Five Steps to Accurate and Compelling Physical Security ROI

Introduction

In today's physical security industry, return on investment (ROI) is one of the most talked about concepts, yet least understood. A well-documented and supportable ROI case can be a powerful tool for the physical security professional competing for limited business resources.

Security investments can have two kinds of payoffs: an improved security picture and an improved financial picture. Security practitioners are used to making the case for improved security, but are not so experienced with showing how security improvements can contribute to a company's profitability.

When making the business case for a security technology investment (software or hardware), it is imperative to accurately capture the costs and benefits, and present the results in compelling financial terms. Knowing how to quantify an investment and its projected return—in ways that the CFO and other financial decision makers are used to seeing—can be pivotal to obtaining approval, especially in today's tough economic times.

This paper, the first in a series dealing with the ROI of network-based physical security, takes a close look at what security ROI is, and presents five steps for accurately developing and communicating the ROI for a physical security technology initiative. Its intended audience includes physical security practitioners and others seeking to understand the financial return possible with physical security.

What Is ROI?

ROI is a concept used to maximize benefits to an organization for monies spent. Used in determining a project's financial worth, ROI helps decision makers prioritize how investment dollars will be spent. ROI is the annual rate of return on an investment; for example, interest paid on a savings account is one type of ROI. It is the ratio of money gained or lost (realized or unrealized) on an investment relative to the amount of money invested. Other techniques focus on minimizing cash outlay without full consideration of the benefits involved.

For example, a $1,000 investment yielding a return of $120 per year has a 12-percent ROI, if the money is received as a lump sum at the end of each year. This is a simple ROI. If the return was received at the rate of $10 per month, the calculation becomes trickier due to timing differences, and whether the $10 benefit was reinvested at the same rate. For example, when monthly interest payments are placed into a savings account, the next month's interest is paid on the new higher amount. For our savings account example, the annual rate of return with interest compounding monthly (being added to the principal) would be 12.683 percent, and would total $126.83.

When funds are being invested for multiple projects at multiple times, and are accruing at different rates, it can be more challenging to calculate an overall ROI. Although computers can do the calculations, the results are only as good as the data that is entered. The challenge is to accurately measure what is to be invested, to project timing for the actual funding, and to correctly calculate the benefit received from the investment. Fortunately, businesses have already done this. Standard business calculations not only facilitate ROI development, but also help to establish credibility and validity of the business case.

Putting ROI to Work

Security ROI is complex: More and more organizations are interconnected, internally and externally, due to factors such as increased regulatory compliance, governance, and supply chain integrity. In contrast, traditional physical security systems have been proprietary and disconnected. Today’s business models strive to connect, converge, and use every application and technology asset to maximize organizational benefits and reduce total cost of ownership. It is time to include security in this process, as well.

Recognizing and quantifying the value of security helps to better prioritize investments in it. Unless the proposed security investments are framed in terms the CFO understands—quantitative, financial terms—projects may not receive investment. Since corporations have historically viewed security as a necessary expenditure to reduce risk and avoid loss, it is important to help management now see its financial value.

How Is ROI Measured?

Two basic criteria are used in evaluating ROI: costs and benefits. In business finance, a common measure of ROI is known as the Internal Rate of Return (IRR) calculated on a series of cash flows, both negative (outgoing) and positive (incoming). Negative cash flows are investments made or costs, while positive cash flows are the benefits derived. Modified Internal Rate of Return (MIRR) takes into account the cost of capital; this is important when the cost of capital can fluctuate during the period being measured. The complex calculations involved in IRR and MIRR and other financial metrics are outside the scope of this paper. However, the cost and benefit information discussed in this paper can be utilized by a company’s financial experts to develop the kinds of calculations the business normally uses for evaluating business initiatives.

Making a business case to apply technology to a problem requires a clear understanding of the problem. It also requires a 360-degree view of the challenges in deploying the technology. Decisions regarding what, where, when, and how the technology will be used, as well as its impact on the organization, must be carefully weighed by using financial tools such as the ROI analysis.

The objective is not just to establish a credible ROI, but also to define a high-value project by the benefits that it provides. The starting point for establishing the value of a project is its purpose, which takes us to Step 1 of the ROI task.

