ClearPoint METRICS

WHITE PAPER

Best Practice Requirements for Successful Metrics Initiatives

A sound enterprise security initiative requires integration of the right products, processes, policies, and practices throughout an organization.

An increasing number of industry, government, and international regulations require IT organizations to provide confirmative evidence and management oversight of internal security controls. At the same time, best practice frameworks, such as ISO 17799/27002 and PCI DSS, now mandate the use of metrics as a required component of certification. For many organizations, meeting these new objectives requires a revamping of the processes through which IT strategies are formulated and executed. Separate security initiatives and dispersed data silos must become integrated to enable centralized management of IT governance, risk and compliance (GRC) initiatives. And independent tracking and reporting tools must be replaced with strategic metrics initiatives that enable organizations to monitor and communicate the progress of their IT and information security initiatives with greater reliability and consistency.

THE GOAL OF METRICS INITIATIVES

At the highest level, a strategic metrics initiative equips the CISO with the same timely and actionable information that integrated financial reporting and management systems offer the CFO. Metrics enable IT organizations to move beyond self assessments and surveys to deliver hard facts and data that validate the state of IT and information security initiatives and enable better decision making. By automating the entire process of creating, calculating and communicating key performance indicators, IT organizations can:

- Profile high-risk users, assets, and concentrations of risk
- Confidently communicate the state and effectiveness of major initiatives
- Proactively align IT initiatives with business priorities
- Save substantial time and cost in compliance assessment, reporting, and audits
- Drive critical requirements for successful initiatives

A good metrics initiative delivers timely and actionable decision-making information to management so that risk levels can be better identified and corrective actions can be prioritized. Accountability and responsibility for a sound enterprise security initiative requires integration of the right products, processes, policies, and practices across all security disciplines, and all elements of the IT infrastructure.

Based upon intensive interviews with more than 100 CISOs, CIOs, and thought leaders in the area of measuring security, ClearPoint Metrics has identified best practice requirements for both enterprise software and supporting management disciplines. Specific recommendations are offered for designing, deploying, persisting, and publishing metric results in order to obtain strategic and actionable insight for medium to large companies.

Effective metrics design and reporting ensure that each user receives the right trusted information, at the right time, in the right form.

FUNCTIONAL REQUIREMENTS

ClearPoint Metrics has identified five requirements recommended for effective metrics reporting:

- Flexible metric design: Metric initiatives are typically owned by Security analysts, not IT data center operations staff or software developers. Therefore, the tools they use to design and implement metrics should be graphical and intuitive with no programming requirements. This lets analysts adapt metrics to unique business requirements, changing business goals, and changing environments.
- Targeted metric results publication: An adaptable platform supports the communication of metric results with custom processes for entitlement policies, visualization, dissemination, annotation, subscription and notification. Various forms of media such as PDF files, email messages and pre-existing corporate intranets must be supported while leveraging existing tools. The end result is that each user receives just the right information, at the right time, in the right form.
- Metric management framework: A robust, standards-based environment that ensures metrics are: 1) collected from authoritative sources, 2) utilize agreed upon computational techniques, and 3) conform to standards for regular, accurate, and auditable change control. This framework must simultaneously deliver trust, reliability and scalability.
- Metric mapping to business context: A facility for placing metric results into the context of the business and business processes under measurement is required. This is a critical pre-requisite for strategic application of metric results to yield the insight necessary for improving business process effectiveness and efficiency.
- Metric content: Pre-built metrics that can be deployed and run immediately after initial product installation. This reduces time to value, provides examples that can be customized and facilitates the potential for consensus building around industry standards for measuring IT and security issues. Associated with this requirement is the establishment of a Metrics Exchange

– a moderated Web site that offers authorized users access to a library of metric content.

USAGE REQUIREMENTS

The following metric requirements are ClearPoint Metrics' recommended best practices for creating metrics that are effective in guiding an organization to improve security and related processes:

Metrics are intended for strategic and diagnostic use over time spans of at least a week and more likely months, not for operational or minute-to-minute use.

