Driving Excellence in Enterprise Security

A Security Executive Council Thought Leader Paper

By George Campbell, Emeritus Faculty, Security Executive Council

Security Leadership Solutions Executive Council

Introduction. The delivery of excellence in a business' products or services has always been a widely accepted objective. But expectations took on a more formalized agenda in the 1980s, culminating with the Baldridge National Quality Award that was set as a standard of excellence for U.S. business.[1] Global competition in manufacturing spawned several disciplines targeting continuous improvement, defect elimination, cost management, supply chain efficiency and the customer/value relationship. In sum, these and their companions in the pursuit of quality-driven operational performance can all be placed in a bucket labeled "Business Excellence." If enterprise security is to be effectively aligned with its company's strategy and processes, it must be driving a focus on operations excellence (OpEx) into every corner of its suite of products and services.

Objective. The Security Executive Council has several Tier 1 Security Leader™ members who have assigned senior staff resources to the development of programs calculated to drive OpEx into their security operations. Some of these executives are in industrial sectors with established processes like Kaizen and Six Sigma while others seek to explore the results that these proven quality management practices offer. This short review seeks to explore an approach to support those leaders and to inform others who may be interested.

Initial Member Feedback. We conducted brief interviews with several interested members to document organizational context, obtain a working definition of the process they envisioned for their security operations, and gauge their interest in establishing a group effort to share learning and push ideas. Their feedback is summarized below.

- Business excellence is ingrained in our company's processes and we need to be aligned with this way of managing performance.
- I know there are a variety of standards to benchmark, but I think operational excellence is about exceeding those standards.
- Operational excellence is about security process transformation.
- The ideal outcome of a potential OpEx working group would be the creation of a security manager's operational excellence toolkit.
- There is a critical need for security to communicate its value—demonstrating excellence in service is a driver of that communication strategy.
- Relationship between governance and operational excellence—how are we performing in our relationship to the policy infrastructure?
- We should do OpEx benchmarking and exchange ideas across security organizations in companies engaged in these disciplines.
- How can we measure the effectiveness of security programs to business outcomes?
- Explore the opportunity to deep dive on a core security process to examine how excellence is or could be demonstrated.
- We need to understand how operational excellence is made part of business process and how this has influenced corporate security's engagement.

There was agreement that the group could fairly easily "get into the weeds" and miss the big picture. Participants acknowledged a need to find an approach to discussions that would help build real,

[1] In Lean/Six Sigma and Operations Excellence, there is the Shingo Prize. www.shingoprize.org/education.html

actionable tools. These practitioners are too busy for academic discussions that don't contribute to something useful in security practice management.

Conclusions. There were a few key conclusions from these discussions, none of which should be surprising to experienced security practitioners. 1) Each company is approaching this initiative from its own unique organizational framework around the subject and its own equally unique enterprise risk framework. 2) There are marked differences in maturity and focus of approach. Some seek a highly limited application while others seek to apply this across the suite of security services. 3) There is no shared definition of excellence, quality or other key performance measures that would facilitate common benchmarks.[2]

Implications for building a model approach. This document reflects these conclusions and attempts to establish a foundation from which we may attempt to engage interested parties in a structured approach to operations excellence, at least at a trial level. In practice, the various disciplines are so specifically defined that it seems logical to build a model that encompasses a generic process that could feed into more or less mature approaches.

The Process Landscape. Even the most cursory review of the literature reveals the potential appeal to those who find this focus on business excellence enticing. Consider the following table that summarizes key elements of four of the frameworks that may be applied. (There are other disciplines that could be included, but these few appear to contain the common process components.) Note the consistent themes of requirements analysis, innovation, process improvement, quality management, leadership and team involvement, measurement, and a total engagement with the customer. All of these are obvious program management objectives. But as we launch a more defined and deeper dive into individual security tasks wherein we seek measurably improved service levels and outcomes, we need a significantly more structured plan of attack.

Kaizen	Six Sigma	Total Quality Management (TQM)	Operational Excellence
Standardize activities	Define the problem and goals	Customer involvement	Respect the individual; lead with humility
Measure activities	Measure the current process	Process management	Dedication to superior quality; exceptional customer service
Assess measures against requirements	Analyze the data to identify defects and opportunities	Information & feedback	Think systematically; focus on process
Innovate to meet requirements	Improve the process	Committed leadership	Relentless pursuit of continuous improvement
Increase productivity	Control the improved process	Strategic planning	Integration of people and technology to achieve positive results

[2] The IT security world is a notable exception. The Council can provide multiple examples in other areas of security program management but they may not be universally applicable or supportable.