Step 1: Capture the Purpose

When establishing the value of an initiative, it's important to address two primary decision aspects: value and priority. The overall executive decision is: "Is it worth it?" Is the proposed initiative worth the time, effort, and money that it requires? Answering this question requires a general understanding of what the initiative will accomplish, and why it is important.

If that answer is "Yes," the next decision is about priority: "When do we do it?" Although security risk is a key factor in prioritizing security expenditures, financial factors also come into play. For example, there may be an IT project scheduled for upgrading the network, such as to support voice over IP technology. If the security project's network upgrades can be done as an incremental addition to the IT network project, that may provide significant cost savings compared to doing the work as a separate security project. An approach that lowers the cost of the security project increases the ROI for both the security project and the IT project.

Fiscally responsible planning and prioritizing will weigh in the project's favor in the executive decision-making process. If financial prioritization would delay the security project's schedule (such as scheduling a security network upgrade to coincide with a planned IT network upgrade), will the longer period of risk be considered worth the cost savings? Management usually appreciates the opportunity to consider such questions and provide an answer.

The description of the project's purpose should include a clear statement of the problem or problems to be solved, as well as the solution. The description of the problem will set the stage for capturing those costs in the next step. It is important to remember that the real value of ROI calculations isn't determined by just the math; it's also determined by the relevance, accuracy, and completeness of the cost and benefit data captured for the calculations.

Step 2: Capture the Costs

Developing an ROI case requires thinking about costs in a broader way than has typically been done. One comparison to be considered is the cost of doing nothing (i.e., costs associated with the status quo) versus the cost of the solution (the proposed initiative). "What if we do nothing?" is a question frequently asked by managers faced with expenditure decisions. On the surface, the choice may seem to be between "spending something" and "spending nothing." However, often there are ongoing costs related to the status quo. Sometimes, such costs are risk-related, such as those from ongoing shrinkage in a retail business. At other times they are operations-related, such as the cost of maintenance, or the cost of performing a process using manual labor (compared to automating the process). Measuring ROI fully requires identifying the costs of maintaining the current state versus the costs of implementing and maintaining the solution. If several alternative approaches are being considered, the costs and benefits associated with each should be understood and compared.

Total Cost of Ownership

It is important to capture **all** the relevant costs of a project. Doing so allows the following:

- Proper budgeting, funds allocation, and accounting
- Assessing project management
- Validating vendor claims
- Measuring the project's worth (ROI)

Total cost of ownership (TCO) is the cost to an organization to acquire, support, and maintain equipment, programs, or technologies. TCO can be expressed this way:

TCO = cost to buy + cost to install + cost to operate + cost to maintain

This sounds straightforward, but it is not always easy to collect and organize all of the cost data. Accounting processes for tracking overall system costs may not be in place. In many companies, deployed systems are not under the control of a single, centralized manager.

For example, it would be difficult to make the case that a system should be replaced because the maintenance costs are too high, if there is no way to track maintenance costs. It may require extra effort to identify all the relevant costs, including the staff needed, startup and troubleshooting, software upgrades, scheduled and unscheduled maintenance, and repair.

A complete and well-conceived analysis will be more credible; what's more, completely and clearly identifying the project or technology deployment costs reduces the risk of underfunding.

IT-Related Costs

There are many good reasons for moving from legacy systems to newer IP-based technologies. A common error in making a business case for IP technology is to assume that these IP-based systems will be managed in the same way as the legacy systems they will displace.

It is important to investigate and understand what standards are in place for systems that reside on the corporate IP network, and to account for their cost factors. Include the costs associated with industry best practices for the management of IP-based technologies, such as:

- Antivirus technology
- System patches
- OS upgrades
- Database management
- Backup and archiving
- Network bandwidth and quality of service (QoS)

Each of these costs may have associated additional labor costs for personnel who may be dedicated partly or fully to monitoring and maintaining the new systems. Should the existing IT support infrastructure be used to manage these issues, or should the security department be expanded to address or manage them?

Cost Factors

The list and table below contain common cost factors. It is important to estimate both the magnitude and timing of costs to be incurred. These should be captured on an integrated system basis, if that is the means in which the equipment will be procured and deployed.

