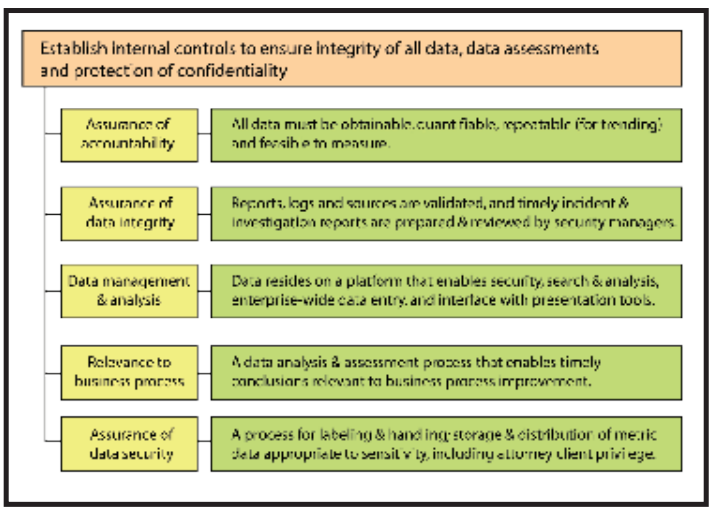
# Accuracy & Integrity: Essential Metrics Characteristics

By George Campbell

There is an old saying that there are three types of lies: "lies, damn lies and statistics." I won't dwell on the obvious downside of lies or damn lies in our job, but I will underscore that statistics, when calculated hastily or from poorly managed data, are no better than lies. We must have accuracy and integrity in our use of data and statistics, or we will undermine our initiatives, our programs and our own standing with senior management. Here are five components of a reliable system for managing metrics-relevant data:




**Assurance of accountability.** You don't need a dedicated staff or individual to maintain a quality metrics program. Whether your scope includes the full range of security services; or, if you are a sole practitioner overseeing the physical security program, you must hold specific individuals accountable for maintaining the integrity of data that could be used for metrics and program management. If you rely heavily on vendors to provide day-to-day security service delivery, do not fail to incorporate contractual standards on reporting and data administration.

**Assurance of data integrity.** Consider these two key objectives for our security measures and metrics: 1) to positively influence action, attitude and policy, and 2) to materially impact exposure to specific risks. The visibility of these objectives imposes the highest standards of data integrity. We can only craft strategy and tactics to effectively target specific risks if we have reliable data processed by competent, focused analysis. Imagine the potential consequences of drawing conclusions and formulating recommendations based on inaccurate, unreliable data overseen by flawed, poorly supervised sources!

**Data management and analysis.** You can maintain a solid metrics program with standard desktop applications like Excel and PowerPoint. But scalable, commercially available incident reporting software provides a more tailored and robust infrastructure for standardized reporting, facilitates customized administrative routines, and enables quantitative analysis and trending.

**Relevance to business process.** Appropriate data management for security metrics supports security program planning, management and performance assessment. But it also enables us to analyze a variety of risk and program-specific data, to draw conclusions of measurable relevance to business risk management. We seek to structure measures and metrics that inform (increase awareness) and assess the effectiveness of internal controls. Remember, we seek to influence policy and enable the business to more securely engage in business activities that might otherwise be too risky.

**Assurance of data security.** A measurably effective metrics program will store and generate a variety of outputs containing highly sensitive information. Reporting on risk is risky business — it may reflect on corporate reputation. Think about a presentation to top management or the Board on investigative findings related to employee misconduct or the need to address significant vulnerabilities in the protection of customer information. This is potential stuff for the upper-right-hand corner of The Wall Street Journal. As the need for such metrics is identified, you may want to discuss special protection of the files and outputs with General Counsel. They may want to apply attorney-client privilege for any material that may be generated with regard to reports on matters of high sensitivity.

A classification scheme consistent with information protection policy should be applied. If for some reason there is no such policy at your company, seek guidance on confidentiality labeling, distribution and secure storage. Remember, the data we cull from our logs, incident reports, storage media and other sources are discoverable in litigation for negligent security or other legal matters.

A qualitative security measures and metrics program is founded on an established and clearly communicated set of internal controls focused on the integrity of the data that is gathered, the quality of the analysis and assessment applied to that data, and the assurance of data protection. Failing to embed these principles into your metrics program will eventually damage the credibility of the security program and its management. ■

*George Campbell is emeritus faculty of the Security Executive Council (SEC) and former CSO of Fidelity Investments. His book, Measures and Metrics in Corporate Security, may be purchased through the SEC Web site. The SEC is a research and services organization. Its community includes forward-thinking practitioners, agencies, universities, NGOs, solution providers, media and industry groups. Backed by a Faculty of more than 100 current and former security executives, the Council creates Collective Knowledge™ research, which is used as a foundation for its deliverables. For more information about the Council, visit www.securityexecutivecouncil.com/?sourceCode=std.* 