Managing and Defending a Security Budget

Laying a Foundation

Scenario 1: Company-wide budget cuts are on the way. You find an opportunity to defend your security budget before senior management, but you only have a day to prepare. The criticality of your security services seems crystal clear to you, but will it be to your CFO? Are you confident that you have the documentation, verifiable data, and business unit support that will convince her that your function should be a high-priority investment?

Scenario 2: Budgets have been sliced across the board. You have five days to find 9% to cut. Do you know where your flab is? Can you without hesitation say where your program transitions from mission-critical to "nice to have"?

Scenario 3: Your company is booming, and you don't anticipate a funding crisis in the near future. Security's budget is safe, but what are you doing with it? Do you know exactly where it's going, and can you make a case for each expense? Do you treat the budget as "your money," or "security's money"—or do you treat it as the company's money, and view yourself as the steward of it?

Most security leaders can identify with one of these three scenarios. Not all, however, will recognize the interconnectedness of the three:

- that responsible daily management is the only way to prepare adequately for budget defense;
- that finding that 9% cut relies upon an existing knowledge of where money is going and what value each expense has for the organization; and
- that if security manages its budget responsibly and proactively, then cuts and defense may not become necessary.

This article isn't intended to delve into the nitty gritty of how to budget. After all, budgets are handled differently in every company, and the security leader will be required to follow the company norm on the specifics of the process. Rather, we'd like to outline a foundation that can be laid beneath any security budgeting process to help enhance efficiency and effectiveness and perhaps, in the long run, even help position the security leader for advancement.

Catalog Services and Cost

The first step in managing a budget well is knowing what services the funds will have to support. This may seem simplistic, but it's a step many security leaders can't complete without a great deal of thought and research. Being new to the position is one common reason for this difficulty, but there are others. When security programs grow organically over time, it can be hard to keep track of added services without concentrated and continued effort. The same may be true when security leaders must quickly develop their programs based on what they're required by regulators or management to provide.

Security and risk management operates across other business functions, up and down the organization. It is a complex function, and in many companies large and small, security's work extends well beyond the barriers of "security." Because of this, cataloging services can be challenging, but all the more necessary. If the security leader can't point to a file, document, or presentation that clearly states exactly what the function is doing, none of the rest of the business will fully appreciate the breadth of services offered.

Once services are cataloged, the question becomes "What do these services cost?" How many full-time employees and contract staff are dedicated to each service? Are there staff outside the department that participate as well? How many hours do they spend on that part of their duties? What technical or

material resources does the service require, what does upkeep and maintenance cost, and what is the price of purchase or planned replacement (both within and outside the department)?

Gathering all of this information will take a commitment of time. Staff members and non-security colleagues may need to be brought in to share input and contribute data, but some of this task can likely be done by going through existing records and brainstorming. For many security leaders, the heavy lifting actually starts with the next step.

Where Is Security's Value?
When a finalized list of services and service costs has been developed, it's time to determine the service value.

Take the list and pick apart who the beneficiaries are of each service. Which business units gain opportunities or risk mitigation from the service, and how? If possible, develop or include metrics that show the benefit in a tangible way.

Then present this information to the business unit leaders by e-mail, conference call, or in-person meetings. Ask them what their critical business goals are. Then discuss how security services help enable them to meet those goals, both by opening up opportunities and mitigating risks that could compromise them. In many cases the business unit leaders will be unaware of the risks inherent in their operations, and the security leader needs to share this information. Have a dialog; listen to your colleagues if they have concerns or complaints about security's value, and work with them to uncover mutual benefits.

One of the purposes of this exercise is to remind the business unit leaders (and sometimes the security leader him- or herself) that Security doesn't own organizational risk. The organization does, and its business units do. Sometimes business unit managers will be willing to take on some of the cost of a program or service once they are shown the value in a concrete way.

Keep in mind, however, that examining any service's value to the business may be a double-edged sword. Sometimes you discover that you have more resources than you thought dedicated to a service that isn't needed or isn't valued by the organization, and your analysis provides support for cutting that service entirely. While that may be painful at first, look at it this way. You are a business leader. Your main concern is the good of the business. If a service isn't valuable to the business, why retain it?