List 1. Typical Cost Factors for Physical Security Systems

Video

- Cameras
- Encoders
- Fiber transceivers
- Monitors
- VCR-DVR-NVR
- Mass Storage

Access control

- Panels
- Doors (including locks)
- Readers
- Gates
- Other sensors

Communications

- LAN
- WAN
- Leased line costs
- Cost associated with interoperability of systems

Cabling and power supplies

Employee, visitor, and contractor management

- Receptionist
- Credentialing
- Contractor administration
- Lock and key management
- Package and vehicle inspection

Monitoring and control rooms

- Alarm and video monitoring personnel
- Operations support personnel
- Physical security information management systems
- Awareness and response systems

General system-related costs

- Engineering and design
- Infrastructure and maintenance
- Software and licensing
- System deployment
- Application integration
- Administration and troubleshooting
- User training

Table 1. Sample Access Control System Cost Analysis Worksheet (Year 1)

Feature	Cost
Planning and Design	
Engineering and design	$ -
Infrastructure and Maintenance	
Storage	$ -
Infrastructure software support (OS)	$ -
Database software	$ -
Hardware support (% annual)	$ -
Database administrator costs	$ -
System administrator costs	$ -
Power	$ -
Total	**$ -**
Deployment Software	
Base software	$ -
Application subscription/license (per reader or %)	$ -
Enterprise version	$ -
Application software support	$ -
Data conversion or migration	$ -
Configuration	$ -
Total	**$ -**
Deployment Hardware	
Device/controllers/readers/auxiliary	$ -
PoE power supply/panel power supply	$ -
Other door devices	$ -
Cable system	$ -
Electrified locks	$ -
Rack space or panels	$ -
Total	**$ -**
Application Integration	
Integration software	$ -
Integration software training	$ -
Hardware	$ -
Hardware support	$ -
Total	**$ -**
User Training	
Pre- and post-installation training	$ -
Ongoing training	$ -
Total	**$ -**

The Challenge of Gathering Cost Information

Many corporations have field offices and remote locations scattered around the world, often the result of growth through acquisition. The variations in financial governance and data collection can add complexity to gathering the data necessary to build a sound ROI analysis. The following questions can help, even though it may take some effort to fully answer them.

Q. **Who manages the service budgets for remote systems? If it's the local facility manager, how will information be gathered regarding historical maintenance costs?**

Q. **How much is spent on the maintenance of the host servers or workstations?**

Q. **If the system is hosted outside of the IT infrastructure, are there any additional costs associated with maintenance or backup?**

Q. **What is the amortization schedule the company uses to depreciate equipment or capital projects? (This can be extremely important, but challenging. Examining how the organization treats depreciation and the thresholds for asset classification are important factors. These determine how the organization values assets, and cost factors to be used in ROI calculations.)**

A. Gathering information that resides outside of the security department requires collaboration with other information stakeholders within the organization. This may be a department head in a small or medium-sized organization, or a program manager, analyst, or other position in a large organization.

Step 3: Capture the Benefits

As with costs, benefits must be considered in a broader way. It is best to start with the direct benefits, which are verifiable and easy to understand. Indirect benefits can be selectively included later, based on their contribution to the ROI case. It is not uncommon for indirect benefits to be 30 percent or more of the total benefit when included.

Direct Benefits

An ROI calculation should justify a project based on the direct benefits attributable to that project. Too often, managers have tried to justify a favored project based on a number of intangibles. In addition to being difficult to measure or prove, the intangible benefits often do not materialize. The following list contains potential areas for cost reduction that may produce direct benefits from IP-based physical security technology.

List 2. Direct Benefit Factors

- Planning and design
- Headcount
- Space
- Wiring and communications infrastructure
- Servers, applications, or systems
- Storage
- Integration
- System maintenance and upgrades
- Power
- Training

As an example, consider the effect of automation or system consolidation that enables alarms or information to be routed to a single workstation, instead of several. Reducing the personnel headcount from multiple posts lowers direct payroll and training costs.

The timing of benefits is another element in determining accurate ROI. It is common practice to measure benefits over the time period in which the project will be amortized, typically 3, 5, or 7 years.

> For a 3-year amortization schedule, the following case can be made. With an annual cost for a single 24-hour guard post of $157,000, the consolidation of four posts ($157,000 x 4 = $628,000) into a single post would save $471,000 ($157,000 x 3 = $471,000).
>
> The total savings over the 3-year amortization period would be $1,413,000 ($471,000 x 3 = $1,413,000).