- Trust: All users must trust the metric accuracy, both in terms of the processes used to generate them and the authority of the raw data that drives them. When metric results are reviewed, follow-up discussion should focus on what they mean and how to improve them, rather than the existence of computational or data errors.
- Consensus: The details associated with the computation and raw data used by metrics must first be well understood and represent broad agreement across the user population. Once consensus is reached, the metric definition must be well documented and under strict change control.
- Strategic Focus: Metrics are intended for strategic and diagnostic use over time spans of at least a week and more likely months, not for operational or minute-to-minute use. This contrasts with the many metrics that are currently delivered as part of operational security products such as Security Event Managers, Vulnerability Scanners and Patch Management Systems.

The purpose of a metrics management product is to enhance the maturity of an organization's use of measurement and analysis to transform raw data into valuable information. A metrics management system delivers on this objective by providing a trusted environment that enforces and perpetuates regular, repeatable and auditable metric results collection, computation, persistence and publication. Strategies for improvement are the focus; therefore disputes over data quality or processing algorithm validity are minimized, if not eliminated.

TECHNICAL REQUIREMENTS

In addition to functional and usage requirements, ClearPoint Metrics has also identified several key architectural requirements recommended for security metrics.

- Portability: Metrics are defined in terms of the data sets needed to drive them. This specification has no dependency upon the specific external systems that will be used to populate the data sets when the metric's business logic is executed. Metrics are bound to a customer's unique set of authoritative data sources when the metric is deployed. This enables metric business logic to be equally applicable to any customer environment that can identify authoritative sources for each required input data set.

The separation of metric calculation and communication helps to ensure the consistency and auditability of all published metric results.

- Autonomy: A metric is packaged as an autonomous entity whose only external dependency is the data sources required to populate its input data sets. By imposing this requirement, management of metrics is greatly simplified and sharing of metrics between independent designers is facilitated.
- Scalability: Metrics do not require a data warehouse to run. Metrics can mine data at the edge of the metrics network in which they run. This means that sensitive data is localized typically to a single node and that retained data is limited strictly to the results of metric computation — not all the detailed data that may have been used to create it. External data sources provide precisely the data needed to compute a metric, drastically reducing the amount of data used when compared with classical data warehousing extract-transform load strategies.
- Separation of Design and Production Operations: The environment for designing metrics is physically and logically distinct from the environment in which the metrics execute to generate results. Consequently, introduction of new metrics and their resultant data into production operations can be carefully controlled. Specifically, versioning of metric business logic and assuring the collected results are consistently generated are two key functions that are facilitated by this separation.
- Separation of Calculation and Communication: All communication logic for a metric is encapsulated within the metric business logic and placed under strict version control. The incorporation of computational operations within any publication function is prohibited. This has the key consequence of ensuring consistency and auditability of all published metric results. It also ensures that all metric results are available to the widest possible range of publication facilities without any dependence upon computational idiosyncrasies embedded in publication logic.

Aside from external providers of raw data, ClearPoint Metrics recommends four primary functional components to include in a security metrics program:

- A dedicated, special purpose metric design/test environment
- A network of cooperating computers that forms a distributed, scalable execution environment for metrics that are deployed to run in it
- A framework that allows external publication and reporting systems to access metric results to create Web pages, PDF files, emails and other popular delivery media for metrics
- Pre-built metrics with a plan in later releases to support a metric exchange

Ideally, the sole integration point between the test environment and network execution environment is a “metric deployment package” or MDP. An MDP is

physically a file that contains an install image for a metric into an existing production network. The sole integration point between the metrics network and the publication framework is the metric results database, a standard accessible repository. Typically, each metric is associated with precisely one table in this results repository.

SUMMARY

Security metrics are essential to managing and communicating strategic IT and information security service objectives and establishing processes for constant improvement. The most effective vehicle for instilling responsibility, accountability, and ownership for a program of constant improvement is through the implementation of an enterprise-wide IT and security metrics management program. Measuring and reporting on the performance of IT and security meets the emerging executive demand for better alignment and improved communication of IT and security initiatives with business objectives and processes, as well as the replacement of costly and inefficient manual procedures. By following the recommended requirements in this paper, organizations can successfully achieve a performance management and metrics program based on best practices.

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. www.clearpointmetrics.com.

8 New England Executive Park • Burlington, MA 01803 • P(617)-456-1900