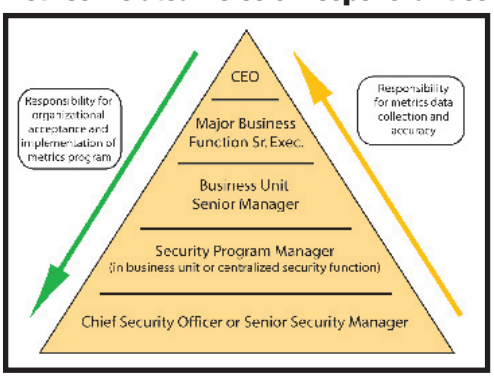
Who's Accountable for Metrics?

By George Campbell

Over the past several months, we have discussed a number of metric examples. It is important to place these in a context of organizational accountability. Where does accountability lie for the maintenance of a proactive measurements and metrics program? The answer, as shown in this month's graphic, is that it is shared up and down the organization, but the CSO is the initiator who must design and sell the program up and down the chain of accountability.

Many security managers believe their executives do not clearly articulate what types of business-related security metrics they would like to see. However, in many instances these same security managers fail to sell their own unique perspectives on enterprise risk to influence corporate risk perspective and policy. The responsibility for the failure or success of the metrics program rests with both these roles and with other employees and executives on the chain. To ensure that metrics receive the support they require, both in development and in organizational acceptance, security must seek to institutionalize protocols and expectations for security risk awareness and shared responsibility for risk management.

Metrics-Related Roles & Responsibilities



Adapted with permission from IT Security Metrics Guidance, Hash & Grance, National Institute of Standards and Technology.

The graphic to the left clearly implies that the hierarchy of responsibility commences and terminates with the security leader. Look at where the upward arrow establishes accountability. We are responsible to start the process using our unique perspective and databases. We have the expertise to conduct an after-action review and determine how an event unfolded and where the gaps lie with regard to responsive internal controls. The real challenge lies in penetrating the higher levels of senior management and encouraging them to embrace our value-added services.

Let's look at the levels of responsibility, because they say a lot about real ownership and buy-in for security measures and metrics.

CSO or Senior Security Manager: Responsibility for metrics data collection and accuracy. This is the owner of the central warehouse where all security-related data is stored and analyzed. If you don't "own" the full spectrum of security data, you should think about establishing a Security Committee comprising representatives from internal organizations that own various pieces of the overall picture. Examples for membership include Internal Audit, the CIO's Chief Information Security Officer, Risk Management, Compliance, Legal Counsel and business unit representation with specific attention to a higher risk unit.

Line Security Manager: In many organizations, line business units staff a security function that relates specifically to the risks in that business process. Many corporations decentralize line security responsibility to appropriate line functions with a centralized CSO as the focal point for security policy and investigations. Other examples are found in fraud risk managers, contingency planners and specialized risk management units.

Business Unit Leader: Senior management often fails to make the responsibility of this first line of defense clear. These are the custodians of the assets, and they set the expectations for integrity and corporate asset protection. The metrics program needs to strongly focus upon this level of accountability.

CEO (or COO or other senior executive): Responsibility for organizational acceptance and accuracy of the metrics program. The CSO's access to this level allows him or her to make senior management aware of the implications of various measures and provides the platform for holding subordinates accountable.

Failure to build the metrics program around an accountability model like this can severely impact the potential benefits and effectiveness of the program. Metrics are designed to inform and impact policy and decisions. The reach of your work is critical. STD

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