Indirect Benefits

Indirect benefits can be defined as benefits whose contributions do not obviously relate to the investment. They are not easily measured. Productivity improvement is an example of an indirect benefit. Since indirect benefits may involve some subjectivity, separating indirect and direct benefits makes proposal evaluation easier, increasing its chances of receiving thorough consideration.

Should indirect benefits be quantified? The value of some benefits is apparent without quantification. For example, included among the indirect benefits of cameras are two effects of visibly employing cameras: the deterrent effect for would-be wrongdoers, and the reassuring effect for personnel who see that security measures are in place. These benefits are understandable without quantification and can be included as additional factors in an ROI business case.

For items that are hard to quantify, often a rough “lowest-benefit” estimate will serve to provide an acceptable minimum value. For example, an upgrade to the credentialing system may reduce the average time employees wait for temporary photo IDs or access badges from 35 minutes to 5 minutes. Most people will agree that all 30 minutes saved will not necessarily be used productively. However, if management believes that employees are on average 70 percent productive, counting 50 percent of the recovered time as value returned to the business may provide a credible measure of value for the proposal. If the benefit value is significant (a large dollar amount), using a conservative means of quantification can strengthen the acceptance of the number.

IP-based physical security can be used to increase efficiency and/or provide labor reduction by improving or automating various aspects of security operations. Security elements shown in the following list can be sources of indirect benefits when upgrading to IP-based solutions.

List 3. Potential Sources of Indirect Benefits

- Physical credential administration
- Visitor management administration
- Provisioning or access privileges assigned
- De-provisioning or access privileges revoked
- Segregation of duties
- Parking permit administration
- Property pass administration
- Compliance/governance reporting and auditing

- System troubleshooting and maintenance
- Alarm correlation and response
- Emergency communication and notification
- Video analytics applications (people counting, behavior tracking, etc.)

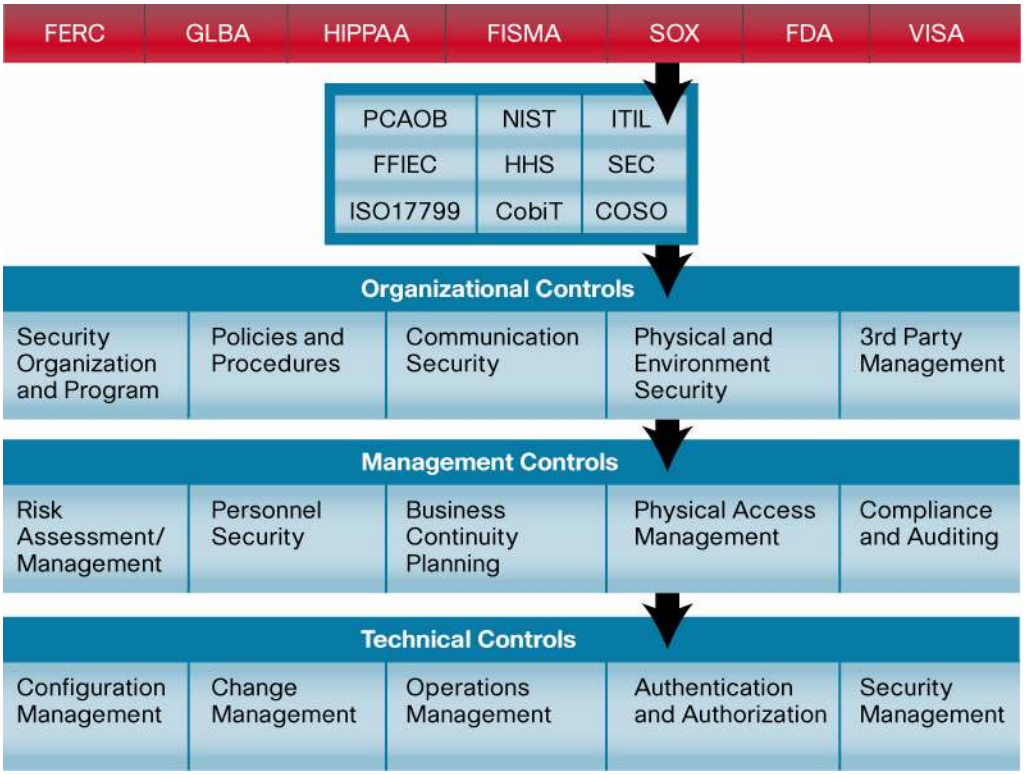
One source of guidance in handling indirect benefits may be other company proposals that have been successful. Such proposals may provide clues as to the type of indirect benefits that are considered valid and usable for ROI. Often, successful proposal writers can provide sound advice in these matters.

