

A Case for Centralized Security Metrics Reporting in State Governments



*Prepared by the Multi-State Information Sharing and Analysis Center
Cyber Security Metrics and Compliance Workgroup*

www.msisac.org

This document was prepared by the Multi-State Information Sharing and Analysis Center's Cyber Security Metrics and Compliance Workgroup, whose members are listed here. Special recognition to Julie Schuller for her work in drafting the document.

Art Bess	Alabama
Aaron Carpenter	Arizona
Leesa Morrison	Arizona
Seth Kulakow	Colorado
Sree Shama	Georgia
Caroline Bradley	Indiana
Richard Smothermon	Kentucky
Mark Kemmerle	Maine
Eric Tumbarella	Michigan
Mark Mathison	Minnesota
Christopher Sinrud	Montana
James Delaney	New Jersey
Karen Sorady	New York
Scott Hicks	North Carolina
Jeff Brown	North Dakota
Ken Ontko	Oklahoma
Keith Boden	Pennsylvania
Jason Gunnoe	Tennessee
Michael Allred	Utah
James Lipinski	Vermont
Michael Biagioli	Wisconsin
Ron Last	Wisconsin

A Case for Centralized Security Metrics Reporting in State Governments

Introduction

In the words of Lord Kelvin, “If you cannot measure it, you cannot improve it.” This maxim holds true today as it applies to information security and the need to accurately measure an organization’s security posture. Meaningful security metrics are critical as States grapple with regulatory and risk management requirements and diminishing state coffers require shrewd security investments.

The Value of Security Metrics

Security metrics can be an invaluable resource for assessing the effectiveness of an organization’s information security program. Meaningful metrics can be used to continually improve a security program’s performance, substantiate regulatory compliance, raise the level of security awareness among management and stakeholders, and assist decision-makers with funding requests.¹ Although some may argue the value of metrics, leading corporations and entire industry sectors deem it the only feasible means for managing information security risks. Without metrics, organizations are reduced to operating their security programs under FUD: fear, uncertainty, and doubt.²

Road Map to Effective Metrics Reporting

Security is all about control and “security controls” are a key objective of any information security program. Meaningful security metrics allow an organization to determine the effectiveness of its security controls.² In order to effectively measure the security posture of an organization, States must first ensure that the proper framework is in place in order to derive meaningful metric data. This includes a security governance model suited to the entity’s strategic and operational requirements. Such a model should support implementation of practical information security policies and procedures, consistent deployment of best practices and measures, and require strong executive management support across the organization.³

Best practices dictate a model where “security is managed as an enterprise issue, horizontally, vertically, and cross-functionally throughout the organization.”⁴ This model is better suited to enable consistent monitoring, measurement and reporting of an

¹ S.C. Payne, Guide to Security Metrics, Charlottesville, VA: IT Security and Policy, University of Virginia, July 2008

² A. Jaquith, Security Metrics: Replacing Fear, Uncertainty, and Doubt, Pearson Education, Inc., March 2007

³ S. Radack, Using Performance Measurements to Evaluate and Strengthen Information System Security. Gaithersburg, MD: Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, July 2008

⁴ J.H. Allen, J.R. Westby, Governing for Enterprise Security (GES) Implementation Guide. Pittsburgh, PA: Carnegie Mellon University, Software Engineering Institute, CERT, August 2007

organization's security posture. An article in CSO Magazine advocates centralized governance or a somewhat hybridized model:

“This structure gives executive leadership and board better oversight as there's only one place to go to assess the posture of an organization. Managing the controls once implemented is generally a unit-level function, however monitoring and measuring the effectiveness of the controls should be shared. While the business unit will likely want to monitor the results, the central governance group will need insight as well. Reliable, objective metrics will be required to assure senior leadership that the program is effective. To ensure unbiased reporting, unit personnel should have reporting relationship to the central governance body.”⁵

However, some States' security programs may be less mature, utilizing a more distributed or ad-hoc model. While decentralization may allow flexibility and empower individual business units, this model may adversely affect the organization's ability to assess and improve its security posture, particularly if there is not a consensus on the implementation and measurement of security controls. As a best practice, organizations should implement a high-level control over its security function that includes a steering committee or equivalent body that has support from executive management in order to coordinate information security activity throughout the organization. In addition, information security activity should be coordinated in individual business units.⁶

The Control Objectives for Information and related Technology (COBIT) considers an organization to be at the high end of its maturity model when it integrates metrics across all IT projects and processes and “the reporting of monitoring results is being standardized and normalized.”⁷ By implementing a consistent centralized reporting mechanism, a State will facilitate the efficient and consistent collection of quantifiable metrics to reach the overall goal, which is continuous process improvement.

The reporting of metrics is as important as the metrics themselves. To ensure the quality and validity of metrics data, a State should have a standardized and clearly defined metrics collection and reporting process in place. The National Institute of Standards and Technology (NIST) advises:

“The importance of standardizing reporting processes cannot be overemphasized When organizations are developing and implementing processes that may serve as inputs into an information security measurement program, they must assure that data gathering and reporting are clearly defined to facilitate the collection of valid data Establishment of an information security measurement program will

⁵ A. Agle, Information Security Governance: Centralized vs. Distributed. CSO Magazine, September 2008

⁶ Information Security Forum, The Standard of Good Practice for Information Security 2007

⁷ The IT Governance Institute, Control Objectives for Information and related Technology COBIT 4.1. Rolling Meadows, IL, 2007

require a substantial investment to ensure that the program is implemented in a way that will maximize its benefits. Benefits of the program are expected to outweigh the costs of investing resources to maintain the program.⁸”

Summary

Security must be managed effectively in order to be measured effectively. As states struggle to protect valuable information assets and justify risk-based decision making, a centralized metrics reporting mechanism is crucial for producing meaningful metrics and providing an ongoing assessment on the state of security.

⁸ E. Chew, M. Swanson, K. Stine, N. Bartol, A. Brown, W. Robinson, Special Publication 800-55: Performance Measurement Guide for Information Security. Gaithersburg, MD: Information Technology Laboratory, National Institute of Standards and Technology, July 2008