

Demonstrating Value > Communicating Value >

# Security State of the Industry (SSoI): Measuring Security Leader and Program Value Potential and its Relation to Being Valued by the Business

Created by the Security Executive Council

*After the Next Crisis Happens, Will You be Ready to Quickly Explain Security's Value to the Business?*

Corporate security success is multidimensional. It's complex and interrelated: a fluid and ever-changing value proposition. With close to two decades of research, the Security Executive Council (SEC) is working on collating its comprehensive findings to benefit chief security officers—with the goal of developing a tool to measure the potential value of security programs.

“Our constituents call us all the time to ask ‘What’s the best metric of the success of a security program?’ and ‘What’s the best plan?’ Many factors have an influence. You need to be constantly evaluating your value potential to your organization because it’s related to your success, and SEC will soon provide a tool to do that,” said Bob Hayes, Managing Director, SEC.

“Measuring Security Leader and Program Value Potential and its Relation to Being Valued by the Business,” was the topic of the SEC Security State of the Industry online briefing presented in March 2018. Speakers included: Bob Hayes; Kathleen “K2” Kotwica, Executive Vice President and Chief Knowledge Strategist, SEC; and Francis

D’Addario, Emeritus Faculty, SEC. More on their bios here:

<https://www.securityexecutivecouncil.com/about/people.html>

“We have been studying programs and leaders even before the official establishment of the SEC and have compiled those learnings,” said Bob Hayes. “Our goals are to identify the elements of success; find ways to benchmark various leadership styles against programs; and help our security leaders conduct a self-assessment of their program”

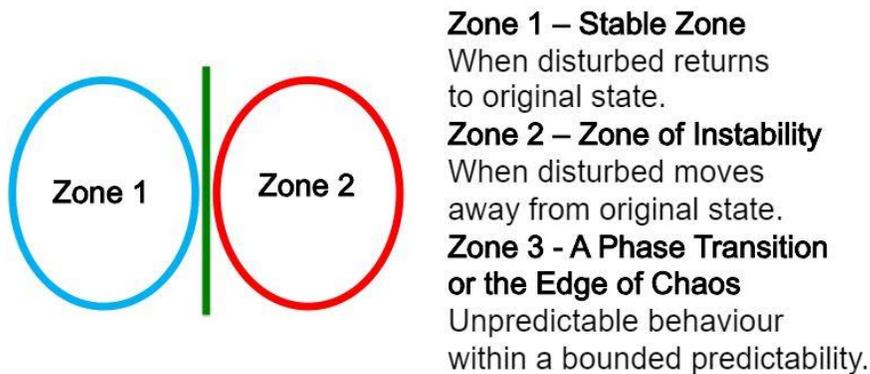
### **Success is Slippery**

The “big picture,” said Kathleen Kotwica, is that success in corporate security has many interconnected elements. “It may seem simple, but there are many facets that contribute to being successful and bringing value to your organization, all interrelated,” she said. She used complexity theory as a way to explain how something simple can also be complex.

“Complexity theory,” said Kotwica, “looks at complex behavior patterns and how they can self-emerge from simple rules. These patterns can be impacted by external events. Dynamic Systems (the origins of chaos theory) looks at complex systems and their relationships and where a change in one part can influence all of the other interrelated parts.”

The lesson is there is no “12-step” program to guarantee success, she added. Using a diagram that depicted stable and unstable zones from concepts from the theories (see Figure 1), she stated, “You can be in a stable mode, where we all want to be relevant to success, but seemingly simple events, like the introduction of a new member of senior management, can cause huge, far-reaching change. And we have seen it happen. You need to be adaptable to future states.”

