SEC
SECURITY EXECUTIVE COUNCIL
A research and advisory firm

Metrics > How to Get Started with Security Metrics >

Security Metrics in Context

Created by George Campbell, Security Executive Council Emeritus Faculty

Why go through the trouble of applying metrics to your program? George Campbell explores this question in his book, *Measures and Metrics in Corporate Security.* In this exclusive excerpt, Mr. Campbell describes how metrics improve security's chances for success in various contexts.

What Are Security Metrics?

At a high level, metrics are quantifiable measurements of some aspect of a system or enterprise. For an entity (system, product or other) for which security is a meaningful concept, there are some identifiable attributes that collectively characterize the security of that entity. Further, a security metric (or combination of security metrics) is a quantitative measure of how much of that attribute the entity possesses. A security metric can be built from lower-level physical measures.

Security metrics focus on the actions (and results from those actions) that organizations take to reduce and manage the risks of loss of reputation, theft of information or money, and business discontinuities that arise when security defenses or protocols are breached. They are useful to senior management, decision makers, users, administrators, or other stakeholders who face a difficult and complex set of questions regarding security, such as:

a) How much money/resources should be spent on security?

b) Which system components or other aspects should be targeted first?

c) How can the system be effectively configured?

d) How much improvement is gained by security expenditures, including improvements to security processes?

e) How do we measure the improvements?

f) Are we reducing our exposure?

The Business Context

There are a variety of metric and performance indicators that may be employed to assess security programs in a number of different ways. Before discussing these, it is important to note that it is the quality- and cost-performance-based models that drive many corporations. These models find traction with boardrooms under pressure and senior executives with an appetite for enhancing share price by reducing the cost of doing business.

Reengineering, cost reduction initiatives, efficiency studies and any number of highly organized, data-dependent (and costly!) management reviews should all be familiar to anyone working and awake in a major corporation in the past decade or two. The criteria for the Malcolm Baldrige Award presented by NIST's Baldrige National Quality Program underscore the wisdom of having an organized set of performance metrics embedded within the operations of each security function ...

“A major consideration in performance improvement involves the creation and use of performance measures or indicators. Performance measures or indicators are measurable characteristics of products, services, processes, and operations the company uses to track and improve performance. The measures or indicators should be selected to best represent the factors that lead to improved customer, operational, and financial performance. A comprehensive set of measures or indicators tied to customer and/or company performance requirements represents a clear basis for aligning all activities with the company's goals. Through the analysis of data from the tracking processes, the measures or indicators themselves may be evaluated and changed to better support such goals.”

While the Baldrige award may be a quest for few, it should be noted that similar criteria are found within a majority of internal audit departments or external auditor organizations that may stand in annual judgment of our operations or, at a minimum, our abilities to contribute to the management of risk within the corporation. In 1992 the Committee of Sponsoring Organizations (COSO) published what is now an accepted model of an internal control framework that emphasizes risk and internal control assessment with formal reporting to the Audit Committee. In a similar timeframe, we find the U.S. Sentencing Commission Guidelines for Corporations influencing risk reporting and corporate crime prevention. These admonitions apparently went unnoticed by multiple corporate executives, boards and internal control infrastructures in the '90s and into the new millennium thereby setting the stage for Sarbanes-Oxley, a reinvigorated edition of Sentencing Guidelines and a new round of risk management standards. A variety of regulatory initiatives also spun off post-9/11 Homeland Security legislation, much of which incorporates elements of metric-oriented analysis and reporting.

We live in times where anticipation of risk is a basic expectation of shareholders and management. The means we select to mitigate risk must be measurable. The advantage of a system of measures embedded within the control infrastructure is in the setting of expectations that eliminates plausible denial and incorporates many of the metrics available to the security of the business or organization.

The Risk Management Context

Consider this: It is only because there are unacceptable risks that the cost of a security program is tolerated. Risk management is the process of identifying and understanding applicable risks and taking informed actions to reduce potential failure, achieve business objectives and decrease business performance uncertainty. There are four categories of risk confronting businesses:

- Strategic Risk - risk that is an inherent part of the business environment and has a significant effect on revenues, earnings, market share and product offerings.
- Organizational Risk - risk that is part of a unit's environment relating to people, politics, and values that can impact organizational effectiveness.
- Financial Risk - market, credit and liquidity risk that creates uncertainty, exposure to loss and the potential that the business will not be able to meet its future obligations.
- Operational Risk - the risk of loss from inadequate system controls, human error or other management failure. These areas have increasingly become a part of Security's realm, encompassing fraud, data integrity, risky operating environments, information security, business continuity, inadequate policies and controls and the rich variety of good old problems with people.

Metrics abound in these arenas because we need to know where to devote scarce resources to their management. Corporations spend millions in measuring, anticipating, preparing and responding to their implications. Where we manage them well we reduce the likelihood of occurrence or minimize the impact of reality.

The Regulatory Context

Security no longer enjoys the cover of executive ignorance and inattention. Look at any number of corporate and natural disasters and see how politicians protect their seats and insurance companies protect their pocketbooks. Why did the majority of our fire laws follow the Coconut Grove fire in 1942; Executive Order 13224, C-TPAT, Hazmat, Maritime Transportation Act, as examples, after 9/11; Sarbanes Oxley after Enron (and others); and privacy and information security regulations after the flood of identity thefts? Regulators and insurance carriers love measures and metrics; for example, “As you can see from the attached schedule, we are 63% in compliance and will complete the balance of our security enhancements within the next 240 days.” Typically security-related regulations require risk assessments that are measurable, security enhancements or indications of the degree of current compliance that are measurable, time and cost to comply that is measurable, and schedules and other indicators of conformance with the letter and spirit of the legislation.

The CSO's Context

It pays to advertise. As CSOs, we may get caught up in the response and forget that we're in the education business. Put more bluntly, we need to empower those who get it and eliminate plausible denial from those who don't. We have to continually drive home the notion of business unit responsibility, meaning security happens when employees exercise knowledgeable oversight. Where correctly focused, measures and metrics are pointedly informative and enable our constituents to see the results of measurably effective and ineffective security measures. In the wake of corporate meltdowns to the ethically deficient, this focus needs to reach to the Board of Directors and across the ranks of senior corporate management.

Security executives must know how to influence the corporate population and business focus. There are five key pillars in a measurably influential security program:

1. A framework of security policies explicitly endorsed by top management to provide the legal framework for positive influence.

2. A core management philosophy that holds line managers accountable for protecting the firm and establishes the security executive as the content expert prepared to empower those managers with the information they need to be effective custodians.

3. A clearly established role in the firm's risk management program enables the security executive to better understand the adequacy of business process controls and to influence the governance infrastructure on lessons learned.

4. A qualitative analysis and reporting program provides the metrics dashboard, connects the dots and draws actionable conclusions.

5. A comprehensive communication and awareness program provides the script for influence and employee empowerment.

It is generally accepted that the truly effective executive is the one who has mastered the ability to influence up and down in their organization. Influence as a core competency is the heart of the measurably effective CSO. Metrics are a tool used to facilitate influence, to demonstrate, argue, support and convince.

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 information in this article is copyrighted by the Security Executive Council and reprinted with permission. All rights reserved.*

Originally published in Security Technology Executive

Visit the Security Executive Council website for other resources on 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/