What's State-of-the-Art in Security Metrics?

By George Campbell

File this in the opinion folder. I have always pinned my metrics hunt to that day very early in my CSO career when the boss asked what kind of metrics we had in the can. As I stumbled for a defensible answer, he said, "I want you to think about what metrics we should follow in our organization and why you think they are important for the senior management team." But the more I dig into this security space, the more I have found that measuring and plotting program performance has been an expectation of every boss I've worked for over these past (gulp!) 50-plus years.

Why then is there such a vast wasteland of security metrics available to us for our disparate security operations? Google "security metrics" and you will find page after page of solid, established results…on information security. Dig for the rest of the content we loosely label "corporate security" and then try to dig some more. It is not surprising — the crown jewels are virtual, moving at the speed of whatever from wherever to somewhere out there. Management's perception of risk has expanded almost as fast as the intelligence of the evil propeller heads who know how to find those jewels. If you were to ask the average CEO what security concerns keep him awake at night, you would likely get something about information protection. Our information security colleagues have done an outstanding job of understanding their universe of risk, developing detection and prevention tools, and building a body of standards and measures of security program performance. Why have we not followed suit?

Contract security guards in the United States alone account for more than $16 billion and employ significantly more people than public law enforcement. Businesses spend billions on physical and logical security technology and tens of millions on background checks and an array of investigations. Yet, when you ask a source that should know what the total cost of security is in their company, they typically don't know the answer because there are too many variables spread across multiple parts of the business.

Given the expanse of the larger corporate security universe, where are the established standards, measures, metrics and benchmarks to guide comparison and program performance assessment? Why did ASIS struggle for so long before uttering the word "standard"? If NFPA and OSHA can issue codified standards on workplace safety, where are the statistics we can use to assess how we stand vs. industry peers in workplace violence and other key risk areas? How do my security program costs compare to others by revenue, sales or size? How about a measure of ethical health like the ratio of employees as subjects of investigation per 100 employees? I've got a few hundred of these, but so would you if you really thought about it.

Why is this important anyway? I think there are several reasons, but here are a few:

1. Because if you're not measuring, you're not managing.
2. You are in the risk management business. What impact are your security expenses having on your exposure to risk? Is your organization safer and more secure than it was at this time last year? How are you measuring that, and what have the adjustments accomplished?
3. Management gets metrics from just about everybody else in the company. What are they to think if you aren't advertising your performance metrics?
4. You organization's level of security depends on non-security staff to engage in a variety of actions to protect your assets. How are you measuring their performance?

I am currently engaging in a poll of security practitioners, trying to nail down a few transferable metrics we can use for internal performance measurement and benchmarking with peers. It is a beginning, and hopefully it will serve to build a bigger, acceptable inventory of actionable metrics. If you would like to participate, please e-mail me at contact@secleader.com and I will send you a copy of the short survey. ∎

George Campbell is emeritus faculty of the Security Executive Council and former CSO of Fidelity Investments. His book, Measures and Metrics in Corporate Security, may be purchased through the Security Executive Council Web site. The Security Executive Council is an innovative problem-solving research and services organization that works with Tier 1 Security Leaders™ to reduce risk and add to corporate profitability in the process. A faculty of more than 100 experienced security executives provides strategy, insight and proven practices that cannot be found anywhere else. Through its pioneering approach of Collective Knowledge™, the Council serves all aspects of the security community. To learn about becoming involved, e-mail contact@secleader.com or 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.

Proven Practices from George Campbell

Looking for more metrics help? The Security Executive Council's new Proven Practices Library includes a detailed presentation by George Campbell on Building a Security Measures & Metrics Program. This 45-minute presentation includes

- a ground-level explanation of why security metrics are important;
- specific examples of measures & metrics adaptable to your data input; and
- a framework for assessing the need and building a tailored program.

SecurityInfoWatch.com is currently offering a preview of this presentation at http://video.securityinfowatch.com/Security_Metrics_Program. SIW viewers who choose to download the full presentation will receive a 10% discount on their purchase.