Standardize improved activities	Correct deviations from the target	Cross-functional training & employee involvement	Strategic focus on maximizing the value the operation delivers to the customer

Setting the Stage: Security's Balanced Scorecard. The balanced scorecard was introduced in 1992 by Kaplan and Norton in a Harvard Business Review article. The authors believed that the excessive use of financial scorecards in business failed to encompass the full scope of performance measurement. For our purposes, the four perspectives they introduced are seen here along with a translation that emphasizes the connection to our security mission.

- **Financial Perspective**: How do we look to shareholders? What capabilities, goals & measurements in our safeguards are perceptible to shareholders?
- **Internal Business Perspective**: What should we excel at? What elements of our key protection programs demonstrate best-in-class practices?
- **Innovation and Learning Perspective**: What security goals, activities and measures are calculated to improve security at reduced or avoided cost and thereby add value?
- **Customer Perspective**: How do customers see us? What specific security programs and activities visibly contribute to our customers' satisfaction and measurably add value for them?

These four perspectives effectively summarize the multiple concepts in the various business excellence disciplines noted above. Importantly, they provide a significantly more comprehensive view of an organization's performance and, in this framework, force a critical assessment of security's value. If one only endeavored to explore answers to these few questions, the quest for excellence in enterprise security would receive a solid kick-start.

Establishing a Baseline. There are additional questions that further serve to frame our considerations for an approach that could support our differing organizational needs.

What is "Excellence"? As professionals we can all agree that achieving excellence in our work is our goal. And it goes without saying that excellence is an expectation of those we serve. But how should we—our stakeholders *and* ourselves—define excellence in our suite of services? Is it in the quality of security program results and, if so, where are the established standards to measure a requisite degree of quality? At the end of the day, customers define quality and value. The "owner" of the security process cannot be the sole arbiter of its level of quality and excellence. But it is also true that the security function is not the sole contributor to a secure business process. It is a shared accountability with degrees of contribution linked to the requirements of protection. Clearly, engaging stakeholders and customers in analysis of our activities is an essential ingredient in the process. Our customers do not typically understand security activities, and a well planned examination of what service excellence means to them will make activity analysis and measurement more effective and more valuable.

Consideration: Some measurable description of excellence needs to be established for the activity being addressed. What is the "best" outcome or result of the work as defined by the security team and by the customer and, if the answers differ, what is it about the customer's assessment that needs to be factored into an improved process?

Is the security program effectively aligned with its customers? Every business excellence discipline shares a singular focus on the customer. A legitimate question to ask every member of the security team is "Who is your customer?" This may be a multiple choice question:

a. Is it the employee seeking our assistance or expecting a safe and secure place to work?
b. Is it the business unit owner of a risky process?
c. Is it the CEO who expects us to deliver the promised results?
d. Is it the Board or the shareholders who need to know that risk is being managed?
e. Or is it the external customer who may be served by a corporate commitment to security and integrity in products and services?

It's likely that all of these are Security's customers. Each group likely brings their own definition of excellence to the transaction and the perception of value. And few or none of these have the requisite information to know the intricacies of what we do. But whoever the customer is for a given transaction, he or she has a critical opinion of the quality and responsiveness of what you have delivered and whether it is worth the price. Therein lies the challenge in this process of analyzing, defining and delivering excellence through best-in-class security services.

Is a "best practice" equal to excellence in that practice? Where a security practice can be shown to deliver results consistently superior to an alternative process that has been applied and tested by others, it should be advertised as having achieved a level of excellence. The key is measuring the "superior results," and that requires detailed task and process analyses, which are consistent elements in virtually all business excellence disciplines.

What is the relationship of risk management to operations excellence? *If our security activity was the singular source of identification and proven elimination of an exploitable vulnerability, would that activity be accurately labeled as having achieved excellence?* If I can demonstrate the business impact of adversary exploitation of that vulnerability, have I demonstrated measurable value? There has to be some element of stakeholder value and therefore a perception of excellence in the elimination of avoidable risk.

Consideration: The presence of risk is the business driver for the security program. Excellence in our business mission has to link to a positive impact of security activities on the reduction of targeted risk. It may be said that excellence in security operations cannot be achieved without a robust process of security risk assessment that results in the measurable elimination of business process vulnerabilities.

Security Leadership Solutions Executive Council

Where is value in the excellence equation? *If the value of a security process was starkly visible to every individual involved in its engagement and delivery, would that process be justifiably labeled as having achieved excellence?* Customers expect flawless service at the lowest cost, and that is especially true when they only see security as a cost center. We do not tell our value story well, and a process to document the measurable return to the enterprise will invariably require the documentation of activity metrics.

