NGS GLOBAL

PERSPECTIVES ON EXECUTIVE LEADERSHIP

Managing Risk in a Global Organization: The Leadership Requirements of Today’s Security Executives

David Nosal
Managing Partner, NGS Global Americas, LLC

The days of simply installing surveillance cameras and hiring security guards to protect against the many inputs that affect an organization’s operational effectiveness are a distant past for corporate security executives. As businesses continue to grow on a global scale, so too, do the requirements and scope of the corporate security function.

June 2013

Many organizations, ranging from Fortune 50 multinational corporations to recently-launched start-ups, plan to grow their geographic footprints to tap into emerging markets and leverage lower cost structures. This expansion, however, introduces a number of internal and external risks that could potentially derail a brand's reputation, profit margin, and overall trajectory for success. To better understand the key leadership competencies required for effectively defining, addressing, and mitigating security threats, we spoke with leading security executives at some of today's most recognized global brands. We discovered that in order to protect corporations against the risks inherent in a widespread geographic network, security executives must adopt proactive risk management strategies, demonstrate the business acumen to relate security objectives back to corporate goals, all the while staying attuned to market and sociopolitical pressures impacting global operations.

Shifting Focus: Reactive to Proactive

Companies' rapid diversification and expansion in recent years have stretched the corporate security function to new limits, adding elements such as cyber security, geopolitical unrest, and natural disasters to the laundry list of inputs that affect operations and corporate goals. As such, security professionals have been forced to adopt a more proactive approach to risk management and business continuity. In the past, many security executives had set processes and rules that outlined appropriate responses to threats and events, yet very few proactive, ongoing risk mitigation initiatives. The Director, Worldwide Security Operations at a $60B+ global retailer explains, "We speak more about business operating risk than we do about security; it's not all about gates and guards anymore. It's more than just physical security—it's loss mitigation and prevention, inventory control, business continuity, and emergency preparedness and investigations. It runs the gamut of all security and ancillary functions, so we take a much larger view of things than just to say, 'OK, let's put a guard here and a camera here and we're done.' It's much more holistic." With responsibility for more than just physical security, today's security executives have had to rethink traditional security tactics and develop robust, proactive systems to stay ahead of the inevitable threats and risks present in a global network.

The Vice President, Global Security at a $40B+ global diversified technology and industrial company, believes that proactive security strategies safeguard growing organizations against the incremental risks and threats that accompany expansion. He says, "When I first came to [the company] six years ago, there was a gap of about 10 months between when my predecessor lefts the company and I joined. He was a one man show and extremely reactive, whereas I am a firm believer in being proactive. I think management saw and understood the value of proactive security programs and gave me the opportunity to build out the department from a one person, reactive program to a global, proactive system." A reactionary approach to security may suffice for a small business with no aspirations of expansion, but for a multi-site organization, building a security strategy around preventative measures better prepares the organization and its team to respond appropriately when incidents occur.

Growing Globally

With each new territory into which an organization expands come additional factors that impact business decisions around security. An event in one part of the world—such as a hurricane that causes a production facility to cease operations or a cyber attack that leaks the specifications of a much-anticipated new product—inevitably affects operations and production across

all other lines of business. For companies adding multiple sites to an already widespread geographical footprint, the incremental risk must be addressed with a comprehensive suite of security initiatives and programs.

> "Global perspectives are critically important... We always try to think globally."
>
> *—Director, Worldwide Security Operations, $60B+ global retailer*

The case is even more severe for companies positioned in high-risk geographies. The Vice President and Chief Security Officer at a $40B oil and gas conglomerate, explains: "The onset of the Arab Spring in 2010 prompted ongoing security challenges in the Middle East and North Africa for organizations such as ours. It had, and continues to have, a major impact on the business and how we operate safely and with due care. With over 80,000 employees in 106 countries, safety of our people is the number one priority.

