SEC
SECURITY EXECUTIVE COUNCIL
A research and advisory firm

Risk-Based Security > Board Level Risk/Enterprise Risk Management >

The Mission is Not Cybersecurity- It's Enterprise Security

Presented at: Command Control Cybersecurity Conference, in Munich, Germany, September 2018

By: George Campbell, Emeritus Faculty, Security Executive Council

I have worked in some front-line element of public law enforcement and private security for fifty-four years culminating as a Chief Security Officer in a totally converged global security organization. This combined experience and the consultancy engagements which have followed heavily influence my remarks today. When I was asked to speak to this venue of cyber security it struck me as an opportunity to share some observations- and some concerns- about security and the current state of its' place in the business of enterprise risk management or ERM.

This is not to exclude cyber security, quite the contrary, the threats cannot be overstated nor can our diligence in meeting them head-on. I acknowledge these challenges but seek to include them in a broader and deeper set of considerations regarding enterprise security and the accountabilities that align with this *shared mission*.

The mission is not cybersecurity, it is enterprise security.

The intelligence and sophistication of threat is expanding exponentially. While technology enables the business, it also opens a multitude of opportunity to insiders and highly resourced external adversaries. Our companies extend our perimeters and critical processes into often defenseless layers of external partners. Security's current business model can deliver on the routine service demands but our role in meeting these increasingly consequential risks will require a much more inclusive and mature presence if we are to become an equal contributor to senior management's risk awareness and decision-making.

There is an alliance of senior security executives whose collective knowledge and multi-

disciplinary experience believe it's no longer meaningful to align risk and their associated countermeasures in silos. They note that the "silo approach leaves too many gaps and provides no credible means of understanding or being able to evaluate an organization's overall risks. Some proponents of ERM have referred to it simply as common sense. In other words, when the organization begins to share risk and control knowledge systematically across its functions and departments, only then can the interconnectedness or correlations among risks be identified and managed. This is the essence of Enterprise Security Risk Management."[1]

Therein lies the core focus of my remarks today. There are several barriers that we continue to foster, practice and reinforce that keep us from debating and acting on this common-sense notion of shared knowledge and interdependent programs of protection. I believe it has relevance for cyber security because so much of what we learn about how our adversaries succeed in that arena of threat is found in the vulnerabilities we see in the other silos of risk. Risk connectivity is why ERM is such a critical perspective.

Across our varied disciplines we speak in specialized language with differing definitions and turf-based bias on the relevance of mission and value. A recent report by Accenture and Chartis Research underscored the problem for financial services like this:

> "The main definition problem that Financial Institutions encounter is around scope. Broad and narrow definitions of cyber security both have strengths and weaknesses. A broad definition provides wide coverage and lends itself to a cross-silo approach. However, it can lead to confusion over responsibilities and cause significant overlap with other areas like IT security. A narrow definition can result in the creation of another tactical risk management silo, which is undesirable. The aim must be to develop an open definition that covers all of the threat vectors, but clearly assigns responsibilities."[2]

I like the direction the authors take in this assessment but disagree with the idea that a broad definition of cyber security lends itself to a cross-silo approach. I think it's still too narrowly aligned within the IT framework, while my vision is for a holistic operating concept of enterprise security. We ideally want to reach all security and governance elements and frame them under some form of common mission; one that emphasizes processes that crosses organizational lines. This is a service model that engages senior executives and board members with one voice for a more mature and fully informed conversation on risk appetite and a responsive protection strategy.

So, here is where we arrive at a critical intersection in the road to an enabled, mature and integrated security program. In this culture and model, security is expected to be focused more on measurable results rather than defined turf. But what if the road taken is dictated by a culture or business model that inhibits strategic maturity and limits an integrated, collaborative

[1] The Convergence of Physical and Information Security in the Context of Enterprise Risk Management, The Alliance for Enterprise Security Risk Management (AESRM) & Deloitte, & Touche, Canada, 2007
[2] Convergence of Operational Risk and Cyber-Security, Accenture & Chartis Research LLC; 2018, pg. 4

assessment of threat and risk? How might that compartmentalize or dislocate the key organizational elements that should be working off a common, shared agenda? What indicators might we see with what possible consequences?

