Showing the ROI of Contract Security Forces

By George Campbell

It is great to get feedback on my metrics columns. Let me share some thoughts on a recent e-mail I received from a thoughtful security manager in Arizona:

"I can't think of a more relevant issue for physical security than a series of metrics regarding contract security costs. The one item we've never been able to tie down during benchmarking was the ROI related to contract security. Obviously there are many moving parts to the issue, but when my director asks about value vs. cost regarding contract security, we get back to proving the negative (minimal losses to theft, no intrusions, etc.)."

Return on investment is fundamentally a measure of whether some activity is worth doing. Clearly, we can employ more sophisticated approaches, such as Annualized Loss Expectancy (ALE), that estimate frequency and impact and then apply various safeguard improvement options. But in my view, ROI for contract security operations has to be tied to an operational risk management strategy.

Our reader serves in a critical infrastructure where security compromise is intolerable, but he nevertheless is in competition for increasingly scarce resources. In this case, I think the return is not a financial metric but a policy decision that concludes that the consequences of not having a competent security presence are intolerable. While the likelihood of an event may be perceived as low, we increase the potential by not making prudent investments in protection.

Herein is our dilemma: Is the perception of risk low because we are so effective, or because there is little real threat out there? If the latter, then why do we have all this expense for security? Law enforcement has a deep reservoir of data on crime, calls for service, victimization and clearance rates. Where do we look to support the effectiveness measures of our security operations teams?

1. Defect detection and elimination. What is the potential financial impact of various events that are within the response profile of your security force? The organizations we serve are complex and house thousands of processes and activities, many of which are prone to malfunction, breakdown, accident, human error or malfeasance. A trained 24/7 security force can proactively identify and mitigate many of these defects. Does that demonstrate a potential return?

2. Penetration testing. Not a lot of apparent threats rearing their ugly heads? Find ways to test the effectiveness of your security measures. If you had 10 attempted penetrations for each of a variety of sensitive areas that demonstrate an 80-percent or 90-percent failure rate — that is, the would-be adversary did not succeed in getting to the asset the overwhelming majority of the time — does this not advertise the effectiveness of your security measures, including your security force surveillance and response capabilities? We know that we have assets that are potentially attractive to motivated individuals. That motivation can be deterred by clearly effective safeguards, including a professional security presence.

3. Response time. How long does it take for EMT or police to arrive at your facility? (Note that the time may be increasing due to local government budget shortfalls.) If your people are there in five minutes and can sustain a life or apply definitive care until EMTs arrive five or 10 minutes later, is there a benefit? How about responding to that water detection alarm in the computer room or being outside HR during a potentially hostile termination?

4. Cost effectiveness benchmarking. We are charged with protecting people, property and corporate assets. How do you compare with other colleagues? Determine how many security officers you have per square foot of coverage, and how many officers per employee. If you show one officer per 5,000 square feet, and many other comparable organizations post more officers in the same area, you are demonstrating clear cost efficiency — a solid result in these hard times.

"We know that we have assets that are potentially attractive to motivated individuals. That motivation can be deterred by clearly effective safeguards, including a professional security presence."

5. Service-Level Agreements. SLAs are fairly common in outsourced service contracts and deserve consideration for their ability to establish clear performance standards. Common elements for contract security are supervision, first call resolution, response times to emergency events, incumbent qualifications and levels of training, tour and staffing of specific posts. These may include both penalties for non-conformance and potential rewards for exceeding standards.

These are a few measures to consider when you are determining whether your contract or proprietary security force is delivering value for the cost. Clearly, much of the focus is on "what if." But that question is at the heart of management's obligation to manage risk on behalf of the shareholders' or the public's safety. ▮

George Campbell is emeritus faculty of the Security Executive Council (SEC) and former CSO of Fidelity Investments. His book, "Measures and Metrics in Corporate Security," may be purchased through the SEC Web site. The SEC is a member organization for senior security and risk executives from corporations and government agencies responsible for corporate and/or IT security programs. In partnership with its research arm, the Security Leadership Research Institute, the Council is dedicated to developing tools that help lower the cost of members' programs, making program development more efficient and establishing security as a recognized value center. For more information and inquiries on membership requirements, visit www.securityexecutivecouncil.com/?sourceCode=std.