difficult to overcome. But identifying operational benefits, or introducing cost savings and/or revenue producing measures as an added benefit to the increased security, can go a long way in establishing good rapport and gaining stakeholder buy-in. Here are just a few examples of value adds of security technologies to other aspects of operations:

- Video analytics used to count customers entering a store and predict upcoming teller requirements before they are needed.
- Buried vibration sensors used to detect faults on a buried transmission line, significantly decreasing the time required to identify the location of the fault and allowing for faster repair of the lines.
- Ground based radar used to detect wildlife along a roadway and notify drivers to slow down and use caution.

- Thermal cameras used to measure the temperatures of transformers and notify operators if they raise above a specific level, allowing operators to conduct maintenance before overheating inflicts major damage to the transformers.
- Cameras with analytics used to detect the level of fluids in a tank and notify operators if the level gets above or below certain levels, thereby reducing costs of sending personnel to the tanks on a regular basis to check the fluid levels.

These examples may not apply directly to all businesses. More than likely, some operational benefits that can be identified with any given security program, further supporting stakeholder buy-in.

Shortlisting Technology

Before investigating new technologies, an organization should determine if any technologies currently deployed can be used to meet the new security requirements. This can be accomplished by simply comparing the currently deployed technologies to the metrics identified earlier. The goal should be to minimize the number of technologies implemented to reduce the overall complexity of installing and maintaining your system.

Once an organization has determined that current deployed technologies will not work, it is time to begin evaluating outside products to meet the new performance requirements. The list of security technology providers is generally too long to allow testing of every potential solution. So, before investing significant resources in any level of design or testing, the list of potential products must be narrowed to a manageable number.

To reduce the list of potential solutions to a manageable level it is necessary to create a list of qualifying "yes/no" questions that can be answered with minimal time researching specific products. The questions should reflect the performance metrics outlined earlier. An independent security consultant can assist in the process of developing the questionnaire and shortlisting technologies if needed. Once the list of questions and answers has been developed, any technology that fails to meet the criteria should be removed from further consideration.

The goal at this point should be to shortlist the technologies to no more than 2-3 times the number of technologies an organization believes will be viable to test. In most cases this is somewhere between 5 and 15 technologies. If the list is too long, then adding additional qualifying "yes/no" questions may be required. If the "yes/no" questions eliminate all but one or two technologies, an organization may consider reevaluating your shortlisting criteria.

Next, an organization must develop a scoring matrix to rank technologies that pass the "yes/no" questionnaire. The matrix should incorporate all performance metrics already discussed and may be constructed using either a ranking system or a weighted point system based on which criteria has the highest priority for your organization. Regardless of how the scoring system is constructed, the result should lead to a justifiable ranking of each candidate technology.

Testing Technology Performance

Once a few technologies have been shortlisted the next step in the process is to conduct an on-site test, or pilot, of the top two or three technologies in the ranked list.

The pilot serves a distinct purpose. This is to determine if the technology can deliver what it has been promoted to accomplish. The technology needs to operate in its designated environment as expected. If it doesn't, it may be a waste of time and money to implement. Worse, it may increase, rather than decrease, a facility's overall vulnerability.

The pilot should assess not just performance but system integration, ease of installation and operation, reliability, environmental protection, and maintenance requirements. Effectively writing test procedures for all these metrics requires an understanding of how the technology works. This knowledge helps an organization better grasp the limitations of the technology and write tests that reveal their limitations and highlight their strengths. Every technology has weaknesses, so revealing a limitation should not preclude a technology from use — identifying the weakness will help anticipate the need for supplementary technologies and procedures to mitigate the risks presented by the weakness of that technology.

When planning the tests, it is important to consider the following guidelines:

- Incorporate as many methods of defeat as practical.
- Run multiple repetitions of each to determine technology consistency.
- Conduct tests in environments similar to real-world deployment environments.
- Test across as many weather and environmental conditions as feasible.

As tests are conducted, an organization should denote the results of each test and document any conditions or results that were unexpected in a test report. The test report should also include a description of the testing procedure, a description of the technology being tested, how it is to be deployed for the test and how each test phase was performed. Once performance testing has been completed on each technology, results can be compared and incorporated into the scoring matrix developed earlier.

