Warning Signs of Security's Decreasing Influence, Part II

By George Campbell

Last month, we began exploring how to determine whether our corporate security program is effective. To start, we should be able to answer "yes" to these three questions:

1. Does the program have the influence to help eliminate risky business practices? If we clearly and competently advise on risk and things do not change, something is wrong.

2. Do employees and management accept the concept of shared responsibility for asset protection? If the business thinks you protect the company, you have failed to communicate and ensure that line business managers are the custodians of the assets and you provide the tools and first response.

3. Does management believe the security program is adding value? Where is the perceptible value here? If you really look at these examples, you are calling and nobody is answering or your risk management programs are *visibly* ineffective.

In the previous column, I listed five warning signs of decreasing or deficient influence. The following five examples clearly indicate deficient influence: 1. Imposed budget reductions made without consideration of increased risk; 2. Realignment of Security at a lower level, impacting unfettered access to the top; 3. Increased number of risky external relationships with no security review; 4. Increasing frequency of *inadequate* first response to security incidents; and 5. Failure to uncover common contributing causes to multiple, diverse security incidents.

Here are five more warning signs that could result in serious risk to the company. Examine your own program to see if any of them apply. If you think they may, what steps can you take to affirm your concerns, and how would you propose to reverse the trend?

Five More Warning Signs

1. Continuing findings of exploitable vulnerabilities. You have conducted a risk assessment or a post-incident lessons-learned exercise that revealed exploitable gaps in security measures. You have notified responsible managers and business units of these gaps and recommended ways to close them, but in spite of your advice, on inspection, the vulnerabilities persist. Where and why has your ability to influence change broken down?

2. Increased (or unresolved) audit findings of security program deficiencies. Serious security deficiencies are on auditors' watch lists. When the identified vulnerabilities go unresolved, management will wonder why security has not been successful in either directly or collaboratively impacting the elimination of the known problems. Increased deficiencies are a clear red flag that the security program, at some level, does not take the threat seriously. This may escalate to the Board's Audit Committee and you do not need this sort of top management attention.

3. Increased bypassing of basic security safeguards. Propped doors, card readers consistently in access mode, hiring persons with adverse background findings, discounting specific asset protection procedures — the list goes on. You have installed safeguards that are being disabled. Have you effectively sold the rationale for these security measures? Are you tracking the consequences? What do you need to do to gain the confidence of employees and managers?

4. Decreasing ability to influence or have a say in sanctions on internal misconduct cases. Your investigation has validated that an employee has been involved in wrongdoing. Now the employee's advocates totally discount (or worse, even fail to consider) your views on precedent and sanctions. While Security does not decide the outcome in these cases, your ability to bring your findings to bear is a legitimate test of your influence.

5. Increased frequency and/or severity of security infractions, accidents, crime or other *preventable* risk events. The risks on our watch are dynamic. We have a responsibility to develop and maintain metrics on the direction of key trends and recommended mitigation strategies. What are we to conclude when the trends continue to grow after we communicate information on increasing risk and attempt to engage appropriate parties in solutions? Are they listening and taking positive action based upon our good advice? We need to look inward at how we frame our messages for influential impact.

Next month, I will share five more alarm bells related to our influence over specific types of business risk. What does this have to do with security metrics? Everything! Our measures and metrics are the stories we tell to inform management on, influence and assign accountability for maintenance of standards of protection. ST&D

George Campbell is emeritus faculty of the Security Executive Council and former CSO of Fidelity Investments. His book, "Measures and Metrics in Corporate Security," may be purchased through the Security Executive Council Web site. The Security Executive Council is a member 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 effective tools members can apply in their programs, program documentation and establishing security as a recognized value center. For more information and inquiries on membership requirements, 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.