In a 2018 Raytheon-sponsored survey of 1,100 global information security professionals, 68% reported that their boards of directors were not being briefed on what their organizations were doing to prevent or mitigate the consequences of a cyber-attack and that communications are too siloed and occur at too low a level.[3] While executive access has improved over the past decade, my experience reviewing significant numbers of corporate security organizations is consistent with this lack of influential, risk management engagement.

What's behind this lack of Security and all-hazards risk awareness connection to the boardroom? I believe there are five issues that have combined to shape the less than optimal state of our influence on risk management strategy and visibility to the Board's considerations of perceived and actual risk.

First, we've not dug deeply or well enough to identify, qualify and quantify the risks we are accountable to know the most about. Our stakeholders expect us to anticipate risk, but respected industry surveys consistently find less than half of companies engaged in a formal, on-going risk assessment process. The data for far too many security organizations demonstrates even less discipline around root cause analysis that provides the leading indicators of *foreseeable* risk likelihood that can be so informative in risk awareness and strategy development. In the resulting absence of knowledge, we find senior executives relying upon "it hasn't happened here" as a satisfactory conclusion for their engagement and tolerance of security-related risk.

An inclusive, all-hazards risk assessment program qualifies how "it can happen here". It provides the lens to clearly see the commonality of vulnerability, directs responsive mitigation and establishes accountability for action.

Second, we have collectively been satisfied with being assigned to functional silos while failing to build bridges for essential collaboration. We lose collective knowledge and visibility of the connected dots when we put the likely risks and their assigned areas of response in distinct silos. Why? Because silos don't communicate well. They do very little to share information, to seek out common denominators and engage in truly integrated and collaborative program planning and delivery. In fact, silos maintain their own vertically oriented merit systems that reinforce internal rather than cross-functional collaboration.

And what of those Security programs that have been forcefully blended in the pervasive frenzy of mergers, acquisitions and third-party outsourcing? Here we meld unique cultures with radically divergent levels of program content and maturity to the new organization. We then try to approach responsive protection while adapting to the new silos and realities of inherited

[3] 2018 Poneman Institute Study on Global Megatrends in Cybersecurity, Raytheon, pg. 2

threat and risk. The specter of unassessed insider threat is expanded exponentially.

We know from root cause analyses and after-action-reviews that there are common vulnerabilities that may be more effectively attacked through shared strategies and multi-disciplined teams rather than retention within silos. We also know from experience that well managed silos operating at levels of superior performance are potential centers of excellence and knowledge banks within our organizations. These are assets that need to be connected. It takes a mature, measurably inclusive enterprise risk management strategy to leverage these resident benefits.

Thirdly, I believe the debilitating impact of limited knowledge of risk and hardened organizational silos has its roots in an immature enterprise risk management model. To be clear, we need an enterprise *security* risk management model. One that provides policy to establish connectivity and drive the systematic sharing of relevant risk and control knowledge across functions.

The Risk & Insurance Management Society approached the opportunity of a more comprehensive convergence model in a recent article entitled "ERM and the Security Professional". In it, the authors proposed "an enterprise security risk management (ESRM) model; a holistic risk management process that aligns organizational drivers affecting strategy, processes, people, technology and knowledge to protect key assets in accordance with governance, risk and compliance requirements. The traditional silo approach is replaced with a new paradigm in which everybody must understand and share the responsibilities for the coordinated management and treatment of risks."[4]

This is the enterprise model that we need to be talking about. But the traditional silo approach provides a set of cultural barriers that are hardwired into our whole service delivery culture. As stand-alone cost centers, Security continues to be seen by senior executives as a tactical function, remaining largely outside the influence of executive strategy and decision making. We need a new paradigm to move risk mitigation from a functional, technical orientation to a business-based adaptive approach.

