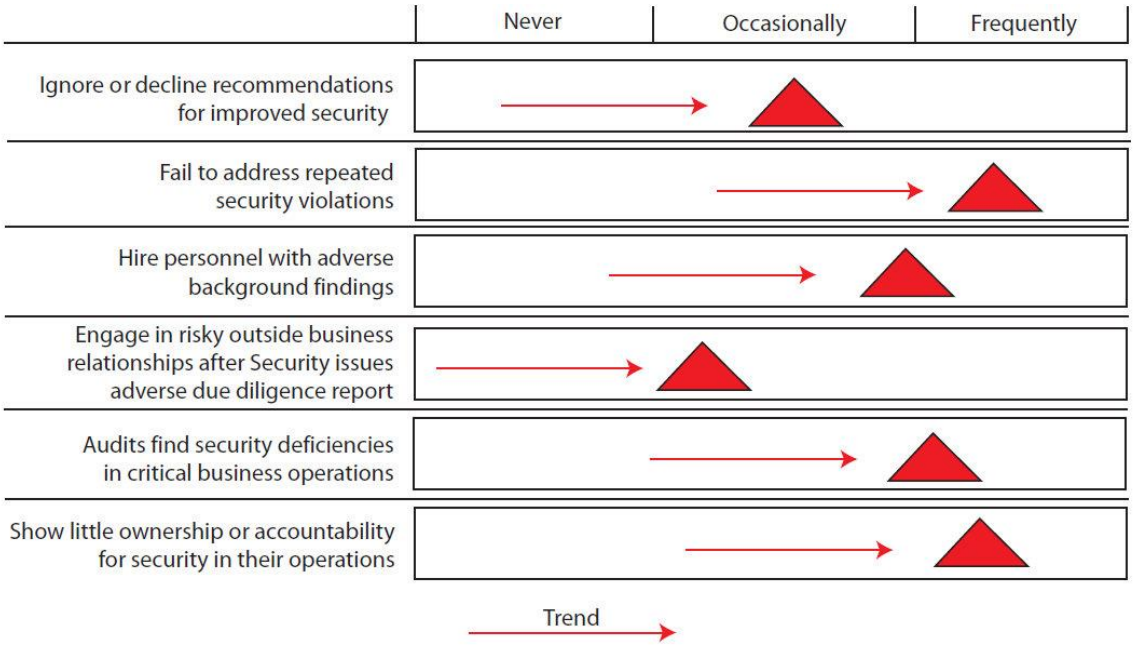
SEC
SECURITY EXECUTIVE COUNCIL
A research and advisory firm

Security Metrics > Business Alignment >

Do Business Units Value Security Recommendations?

Created by George Campbell, Security Executive Council Emeritus Faculty

Our ability to influence internal customers starts and ends with their perception of the effectiveness and value of security programs. We have to test this perception on a periodic basis, because the results provide opportunities to consider the effectiveness of our programs and alternative approaches to both risk and relationship management.



An obvious way to track customer confidence is to look at whether business units are accepting Security's recommendations in key areas. In the example from which the graph above is drawn, the security director has been tracking several program criteria that should be valid indicators of Security's perceived credibility.

There's a little good news and a lot of bad in these results. The good news is that there is a program to track results in several core areas. The bad news is that there seems to be a dramatic disconnect between security and the rest of the business.

First, there is a consistent set of adverse trends across the range of programs. Next, these findings may indicate more fundamental exposures to corporate risk that are not being effectively mitigated by established security measures, and that points to weakness in the security director's leadership. Finally, I have to conclude that senior company management has failed to communicate that they expect business units to play a role in brand protection and corporate integrity. This is clearly impacting the security director's ability to lead and influence results.

Consider these findings:

1. Business units ignore or decline recommendations for improved security *occasionally, but trending up.* This is about as basic a measure as you can find. You have delivered multiple recommendations to address security gaps, but your findings have had a minimal impact on the state of protection. Did the business fail to connect the findings to real business risk? Security needs to take a hard look at the quality of its findings and presentation. They should also consider a new approach to visibly escalating non-compliance.

2. They fail to address repeated security violations *increasingly frequently.* If this company had any sense of the relationship of security risk to corporate risk, this would be on the audit committee agenda. This result clearly shows the security director's failure to lead and influence with the facts, exacerbated by an unsupportive tone at the top.

3. They hire personnel with adverse background findings *occasionally, but trending up.* Business units do not know how to relate a bad background to a potential risk in their midst. Security has not adequately communicated the consequences of hiring people who have not been truthful in the process. The Director needs to engage with his counterpart in Human Resources to validate this program. Here is another area where Security should be helping senior management to connect the dots.

4. They engage in risky outside business relationships after Security has issued an adverse due diligence report *infrequently, but trending up.* Security is showing the business that there are risks in a proposed relationship, but they choose to partner anyway. The business doesn't get it, so Security needs to work with Audit to maintain a risk watch on these outsourced operations.

5. There are notable audit findings with regard to security deficiencies in critical business operations *frequently, and trending up.* This is a clear and independent assessment that reinforces a failure in the status of corporate governance and security management leadership.

6. Business units show little ownership or accountability for security in their operations *frequently, trending up:* An obvious conclusion of significant shortcomings in the objective of shared responsibility for asset protection.

Is this quarterly assessment a reflection of totally inadequate security management or an indictment of this company's senior leadership's failure to provide the Security Director with a clear charter and mandate to impact corporate policy and behavior? Perhaps it is a combination of both. Remember that this is an ongoing assessment process.

What would you do to turn this company around on these performance indicators?

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 information in this article is copyrighted by the Security Executive Council and reprinted with permission. All rights reserved.*

Originally published in Security Technology Executive

Visit the Security Executive Council website for other resources on the Security Metrics: Business Alignment series.

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.

Contact us at: contact@secleader.com
Website: https://www.securityexecutivecouncil.com/