Conducting an analysis like this in the good times, when cuts aren't on the horizon, is ideal. Then, if a service is found to cost more than it is worth, that service can be eliminated or downsized proactively, and the funds that were dedicated to that service can be put to use in another area that provides value and is more valuable to the company. If, instead, none of this occurs until the eleventh hour of mandatory budget cuts, then the money is gone, and that's that.

Finding Efficiencies for Reallocation
George Campbell, former CSO of Fidelity Investments and author of Measures and Metrics in Corporate Security, works with the Security Executive Council to help leaders analyze their programs as described here. When companies document their security services and costs, many of them find that guard force services are in the top three most expensive services for the function.
"This analysis is all about drilling down to learn how well time is directed to value-added, risk-reducing, business-centered services," says Campbell. "Economies can be found in wasteful administrative tasks, fixed posts that can be eliminated with technology, chasing invalid alarms, and time not directly

connected to hazard identification and mitigation. If you can't find non-productive time—often lots of it—in the daily three-shift routine, you haven't been serious about the process."

During budget cuts, management is likely to demand slashes to high-cost services like guard force. Organizations can use targeted metrics proactively to see how well such services are performing against expectations and standards. "Where programs fail to document value, they become opportunities for reduction," says Campbell. "An objective, internal analysis tends to prioritize reallocation of resources to measurably higher-value programs. That's the mission, after all."

Campbell asserts that security leaders' biggest challenge in finding efficiencies of any sort is partly habit. "Much of security's work is based on established routines: guard tours, background vetting, investigation processes, service level agreements, etc. We get comfortable and fail to challenge the routine. It's reasonably easy to document where the time is being spent. The hard part is finding new ways to do the work differently with consistently better results at lower cost."

Benefits Beyond Avoiding Cuts

The most common complaint from security leaders approached with this process is the amount of time it takes to pull the information together, do the footwork, and create a plan based on that. It's true that compiling this data is time consuming and often difficult, but it's time well spent. Failing to gain an in-depth understanding of where the money goes has implications that extend well beyond the budget. If your team can't talk about the services the function provides in a consistent language, and you don't have documentation to show how many people and how much time are dedicated to each service, then you don't have a function like all the other functions in business. What other business function would put something out into the marketplace and not assess who uses or values that offering? Neglecting this kind of research and development limits Security's influence with the rest of the business.

The benefits also range beyond simple budget cut avoidance. The Security Executive Council provides templates and frameworks for security leaders to use as they collect information on services and cost, and we have seen CSOs make important strides through this process. Besides avoiding cuts, they have eliminated inefficiencies. If the process shows that there are 13 business units responsible for disparate aspects of investigations, for instance, the security leader can drill down to cut out the redundancies, centralize where necessary, and not only reduce cost but greatly improve the execution of investigations company-wide.

Further, imagine what a clearer and more detailed knowledge of security services, staff, expenditures and value can do for strategy development. Six-month, one-year, even five-year strategies will be much more realistic and informed when they're built on an understanding of the content and value of services offered now. The same is true for business alignment-- security can much more easily demonstrate that its offerings line up with the goals and needs of the business if this fundamental work has already been done. The path forward becomes clearer once you know where you stand today.

If the security leader commits to documenting his or her programs as outlined here, he or she is more likely to be recognized by senior management as a proactive business leader, someone who knows the function and the business and who is looking beyond security to the good of the organization as a whole.

About the Security Executive Council

The Security Executive Council (www.securityexecutivecouncil.com) is a leading problem-solving research and services organization focused on helping businesses build value while improving their ability to effectively manage and mitigate risk. Drawing on the collective knowledge of a large community of successful security practitioners, experts, and strategic alliance partners, the Council develops strategy and insight and identifies proven practices that cannot be found anywhere else. Our research, services, and tools are focused on protecting people, brand, information, physical assets, and the bottom line.