Indirect benefits can come in the form of individual, collaborative or management benefits to productivity. These benefits may be incremental and may represent a small improvement per employee, but, when multiplied across an organization's population or a large number of transactions, they may represent significant value in both productivity and cost avoidance. In particular, indirect benefits related to corporate governance and regulatory compliance can have a broad financial impact on organizations.

Managing Compliance and Corporate Governance

Managers in the corporate enterprise must work together to provide a platform for compliance and governance that will adapt to the ever expanding body of regulatory guidelines. In the United States, Sarbanes-Oxley (SOX) regulations (Section 404) mandate that a company must establish controls that protect the company's assets and financial information. These controls must provide a framework for "adequate safeguards over access to and use of assets and records, such as secured facilities and authorization for access to computer programs and data files." Figure 1 presents an overview of regulatory compliance elements, and highlights the elements involved in SOX compliance.

Figure 1. Regulations, Compliance Frameworks, and Controls Related to SOX



The following list shows some of the processes required by SOX. These rely heavily on manual tasks in a traditional corporate security environment.

List 4. SOX Requirements Typically Implemented as Manual Processes

- SOX (Section 404) internal controls for physical access
- Physical access provisioning and de-provisioning
- Cardholder identity management
- Security event and alarms management
- Change management
- Configuration management
- Segregation of duties

Workflow automation and integration between IT systems, building management systems, and physical security systems can provide significant opportunities for efficiency and effectiveness improvements. List 5 presents opportunities for high-ROI improvements related to SOX that use networked IP-based technologies.

List 5. SOX-Related Benefit Opportunities for Physical Security Processes

- Automated cardholder administration and reporting across physical access control systems (PACS) for SOX compliance
- Reduction in manual interventions needed in existing PACS for identity and credential management processes
- Reduction in or reassignment of existing security resources to lower TCO
- Reduced security vulnerabilities by correlating IT and physical security access events

- Framework to support disaster recovery, smart cards, background checks, visitor management, building automation, etc.

The challenges of lowering risk exposure and streamlining change control, with better resource utilization, are becoming greater. Further, the enterprise must seek to improve their internal controls and reduce the cost of compliance. It may be argued that ROI cannot be gained in a compliance-driven setting, as this is simply a cost of doing business. If a process is required for compliance or governance, and that process can be simplified while costs are reduced, positive ROI contribution is possible.