"The recent events in Al Amenas, Algeria, are a great example of this impact, where 39 hostages were killed in the oil and gas community. This incident itself had connotations on our own business, and highlights the complexities of how organizations must continually asses risk, threat, security, and their operating footprint around the world."

Understanding a particular geography, political landscape, and culture is crucial to delivering strategic risk management programs that protect the people and property—both physical and intellectual—of an organization.

As organizations grow their global footprints, it is important to have security leaders to support each geographical area. The Vice President, Global Security at the $40B+ global diversified technology and industrial company strategically grew his security team region by region based on risk. He explains: "Because of all of the threats and risks that were occurring in the business, our model was to basically take baby steps. There is a lot of pressure in terms of what's happening with business in Europe, Asia, and elsewhere that's impacting our business. Since we are in 160 countries and our footprint is so massive, there are a lot of things that can happen. We started by adding a regional director in Europe, then we added one in Asia Pacific, then one in the Americas. We just kept growing and growing to better support our customers and the risks they face." Local security managers ensure that company-wide initiatives are adopted and implemented, which increases coordination across geographies and decreases opportunities for attacks.

Apart from hiring regional leaders to drive security programs in various locations, it is equally important for security executives and their teams to have experience operating on a global scale. The Director, Worldwide Security Operations at a $60B+ global retailer believes, "Global perspectives are critically important because we are a global company. While we have security colleagues throughout the regions, a lot of support comes from our headquarters, so everyone we hire here has to have a global focus. When we create policies, procedures and strategies, and decide on the technology that we are going to use, we always try to think globally; we try not to be North American-centric. We have to think about how well or how effective something will be in Italy, or how to use it in Germany." Security teams that understand the culture, barriers, and sociopolitical factors at play in geographies with varying degrees of risk allow security leaders to deliver strategic, comprehensive programs that can be implemented in every region of the world.

Partnering with Business Leaders

Just as coordination across geographies is crucial to maintaining smooth operations, so too, is alignment across corporate functions and business units. The mission of the security function is to support the organization's goals and objectives; as such, it is important for security leaders to have the business acumen to understand the ways by which certain breaches in security impact operations. The Executive Director of Global Security at a $150B+ automotive manufacturer, says, "First and foremost, security leaders must have business acumen—no longer can security be simply an overhead function. We need to be true partners with the businesses, helping in any way we can to assist our leadership and business complete their work. Security leaders who understand financial controls and work

closely with both functional and business leaders to address their concerns is probably the biggest thing I look for."

The Director, Worldwide Security Operations at a $60B+ global retailer expands on this idea: "We like to think much more big picture and look at the totality of the risk under which we operate, which makes us a more effective partner with the business units we support and or internal customers. We like to think of security as not being a place where good ideas come to die. So many times previously with security, a business unit would come up with a great idea and security would say that it's too risky and that they couldn't do that. We don't do that here. We like to think of ourselves as a collaborator with the business, and if they come up with an operational idea that improves the business practices and better supports our customers, then we will certainly bend over backwards to make that happen. Conversely, we've never tried to force feed anybody with a program here; we've always assessed the need and worked collaboratively to develop a program together." Collaboration between senior business leaders and security executives allows organizations to leverage security to mitigate the risks that result from expansion and innovation, while simultaneously fostering sound and productive business relationships.

