

Metrics > Getting Started with Security Metrics >

Measure Your Metrics

By George Campbell, Emeritus Faculty, Security Executive Council

Why Measure?

Why measure, why metrics? The fact that established metrics for the full range of security programs are few and far between tells a story about the historical disconnection of these functions from the core businesses they serve. We all know how the risk environment has changed over the past few decades with wake-up calls to Boards and senior management.

Attentive corporations have uncovered their exposures with more in-depth risk assessments and have addressed them by building and mainstreaming corporate security organizations. With this increased visibility and accountability comes the obligation to better measure performance and to demonstrate contribution to both enterprise protection and the bottom line. Relevant, actionable security metrics are natural descendants of this evolution.

A security metric is not a number plucked from a list of other numbers; it's simply not meaningful standing alone. Don't get me wrong — you need lists of numbers and their descriptive data. You also need a data management system to enable collation and analysis. Analysis enables metrics to tell a story, describe the root cause of a trend and demonstrate how risk has been impacted by our collective efforts to mitigate.

Over the years, I have been constantly struck by the high level of sophistication of so many corporate security departments that fail to effectively use the event, workload, feedback and collective knowledge they have stored in their operations. As I have noted in the past, simply counting things does not provide good, actionable information. Too many security organizations are working to generate data daily but have far too little knowledge to show for their time and effort.

What is the business case for your security program? What are the quantifiable measurements that ought to be applied to management's assessment of value? How do you measure the relevance of the information you are communicating to your team and business unit customers? If you spend a moment or two to consider these questions, how would you grade your security metrics? If you had to pick half a dozen metrics that would have the most beneficial impact on managing risk in your company, what would they be and why?

As part of a larger effort within the Security Executive Council aimed at building a comprehensive security program assessment process, I have recently developed a metrics self-assessment that walks the security manager through a number of questions about their program's maturity. The format uses several categories of key metrics indicators and asks you to rate your level of program development on a 1-3 scale. For example, one question asks about the "current status of metrics within the Security Department" and offers five choices:

- Recognized need and trying to understand best first steps
- Established objective but just in early stages of development
- We have a variety of data and now are moving to identify best approach for desired results
- We have several focused metrics outputs for targeted constituents but now want to elevate the content for management (and Board) targeting
- We have a well-established program with quality reporting and now desire to develop a more directed and influential set of measures and metrics

To help you identify where your program is, we are offering a sampling of the metrics maturity assessment to our readers. E-mail me at contact@secleader.com to receive the information. Your answers will be reviewed and sent back to you with a score. Perhaps if there is enough interest I will be able to report on the aggregate trends from readers. Any results will be reported without identifying information.

Originally Published in CSO Magazine

Visit the Security Executive Council web site to read other articles in the [How to Get Started with Security Metrics](#) series.

About the Security Executive Council

The SEC is the leading research and advisory firm focused on corporate security risk mitigation solutions. Having worked with hundreds of companies and organizations we have witnessed the proven practices that produce the most positive transformation. Our subject matter experts have deep expertise in all aspects of security risk mitigation strategy; they collaborate with security leaders to transform security programs into more capable and valued centers of excellence. Watch our [3-minute video](#) to learn more.

Contact us at: contact@secleader.com

Website here: <https://www.securityexecutivecouncil.com/>