Fourth, when it comes to really understanding how well we are delivering results, as a profession we are doing better at counting things than measuring them. I have spent the past fifteen years exploring how various global security organizations across all industry sectors approach their performance analytics and value metrics. Why? Because if you want a reasonably reliable measure of how well an organization is managed, find out how they measure the performance of their programs and results of their work. What does all that siloed and warehoused data deliver for meaningful, actionable information? How well do we communicate what we can and should know to those who need most it? The concept of unified risk management relies on the inter-relationship of policy and standards, assessment of risk and proof-based mitigation strategies. Metrics are key to building effective measures into

[4] ERM and the Security Professional, Michael Johnson and Jeff Spivey, RIMS.org magazine, May, 2018, pg.2

both inputs and outputs of these processes. They are the meters and dials on management's dashboard and I've found too many of them disconnected from the engine of knowledge.

No organization can say that they have embraced enterprise security risk management if they have weak or unreliable ways of measuring the maturity, competency and results of ESRM initiatives and programs. Nor can they celebrate convergence when sharable information and interdependent program objectives remains secured within the silos.

Fifth, the push for essential performance standards across security programs and disciplines over the past two decades has built stronger walls among the silos rather than challenging executives to execute more formally aligned protection and service delivery strategies. Individual silos across virtually all of the security disciplines continue to develop their own vertically-oriented standards and certification models. ISO 27002 begins to give credibility to the conforming elements of physical and human resource security but it's ownership clearly lies within the InfoSec silo.

We need to coalesce if not standardize the standards guidance, some over-arching assembly to connect common objectives, interdependent processes and linked performance measures. One option that might emerge from a serious dialogue on standards is the benefit of enterprise security program accreditation which would underscore cross-disciplinary standards of program performance linked to a unified approach to enterprise protection.

I'm not advocating for an enterprise convergence Czar, but I do see the clear need for management's acceptance of an adaptive enterprise security risk management model featuring significantly greater shared knowledge and persistent oversight of risk. This may be achieved by having the Board's Corporate Risk Committee expand their scope and reach by effectively chartering an enterprise security risk management strategy with *all-inclusive* representation and senior leadership. The key elements in this strategy would be grounded on the following pillars:

- ***Risk anticipation and mitigation***- *a* strategic view of enterprise risk across all threat vectors and critical business processes; coordinated risk intelligence and identification with integrated deployment of mitigation strategies.
- ***Expanded competencies***- shared objectives with value for generalist skills to support the drive for the broader perspective and connected strategy.
- ***Formalized risk and performance indicators*** to drive ownership and accountability for results.
- ***Operational excellence***- superior performance and proven practices in prevention, detection, response, mitigation and recovery to drive credibility and influence.
- ***Qualitative, actionable reporting and communication***- root cause discipline and risk information keyed to business strategy and engagement in the Board's overall risk position and appetite.

This is a strategy capable of bringing the best of our security and governance resources to

improved board-level engagement and moving a more risk-aware culture. But it must begin with committed leadership and that should be from the CSO and CISO with active support from the Chief Risk Officer or the Chief Operations Officer. There are multiple corporations where progressive alignments like this are building adaptive enterprise security risk management frameworks. They are focused on embracing the dependencies and delivering integrated solutions. Their Boards and shareholders are the beneficiaries.

Measurably effective cybersecurity is an imperative. My thesis has been that it should be managed within an enterprise security risk management framework that enables a holistic strategy of connected imperatives. I believe these five barriers, perhaps some in more ways than others, combine to block management's vision of the connectivity- a holistic picture- of both the risk and opportunity landscape. It also conceals our strategic value in both business and risk management terms. If we can envision an enterprise protection strategy that leverages and connects the best practices of the component parts, could it also provide a forum for multi-disciplinary discussion and consideration of a more collaborative and unified model?

Related resources:

Making the Case for an Operational Risk Leadership Advisory Council: A Guide for Influencing Enterprise Risk Management at the Operational Level

Managing Enterprise-Wide Board Risk

Visit the Security Executive Council web site to read other articles in the Risk-Based Security : Board Level Risk/Enterprise Risk Management 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/

