Warning Signs of Security's Decreasing Influence

By George Campbell

How can we tell if our corporate security program is effective? To start, we should be able to answer "yes" to these three questions:

1. Does management believe the program is adding value? Absent that, you are a liability in a competitive marketplace.

2. 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, what is wrong with this picture?

3. 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.

In the next few months, I would like to share some alarm bells that may indicate that the security program is falling short of success in these critical areas.

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.

Take a look at the following five indicators of decreasing influence and examine your own program to see if any of them apply. If you think they may, what steps could you take to affirm your concerns and how would you propose to reverse the trend?

Five Warning Signs

1. Imposed budget reductions made without consideration of increased risk. I am aware of a number of examples of this, especially in these challenging economic times. But while we may want to rack this up to tough decisions on priorities, we have to ask how well we have made the case for exposure to risk and the cost of protection.

2. Realignment of Security at a lower level, impacting unfettered access to the top. This is a frequent follow-on partner of risky budget cuts, but it may have even greater impact on the program. The more we are insulated from access to those who influence policy and behavior, the less able we are to make change happen. Every level imposes its own agendas, and yours may not make the list.

3. Increased number of risky external relationships with no security review. Outsourcing is a business paradigm and is likely to remain (if not increase) as we compete globally. Where the processes being outsourced are acknowledged as inherently risky, to what extent are your programs engaged early on to be an integral element in the due diligence process? How are the contractual conditions structured to incorporate elements of security oversight or affirmation of compliance? Are you a real part of the strategic business model?

4. Increasing frequency of inadequate first response to security incidents. You do not share this one, you own it! You are paid to understand the more likely events that are assignable to your portfolio. Your resources (plans, people, equipment, etc.) should be prepared to respond in a highly competent manner to mitigate the threat on a timely basis.

5. Failure to uncover common contributing causes to multiple, diverse security incidents. This one may seem less clear than other indicators, but it may be the most critical given the unique perspective on risk your data should provide you. If you have done your lessons-learned on various types of incidents, you should have a body of data on the real contributing causes of events and what needs to be done to mitigate future risk. If you have not, you do not understand your obligation to learn on behalf of your employer's risk management objectives and to influence policy and behavior on eliminating future events.

Are they listening and taking positive action to our advice? Next month I will have thoughts on how you might approach greater influence over specific types of business risk. STD

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 SEC Web site. For more information on the SEC and inquiries on membership requirements, visit www.securityexecutivecouncil.com/?sourceCode=std.