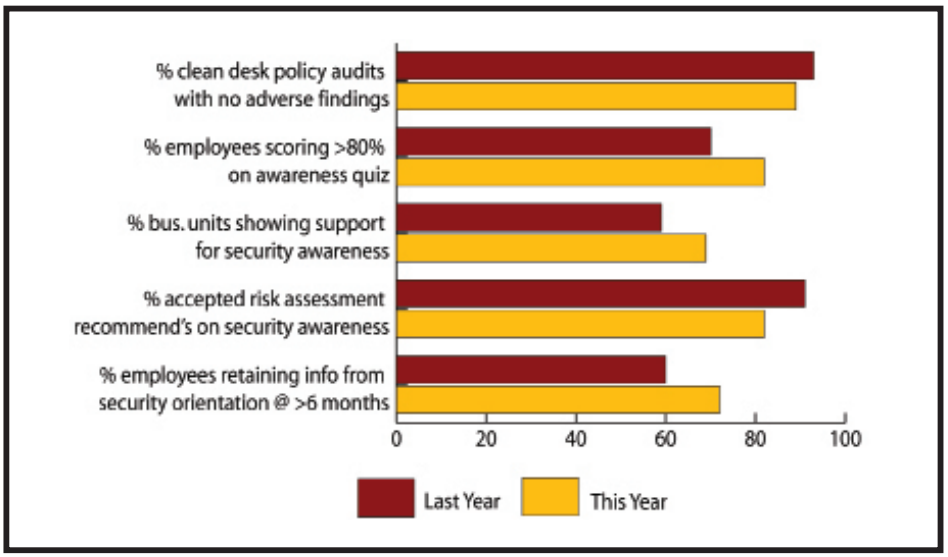
Security Awareness: A Few Key Indicators

By George Campbell

Security's ability to educate and empower their customers in their risk management responsibilities is a fundamental element of any business protection strategy.

Objectives: To develop a multidimensional security awareness program that incorporates a marketing and communication strategy focused on key areas of employee safety, corporate integrity and business process security and resiliency. To identify relevant areas of risk awareness that the targeted population should address.



Strategy: If your company thinks Security is the owner of security-related business risk, get your résumé up to date! We are paid to understand the range and depth of risks confronting the business in its various environments, to build strategies to mitigate them, and to educate our constituents on their responsibilities. Business process owners' awareness is a fundamental element in a security risk mitigation strategy.

If you expect key individuals and groups to conform to policy and procedures, you must use focused communication to ensure that they are aware of those requirements. So, what is Security's brand at your company and to whom do you sell it? Think about it. You have products to sell to senior management, the Board, employees, partners, vendors and visitors. What is your tagline — your brand that guides and frames the message for your constituents? How are you "selling" accountability for business protection?

We have to craft messages that connect in actionable ways with the individuals and organizations responsible for business process integrity and continuity. Your unique knowledge of and perspective on business and personal risk is the raw material you must use to design your mix of products and services. The challenge is to determine what risk management knowledge has to be passed on to whom. Seek out advice from your company marketing and communications departments. They can point your messages in highly productive directions.

Security awareness is measurable. Actionable measures and metrics for risk awareness may be derived from a variety of sources:

- Risk assessment findings provide qualitative data that needs to be fed back to appropriate business units to make them more aware of their accountability.
- Risk events and profiles identify unmanaged exposures that need to be communicated. You can determine the absence or degree of measureable improvement in risk exposure or conformance to policy by conducting follow-up testing of your awareness initiative to see how well the messages got across.
- Formal feedback surveys and interviews can identify the level of security awareness within targeted populations. A useful technique is to use the corporate intranet to quiz users and engage in random polling on risk or procedural responsibilities.
- Incident post mortems, lessons learned and victim interviews provide a rich source of information on gaps in security awareness.
- Security department customer satisfaction surveys can ask how well respondents understand Security's messaging and how effective the communication media is.
- Policy audits, such as clean desk policy checks performed by evening shift security officers during rounds.

The graphic above provides several simple examples of key security awareness indicators. By using percentages of movement over time, you can easily measure improvement or decline. Do not neglect to measure the level of support that business unit management shows for awareness initiatives and corrective actions resulting from risk assessments.

Corporate security and brand protection is every employee's job. The quality of your connection — your actionable messages — with them is a key element of security 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 that involves a range of risk management decision makers. Its community includes forward-thinking practitioners, agencies, universities, NGOs, innovative solution providers, media companies and industry groups. Backed by a Faculty of more than 100 successful current and former security executives, the Council creates groundbreaking Collective Knowledge research, which is used as an essential foundation for its deliverables. For more information about the Council, visit www.securityexecutivecouncil.com/?sourceCode=std.