@ISACA
RELEVANT, TIMELY NEWS
Volume 6, 14 March 2012

Five Things to Consider When Developing Information Risk Management and Security Metrics

By John P. Pironti, CISA, CISM, CGEIT, CRISC, CISSP, ISSAP, ISSMP

1. **Provide enhanced business value via metrics with thresholds and business context**—When developing, analyzing and reporting metrics it is important to identify if the corresponding measures are considered acceptable or unacceptable to the intended audience. When developing metrics and reporting capabilities collaborate with the intended users to establish positive and negative thresholds that can be used to identify when greater attention or action is required. Metrics should also incorporate contextual parameters and insights (such as seasonality considerations) to ensure that they are agile enough to account for changing business activities and conditions.
2. **When developing metrics and reporting capabilities, collaborate with the intended audience to ensure value to them**—Metrics and reports that are developed without direct involvement of the intended audience can result in them not being useful. When developing metrics and reporting capabilities, do not assume you know what the intended users will find valuable. Instead, collaborate with them to understand their requirements and interests. This can be an opportunity to develop expanded requirements that you have identified could provide them value, but that they may not have considered.
3. **Be consistent in metrics data collection and activities processing**—For metrics to provide consistent value to an organization, they must have integrity. It is acceptable to make adjustments to the methods and practices used for the collection and processing of data; when in their initial deployment, metrics should be noted in any reporting that is provided. If possible, data collection and processing should be kept consistent for at least one year or business cycle prior to making any material adjustments. This will minimize any concern about the integrity of the metrics or measures and will allow for the comparison of historical data when the adjusted methods and practices are implemented.
4. **Ensure that the legal and enterprise risk elements of your organization are comfortable with the metrics and reporting that are being collected and**

documented—Metrics and reporting can be both a positive and negative force within organizations. Metrics and their associated reports often provide value to stakeholders within organizations by increasing visibility into their activities. At the same time, metrics can be used against the organization in litigation or misinterpreted by public opinion, if they are disclosed. It is important to consult with the legal and enterprise risk management functions within your organization, to ensure that they are comfortable with the tracked metrics and generated reports. In some cases, the existence of these metrics and reports may be considered a liability to the organization, in which case they should not be generated or documented.

5. **Identify actionable vs. informational metrics and measures**—Metrics and measures typically fall into one of two categories: actionable or informational. When developing metrics and measures, identify this classification to allow the intended audience to understand the purpose of the metrics and measures. Actionable metrics and measures typically have a specific purpose and audience. Informational metrics and measures often have a broad-spectrum of uses and interested parties that can benefit from them.

John P. Pironti, CISA, CISM, CGEIT, CRISC, CISSP, ISSAP, ISSMP, is the president of IP Architects LLC.