

Create a Security Awareness Dashboard

By George Campbell

One of the fundamental obligations we have in corporate security is to understand the potential for “what if” and communicate our knowledge and concerns to 1. those who could be affected; and 2. those who have accountability for protecting the assets of the enterprise.

Objective: Security awareness is a core element of our mission, and one of our core competencies must be effective communication. We view the security risk landscape from a unique perspective, and this provides us with the knowledge that is essential to assigning accountability throughout the business — to ourselves and to others.

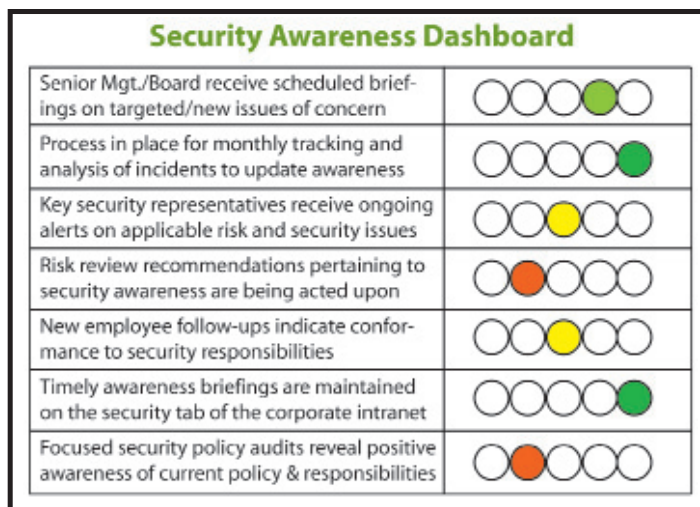
Strategy: What you see here are seven fairly obvious checkpoints for a basic security awareness program. They involve and reflect a few key management principles:

- **Management needs to communicate their expectations to employees.** New employees are made aware of their security responsibilities, and there is a process in place to affirm their ongoing awareness. We know that when employees are first hired, the messages they receive in the sea of signing forms, learning about benefits and listening to speeches are too soon lost in the transition. This post-orientation process is essential to ensure that security-related responsibilities are understood and fulfilled.

- **There are processes in place to proactively identify areas of risk and their root causes.** Security management has established a process for monthly tracking and analysis of incidents to update awareness. Are you just storing your workload and investigative data, or are you routinely using it to enhance your understanding of risk dynamics and the effectiveness (or ineffectiveness) of your security programs? Risk is a moving target. If we are to depend on people in the business to share the responsibility for asset protection, we must keep them up to speed with timely risk assessments. Where risk assessments indicate a lack of security awareness or understanding of responsibilities, there is a process to resolve these gaps and confirm the responsiveness of appropriate individuals or groups. We know that proactive risk assessments combined with incident post-mortems often find that a lack of employee awareness or apparent ignorance of policy or procedure directly contributes to or exacerbates incidents. Our example raises concern that appropriate corrective actions are not being taken.

- **Responsive actions are taken when risks are reported.** In the simple dashboard above, we see that senior management and the Board are routinely briefed on emerging areas of risk and the effectiveness of programs calculated to mitigate risks targeted for action. Regardless of where the security function is placed in the organization or what piece of the risk management mission it serves, it should be routinely informing and advising senior management on selected areas of risk and brand protection. Accountability can only be ensured when selected individuals within business functions — your key security representatives — receive actionable information and alerts on risk and security issues appropriate to their responsibilities. Timely awareness messages or short briefings should be maintained on the “security” tab of the corporate intranet. This is another way to keep employees engaged and ensure that appropriate awareness messages are out there. Messages need not be flashy and should not be lengthy but should eliminate plausible denial.

- **There are internal controls and checks to confirm that accountable parties are fulfilling their responsibilities.** Focused security policy audits reveal positive awareness of current policy and responsibilities. Just as an incident post-mortem can reveal a vulnerability



related to the lack of awareness or knowledge, so the internal audit program should incorporate reviews of employee awareness of security policy and procedure.

This simple chart conveys the Security manager's status report to his boss on a few key security awareness indicators. What story would you tell if this were your assessment of security awareness in your company? ■



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 problem-solving research and services organization that involves a wide range of risk mitigation leaders. Its community includes forward-thinking practitioners, agencies, universities, NGOs, innovative solution providers, media companies and industry groups. The Council creates groundbreaking Collective Knowledge™ research, which is used as an essential foundation for its deliverables. For more information, visit www.securityexecutivecouncil.com/?sourceCode=std. The information in this article is copyrighted by the Security Executive Council and reprinted with permission. All rights reserved.