MANAGEMENT TOOLS

MEASURING SECURITY PERFORMANCE & ROI

One way to assess if you're getting from security what you put into it is to tweak for security a financial model commonly used to calculate return on invested capital. The mathematical formula provides security departments a method to coalesce their various performance measures into a larger framework to yield a high altitude rating of performance.

By grouping metrics and doing some easy math, the calculation provides a baseline on the return on security investment (ROSI). And the same hard numbers provide management an easy way to understand the result of its current appetite for risk and to see, if it allocates more for security, what it can expect in return and whether new expectations are then met. (For a step-by-step explanation of this model, see the accompanying figure.)

BAE Systems has been using this strategy for two years as part of a broader effort to build trust and confidence in the security program, according to vice president Jeffrey Dodson, who described his company's ROSI formula at the 2007 ASIS International Annual Seminar in Las Vegas. "The security team needs to have experts in operations, research, statistics, and engineering so when people from outside come in, they have someone they can have a conversation with." BAE Systems believes conducting measurements of security performance is a basic part of building credibility, and doing it consistently helps security to be more scalable for meeting business needs, replacing a reactive approach that often causes manpower to fluctuate.

As described in the accompanying figure, metrics—as they are in most dashboard-scorecard projects—are the centerpiece of BAE Systems' formula. Dodson said the company struggled with the typical challenge of trying to measure security performance—a field in which a good outcome is that nothing happens—but that by dialoguing with business unit leadership on its view of meaningful security objectives, BAE Systems was able to generate metrics and weight them so that, taken together, they provide insight into overall security performance. The six major categories of metrics BAE uses include budget execution; timely closure of corrective actions; performance on inspections and audits; and completion of employee training. For data inputs, BAE Systems not only focuses on objective measures, but also uses selective subjective ones. BAE Systems also tracks some subjective aspects of security that it doesn't include in its ROSI model because it doesn't think they are a good fit.

One aspect of the model we like is that it can start simple, providing a cursory snapshot of security for department use only, and grow over time into a more detailed and exact formula for calculating security's performance versus expectations—one that is shared with senior management. Dodson says after two years, his company is still making and considering adjustments to its model. For example, each facility currently uses the same weighting, although it's likely that, at certain facilities, some security measures are more or less important than at others. Dodson said, "We're looking at that, some customization for different lines of business. But we also don't want to get into fine-tuning every knob; it's not our approach." BAE Systems has also decided to keep a system of objectives for measuring the performance of its contract guard force separate from the one it uses for its in-house officers.

To date, Dodson thinks his company's methodology has served it well. It has already emerged as a process for reallocating resources and has highlighted areas needing attention before problems developed. It has also produced collateral benefits.

Most importantly, performance measurement and reporting has become the norm within the security function, and continuous improvement is now a self-sustaining system. Finally, it has helped to change the very role of security within the company. "It helped create a cultural transformation, from the role of cops to a coaching role."

Calculating a Return on Security Investment

1) Based on your unique security objectives, define performance metrics.

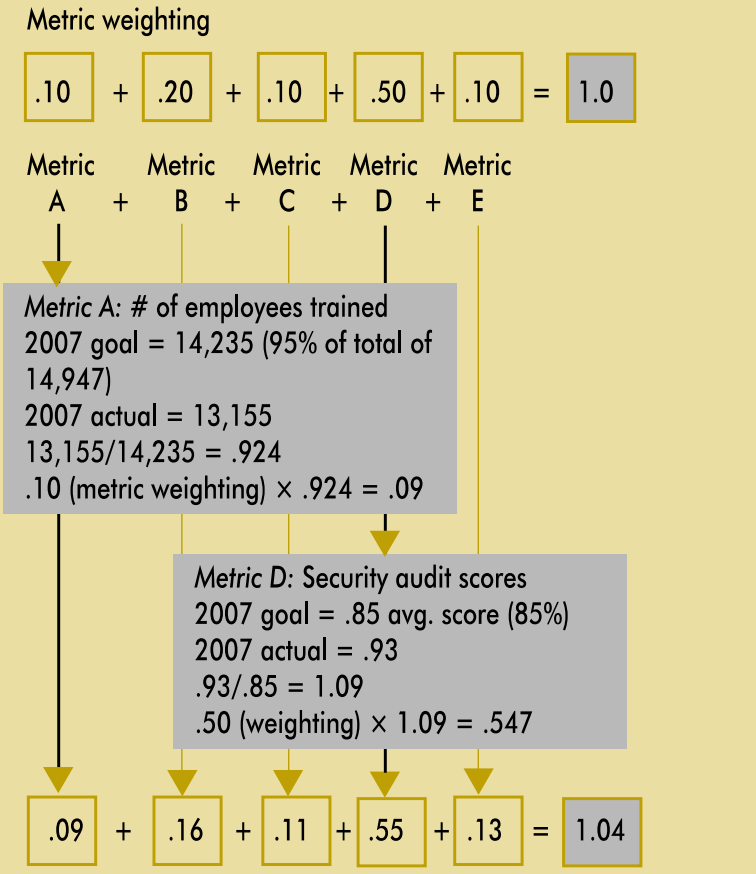
2) Weight each performance metric to reflect its overall contribution to strategic objectives of the security department. The total of the weighted performance measures should equal 1.0.

3) Calculate your scores for each metric based on your actual performance in that area versus your defined performance goal. Then multiply your metric score by its weighted value.

4) In this mathematical formula, your security investment is equal to the total of the weighted metrics (1.0). This reflects your baseline expectation that your current level of investment should be sufficient for approaching your strategic security goals.

5) Total the weighted scores for each metric and then divide by the security investment (1.0) to identify the value of security relative to the investment made. A score above 1.0 reflects a positive value for security investment.

6) Comparative scores over time (monthly, quarter, year) denote an improvement or decrease in operational effectiveness.



ROSI Year-to-Year Trend

2004	2005	2006	2007
1.01	.99	1.03	1.07

(Source: BAE Systems and other resources)

Of course, there are typically some bumps on the road to change, and BAE and others offered the following lessons they learned during implementation of a data-centric approach to measuring security performance.

- Examine how your new data-collection efforts will impact others. For example, BAE wanted to improve traveler security by keeping better track of employee travel, so it implemented new procedures under which employees who didn't complete forms couldn't purchase a ticket. Dodson said problems cropped up because BAE failed to adequately train workers on the change before implementing it. Overall, he thinks BAE "spent a lot of time coming up with concepts on how to improve things, but we didn't spend enough time on rolling out the ideas and training people on how it would impact them."
- Create milestones 30, 60, and 90 days out so that security and people implementing aspects of the program can realize success. You need some initial victories to maintain momentum.
- Build program measures into new initiatives. Security departments should always aim to initiate change in line with the organization's ability to handle it, but because there is a chance you'll misjudge it, you need measures to spot mistakes.

"We initially exceeded our organization's bandwidth for change with too many new processes and procedures and rolling them out too fast," said Dodson. "If we weren't measuring, we would have kept rolling right off the cliff."