SEC

SECURITY EXECUTIVE COUNCIL

A research and advisory firm

Advances and Stalemates in Security

Bob Hayes and Kathleen Kotwica, Ph.D.

Last Updated December 2016

Advances and Stalemates in Security

Created By: Bob Hayes, Managing Director and Kathleen Kotwica, Ph.D., EVP and Chief Knowledge Strategist, Security Executive Council

The SEC reflects on who we are as an industry, what we're doing, and where we hope to be – both advances that have been made and what is still holding corporate security programs and leaders back.

At the start of each New Year, we always find ourselves reflecting on who we are as an industry, what we're doing, and where we hope to be. The Security Executive Council's ongoing research and trending of security-related issues has shed light on some remarkable changes in the security industry in the last seven to ten years, many of which are driven by technology advances and shifts in the business environment.

Let's focus specifically on management, strategy, and leadership issues. Based on our research and our collaborations with senior security executives in all types of organizations, here are our thoughts on how security leaders have advanced and where they seem to have hit a wall.

Advances

• More security practitioners are coming to their roles from varied backgrounds – not just military or law enforcement – which is gaining influence with senior level hiring managers who are looking for a role more inclusive of business skills in addition to security skills.

• More practitioners are beginning to infuse business theory and processes into every facet of their function.

• There is more interest in the business community in educating executive business leadership about security risk.

• We are seeing more security titles at the executive level and a higher level of executive interaction in many organizations.

• Risk is becoming a more common focal point for senior management, and they are communicating with security more about that risk.

• More practitioners are connecting the dots between security and the risks to each function of the organization, seeing the bigger picture and where their function resides within it.

• Security leaders are giving more consideration to aligning their services with the board-level (10-K) risks that are critical to the business.

• More leaders are recognizing the need to brand or re-brand their security department —to reposition how the organization and executive leadership views security, its capabilities, and its actions and how security responds in a business manner to those views.

• Operational excellence is increasingly a focus of future-oriented security leaders. While most of the work we've seen is preliminary, we have worked with and heard from a number of practitioners who are hoping to develop quality management programs for their functions. (For more information, visit https://www.securityexecutivecouncil.com/spotlight/?sid=27289.)

• Similarly, more security leaders are noting and moving forward on the need to build credible measures and metrics programs for security.

Stalemates

• Security practitioners continue to offer on-demand, ad hoc services in reaction to events, but not enough strategic, long-term programs that are built upon a solid understanding of the business, its risks and opportunities.

• Although senior business management is now savvier about security risk issues, there has been little forward progress in their understanding of the security function's role in the business.

• While more practitioners are beginning the process of aligning their services with business goals, few are using this exercise to its full potential. Recognizing a business goal to increase revenue, a security practitioner may

simply make a strategic statement that security will work with the business to increase revenue. However, this statement has limited value unless it's backed up by specific, actionable plans for accomplishing it.

• A surprising number of practitioners cannot articulate or do not know exactly what resources their function consumes or their capacity for delivering those services. They can't quantify how many full-time equivalents (FTE) are dedicated to a given project or service, they don't know whether the business units that benefit from their services actually value them, and in many cases they cannot sit down and list all the services security performs and for whom.

• In a similar vein, practitioners and corporations are generally unable to calculate the total cost of the security services being consumed by the organization.

• Security practitioners often view their department as something different from all the other business units and feel that exempts the function from behaving as the other units do – measuring performance, quantifying value, delivering on strategy initiatives, for example. Increasingly, executive management disagrees.

• Many security leaders have reported that they continue to have little control over budget allocations and discretionary spending. There are many potential reasons for this, but one significant factor is security leadership's inability to effectively influence executive management and to justify the spending they feel is necessary.

• Rarely are security services communicated in terms of what risk they mitigate, and this causes gaps in staff and leadership understanding and investment in those services.

• While metrics are an increasingly hot topic, many of the security practitioners continue to count things rather than to provide true, meaningful metrics. Metrics are intended to influence and to tell a story. It's good to know how many laptops have been lost, but that number isn't a useful metric. The metric provides context and points to solutions.

• As an industry, we still fail to have research-based documentation that provides baselines and templates for successful security.

In too many organizations, security remains an antagonist or an afterthought. This amounts to more than a public relations problem. True, in some businesses the biggest issue is that organizational leaders simply can't or won't see the value in robust risk management. However, our observations have shown us that often, the problem is that the security leader doesn't see himself or herself as a leader, so sees no need or desire to grow as a leader or to take the initiative to innovate the program or learn the business.

If you're reading this article, it's likely you do want to strengthen or maintain the quality of your security program. Do you consider yourself a leader? How much do you know about the inner workings of your business? When was the last time you created or monitored relevant metrics about your program's operations and return on investment (ROI)? How often does your top management ask your opinion? Can you articulate your strategy? What do you need to do in the next year?

About the Security Executive Council

We are a research and advisory firm for security leaders. We have a collective of close to 100 security subject matter experts that have been successful security executives or are recognized industry experts in their field. The resources and tools we develop are constantly evolving to provide maximum value. Some engage with us by way of multi-year "retained" services agreements (Tier 1 Stakeholders). Tier 1 Stakeholders are those that want support on an ongoing basis but also want to have an active role in identifying solutions for the industry. Others come to us seeking a specific solution to a contained issue. In all the ways people engage with the SEC the bottom line goal is to help define and communicate the value of the Security organization.

Contact us at: contact@secleader.com
Learn more about the SEC here: https://www.securityexecutivecouncil.com