Capital Investments and Security Management Pitfalls
By Calvin Daniels

Investments within today's business world influence how successful organizations are in the future. Funding utilized during any procurement process must be tactfully allocated and produce some form of return on investment. The capital that organizations spend on security measures is no different. These measures must have some purpose (reduce risk) and be justified through cost benefit analysis. With this, the security industry has shifted from a labor intensive market to a capital intensive market. Through the acquisitions process organizations request and procure services that have lasting effects on security postures. These services consist of technical/physical security evaluations, guidance on security management practices and guidance on forensic security (expert witnesses) issues. You would think that the capital invested in security is managed effectively. After all, isn't the capital that is being invested used to protect against loss, prevent shrinkage and prevent pilferage?

Since 9/11 the security industry has witnessed a spike in demand. With this demand has come the requirement for security professionals to effectively manage the capital spent during new construction projects and during retrofit projects. On the national level the United States has spent $451 billion (as of August 2014) on national defense and has spent over $767 billion on Homeland Security since 9/11. Consumer reports have also outlined that Americans collectively spend $20 Billion each year on home security. Technical trends have outlined that organizations spend $46 Billion (combined) annually on Cyber Security. The asset protection market outlines that investments within the contract Security Officer (formally labeled guard force) industry has grown to $18 Billion a year. In an effort to prevent shrinkage retailers have also invested $720.3 Million annually on loss prevention measures.

You would also think that with the amount of capital being spent within the security industry that more industry benchmarks (to include lessons learned) would exist to help guide stakeholders toward sound security investments. This is often not the case. Most security project designs are the result of different security management mentalities. Many security management pitfalls are the results of a: Knee Jerk Mentality – security posture based on a single security incident; Cookie Cutter Mentality - if a security measure works well somewhere it will reduce the risk at multiple sites; Pieced Mentality - as capital is available some risk(s) are mitigated; Maximum Security Mentality - there is never too much security; and the Sheep Herd Mentality - everyone is doing it so we better follow suit. Each of these pitfalls limits the return on security investment. They each divert capital away from true risk(s) and very often require organizations to make additional investments in security programs to correct design flaws.

Two issues that contribute to these pitfalls are: The stakeholder(s) do not know what security measures are needed and rely on vendors for guidance; or the vendor does not have the stakeholders' best interest in mind and recommends that the stakeholder implements measures that are out of scope from the client's true need. From a security management stand point the question has to be asked, "Does the vendor understand the stakeholder's security needs and/or does the vendor really care?" To be clear, there are many vendors in today's security markets whom meet/surpass stakeholder requirements and make positive contributions to the security industry.

Stakeholders very often have not identified their specific security requirements (industry or local). They tend to identify different issues within their Physical Protection System, but never realize that these issues are symptoms that hide true security vulnerabilities. One of the biggest contributions to this misunderstanding is lack of security industry training. A question that can be asked is, "Does the organization providing training opportunities to its staff in an effort to identify industry best practices and expose them to new ideas?" In most cases, organizations rely on the experience that has been listed on resumes which negated the need for an investment in security training. When in house personnel do not evolve with a changing security industry the organization normally pays for this by outsourcing research work and is often taken advantage of by dishonest vendors during the acquisitions process.

Within the industry there are many issues related to the installation of security components. The functionality of the system is often overlooked and acceptance tests are often rushed. This issue can be linked to security personnel not being properly trained. If security personnel have not been trained to benchmark security practices and identify manufacturer requirements, how can they accept a system and with good faith tell top level management that an effective Physical Protection System is in place?

Another pitfall that exists is the development of unclear Statements of Work during the invitation for bid or request for proposal process. When the planning aspect of a project is neglected little changes in scope can cost the organization additional resources. When this lack of understanding occurs, there is no true definition of what the end product should be and the vendor may rely on gut instincts to get a security system in place to meet these unclear requirements. Not having a clear understanding of security goals can lead to scope creep (deliberately or by oversight) which will require an organization to make additional investments.

Service pricing is another pitfall. During the invitation for bid and request for proposal process stakeholders often rely on cost comparisons when selecting vendors. Limited amounts of capital may influence a stakeholder to select the lowest bid on a project in an effort to meet budget requirements. Buyer Beware! Any security system that does not meet technical requirements should not be accepted. At least 50% of the cost associated with security projects are generated by labor. A vendor may be inclined to submit cost estimates that are low and after being selected will identify costly scope changes that are needed.

Another security management pitfall exists in the system life cycle management process. Stakeholders are often fearful of change and don't seem to recognize that security systems will have to be upgraded within 10 years (if not sooner). Stakeholders also allow vendors to dictate what systems are installed and often leave them with systems that have very limited upgrade options. During any retrofit/new project stakeholders should take on the adage of the need to "Design to Upgrade." This means that if a substantial amount of capital is invested into a security system, organizations should invest in systems that are expandable and that can be easily upgraded. Far too often this is overlooked during the security planning process.

In an industry that is forever changing, security professionals need to be aware of the various pitfalls and the effects that these pitfalls have on organizational capital. The following benchmark can be used as a guide to reduce the effects of security pitfalls:

1) Ensure security personnel receive annual industry training.

2) Identify security requirements that may be industry driven.

3) Identify assets and their associated security vulnerabilities.

4) Identify the threats that may exist within a 'one mile' radius of the site/asset.

5) Identify industry best practices.

6) Plan for the security system to be upgraded at some point.

7) Implement sound security management practices in an effort to utilize resources effectively.

8) Vet vendors base on technical responses and past performance.

9) Never base vendor selection on cost.

10) Inspect vendor accomplishments as projects progress.

11) Conduct thorough functional tests (to include inclement weather and after hour tests) on system components.

In today's security industry there are many pitfalls associated with Physical Protection Systems and their implementation. Untrained employees, unclear security goals, misidentified issues, incorrect vendor selection and premature system acceptance are each security industry pitfalls. These pitfalls often require stakeholders to invest additional amounts of capital into existing or new systems in order to obtain balanced protection. Fortunately, today's security industry has industry leaders that can provide resources to stakeholders that prevent these pitfalls and that help organizations recover from these pitfalls. These organizations are CTCH Security Business Consulting, International Association of Professional Security Consultants (IAPSC) and American Society for Industrial Security (ASIS) International. Each of these organizations are supported by security professionals who have set the precedence within the security industry and who are dedicated to reducing pitfalls within the industry.