SEC

SECURITY EXECUTIVE COUNCIL

A research and advisory firm

METRICS FOR SUCCESS

Is Your Security Program Viewed as Effective?

Warning Signs of Security's Decreasing Influence

George Campbell

Originally Published in Security Technology & Design

November 2008

How can you assess if your corporate security program is effective? To start, you 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.

I will 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?

Warning signs to watch for

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 like-y 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 pre- pared 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 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.

Five more warning signs that could result in serious risk to the company

Examine your own program to see if any of these apply. If you think they may, what steps can you take to affirm your concerns, and how would you propose to reverse the trend?

1. Continuing findings of exploitable vulnerabilities. You have conducted a risk assessment or a post-incident lessons- learned exercise that revealed exploit- able 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.

Alarm bells related to influence over specific types of business risk

I have covered several kinds of warning signs, from budget reductions without consideration of increased risk, to continuing findings of exploitable vulnerabilities, to unresolved security-related audit findings. I will conclude with five more:

1. Security is not consulted before management makes changes to processes, products or relationships with evident security risk impact. Note the word "evident" in this sentence. Ignorance is one thing, but when it is clear that changes involve probability of risk and management still decides not to include us, we are a marginalized player at best.

2. Management fails to approve Security's recommendation for development and communication of a new or revised security policy to mitigate a consistent pattern of risk. What should we conclude when we have a convincing story on what steps should be taken to mitigate risk and they decide to leave things as they are?

3. Increased downtime of critical security safeguards that fail and go unattended. Think about this one! You have a "critical" safeguard (like a duress alarm in the executive suite or consistent unauthorized access to a sensitive area) that is unreliable and nobody is fixing it! Are you watching the dials on your dashboard? Two possibilities: either you are

unaware of these vulnerabilities, or you have failed to take appropriate action. In both cases, count on your stock taking take a big hit sooner rather than later.

4. Security fails to effectively analyze its data on security incidents and there- by invites future risk that will seriously deplete leadership's confidence in us. While this closely resembles #3 and others, it really goes to the failure to establish a comprehensive, disciplined and ongoing process of incident and workload analysis. What are the trends and the common denominators? What steps are working and where are the gaps?

5. Decreasing engagement of essential internal partners in matters of clear security concern. This is not an isolated shortcoming — it is a summary result of all the failures mentioned in this series. You have not connected the dots between your security and risk message and the responsibilities of your organization's employees and business leaders. You either have not spoken their language or they have tuned you out.

Why metrics can proactively protect against waning influence

I have illustrated 15 danger signals that may indicate failing influence on critical issues or will clearly damage the credibility of the security organization and its leadership. Metrics provide an early warning system — they enable positive influence, action, attitude and policy. You have the data, now take an objective look at the competence of your data management capabilities. What metrics really make a difference in your contribution to value and your ability to influence results and standards of protection?

For a guide on how to build a security metrics program that will help you demonstrate security's value through clear alignment with business strategy and objectives, see "A Security Metrics Story: Turning Data Into Metrics."

About the Security Executive Council

The SEC is the leading research and advisory firm focused on corporate security risk mitigation solutions. Having worked with hundreds of companies and organizations we have witnessed the proven practices that produce the most positive transformation. Our subject matter experts have deep expertise in all aspects of security risk mitigation strategy; they collaborate with security leaders to transform security programs into more capable and valued centers of excellence. Watch our 3-minute video to learn more.