SEC
SECURITY EXECUTIVE COUNCIL
A research and advisory firm

Security Program Strategy & Operations > Budget >

Dealing with Security Budget Challenges

By J. David Quilter, Emeritus Faculty, Security Executive Council

There are many ways to deal with the never-ending challenges of reduced resources. Doing more with less is the norm, not the exception. So, what can you do to shore up essential security initiatives and programs and garner support from your business leaders to address known as well as under-resourced or unanticipated security issues?

There are a number of essential proven elements for you to consider. Here are a few:

- Start with the basics: Know the business and its risk.
- A good security budget encompasses security programs' tactical and long-term strategy needs and maps clearly and transparently to the business' operating plans.
- Develop and maintain meaningful security measures and metrics.
- Know how to capably communicate to business leaders, in their terms, how security initiatives improve business results.
- When you do have to realign security resources to achieve mandated cuts, provide business leaders with a clear understanding of the impact such cuts may or will have on their business operations.
- Don't underestimate the value of travel and training.

Let's look at these points in more detail.

Start with the basics: Know the business and its risk.

A surprising number of security leaders do not start their security planning or budgeting processes with an enterprise security risk assessment. Without this, they are missing the basic foundation of strategic planning and defensibility. Security initiatives that are not mapped to assessed risks will of course be targeted during budget reductions. If no recent risk assessment has been conducted, initiate one to ensure that all security operations can be connected to current risk concerns. If they cannot, this exercise will present an opportunity to clean up

security's operations voluntarily, before budget restrictions demand it.

A comprehensive risk assessment, like all other recommendations in this paper, requires an in-depth understanding of the business. How does it work, what is its mission, who does what, where does it make its profits, and where there are opportunities to accomplish meaningful and visible business results?

Assume the role of part-owner of the business. Attend as many operational meetings as possible to observe how various parts of the business deal with both routine and emergency operating issues. Doing so helps you understand the operational culture and gives you "cultural ques" that may help you identify and address tactical security issues.

A good security budget encompasses security programs' tactical and long-term strategy needs and maps clearly and transparently to the business' operating plans.

Identify and document every service and function where security is engaged and why and how security in those areas is contributing to the safety, security, and improved profitability of the organization. Align your measures closely to the operating plans of the business functions. This will help you describe to other business leaders, in tactical and relatable terms, how security goals mirror business goals, the resources required to achieve them, and the programs to be implemented quarter by quarter. It may also help to protect security resources in tight times, because it will help show how a cut to any given security operation is also a cut to the function it serves.

Don't neglect the long game. Strategize and budget up to three years or 36 months out. When facing cuts in a current or upcoming fiscal year, the organization needs to know how current year and subsequent anticipated cuts impact security's ability to stay "in the flow" and keep pace with or fall behind the rest of the organization.

As you develop long-term strategy and budget, some of the questions you might consider asking are:

- Is a new security structure required to better support business operations?
- What are the financial resources needed to support such a move?
- Do you have the right kinds of security skills (investigative, IT, access control, facility assessment, etc.) and personnel to optimize security's responsibilities within the business?
- Is there enough allotted lead time to achieve security tactical and strategic objectives tied to various business functions and operations?

Develop and maintain meaningful security measures and metrics.

Every business has different ways of measuring its success. Some are as simple as cash flow and net earnings after taxes. Other organizations have highly matrixed measures and metrics that encompass what they do, where they do it (international trade balances and exchanges), and how they do it. Learn what your organization prefers, and model measures and metrics that reflect security's contributions in terms your leaders relate to.

For example, it is imperative to lay out the reality of what fraud, theft, embezzlement, information compromise, cyber intrusions, workplace harassment and violence cost in terms of lost net profit. The Cost Recovery Matrix tool provides a formula for security leaders to use to calculate and communicate these losses.

Other security metrics can measure performance by examining such trends as the percentage of incident reduction over time, rate of change in response times, cost per hour of service, and reductions in cost to insure, to name a very few.

