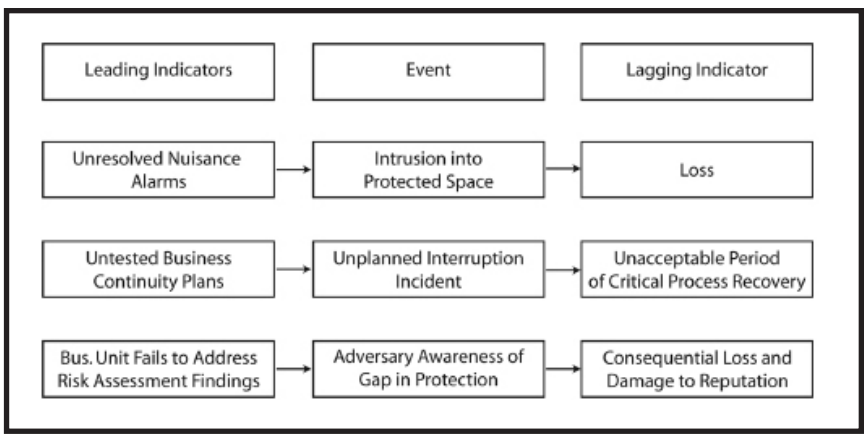
Tracking Leading and Lagging Indicators

By George Campbell



Senior management and analysts in the businesses we serve are constantly tracking and evaluating a host of economic and programmatic indicators to provide alerts on changes in market conditions that need to be addressed. A leading indicator signals a future event — it measures the current state of the market or the business, as well as the future state, in the form of already planned or projected changes. A popular analogy is the traffic light: A yellow light is a leading indicator of a red light, because yellow always precedes red.

A lagging indicator follows an event — it measures past activity up to the current time. A yellow light is a lagging indicator of a green light, because yellow follows green. Both types of indicators can be analyzed to identify repeating patterns that may help to forecast future activity.

Objective: We are paid to anticipate and understand the potential of some event taking the wrong turn. A proactive corporate security program establishes and operates a set of warning signals that provide indicators and clues to various risks. We need to understand which ones offer the best estimate of future problems and risk exposure. Tracking leading and lagging indicators is part of that landscape of risk monitoring and awareness.

Strategy: Leading and lagging indicators can define patterns that may be predictive, although the likelihood of events is subject to a variety of influences. Such indicators should not be seen as templates for knee-jerk response. They require analysis — especially where they relate to more significant areas of enterprise risk. In our world, leading indicators signal future risk of security-related events. They are measurable factors that change before the risk starts to follow a particular pattern or trend.

- Unresolved nuisance alarms are leading indicators of future risk, while reduced false and nuisance alarm rates are a lagging indicator of previous steps taken to improve alarm system reliability.
- A high number of viruses and bugs reported to security administration after a new software implementation may be a lagging indicator of poor preparation for launch, whereas a high number of virus updates and patches implemented before the new implementation may be a leading indicator of launch success.
- Hiring an individual whose background investigation revealed material misstatements on a personal history application and a notable history of prior wrongdoing is a clear leading indicator of potential integrity issues in future employment. In the same space, increasing rates of derogatory background investigation results in regional hiring pools is a lagging indicator of problems in HR recruitment campaigns.
- Could a proposed reduction in first responder headcount be a leading indicator of a decrease in the percentage of security operations response times that meet the four-minute standard?

What would we conclude from internal misconduct incident post-mortems revealing a consistent trend of poor supervisory oversight? What about a workplace violence trend at a facility where notable increases in alcohol-related assaults on a late shift were isolated as a causal factor? Leading indicators can provide good predictive factors if your data is verifiably solid and enables trending over time. Returning to our traffic analogy, tracking lagging indicators without forward-looking analysis is like looking through a rearview mirror and missing the problem in the road directly ahead until it is nearly too late.

Lagging indicators are typically generated by counting — they offer numbers but beg for context and actionable conclusions. Standing alone, they do not reveal much about how a security strategy is working — they can waste the constituent's time, which is a big problem. This is another reason why incident post-mortems are so critical. They use vetted past data to provide verifiable, analysis-based results that can be factored into indicators of future exposure to a targeted set of risks. ▮

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 risk mitigation research and services organization for senior security and risk executives from corporations and government agencies responsible for corporate and/or IT security programs. In partnership with its research arm, the Security Leadership Research Institute, the Council is dedicated to developing tools that help lower the cost of security programs. For more information about the Council, visit www.securityexecutivecouncil.com/?sourceCode=std.