Consideration: Defining the value proposition for our services is a primary objective of an exercise in operations excellence. We seek to document the sum total of the benefits the customer, the stakeholder or the enterprise will receive from the security service we offer. When we can define a level of performance that delivers a measurable benefit (like less risk or faster, better response), we have the ability to not only improve performance but to positively influence the perception of value by key constituencies or stakeholders.

If a security process or activity lacks established performance measures, can excellence be achieved in that process or activity? It is not possible to establish that a security process has achieved excellence or provided value if relevant performance measures have not been vetted and consistently applied.

Probing Potential Measures of Excellence in Security Programs. What statements might sufficiently convey a demonstration of excellence in security programs? Consider the following:

- A security program demonstrates such effective alignment and contribution to the success of a business process that it measurably enables the business to do what would otherwise be too risky or non-competitive. Moreover, business is captured and/or retained solely due to the quality of security measures proposed or applied.
- Measurable capabilities in safe & secure workplace protection result in increased productivity, lower insurance cost, increased worker morale and reduced incidence of injury and fatality.
- A security activity is peer-reviewed or benchmarked against available standards or best practices and *exceeds* qualitative measures of performance. Certain control factors being equal, losses attributable to security breach are measurably less (over time) than industry sector peers.
- The cost of a secure business process or environment is less than the consequences of risk or, the cost is additive but those at risk feel measurably safer and more productive. Or, an incremental increase in asset protection is achieved at reduced cost to the customer.
- A customer's expectation (or service level agreement) is consistently and measurably exceeded.

Target Analysis: A Business Excellence Template. If a process has not already been identified for analysis and application of an established program within your company, you may want to consider the following table as a team exercise. Several components in the disciplines noted above along with a few others that are appropriate have been incorporated under Business Excellence Factors. Each of the Security Programs and Services may be discussed, evaluated and selected for the potential benefits that may accrue as a result of an in-depth application of an operations excellence approach.

Security Leadership Solutions Executive Council

For the purposes of this paper, several items in the table have been highlighted and noted (+/++)[3] where an added benefit may be found through subsequent analysis. (You could probably color every box in green, but this seeks to call out the most obvious.) The idea is to think through how each of the possible benefits on the left may impact and deliver measurable results to the security service targeted. This is only an example of how this matrix may be used; a blank table is offered in the appendix.

Contribution From Examination of Relevant Business Excellence Factors	Security Programs and Services											
	Manage the Business for Results	Align Security with Business Objectives	Establish and Promote a Culturally Responsive Policy Framework	Assess Risk & Develop Measurably Responsive Mitigation Plans	Focus Protection on Critical Assets and Processes	Provide for Timely and Qualitative Incident Response	Provide Safe and Secure Workplace	Obtain Business-Responsive Results from Investigations	Screen Employees and Vendors for Integrity	Anticipate Crises and Provide for Business Continuity	Protect Information	Assure Customer Awareness of Risk
Deliver Measurable Contribution to Business Objectives		++		+	+		++			++	++	
Notable Improvement in Knowledge of Emerging Risk				++	++			+				++
Notable Benefit From Improved Customer Involvement in Security Tasks		++		++	+	++				++	++	+
Improved Responsiveness to Key Risk Indicators	+			++	+	+				++	++	++
Notable Benefit From Continuous Process Improvement	+			++	++				+		++	
Improved Alignment with Key Performance Indicators				++	+	+		++				
Availability of Comparable Best-in-Class Security Practices									+		++	
Ability to Perform Activity-Based Task Analysis and Costing								++	+	++	++	
Notable Benefit From Process Defect Identification and Elimination	+			++		+	++		++	++	++	
Benefit From Reduced Cycle Time						++		++	++			

[3] A scoring routine might enable a more granular assessment. Score 1 for low benefit and up to 5 for an almost guaranteed improvement.

Availability and Reliability of Measurements and Metrics	+					++	+		+		++	
Measurable Improvement in Essential Knowledge				++						++		
Notable Benefit From Improved Training & Employee Involvement				++		++	++		+		++	

Next Steps: Building a Business Excellence Tool Kit. The fact that OpEx is only now gaining some traction in security management circles speaks volumes about our level of alignment with several decades of established business excellence and quality programs across technology, manufacturing and service industries. We have interest from several member organizations and an opportunity to initiate a movement that is overdue in our profession.

What is necessary now is to engage organizational leaders, find answers to the questions we have raised in this paper, and develop a body of practical tools and techniques that may be applied across a wide range of corporate security programs. There is no "one size fits all" in corporate security functions or in the diversity of business missions and models they serve. But we do believe we can collectively put forth a body of workable definitions for various security activities, provide measures and metrics appropriate to assessing performance and service quality and craft tools and templates that will support the pursuit of documented excellence.

