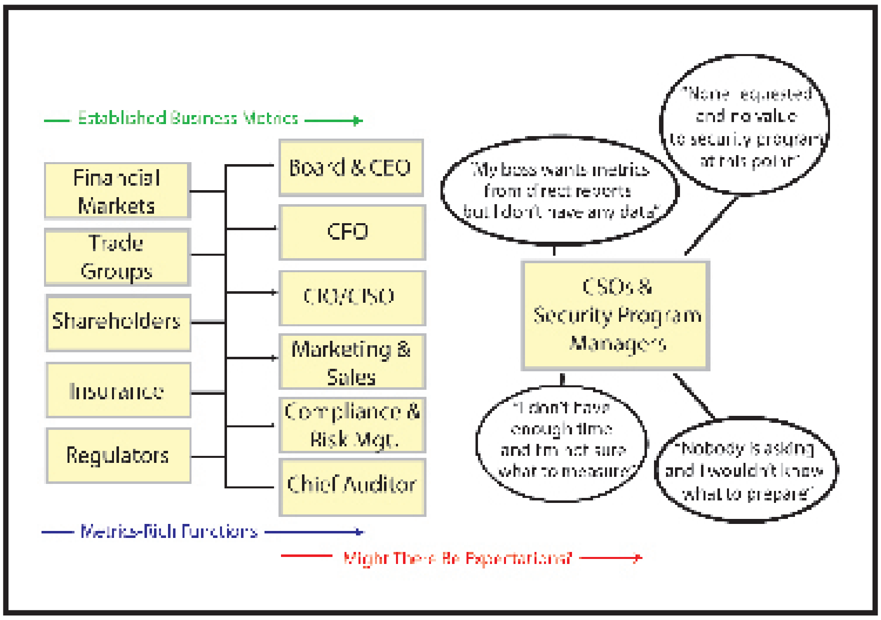
It's Time to Get Security Metrics Savvy

By George Campbell


Established Business Metrics
Financial Markets
Trade Groups
Shareholders
Insurance
Regulators
Board & CEO
CFO
CRO/CISO
Marketing & Sales
Compliance & Risk Mgt.
Chief Auditor
"My boss wants metrics from direct reports but I don't have any data"
"None requested and no value to security program at this point"
CSOs & Security Program Managers
"I don't have enough time and I'm not sure what to measure"
"Nobody is asking and I wouldn't know what to prepare"
Metrics-Rich Functions
Might There Be Expectations?

Across the industry, there are CSOs and security program managers who still don't get it, who think security-related metrics are a waste of time or who don't have a clue where to look to build a metrics program. Every business manager needs to develop and deliver programs and services that demonstrate measurable results, whether good or bad, positive or negative — and that includes security.

Why do all the constituencies and colleagues around us understand that measuring business performance and the effectiveness of planned programs is the essence of management? Given the fact that our companies live and die on a host of well-established business metrics, why do so many of us in the business of security fail to understand and embrace the need?

Whether your company is publicly traded or privately owned, banks, financial markets and shareholders demand and constantly monitor metrics on your company's performance. Your insurance rates are based on risk management metrics (typically your risk, not their's). Look at the security-related regulations that have emerged over the past several years and the requirements that you demonstrate compliance with defensible measurements. How many CEOs can you count who have been sacked for having bad performance metrics? If you are a security manager looking across the table at your information security counterpart, he or she can drown you in measures and metrics to assess the effectiveness of his or her safeguards. These are all metrics-rich functions led by managers who understand and depend on specific measures and associated metrics.

The quotes in the graphic above are not jokes created to make a point. They are real quotes from established security managers: "I don't have the time," "I don't know what to measure," "I don't have any data," or "I wouldn't know what to prepare!" I love the counterpoint between two of the quotes — one in which the boss is asking for metrics, and the other in which no one is asking. I guess you could conclude that the former is in trouble and the latter is dodging a bullet — for now.

As I have written in this space every month, the data for creating useful metrics is everywhere. There is no security program you own or share that fails to possess some associated metrics. There are systems you monitor, incidents you count, funded projects that you have requested to meet some security objective, vulnerabilities and risks you have identified, crime trends in your area you track, the performance of your employees and vendors you direct, and false alarms you have prayed don't come from certain points. The boss who hasn't asked for metrics does not appreciate the risks your programs address on a 24/7 basis. And whose fault is that?

You don't need to get fancy or overfill the bucket with numbers and charts. All of the constituencies you see in the graphic have legitimate need for a targeted few metrics that are meaningful to them. Auditors need to know where the holes in protection reside, senior management needs to be aware of key risks and what needs to be done to address them, your boss needs measures of your department's performance against specific objectives, and you need to keep watch over those key metrics you know are at the core of your enterprise protection mission. **ST&D**

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