How to Use Metrics

By George K. Campbell

(Originally published by *CSO,* August 2007)

CSOs generate security data every day. Knowing what to look for and how to analyze it can spell success for a security operation and the organization it serves.

Why metrics?

The fact that established metrics and measures for the full range of security programs are few and far between tells a story about the historical disconnect between these functions and the core businesses they serve. The risk environment has changed significantly over the past 30 years, with shocking wake- up calls to CEOs, boards and shareholders. Attentive corporations have had to address the exposures uncovered in these times with more sophisticated and mainstream corporate security organizations. With this mainstreaming comes the obligation to measure performance and demonstrate bottom- line contributions. Metrics are a natural descendant of this process.

It is also essential that we recognize security's contribution to the corporate system of internal controls.

Internal controls, established to mitigate a variety of business risks, provide the dashboard to inform management on the status of core activities and to apply the brakes that keep the enterprise safely on course. The security organization plays a critical role in identifying, measuring, preventing and responding to a growing inventory of risks. We must be able to measure the probability and potential consequences of an identified risk, or management has no gauge to assess and prioritize what actions to take. Metrics are central to understanding the adequacy of security controls and where to focus our limited resources for the greatest contribution to the protection strategy.

This excerpt from the book Measures and Metrics in Corporate Security, Communicating Business Value gives a few examples of the ways CSOs can think about the data they collect as part of their security operations and identifies what is important to measure, and how to communicate with senior business executives about what the data indicates about their organization's risk environment and how it's being managed.

1. Aligning security metrics with business drivers

Security programs gather volumes of data every day. If we gather the right information, we generate unique and informative data that, for example:

- Defines what, where and how risk is occurring
- Emphasizes the accountability of business management for safeguarding the organization's assets
- Directly aids in measuring service quality and customer satisfaction
- Provides measurable support for new and existing programs
- Contributes to a variety of value- based assessments

The successful security executive defines his business plan and the performance of resources and services around clearly articulated measures. Those measures should be aligned with core business strategy and priorities. Figure 1 illustrates how a CSO has evaluated the importance of various security metrics, based on their relevance to business drivers such as managing costs and risks, focusing on return on investment, complying with the law and

company policies, and protecting the lives and safety of employees. Note the last column on the right, which is checked every time: internal influence. Effective use of metrics that matter to business leadership, demonstrating the value of security operations, wins a security executive important capital.

2. Risk mapping: tracking security- related incidents over time to identify risks

Every CSO should have half a dozen dials to watch on a regular basis. These indicators could be "survival metrics," the hot buttons on a dashboard you are expected to address that monitor the wellness of your organization or an issue of particular concern to management.

You may find that you have more than one dashboard—yours and the one your boss and a few key players expect you to watch and report on. The CFO could be an excellent resource to advise you on the presentation of dashboard metrics since this officer typically reports performance metrics to management on a regular basis.

While these dashboards view an array of priorities, you need first to identify what risks are important. One way to drill down on a particular risk and determine its priority level is through risk mapping. Risk mapping is about plotting the dynamics of the risk incident landscape. A presentation model of risk dynamics or risk profiling may be found in the risk map on Figure 2. More consequential incidents are at the top of the map, and more frequent ones are to the right.

In Figure 2, eight types of internal misconduct cases were plotted for the month, and the five highlighted all had inadequate supervision and poor policy awareness as contributing causes of the infractions. Half are high severity, indicating a need to address these vulnerabilities quickly. When presented for a specific facility, manager or organization over time, this presentation can be very instructive. If this example proved to be common over multiple samples, it's obvious that the CSO has to engage the appropriate HR resources to review the content of supervisory training and performance evaluation. A variety of risk profiles may be presented and analyzed in an Excel- based format. When contributing vulnerabilities or causes are noted in each cell, common denominators often demonstrate fundamental weaknesses in one control or another. A thorough examination of the case with an incident postmortem should yield contributing causes. There is a valuable story to be told to management, and it is particularly useful in quarterly or annual presentations to display notable trends, their contributing causes and suggestions for mitigation tactics. Work with your governance partners in this process.

And if you want to drill down on an emerging risk issue, consider engaging an audit colleague who is familiar with the targeted business process along with the process owners. Find a whiteboard and break down the business process and consider all the possibilities of how it could go wrong. Push the envelope on potential problems and solutions. You'll build a supporter in that business unit and likely head off a developing area of risk.

3. Measures Mapping: a way to identify risk mitigation strategies and evaluate their effectiveness

We are all familiar with the highway sign "Dangerous Curve, Reduce Speed Ahead." Many of the measures discussed in this story may be applied to provide the CSO and key constituents with similar caution signals. They become the earliest prompts for more in- depth analysis of trend dynamics that allow you to look at the root causes of problems, not just the symptoms.

- Examples of incident trends that help diagnose risks to address include:
- Increased frequency or severity of accident, crime or policy infraction rates
- Reduced mean times between failures on critical equipment with increased downtime
- Increased number or severity of negative background investigation rates in specific hiring populations
- Excessive passwords for access to different "secure" applications, which results in shared passwords and visible posting of passwords
- Abnormal response times to calls for service
- Outsourcing sensitive business processes without requisite due diligence

- Elimination or reduced testing of building evacuation plans, which leads to employee confusion and injury during real incidents

- Degradation of timely software patch application or increased virus activity in specific client groups

Such diagnostic measures identify risks. Then a CSO needs to develop a strategy to address them. Measures mapping helps you do that by looking at areas of risk, the contributing causes to those risks and actions implemented to mitigate those risks, and then measuring the effectiveness of those actions. Measures mapping, a method of analyzing specific hazards or incidents to identify potential tactics, is a modification of countermeasures mapping guidance for licensees of the Nuclear Regulatory Commission, utilized some years ago. It takes the aggravating cause results of incident lessons-learned analyses and the high-level tasks identified to mitigate the risk and postulates measures or metrics for each countermeasure.

Figure 3 takes on the issue of insider risk. In this example, the area of risk identified stems from the increased number of employees in a business unit who were the subject of misconduct cases. Investigations reveal that the problem stems in part from poor supervision of these employees. In addition, there's poor awareness on the part of employees of the company's business conduct policies. Mitigating actions involve the CSO and the security team as well as managers from human resources and legal departments.

There are several examples where measures maps are useful. It could be the need to cut security spending, the failure to respond to a security breach at the CEO's home, business interruptions caused by computer viruses or the frequency of workplace violence incidents. Measures mapping is a useful way for a CSO to brief constituents on a proposed risk mitigation strategy. And it enables status and cost updates in progress reporting.

4. Good metrics are SMART

Good metrics are "SMART"—specific, measurable, attainable, relevant and timely. (That idea originates with the engineering text Winning with Quality: Applying Quality Principles in Product Development, by John Wesner et al.) It's a CSO's job to find the appropriate model for security measurement and reporting objectives that fits his organization. The most important data to the security executive depends on what is most important to his senior management and other stakeholders. It depends on what factors your supervisor will use to rate your performance. It depends on what you use to effectively measure the performance of your people and key vendors. It depends on what you need in your unique security environment to most effectively communicate, manage and influence.

Influence is often data-dependent. If you have a good grounding in the business and have the right radar working, you likely know things about risk, the value equation, the competition and the business risk environment that is not available or obvious from other sources.

- -

Security consultant George K. Campbell, a member of the Emeritus Faculty of the
CSO Executive Council, retired in 2002 as CSO of Fidelity Investments.