Cost of ownership and getting ROI you feel good about

By April Dalton-Noblitt, Allegion
September, 2012

To ensure that campuses stay secure, safety and security departments are charged with designing, developing, and implementing a strategic plan that outlines proactive ways to lessen risks and protect assets. But today's challenge of ensuring the safety and security of students, faculty and staff on college campuses poses some formidable hurdles. Many would argue that colleges and universities should place the safety and security of their campuses at the top of their priority list. However, fiscal realities often force administrators to assess investments in improving security systems using different parameters.

Most measures to improve campus safety are subject to benefit-cost analyses. Some measures may be relatively inexpensive to implement, such as faculty training and the increased visibility of police and security officers in academic buildings. However, the cost of other improvements can be prohibitive. More than ever, campuses are also considering tangible benefits of improved security systems, since both students and surrounding communities are attracted to classes and events held in a safe and secure environment.

The U.S. Department of Homeland Security recognizes that security Return on Investment (ROI) is difficult to calculate successfully. Security practitioners know how to define and justify needs for improved security. But in many cases, they are less experienced with showing how security improvements can contribute directly to an organization's profitability.

In general, a proposed investment for security technology — including both software and hardware — must reflect benefits of the investment, as well as the costs. One way to illuminate the potential benefits of an improved security system is to perform a security assessment. Questions to ask may include:

- What is the financial impact of inadequate security to the organization?
- On average, what is the cost of financial losses without adequate security?
- What is the worst-case scenario of financial loss without adequate security?
- How does the organization protect its assets?

- How much security is appropriate?
- What security measures are most cost-effective?
- What types of security measures are needed?
- What impact will security have on the productivity of the organization's employees?

Answers to these questions may help to define the true purpose of an investment in security upgrades and technology. In addition, an analysis may determine a priority level for the initiative.

Security risk plays a key factor in prioritizing security expenditures, as do financial factors. For example, if a security network upgrade can be combined with a planned IT network upgrade, the organization may recognize significant cost savings compared to upgrading the security network as a separate security project. However, questions need to be asked – and answered – about whether or not the risk involved with the delay is worth the cost savings.

To develop an ROI case, compare the cost of doing nothing versus the cost of the solution. Although the choice may seem to be between "spending something" and "spending nothing," the status quo may incur ongoing costs. Sometimes, the costs are risk-related. Or they may be operations-related, such as the cost of maintenance or the cost of a labor-intensive process compared to automating the process.

To determine the total cost of ownership (TCO) requires data about the cost to an organization to purchase, support and maintain equipment, programs or technologies.

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

Gathering all the relevant TCO data leads to proper budgeting, funds allocation and accounting. It also helps in assessing project management and measuring the project's worth.

Typical cost factors for physical security systems include:

Video

- Cameras
- Encoders
- Fiber transceivers
- Monitors
- 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

Visitor 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

The direct benefits of a project play an important role in any ROI calculation. Unlike intangible benefits, direct ones can be measured or proved. For example, a proposal to automate or consolidate a fragmented security system into a single workstation may result in the following types of direct benefits:

- Streamlined planning and design
- Reduced staffing
- Reduced space requirements
- Simplified wiring and communications infrastructure
- More robust servers, applications or systems
- Upgraded Storage
- Streamlined integration
- Automated system maintenance and upgrades
- More power
- Ongoing Training

Indirect benefits also need to be included as additional factors in a proposal. These are benefits that do not obviously relate to the investment. For example, the addition of surveillance cameras has indirect benefits such as deterring illegal actions and reassuring personnel that security measures are in place. Productivity improvement also adds an indirect benefit to a project.

Areas that may experience the indirect benefits of upgrading to a networked security system may include:

- 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.)

Analysis of cost and benefit data helps to determine ROI and the value of a technology initiative. Unlike simple cost or TCO comparisons that determine the lowest-cost solution, ROI calculations relate how expenditures lead to benefits. The value of the investment considers the cost (in negative terms) and the benefit (positive) over a specified period of time.

To illustrate, consider the costs, benefits and ROI of applying technology to consolidate multiple physical access control systems into a single integrated system. Direct benefits range from reducing or eliminating the need for multiple credentials (cards) to managing separate access control systems. The benefits can be quantified based on the number of system servers, workstations and software modules of those multiple separate systems and the associated direct costs. Indirect benefits, which may not be quantifiable, include better compliance with regulatory issues.

Learn more about cost of ownership and ROI

For more information about ways to use ROI calculations to improve safety and security on your campus, please contact a professional security consultant in your area by calling **888.758.9823** or fill out the **Contact Us** form on our website at allegion.com.

About Allegion

Allegion (NYSE: ALLE) creates peace of mind by pioneering safety and security. As a $2 billion provider of security solutions for homes and businesses, Allegion employs more than 8,000 people and sells products in more than 120 countries across the world. Allegion comprises more than 25 global brands, including strategic brands CISA®, Interflex®, LCN®, Schlage® and Von Duprin®.

For more, visit allegion.com/us

aptiQ ■ LCN ■ SCHLAGE ■ STEELCRAFT ■ VON DUPRIN

© 2014 Allegion
009083, Rev. 08/14
allegion.com