Real Time Networks

6-Step Security Solution Purchasing Process

How to Get Maximum Value from Physical Security Systems

As competition across sectors gets tighter businesses need to extract the maximum value from every operation. That includes their physical security.

Businesses need to run their security strategically, like a business unit, focused on their customers and the marketplace. Seen previously as just a cost center, security can, and should, be seen as an investment source for long term cost savings.

Applying this strategic perspective therefore impacts how businesses purchase physical security technologies. They need to recognize that they are purchasing a system that will impact operations and performance at nearly every level. So as with other capital expenditures, they must ensure that new security systems maximize their value to the business as a whole. That means purchasing according to an expected Return on Investment (ROI).

> “Reliability actually saves you money over time.”

Considered this way, the long term reliability of both the product and of its support services becomes the most important quality to consider. As one veteran security professional of both law enforcement and hospitality put it, businesses that care about long term growth “need to understand that reliability actually saves you money over time.”

This report is compiled with input from professionals in law enforcement, technology, and the hospitality sectors. It details best practices for financially responsible security technology purchasing, and how to calculate an individual organization’s ROI for each technology. This report aims to help deliver the greatest long term, positive financial impact from capital security expenditures.

The Security Purchasing Process

Involve the Right People

By their nature, capital expenditures—security or otherwise—impact businesses in several ways. Most obviously, they can consume a significant portion of their budget. Major security technologies also impact operations across the entire organization over their lifecycle. But without proper planning some of this impact can be negative. For example, modern security technologies are now almost always network-integrated. What impact will their deployment have on the IT department? Will it cause any conflicts with their upgrade schedules?

It is always correct to invite stakeholders from departments that will be involved in the system's deployment and ongoing use. For example, planning to purchase a major network-based video surveillance system should involve the IT department whose infrastructure it will in part use. Or surveillance video systems could also have customer service uses in hospitality and gaming. If the type of system is new to a particular business it may also be useful to include the finance department from the very beginning so that they can assist in sorting through budget and tax implications, before any ROI calculations are attempted. Those departments could bring valuable insight to the purchasing process.

> "It is always correct to invite stakeholders from departments that will be involved in the system's deployment and ongoing use."

Value-based Purchasing Considerations

- **Quality**
  Does it generate actual value for the organization? Industry experts point out that much of the top tier of products are fairly close together in terms of physical quality. The primary quality differentiator is the level of support delivered by the service provider.
- **Longevity**
  How long will it generate value? Higher quality hardware will perform more consistently over time. Also, support levels matter here the most. If a service provider is not able to restore service rapidly, their client's business performance degrades with each outage.
- **Cost Effectiveness**
  Will the total value generated exceed initial investment? Researching, preparing, and calculating Return on Investment (ROI) are key to determining cost effectiveness. As one expert puts it, "Quality is paramount, but you never want to overpay."
- **Industry-Specific Features**
  No two businesses are alike. So while much of the top tier of products are fairly similar, there are some feature differentiations. One business may need real-time location services on security guards. Another may need short range wireless exit alarms on keys or other assets.

Searching

If reliable price estimates are already on hand, then product searching can be delayed until after ROI is calculated. If not, it is important to conduct at least a preliminary product search first.

Vendors can supply a range of information, but it is important to also collect it independently. Experts recommend seeking out a few different sources of information for each initial service provider under consideration:

- Collect opinions from security contacts both in and outside of the industry
- Interview service providers' existing customers
- Product data sheets
- IT data sheets

From these sources it is important to record a few things:

- Scope of service and support
- Deployment timeframe
- Deployment impact on organization

Prepare a Security ROI Analysis

Security professionals usually already know what technical threats they face at their organizations. The problem is that technical security threats on their own do not constitute a business case for a capital security expenditure. Unless the investment proposal is framed in terms that matter to executive leadership it may not get approved. So technical security threats must first be translated into business risks.

Strategic capital expenditure planning is key to an organization's ability to generate and sustain value. So it is important to understand what kinds of return are possible investing against security threats. The returns broadly fall into two different types: a return on quality of security and financial returns.

Financial returns can take a few forms. Most directly through loss or damage prevention, but also through efficiency gains. Automated electronic systems reduce staffing levels and eliminate the need for certain manual operations, such as searching for lost keys.

"Strategic capital expenditure planning is key to an organization's ability to generate and sustain value."

Experts stress that it is important for every organization to perform these calculations for themselves and not rely solely on outcomes provided by vendors. While calculating a reliable ROI value is a large undertaking, the very real security demands of modern business are on the side of making this case.