Step 4: Analyze the Costs and Benefits

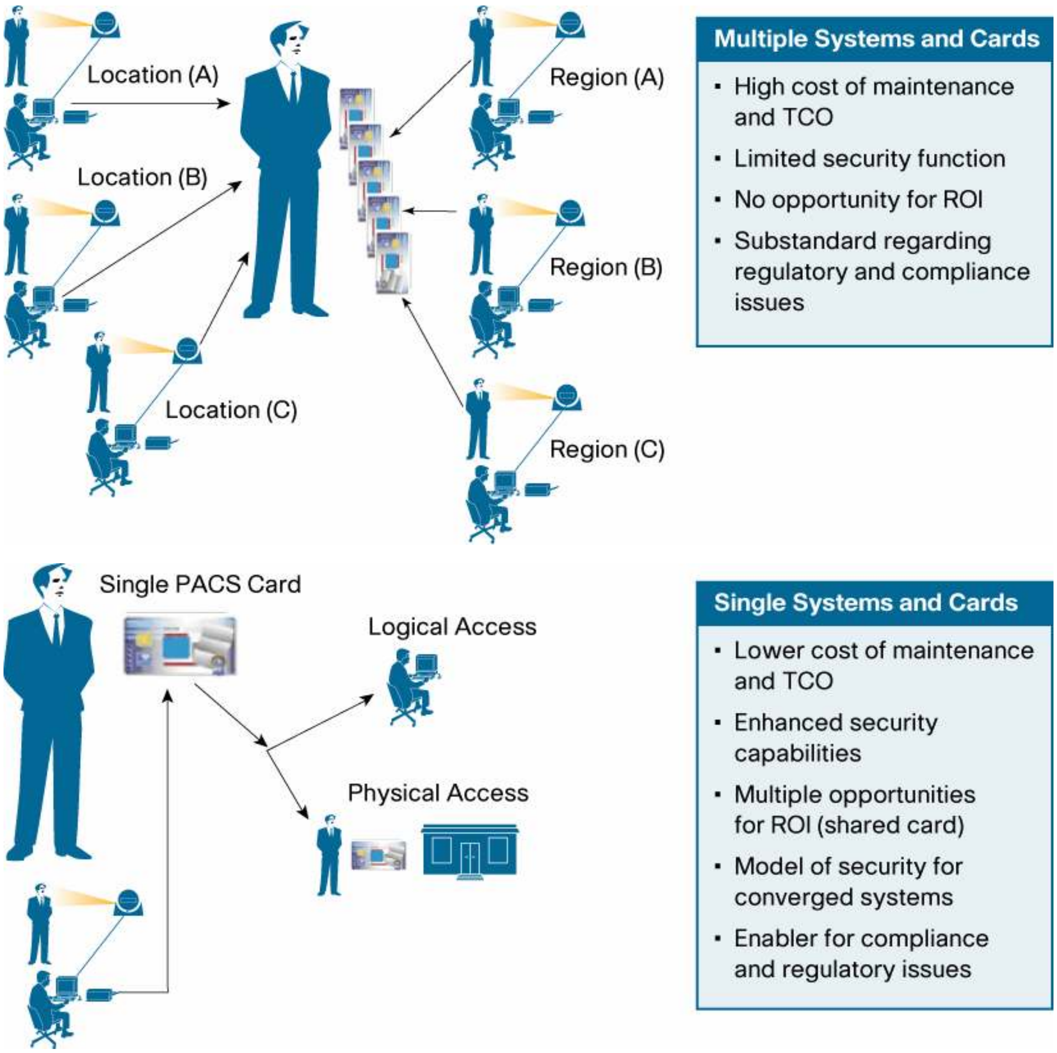
Once the cost and benefit data are collected, they must be analyzed to determine the return on investment. It has been common to use simple cost or TCO comparisons to assess the value of a technology initiative. However, when used alone, these methods determine the lowest-cost solution, but ignore the benefits. ROI calculations force one to consider how expenditures lead to benefits.

The value of the actual return is based upon the timing of the negative (cost) and positive (benefit) cash flows over the time horizon selected. It requires arraying these cash flows by time period (month, quarter, or year) so that the ROI can be calculated and graphically displayed.

Migrating from Multiple Systems and Cards to a Single System and Card

Some organizations have multiple physical access control systems, requiring the issuance of multiple credentials (cards). If the costs associated with issuing several different credentials and managing separate systems can be reduced or eliminated through the application of technology, positive ROI benefits may result. These may be quantified based on the number of system servers, workstations, and software modules of those multiple separate systems and the associated direct costs. Figure 2 highlights the cost and benefit comparison factors.

Figure 2. Benefits of Simplifying a Multiple Card System



Multiple Systems and Cards

- High cost of maintenance and TCO
- Limited security function
- No opportunity for ROI
- Substandard regarding regulatory and compliance issues

Single Systems and Cards

- Lower cost of maintenance and TCO
- Enhanced security capabilities
- Multiple opportunities for ROI (shared card)
- Model of security for converged systems
- Enabler for compliance and regulatory issues

The indirect costs associated with card management from disconnected systems may include incremental costs, such as lack of personnel productivity. Lost productivity can occur when requestors must wait for access to be granted, or when they are denied access to locations or tools that are necessary to be productive.

Step 5: Express the ROI

When presenting the ROI information, clear and concise summary information, as provided in the example below, should be supported by more detailed calculations but should be designed to stand alone and clearly express the ROI case. Expressing the ROI of the proposed project in clear, understandable terms will lead to a discussion of the project elements that really matter.

