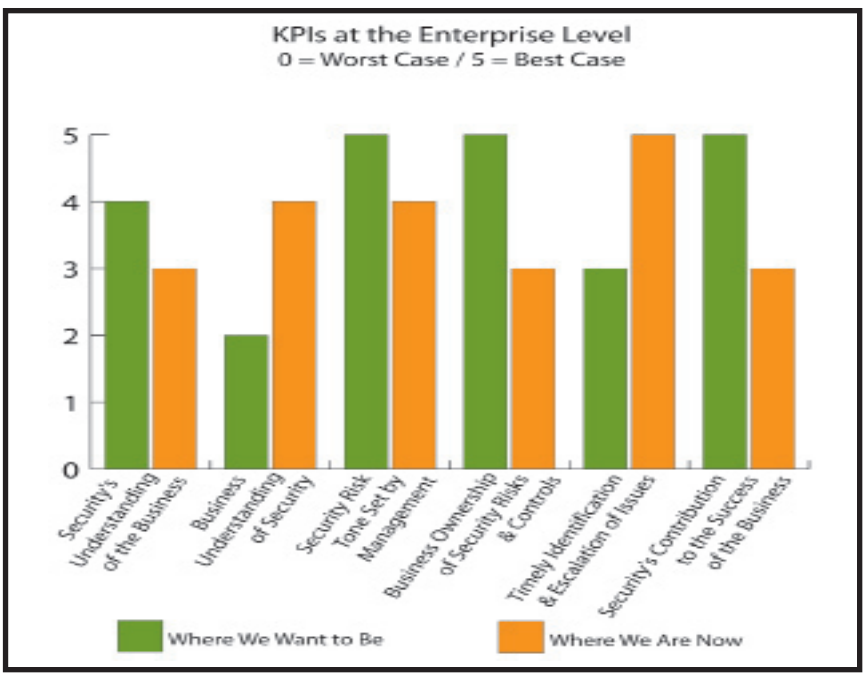
Measuring Key Performance Indicators

By George Campbell



Most of us have heard of Key Performance Indicators (KPI): they are measures of progress toward some goal that often reflect how well a business process is being performed. If you have not considered developing KPIs for your security program, I would encourage you to look at them as a component of your measures and metrics program.

Objective: You have multiple objectives to satisfy your stakeholders and accomplish your longer-term strategy and annual security plan. KPIs provide an effective monitoring tool to measure your progress.

Strategy: In this month's example, a CSO has selected several high-level directional indicators that are critical to the success of his or her security program (as shown in the graph above). Through a series of interviews with key stakeholders and follow-up security team meetings (injected with a lot of honest introspection), Security has assessed the department's and the business' status (where we are now) against a performance goal (where we should be) on these key indicators. Let me address each of these:

1. Security's Understanding of the Business: This is essential to our ability to understand current and evolving risks and how the business strategy and culture impact our options and approach to security operations and risk management. We gain understanding by engaging with business leaders and thoroughly examining business processes.

2. Business' Understanding of Security: It should be obvious that if the business fails to understand security's mission and value, we will neither be able to influence strategy and policy nor obtain the resources we require for mission accomplishment. Here again, we must be engaged with business processes in activities like proactive risk assessments and incident post mortems and thereby use our unique knowledge to inform and influence. The results of these activities feed our metrics.

3. Security Risk Tone Set by Management: Our success is tied to management's expectations for employee conduct and asset protection. If the business fails to understand how security can contribute to success, it follows that management will set the wrong tone with employees or, worse, will not engage them at all. Explore a variety of venues to ensure awareness.

4. Business Ownership of Security Risks and Controls: Top management should expect business unit leaders to share ownership for effective security practices in collaboration with corporate security. When you use your metrics to inform business unit leaders on protection gaps and problems, you eliminate plausible denial.

5. Timely Identification and Escalation of Issues: When our enterprise security strategy successfully incorporates these prior performance indicators, risk incidents will be identified and escalated in a timely and responsible manner. It will be made clear that avoidance and delay worsen the consequences.

6. Security's Contribution to the Success of the Business: Our status on each of the five preceding desired states clearly impacts our influence and thus our ability to the success of the business. Our status on this final indicator will in part be drawn from our progress on the others.

This particular selection of KPIs addresses the question, "What is really important as a measurable contributor to enterprise success?" More quantitative indicators, such as "reduce inventory theft by 25 percent by 12/31/2009," are just as valid and actionable and have a proper place in the measurement scheme.

But having a process to periodically conduct evaluations of these six fundamental indicators anchors the program to a highly qualitative foundation that will pay real dividends to Security's portfolio of value. ▮

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. In partnership with 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, visit www.securityexecutivecouncil.com/?sourceCode=std. The information in this article is copyrighted by the Security Executive Council and reprinted with permission. All rights reserved.