Determine Expected Lifecycle of Technology

It is important to know a service's expected effective lifecycle due to its tax implications. Fortunately, the IRS in the United States and the CRA in Canada publish guidance on the useful life for most types of capital. It can vary by industry, but security systems typically have a depreciated lifecycle between 5 and 15 years. This is a wide range, which is why it may be important for businesses to involve their finance departments early in the planning stage to properly account for tax implications.

Translating Security Threats into Business Risks

Security budgets in general, and capital expenditures in particular, need to be cost-justified to be approved. Even simple ROI calculations can help accomplish that. While the process of identifying threats and converting them into justified business risks is going to vary greatly from organization to organization, there are several basic approaches that work for most.

- **Compare to Status Quo**
  One simple approach is to quantify the costs of existing threats. For example, take known existing loss or shrinkage rates. Or existing compliance penalties incurred. Determine a projected annual average for the expected lifecycle of the security system under consideration.

- **Executive Straw Poll**
  A tried and true method for determining costs is to conduct an executive straw poll. Seek input about the cost of potential security incidents that the proposed purchase could mitigate. Get multiple estimates on what each incident would cost the organization as a whole.

  This is doubly useful as the opinions collected will often be from the same leadership that will consider the purchase request. Using their own data in the justification makes the business risks harder to ignore.

- **Calculate Costs of Downtime**
  This applies most to sectors were security systems deliver a core business service. Such as hospitality where guest safety is essential. Or corrections, where securing inmates is an organization's core function. Quantify the losses for not being able to deliver these core services. Include lost revenue, mitigation costs, compliance penalties, and estimate future losses from reputational damage.

  Organizations focused on long term value and profitability take downtime seriously. One security professional in the hospitality industry shared the story of when their old key management system failed. Their service provider at the time was not able to dispatch a technician for over four weeks, during which all of their affected venues needed to revert to manual key distribution. "That single event ended our business relationship," he said.

- **Identify Regulatory Needs**
  Organizations in regulated industries usually have baseline security and operational thresholds they need to meet. Others, like the gaming industry, have rigorous financial and access control regulations.

  Identify all areas, devices, and other resources that need to be managed for compliance. Total the existing costs for managing them. For example, at a casino their list would include counting rooms, drop boxes, gaming machines, keys for all of these items, and financial records.

  Published noncompliance fines can be used to calculate potential costs as well. Organizations can use their own compliance history as well as industry average fines to calculate the potential mitigated over the lifecycle of the system under consideration.

Calculate Total Cost of Ownership

The Total Cost of Ownership (TCO) is calculated as:

Cost to purchase + Cost to install + Cost to operate + Cost to maintain

One of the main reasons to include all relevant stakeholders is so this figure is correctly calculated. IT and physical plant teams especially can often identify secondary costs not immediately apparent to a security team.

Some examples of ownership costs:

- Staffing
- Training
- Additional IT appliances
- Server rackspace
- Electrical and wiring infrastructure
- Control or guard rooms
- Other administrative overhead

Calculate Return on Investment

Once the business risks and TCO are fully calculated, determining an ROI rate is straightforward. One way ROI can be calculated is:

$$ROI = \frac{\text{(Total cost of expected risks - Mitigation TCO)}}{\text{Mitigation TCO}}$$

The result of this formula lets you compare the relative value of different security solutions when their features allow slightly different risks to be mitigated. ROI calculations must still be supported with concrete evidence for how the system will reduce security incidents and realize an actual return on the cost invested. But grounding that supporting evidence with quantified financial data greatly improves a proposal's chances of being accepted.

ROI Example

An automotive manufacturer has seen dips in productivity and increased rekeying costs over several fiscal years across all of its facilities. And thefts at some locations are suspected to have occurred in-house after keys went missing. A team of managers determines that company-wide the material expenses, loss of productivity, thefts, and loss of sales are costing the company $675,000 annually.

The annual TCO of one provider's combined key and asset management system is calculated at $40,000.00. It is proven to mitigate all related costs. So:

(675,000 - 40,000) ÷ 40,000 = 15.875%

The ROI rate for this solution is 15.875 and is expected to save the company up to $635,000 annually ($40,000 x 15.875). The management team can then compare this rate and amount of savings to other possible solutions to see which delivers the best value, and include these figures in a proposal to their leadership.

As can be seen from this example, it is very important to make sure that risk and savings estimates are grounded in concrete data. Small changes in them can have a significant impact on calculated returns.

Despite that, an ROI calculation is a strong foundation to build a security capital expense proposal upon.