ROI Example

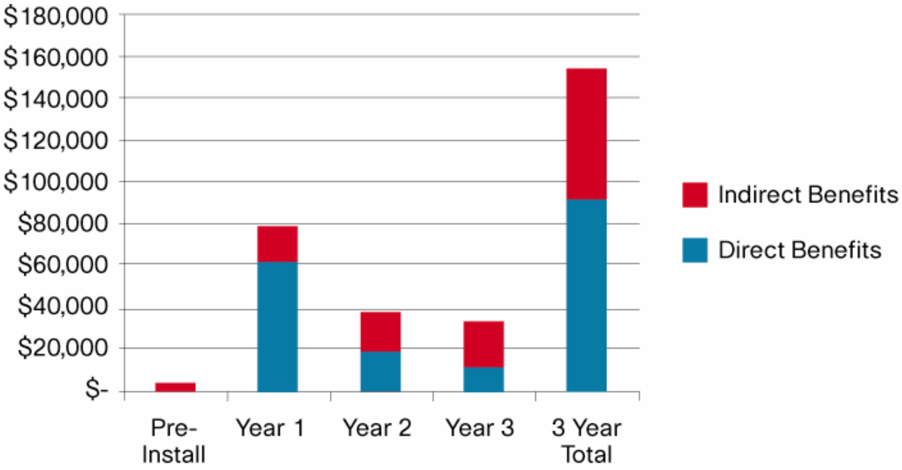
The following example is based upon recent actual data from a Fortune 1000 company. The system involves 85 card readers, processing nearly 4000 employees daily. The company evaluated legacy card access control technology versus a new IP-based system from Cisco. This example is interesting for several reasons. First, as shown in the following table, the IP-based system could be justified on a TCO basis alone.

Table 2. Example Costs of a Panel-Based vs. IP-Based Physical Access Control System (PACS)

PACS TCO Project Case Study	Year 1
Panel-Based	
Engineering and Design	$18,500
Infrastructure and Maintenance	$52,000
Deployment Software	$12,500
Deployment Hardware	$251,0000
Application Integration	$55,000
User Training	$ -
	System Total: $370,500
IP-Based	
Engineering and Design	$18,000
Infrastructure and Maintenance	$31,5000
Deployment Software	$29,000
Deployment Hardware	$183,500
Application Integration	$62,500
User Training	$2,500
	System Total: $309,000
	Year #1 NET Savings: $61,500

Moreover, if only evaluating costs, management might miss the analysis of the other benefits provided by the system. When simple staffing, maintenance, and support costs were figured in, it was realized that the less expensive system actually provided more benefit. Since the access control system itself was a firm requirement, the added benefit took this project out of the realm of “sunk costs” and properly positioned it as an interoperable platform providing value beyond basic security. Figure 3 shows a 3-year summary of direct and indirect benefits, including the $61,500 in initial cost savings.

Figure 3. ROI (Dollar Terms) of Physical Access Control System



Over three years, nearly $160,000 of benefit is realized versus the legacy system.

This illustrates another concept: ROI in dollar terms instead of a percentage. One could argue that, because the purchase of an access control system was mandatory, the baseline for investment should be the cost of the least expensive system to do the job. In this case, that's the IP-based system. (So the benefit received is based on a zero incremental investment, and would literally be infinite in a percentage calculation.) Running the benefit analysis allows a fuller understanding of the ramifications of the new technology, in terms of actual dollars saved and operational efficiencies.

Conclusion

IP-based technologies offer a tremendous ability to provide interoperability and collaboration across platforms, enhancing the overall benefit to the organization, now and into the future. Capturing this benefit in quantifiable and credible terms will allow the calculation of ROI, which, based on its value, will accelerate the implementation of the new technology. In the current business climate, it is crucial to justify the expenditure of financial resources with the most complete ROI analysis available. This demonstrates business acumen, sensitivity to resource limitations, and an understanding and grasp of one's own operations and their impact on others. It builds credibility with management. Ultimately, it provides the best hope for not only getting the project approved, but also for making it successful.

Glossary of Financial Terms

Analysis Period:

The time period for which the costs and benefits of an investment are tallied and analyzed. For this financial analysis, we projected current plan costs and IP telephony plan costs over a 5-year timeframe.

Capital Spending

Capital spending refers to expenditures relating to items such as hardware, software, network equipment, supplies, telecommunications, power, and space.

Cash Flow

Cash flow is essentially the movement of money into and out of your business (i.e., the cycle of cash inflows and cash outflows that determine your business' solvency). This financial analysis focuses on cash flow relating specifically to your company's voice systems and data networks.