Suggested Reading. There are scores of books and reams of Internet data on the business excellence subject. For an outstanding summary, check out *Back to Basics: A Practitioner's Guide to Operations Excellence* by Douglas Sutton, Operations Excellence Services, LLC (2012). For tools and techniques: *The Lean Six Sigma Pocket Toolbook*, Michael George, McGraw Hill (2005); *Balanced Scorecards and Operational Dashboards with Microsoft Excel*, Ron Person, Wiley Publishing (2009); *Shingo Prize Model and Guidelines*, Jon Huntsman School of Business, Utah State University, www.shingoprize.org.

Security Leadership Solutions Executive Council

Appendix: Business Excellence Analysis Template

Contribution From Examination of Relevant Business Excellence Factors	Security Programs and Services											
	Manage the Business for Results	Align Security with Business Objectives	Establish and Promote a Culturally Responsive Policy Framework	Assess Risk & Develop Measurably Responsive Mitigation Plans	Focus Protection on Critical Assets and Processes	Provide for Timely and Qualitative Incident Response	Provide Safe and Secure Workplace	Obtain Business-Responsive Results from Investigations	Screen Employees and Vendors for Integrity	Anticipate Crises and Provide for Business Continuity	Protect Information	Assure Customer Awareness of Risk
Deliver Measurable Contribution to Business Objectives												
Notable Improvement in Knowledge of Emerging Risk												
Notable Benefit From Improved Customer Involvement in Security Tasks												
Improved Responsiveness to Key Risk Indicators												
Notable Benefit From Continuous Process Improvement												
Improved Alignment with Key Performance Indicators												
Availability of Comparable Best-in-Class Security Practices												
Ability to Perform Activity-Based Task Analysis and Costing												
Notable Benefit From Process Defect Identification and Elimination												
Benefit From Reduced Cycle Time												
Availability and Reliability of Measurements and Metrics												
Measurable Improvement in Essential Knowledge												
Notable Benefit From Improved Training & Employee Involvement												

Security Leadership Solutions
Executive Council

About George Campbell

George Campbell retired in 2002 as the chief security officer (CSO) at Fidelity Investments, the largest mutual fund company in the United States, with more than $2 trillion in customer assets and 32,500 employees. Under Campbell's leadership, the global corporate security organization delivered a wide range of proprietary services including information security, disaster recovery planning and crisis management, criminal investigations, fraud prevention, property and executive protection, and proprietary security system design, engineering and installation.

Prior to working at Fidelity Investments, Campbell owned a security and consulting firm that specialized in risk assessment and security program management. From 1978 to 1989, he was group vice president at a system engineering firm that supported government security programs at high-threat sites around the world. Early on in his career, Campbell worked in the criminal justice system and served in various line and senior management positions within federal, state and local government agencies.

Campbell received his bachelor's degree in police administration from American University in Washington, D.C. He served on the board of directors of the International Security Management Association (ISMA), and as ISMA's president in 2003. Campbell is also a long-time member of the American Society for Industrial Security (ASIS). He is a former member of the National Council on Crime Prevention, the High Technology Crime Investigation Association and the Association of Certified Fraud Examiners, and is an alumnus of the U.S. State Department's Overseas Security Advisory Council.

As a founding Emeritus Faculty of the Security Executive Council, Campbell serves as a content expert for Council product/content development.

"The Security Executive Council is the best place for me to learn from my colleagues, and to share my experience. Having access to the quality support provided by the Council will significantly enhance that peer relationship."

Areas of expertise:

- Global security management with concentration in the financial services industry
- Proactive security management assessment
- Risk and compliance assessment
- Strategic security planning & program design
- Measuring Security's outputs and value

Security Leadership Solutions
Executive Council

About the Security Executive Council

The Security Executive Council is the leading research and advisory services firm for risk mitigation solutions. We offer risk mitigation leaders trusted and experienced advice, program decision assurance and help to get all their projects successfully done.

The Council develops proven practices that provide an array of strategies and tactics to solve pressing issues based on your situation. With a large community of subject matter experts (successful former security executives and current industry specialists) we work one-on-one with Tier 1 Security Leaders™ to help them reduce risk and add to corporate profitability in the process.

Through our pioneering approach of Collective Knowledge™ we serve businesses from all industries and sizes, government agencies, educational institutions and NGOs to help them effectively address their risk concerns.

Are you interested in learning more about Driving Excellence in Enterprise Security? Contact George at contact@secleader.com