# Complexity Theory | Dynamic Systems



Centre for Defence Leadership & Management | College of Management & Technology | UK Defence Academy

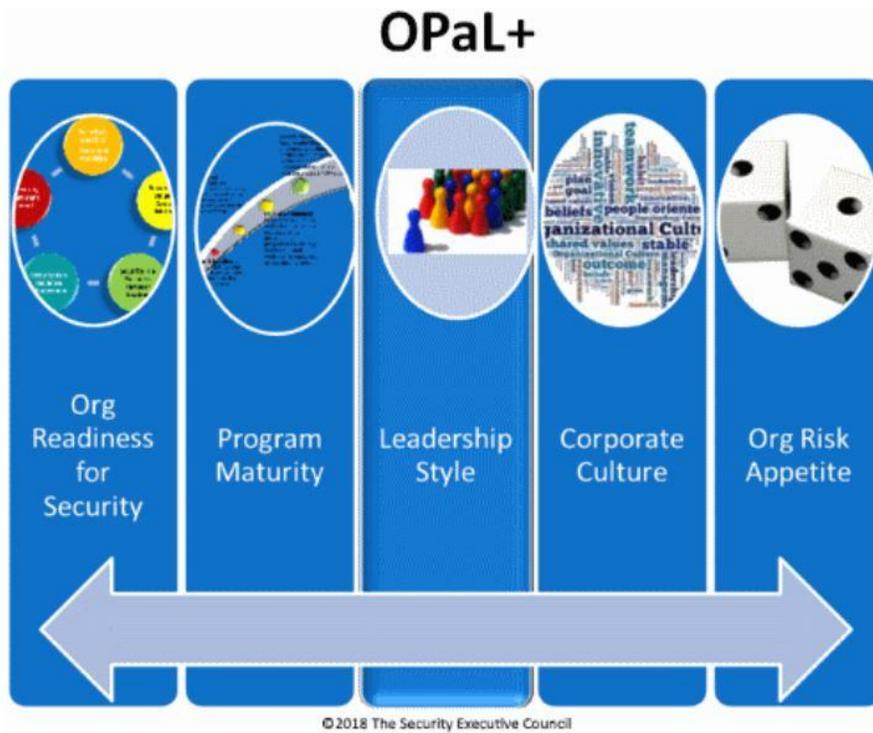
Figure 1. Extracted from a presentation created by UK Defence Academy "Leadership Derailment" slide 9 <http://slideplayer.com/slide/8636632>

Francis D’Addario said there are moving pieces interacting that effectively denote the health of a risk management program. “At the end of the day, our leadership qualities are probably our greatest asset. We bring to the game a Board-level understanding of risk and its mitigation, but there’s always a question mark because we know ultimately there will be an unfamiliar risk issue down the road. The question is this: ‘How can we reshape our mitigation services and programs against that constant change? Why is it that some leaders and security programs weather change better than others?’”

## Tools for Success

The presenters discussed some of the existing success measures the SEC has created:

- SEC’s OPaL+ research (Organizational readiness, Program maturity and Leadership continuum plus corporate culture and risk appetite)—One of the methods the SEC has created for calculating success. It examines the combined impact of the elements that make up OPaL+ for the security leader and team. And it can show how others perceive the security leader and the security program. The particular combination of these can increase or decrease your chances for success.



*Figure 2. OPaL+ Continuum*

- Corporate Security Program Maturity Model—this model is currently being developed by the SEC and is a work in progress. It encompasses 5 levels of maturity: Level 1 (Reactionary); Level 2 (Managed); Level 3 (Documented); Level 4 (Measured and Incorporated); Level 5 (Continuous Improvement). The assessment has 43 “declarations” that are answered to pinpoint where a security organization is on the maturity continuum. This assessment is from a leadership point of view, with each maturity model level building from the preceding one.