Internal Rate of Return (IRR)

IRR calculates the interest rate received for an investment consisting of costs and income that occur over a certain analysis period. By analyzing the amount and timing of the costs and comparing them to the benefits over time, the IRR calculation estimates the returns from the project as an interest rate calculation. When comparing project returns, you should consider a project's return with other factors, such as required investment and risk. For example, consider two hypothetical projects. One project is lower-risk, lower-investment, and has an IRR of 100 percent. The other project is higher-risk, higher-investment, and has an IRR of 200 percent. In this case, the lower-risk investment project may be a better choice.

Net Present Value (NPV)

The value of money changes over time due to inflation. In other words, the value of a dollar (i.e., what it will buy) is different today than it was five years ago—and will be different in five more years. According to an economic concept called the "time value of money," we can project that a dollar today has more worth and buying power than a dollar will have in the future. When analyzing investments, future expenditures and benefits must be normalized to account for the time value of money. For example, if an investment promises a financial return in the future, the value of the return must be viewed in the terms of today's dollar expenditure in order to see if the investment is worthwhile. NPV is a formula that normalizes the cumulative costs and savings over time into today's dollar terms, discounting future benefits and tallying a total net value of the investment.

Operating Costs

Operating costs are the expenses incurred by your business that are not directly related to production, such as utilities, salaries, and office supplies. These expenses do not change when the level of production rises or falls. Operating expenses are also known as overhead, fixed costs, or indirect costs.

Payback Period

Payback period refers to the amount of time until the exact point in time, sometimes referred to as the "breakeven" point, at which the cumulative benefits exceed the cumulative costs, generating positive cash-flow from the project investment.

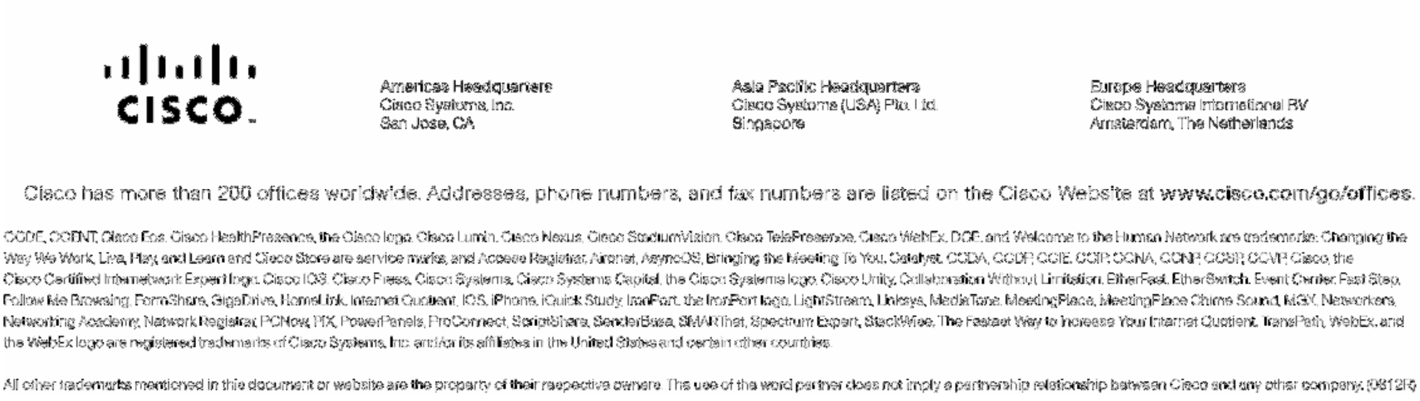
Return on Investment (ROI)

ROI is a return ratio that compares the net benefits of a project to its total costs. For example, if a project has an ROI of 200 percent, the net benefits derived from the project are double those of the expected total costs to implement the project. As such, the ROI calculation represents the relative value of the project's cumulative net benefits (i.e., benefits minus costs) over the analysis period, divided by the project's cumulative total costs, expressed as a percentage.

Sensitivity Analysis

A sensitivity analysis is an investigation into how projected financial results vary, along with changes in the key assumptions on which the projections are based.

Cisco appreciates the contributions of noted security industry consultants James Connor, CEO of N2N Secure, and Ray Bernard, Principal Consultant of Ray Bernard Consulting Services to this paper.



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C11-512820-00 03/09