Seven Steps to IT and Information Security Metrics Success

OVERVIEW
In recent months, IT and information security executives at Global 2000 organizations have become increasing aware of the strategic value of centralized metrics initiatives. It is widely accepted that metrics can help IT and security organizations reliably measure, monitor and communicate the effectiveness and business impact of IT governance, risk and compliance (GRC) initiatives. Yet, few have implemented this necessary and effective management tool at an enterprise level.

According to the Forrester report, “Defining IT GRC” issued December 2007 and written by Khalid Kark, Marc Othersen and Chris McClean, “IT GRC initiatives have traditionally been scattered across the organization without any coordination or synchronization. It is not uncommon for different business areas to develop their own solutions for the same requirement or for IT to deploy multiple technologies to address a common issue. Not only do these separate initiatives create inefficiency, but these silos also make it hard to assess and manage risks holistically. As a result, there is a growing demand for solutions to help IT organizations effectively breakdown these silos and create a centralized approach to managing risk and compliance while simultaneously ensuring good governance.”

In this whitepaper, ClearPoint Metrics will review the seven critical steps of any metrics initiative, as outlined by The SANS (SysAdmin, Audit, Network, Security) Institute. Drawing on ClearPoint Metrics’ own research and client experiences, we recommend an effective process for implementing the seven steps with a goal of driving positive change in security behaviors, processes and investments.

THE VALUE OF METRICS
Metrics and measurements are two vastly different concepts. Measurements are generated by counting and provide specific views of discrete factors. Metrics, on the other hand, are generated through analysis. They are derived from measurements, to which contextual information has been added for comparison, such as to a pre-determined baseline, or observing trends over time. Truly useful metrics indicate the degree to which goals are being met and they drive actions taken to improve organizational processes, such as the percentage of critical systems that meet policy standards for host hardening.

When applied to security performance, a metric is the expression of the state and/or quality of a critical aspect of your IT infrastructure. It is the basis for directing
Applying regular, repeatable metrics to a security performance initiative can benefit your organization in a number of ways:

- Measuring the effectiveness of controls
- Identifying and targeting areas for improvement
- Communicating the effectiveness of risk management programs
- Driving proper actions in focused areas and extending accountability
- Providing hard evidence of compliance
- Providing actionable views across the enterprise, lines of business or specific areas of IT infrastructure

PUTTING THE METRICS PROGRAM IN PLACE

Step 1: Define Goals and Objectives
As with any initiative, defining “big picture” internal goals and objectives is the logical first step. ClearPoint Metrics recommends your metrics project team, comprised of the CSO/CISO, CIO and selected peers, set both a long term strategic view of how your organization wants to leverage its metrics program from the perspective of your business need, as well as short term goals that are tightly tied to specific actions. The short term goals help your project team put a stake in the ground around identifying particular decision making initiatives on which you want to base security metrics and, in so doing, effectively kick start the program.

- Long Term Goal Example: Use metrics to improve the security management of customer-facing information security (e.g., web portals), enabling the company’s strategy of moving business services online.
- Short Term Goal Example: Establish a metrics program to evaluate the value of a specific security investment; such as, establishing a single sign-on system for the next-generation online service.

Step 2: Determine Information Goals
In this second step, your metrics project team uses a “top-down” process to establish a decision tree that specifically identifies the information you want to gather regarding your organization’s overall security strategy and program. For instance, if your organization knew Factor X, you might make Y1 or Y2 decision, which will result in a cost savings of $Z. As a result, metrics can be based around specific activities, such as key investments (e.g., single sign-on, enterprise antivirus system) and key initiatives (e.g., improve patch management, improve password hygiene).
The ability to assign a tangible cost benefit to the value of missing information will help your organization prioritize metrics based on the worth ascribed to them. At this point, it's also appropriate for your metrics project team to begin involving others in the organization that have ownership for various decision making processes, so there's early buy-in around the initiative.

Example: The overall question to be answered is: has this security investment increased the effectiveness of the portal security and, if so, at what cost? Through process diagrams, or cause-and-effect trees, general questions should be decomposed into specific questions, such as:

- Has the control over user access to online applications improved and, if so, by how much?
- Are passwords stronger?
- Are passwords changed more frequently?
- Have support costs increased or decreased?
- Is the extra investment in federated sign-on generating positive ROI?

Step 3: Develop Metric Models

Once your project team has compiled a specific list of what you want to know (e.g., how many weak passwords are in the company), begin the “bottom-up” process of developing the models for generating metrics that produce this information. You should identify all relevant data sources and map them to the information needs to understand gaps and determine strategies for how they can be filled.

Metrics should be calculated and reported by dimensions meaningful to the context, such as access across organization structure (i.e., by business unit), by type of user (e.g., power user), by asset class of system (e.g., critical, low value), by business function (e.g., back office, product line), etc. These dimensions help your team pinpoint common keys and combine data sources to create metric formulas. Metrics combined with one or more dimensions expose concentrations of high and low risk.

Example: Through a series of logical steps, data in the enterprise can be identified, categorized and incorporated into metrics. Carrying the prior example through this process:

- Organize the types of information required into categories (e.g., change in state of access controls, amount of support effort required, password strength)
- Identify data sources across the enterprise that produce potentially relevant information (e.g., access control systems, single sign-on system, trouble ticket system, time tracking system, user directories, password auditing tools)
Connect the types of information produced by the data sources and to the categories of information required (e.g., support effort information and trouble ticket systems, password strength and password auditing tools).