Metrics serve multiple purposes.

- They demonstrate security's value to business operations in quantifiable terms.
- They help enable realistic, targeted budgeting.
- They make security's resource allocations tangibly defensible.
- They allow the security leader to assess and rank services by cost, performance, and other variables, so that if and when budget reductions occur, he or she already has an idea of the least impactful areas to cut.

(For more on developing security metrics, visit our Knowledge Corner)

Know how to capably communicate to business leaders, in their terms, how security initiatives improve business results.

Senior business leaders often are initially hesitant regarding issues of security, and with good reason. By and large they have always focused on driving business results – from a sales, marketing, or finance perspective. They are comfortable dealing in these operational areas because it is part and parcel of their experience. When it comes to security, though, senior management doesn't often see how it directly contributes to the success of the business.

The security budget needs to be explained to business leaders both in numbers and in terms of promised business deliverables. The security leader must demonstrate, in terms of profitability, brand, operational excellence, sales impact – as well as safety and security - that every dollar invested is well worth it.

It's worth noting here that regulatory requirements do get attention. Cyber security regulations are likely to stay front-of-mind because they're often in the news, but the C-suite is seldom as

familiar with physical and operational security regulations. Discussing corporate security investments in terms of compliance and due diligence may help make the security budget more easily defensible.

When you do have to realign security resources to achieve mandated cuts, provide business leaders with a clear understanding of the impact such cuts may or will have on their business operations.

There will be times when you have to bite the bullet and initiate cuts. Go line by line through your cost centers and see where things can be consolidated or delayed to meet the mandated cuts.

It is often the case that mature security program - those that have been in place for many years or even decades - have expanded services well beyond those traditionally thought of as security related. Examples include having guard services providing mail delivery, driving senior leaders to airports, and having guards manage fire extinguishers and AED's throughout facilities. Cutting these kinds of activities may or may not be acceptable, but they take man hours and have to be considered.

Once opportunities to cut have been identified, go back to the risk assessment and the business operating plans your budget is (hopefully) tied to. Communicate to executive management that resources can be slimmed down in specific places but provide a realistic narrative of what these cuts mean in terms of risk.

Remind them that security is not the owner of risk; the business is. Under OSHA regulations it is management's responsibility, not security's, to maintain a safe and secure working environment. It is the business' prerogative to accept certain risks and work to mitigate others, but they must be made aware of the potential consequences of their choice.

Don't underestimate the value of travel and training.

The travel and training budget of the security team is always a prime target for budget cuts. However, these areas and are well worth fighting for. Travel is expensive, but it is security's only chance to be on site, to talk with employees and managers. To be effective, it is important to lead on the front lines of the business, in operations, where things are made, distributed, and sold. In addition, activities like security site assessments and security awareness training are unlikely to be as effective if they are farmed out to other elements within the organization. Security's presence in and around field operations enables it to better learn the business, which is essential to a well-balanced security program.

Likewise, a highly trained and capable core security team will be more effective than one whose training opportunities are severely limited by cuts. Key members of the security team should be

up to speed on the latest developments in security technology, information technology, and investigative skills, especially with regard to fraud and embezzlement. To maintain these skills, leaders in these areas need to attend, at the very least, one security conference or seminar every other year.

Visit the Security Executive Council web site to read other articles in the Security Program Strategy & Operations: Budget series.

About the Security Executive Council

The SEC is the leading research and advisory firm focused on corporate security risk mitigation solutions. Having worked with hundreds of companies and organizations we have witnessed the proven practices that produce the most positive transformation. Our subject matter experts have deep expertise in all aspects of security risk mitigation strategy; they collaborate with security leaders to transform security programs into more capable and valued centers of excellence. Watch our 3-minute video to learn more.

Contact us at: contact@secleader.com
Website: https://www.securityexecutivecouncil.com/