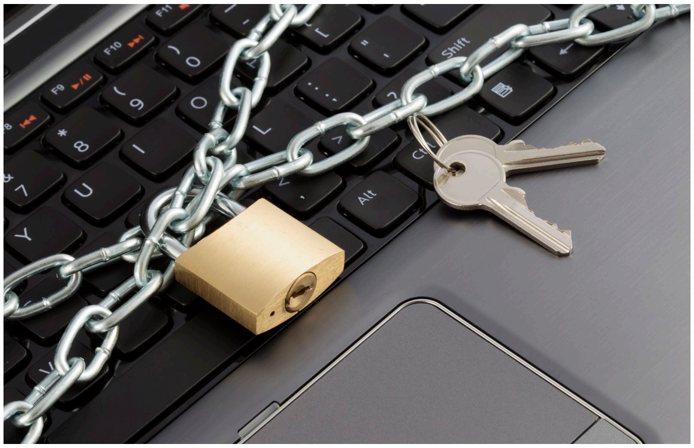
Advocating Security

In addition to having the business acumen to build programs that support corporate goals, security experts must also be skilled in communicating the need for security programs up to the senior-most business leaders, across to different business units and functions, and down through various corporate channels. The Director, Worldwide Security Operations at a $60B+ global retailer says, "You have to be knowledgeable about business risk overall, understand the corporate culture, and align yourself with the business unit leaders to better understand their issues. I think that's the approach you need to take in today's day and age to sell programs. You need to articulate the return on investment. I don't think you can justify a budget just by scaring folks into spending money; you have to especially articulate why the money needs to be spent and what the benefit is to making that financial investment." The key to garnering support from key business leaders is to explain security in a way that demonstrates how certain initiatives will impact the bottom line.

The successful adoption and implementation of security initiatives also depends on buy-in from employees across all organizational levels and locations. With many employees now working remotely and using personal devices, it is important for security leaders to establish clear policies that are informative enough to outline operating procedures as it relates to security, yet accessible enough that it doesn't further confuse or deter staff members from adhering to important security guidelines. Security leaders must view each employee at their organization as resources to strengthen the wall of security. Educational programs and memos can serve as powerful tools for explaining the reasoning behind each security initiative, and will likely prevent people from engaging in behaviors that could potentially expose the organization to threats or attacks. Security leaders who are comfortable interacting with employees and advocating the importance of security across the organization are better poised for gaining stronger internal compliance.

Protecting Against the Cyber Threat

In today's ever-connected society, organizations rely on electronic and digital interfaces to share information across multiple geographies and networks. Add to that the trend of "bring your own device," or BYOD—where employees use personal devices to access networks and work remotely from multiple locations around the world—and the need for comprehensive cyber security strategies is greater than ever before. According to a recent survey conducted by Decisive Analytics, "Nearly half of companies that permit BYOD reported experiencing a data breach as a result of an employee-owned device accessing the corporate network."[1] Companies can no longer protect data assets and proprietary information with surveillance cameras or security guards; lost devices or unprotected networks leave organizations susceptible to a new breed of risk that can only be mitigated by proactive security strategies. For this reason, many security executives have



[1] Cheryl Harris, Mobile Consumerization Trends & Perceptions: IT Executive and CEO Survey, Decisive Analytics, LLC, http://www.trendmicro.com/cloud-content/us/pdfs/business/white-papers/wp_decisive-analytics-consumerization-surveys.pdf (August 2012).

partnered with information technology (IT) leaders to design robust cyber security solutions that support the trend of BYOD while protecting corporate information.

The prevalence of cyber attacks has prompted many organizations to hire Chief Information Security Officers (CISOs) to oversee the IT arm of risk management. According to the Vice President and Chief Security Officer at the $40B oil and gas conglomerate, "Cyber is one of the many changing dynamics in security and risk, for all commercial entities. Many organizations differ where cyber fits as a specific function within their organizational structure and often falls under IT, corporate security, or business resilience. We continue to see change throughout the industry in this relevant reporting structure. How ownership of the program is taken, prioritized and implemented can have major impact to any organization." It is important for security executives, regardless of how responsibility for cyber security is assigned, to acknowledge the importance of robust cyber security initiatives and work collaboratively with the IT team to implement programs accordingly.

Building the Right Team

Many organizations have addressed the increased scope of the security function by hiring team members to own responsibility for specific niche areas or geographical territories. However, security executives must hire additional partners according to need, rather than "want." The Vice President, Global Security at the $40B+ global diversified technology and industrial company explains, "We are an extremely lean organization here. We focus on the quality of service rather than the head count." Continually assessing the state of the security department to determine gaps or redundancies in leadership is crucial to creating a streamlined security department focused on executing and protecting business goals.

