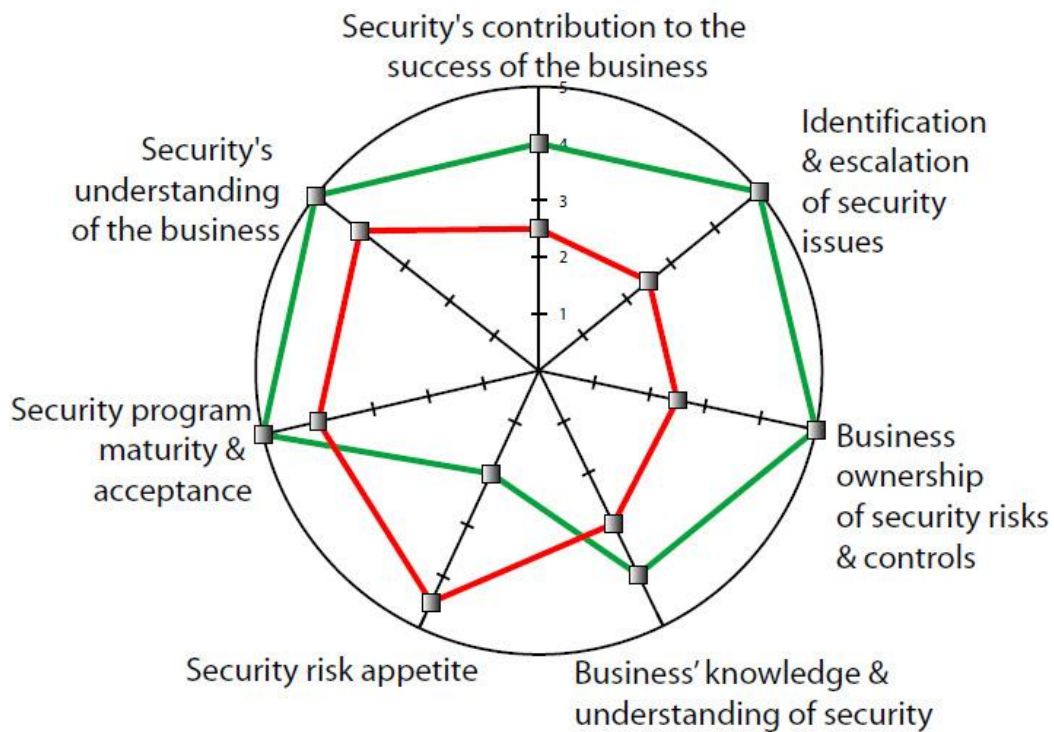Security Metrics > Risk >

Measuring Alignment Using Key Risk Indicators

Created by George Campbell, Security Executive Council Emeritus Faculty

I get a lot of questions about how Security can demonstrate with metrics that we have a positive connection to the core business strategy and objectives. Here's one example.

The radar chart above shows a separate axis for each category of key risk indicator with an assessment of where we are versus where we would like to be on a 1-5 scale.

Which indicators would you choose to demonstrate your security department's alignment with the business? For this example, I've put forth seven criteria that I believe are reliable indicators of a qualitative connection to business strategy and objectives. Start at the top and go clockwise. You might measure your program against the following:

Security's contribution to the success of the business. How is success measured in your business? Is there any connection to managing risk, safe workplaces, protecting customers, safe products, trusted relationships, or simply doing the right things? Have you asked your boss or anyone in senior management how they see a good security program contributing to business success?

Identification and escalation of security-related issues. How educated, proactive and timely are business units in recognizing risk and reporting their concerns to Security? If you say "not very," ask yourself how well you have understood their operational risks and whether you have provided them with the tools to fulfill their responsibilities.

Business ownership of security risks and controls. A lack of ownership at the business unit level is often the root cause of other shortfalls. A company that believes that security is owned solely by the security department has either been misinformed by you or fails to understand any commonsense notion of delegated accountability.

The business' knowledge and understanding of security and security's understanding of the business. I know we're skipping around a little here, but these two considerations share the same DNA. Where there is evidence of various security programs proactively addressing risky business processes, there likely is an institutional commitment to shared responsibility for enterprise protection.

Management's appetite for security-related risk. I think there is a direct link between the disconnects noted above and management's willingness to accept security-related risk. When management shows an excessive acceptance of risk, Security often has not provided a business case focused on current examples of verifiable risk exposure, and this has spilled over into the lack of ownership and identification of security risk issues.

Security program maturity and acceptance. A mature security program that is accepted by management and business units works to improve the knowledge of and connection with the business that security serves.

A chart like this provides an excellent opportunity to discuss the relevance and resilience of key business relationships with the security program. Take the test and then go and see the boss.

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: Risk](#) 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 here: https://www.securityexecutivecouncil.com/