Planning Ahead With Burn-In

After performance testing is complete, an organization should implement a more in-depth burn-in test to evaluate environmental factors and additional functionality.

A burn-in test entails long-term testing of performance and system robustness. If the system is deployed outdoors, burn-in phases should test the system's ability to perform during both the hottest and coldest months of the year. Running performance tests during periods of extreme weather, including heavy rain, snow and fog, is also advised as many systems experience decreased performance during adverse weather.

The burn-in phase is also a time to closely monitor undesirable system behavior such as down-time, false alarms, nuisance alarms, poor image or video quality, incorrect classifications or lost data. Monitoring this information helps an organization better predict what efforts will be required to properly program and tune the system and may also reveal some system vulnerabilities not identified in the initial functionality. What is learned during the burn-in phase assists in planning for system deployment and in some cases may affect the decision to deploy a system.

Integrating New Technology

Integration is essential to seamless operation whenever multiple technologies are involved. Whether the integration is a simple relay trigger from the sensor to the access control software, or a software integration bringing geospatial data into a map interface and triggering different events based on criteria defined during programming, the integrated system should be tested as part of the pilot.

If the technology is a sensor, a tester may monitor alarms at the sensor level and the system level during the burn-in phase. Then, they may compare to see that all alarms are making it through to the head-end operating system.

During the integration phase, it can be worthwhile to begin incorporating and testing integrations with any other systems that may also benefit from the implementation of the new technology. If the devices will have shared access and/or shared control, organizations should work out the polices and procedures for accessing and/or controlling the devices so that everyone who has a stake in the system understands their access rights and limitations before it goes live.

Scaling the System

For large scale projects, organizations may want to conduct a scale test, especially if the project calls for a quantity of systems greater than what has been deployed by the manufacturer in previous scenarios. A scale test assesses the system's capacity to handle the traffic produced by many devices. This will confirm the load-bearing capability of the software, as well as identify functionality issues that may not present themselves with just a few units. Scale testing also helps uncover issues that may occur when many systems are integrated.

Setting up sufficient hardware to run a full load test can be difficult, especially when it is necessary to deploy the system at many sites. To simplify this process, virtual devices may be able to be replicated in a simulated software environment at minimal cost. Scale testing can require some effort but working with the manufacturer and a security consultant can assist in conducting a successful scale test.

Developing Training

Training on system operation is an often-overlooked key to system implementation strategy. Organizations should avoid waiting until after a technology is decided upon to conduct operator training. Instead, training should be included as part of the evaluation criteria. Operators can provide vital insight into the overall usability of a system. Many technologies have been purchased and installed only to be abandoned shortly thereafter because they were too complex to operate, or the operators were never trained properly.

Depending on the size and skill of an operating group, an organization may consider assigning only a few operators to train on and test the new technology during the pilot or burn-in phase. If the same operators test multiple technologies, they may be asked to provide feedback on which they prefer and why. This information can then be incorporated into the overall scoring matrix. If other stakeholders beyond security will have access to the system, now is the time to train them on how to properly access and interface with the system.

Conclusion

Developing a strategy before deploying any electronic security technology is key to any implementation effort. Clear and measurable performance metrics allow organizations to identify and thoroughly vet technologies. Conducting comprehensive testing means the odds of successful product selection and implementation are increased.

By incorporating a strategy for continual adoption of new technologies into your existing security technology strategy, your organization lowers costs, invests more effectively and gains stakeholder buy-in. Ultimately, these efforts made on the front end of the project will provide benefits later on, such as faster and more predictable implementation, improved overall functionality of the integrated security system and additional business value to the organization.

About Burns & McDonnell

Burns & McDonnell is a family of companies bringing together an unmatched team of engineers, construction and craft professionals, architects, and more to design and build our critical infrastructure. With an integrated construction and design mindset, we offer full-service capabilities. Founded in 1898 and working from dozens of offices globally, Burns & McDonnell is 100% employee-owned. For more information, visit **burnsmcd.com**.