Develop information models for each question, using the available data (e.g., password strength as defined by policy and tested by password auditing tools, password age as the number of days since password change, time spent on support as “lights on” support hours as tracked by timesheet software, etc.)

Identify any gaps remaining between information needs and availability. Some desired data may not be directly observable; as such, proxies or secondary models can be used (e.g., value received from a federated sign-on system can be modeled as the support costs avoided by not directly managing this user base).

Codify the metrics in a specific formula that can be recorded and communicated (e.g., Federated Sign-on ROI from Cost Avoidance = support costs avoided – system cost = current support cost per supported user * number of federated users – investment).

Express metrics by dimensions, obtained by joining source data with organizational or other information (e.g., password strength by business unit, obtained by joining organizational tables with password audit data).

Complete the metric design by establishing and recording the metric specification.

Step 4: Determine Metrics Reporting Schedule and Format

With metric formulas in hand, your project team must next determine how you will present the information in a repeatable and useful format. Your team must create a consistent monitoring schedule and format that fits into your organization’s existing decision making process. This is where “the rubber meets the road”: the metrics solution must enable your organization to produce facts that are useful for real business purposes. The key is to ensure metrics are practical and useful in the day-to-day business environment. A repeatable, regular reporting schedule in a flexible format helps fulfill this challenge by giving managers ongoing critical information in a manner that is easy for them to use, such as scorecards.

Example: In this example, security metrics will be incorporated into existing weekly project review meetings. Once the project is complete, the metrics scorecard will be included in monthly management meetings. The metrics will be distributed as PDF files in the meeting packets, as well as made available through the intranet reporting portal. Metrics will be presented in scorecards, which show complementary sets of metrics designed for specific audiences (e.g., effectiveness metrics for security personnel, efficiency for executive management).
Step 5: Implement Metrics

In this phase, your project team actually implements the metric(s). As with any production process, logical roles should be assigned:

- A metrics lead who selects/approves metrics
- A metrics designer who builds/modifies metrics definitions
- Someone responsible for metrics orchestration throughout the deployment of metrics and management of operations

Ideally, metrics should be implemented so they meet the requirements for a trusted metric -- one that is transparent, in context to the business, flexible, and scheduled. This requirement begs for an automated solution, but one that can embrace transparency and control, while having the flexibility to respond to external changes in data sources, systems, and formulas.

Example: In this case, the metrics were completely automated. Data was pulled on a regular schedule to a central metrics server. Metric results were calculated, the results persisted in a database and the metrics displayed in scorecards using existing enterprise reporting systems. To improve the “buy-in” to the metrics project, each metric result could be viewed stand-alone as a chart and table on the web to check for accuracy and completeness. In addition, the complete specification of each metric was made available for review.

Step 6: Set Benchmarks and Targets

For a metric to be meaningful, it must be accepted. The notion of transparency plays strongly into this concept, meaning stakeholders (CEOs, CFOs, line of business managers, etc.) must understand and trust the formulas on which the metric is based. Additionally, the metrics project team should not overwhelm users with too many metrics. ClearPoint Metrics recommends initially not showing more than seven metrics. Establish a trial period where a number of metrics are tested. Once your metrics project team has generated acceptance around this first set of metrics, you can add targets and levels to the metrics program. Data from this trial period can provide understanding of baseline levels to be used as benchmarks for notifications, goals for improvement, or for establishing action triggers.

Example: Rather than setting specific performance targets, the current states were compared with a baseline measured through manual efforts at the start of the project.
The primary focus was on the change from this baseline due to the security investment. Once the metrics system was fully operational, target setting occurs through the existing “management by objective” process.

Step 7: Establish a Formal Review Cycle

Lastly, organizations should establish a formal review cycle to ensure the metrics remain fresh and useful. Remember that metrics serve purposes and need lifecycle management: data sources, environments and risks are all subject to ongoing change. ClearPoint Metrics recommends a bi-annual review during which the impact of the metrics program is evaluated, the metrics lifecycle is reviewed and those metrics that are no longer relevant to the organization are retired. The metrics should remain focused on current business initiatives to consistently drive results.

Example: Metrics are reviewed annually by the CIO, along with other operational metrics (as part of a review in monthly meetings). In addition, the security department reviews these and other security metrics in depth bi-annually.

MEETING THE SECURITY METRICS CHALLENGE

Your organization can ensure success by following a structured process for implementing a metrics program. ClearPoint Metrics is committed to being at the forefront of helping Global 2000 organizations implement security metrics that have a real impact on business ROI and sharing best practices for putting these programs in place.

ABOUT CLEARPOINT METRICS

ClearPoint Metrics solutions enable IT and Security executives and their teams to consistently and reliably measure, monitor and communicate the state, business impact and effectiveness of their IT governance, risk and compliance initiatives. As both regulatory and best practice frameworks mandate the use of metrics, ClearPoint delivers the hard facts and data that evidence the existence and efficacy of internal controls and the executive views and scorecards that enable evaluation of performance and alignment with business objectives. CIOs and CISOs of leading Global 2000 companies rely on ClearPoint Metrics software and best practice know-how to quickly and cost effectively implement a successful metrics initiative supporting their strategic imperatives and establishing a foundation for constant improvement in safeguarding their organization’s information assets.