Additionally, identifying, attracting and hiring key leaders who have the right set of skills and competencies, who also integrate seamlessly into the corporate culture, is essential for efficient security programs. The Vice President and Chief Security Officer at a $40B oil and gas conglomerate elaborates, "At the end of the day, security functions can be perceived as not making money for the business, i.e., not a revenue stream; so in the ever changing world, you really have to justify how you're spending the organization's money. I need security professionals who not only understand the complex services and operations we deliver around the world, but who can also sit and interact with our senior management on a daily basis and understand their business needs. Security is an ongoing education for all, and should be an integrated business partner rather than just a bolt-on function." Security professionals must walk a fine line when building security teams, keeping in mind the strategic know-how required to be successful in a particular function within the security department, the ability to assimilate into an established company culture, and the cost constraints limiting talent acquisition activities. Knowing when to grow, develop and restructure the security function is a critical leadership requirement of today's security leaders.

Closing Thoughts

Although the evolution of the security function elicited new leadership requirements from the executives in charge, a security leader's agility and ability to evolve with the trends, as opposed to fighting against them, is perhaps the single greatest attribute one could possess. The threats present in today's environment strengthen and multiply when ignored, and evolve into new risks once contested. The modern security executive must have global experience, an ethical background, and sound decision-making principles to guide security activities and be successful in an ever-evolving business landscape.

NGS GLOBAL

AUTHOR

DAVID NOSAL
Managing Partner
NGS Global Americas, LLC

ABOUT DAVID NOSAL

David Nosal is Managing Partner at NGS Global and is a member of the firm's Global Operating Committee. He founded NGS firm Global's predecessor in the Americas, Nosal Partners, in 2005.

Mr. Nosal has conducted numerous executive search assignments across multiple industries throughout North and South America, Europe, and Asia on behalf of FORTUNE 1000 companies, as well as small- to mid-sized organizations. As part of his overall efforts, he has handled assignments for both public and private-sector organizations, working closely with a diverse selection of companies and their boards of directors in identifying, evaluating and attracting senior management teams.

The majority of Mr. Nosal's executive search assignments over the past 25 years have focused on recruiting CEOs/Presidents, board members and other C-level executives into a wide range of global companies - from early-stage private to multi-billion-dollar public firms. His problem-solving approach and commitment to quality and service are recognized assets in the industry, as evidenced by his substantial repeat business.

Mr. Nosal was formerly with Korn/Ferry International, where he was Head of the firm's CEO Practice. He also led Korn/Ferry's West Coast Board Practice. In addition, Mr. Nosal was Managing Director for Korn/Ferry's Central and Northwest Regions, overseeing the firm's San Francisco, Silicon Valley, Seattle, Denver, Chicago, and Minneapolis offices. Prior to joining Korn/Ferry in 1996, Mr. Nosal was with another international executive search firm as a senior partner. He was previously a consultant with a senior-level executive search firm in Minneapolis. Mr. Nosal's career also includes tenure as a consultant with the American Consulting Association in Chicago, as well as at Abbott Laboratories in its Chicago corporate office.

Mr. Nosal graduated with a BS degree from the University of Wisconsin Whitewater.

ABOUT NGS GLOBAL

With 17 offices across the Americas, Europe and Asia, NGS Global provides the extensive resources of major global executive search firms along with high-touch service, accelerated completion cycles and superior candidate access made possible by a mid-sized platform without external shareholders. Through our commitment to industry expertise, cultural knowledge and partner-led search execution, we deliver exceptional value to our clients.

GLOBAL COVERAGE

AMERICAS

Atlanta
Cleveland
Los Angeles
Milwaukee
Minneapolis
New York
San Diego
San Francisco (Americas HQ)

EUROPE

Frankfurt
Munich

ASIA

Beijing
Hong Kong
Melbourne
Seoul
Shanghai
Singapore
Sydney
Tokyo