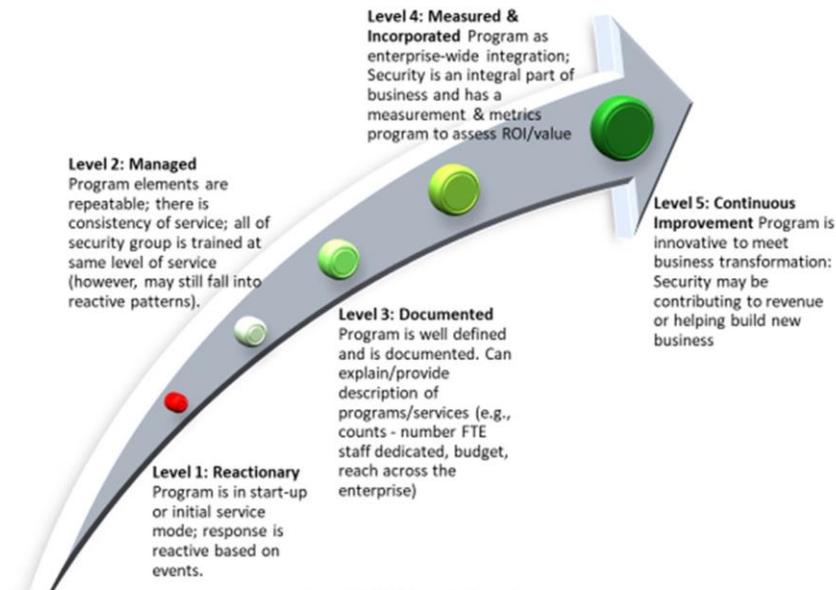


Figure 3. Program Maturity Model

- [The 9 Practices of the Successful Security Leader](#)—The 9 Practices is SEC research based on interviewing 30+ high-achieving practitioners. These are things practitioners do (their practices at a high level) that are shown to demonstrate successful leadership.

Hayes recounted an experience related to OPaL+: “I thought I had a lot of security knowledge and capabilities and could design the right programs, systems and services. When I took a new job, I would go in and work night and day to implement the programs I felt were best for the organization. But I was totally unaware of the organizational readiness factor. It took me two years at one organization to find out that there were only a handful of people who thought we needed what I was charged to do. So how do you identify this and what’s the strategy to change it? Culture has so much impact on success.”

Also, risk appetite can vary immensely in an organization—from those who don’t think they need security to people who are overreacting to risk. There are many elements in changing risk appetite. Awareness is key, but executives need to be changed one at a time.

“There are so many areas a security executive is now responsible for,” said D’Addario. “The ‘asks’ from the CEO are more variable, changing and morphing,” he said. “The CEO wants to have confidence that security executives are spending money on the right things. Roles and responsibilities need to be spelled out and metrics and key service deliverables established.”

## Value = Success

“The SEC has always been focused on the needs of its constituency, going beyond products of personal opinion and instead providing ways to measure the value of security to the business,” said Hayes. “We want to be able to provide a way to analyze, measure and score security’s value at an organization, and then create strategies to improve it. We are building a Security Value Potential assessment that will take all the elements discussed today and more into consideration.”

The new success measure will look at the universe of areas where a security program can add value. Some of the 13 areas it looks at are Risk Identification, Governance and Guidance, Risk Mitigation, Budget Defense, Validation, and Management and Optimized Operations. It is currently not specific to individual programs and services, such as investigations and GSOC, but there are plans to make it so in the next phase.

### Value Potential Assessment Categories



Figure 4. Proposed categories for the Value Potential Assessment

The SEC has developed this process as another way to help security leaders on their path to success. One outcome is a roadmap for security leaders who are seeking to better demonstrate their business value to executive management. It is possible for leaders to create and manage a process that continually moves their security organization toward demonstrating value. However, it requires dedicated focus and a time commitment that is often interrupted by day-to-day activities and incidents. The SEC can help security leaders manage this process with the goal of being ready when organizational transformation creates an urgent need to demonstrate value to senior management.

The first iteration of the value potential assessment is being tested with the Security State of the Industry attendees. Respondents will be scored on the value they are bringing to their organizations. The SEC theorizes that those that score higher are more resistant to damage from change or unknown issues than those that score lower.

### **Additional Resources**

A few of the resources listed during the briefing included:

[The Nine Practices of the Successful Security Leader](#)

[OPaL+ Executive Summary](#)

[Security Barometer - Maturity Model](#)

[Insight into Security Leader Success](#)

Contact the [Security Executive Council](#) for more information regarding the Security Value Potential Assessment.

Visit the Security Executive Council website for other resources in the [Demonstrating Value: Communicating Value](#) 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](mailto:contact@secleader.com)

Website here: <https://www.securityexecutivecouncil.com/>