Eleven Areas for Improvement

By Bob Hayes

By Kathleen Kotwica

In our July column, we discussed the dangerous gap in the transfer of knowledge between visionary security leaders and the next generation of leaders who will have to take up the mantle after them. Then in August, we laid out a roadmap for a new type of training that would help to close that gap. But what topics do up-and-coming leaders need to know more about?

For six years, the Security Executive Council has worked with top-tier security leaders to develop research, track industry trends and solve problems. In the course of this work, these Tier 1 Security Leaders have shared with us their thoughts on the skills that are lacking in the deputies and other potential leaders they are grooming. Most often they are concerned with the lack of strategic thinking and planning skills in these individuals. This shouldn't be surprising; many deputies have to work 10 hours every day on critical operational issues and have little time to devote to strategy.

We've identified 11 key strategic areas in which Tier 1 Security Leaders would like to see their direct reports take on.

• **Aligning Board-Level Risk and Business Unit Mitigation Strategy.** The next generation of leadership will need to know how to line up their programs with the risk categories most important to the Board.

• **Communicating Hazards and Risks, Mitigation and Performance Metrics.** Management and board members make critical decisions based on a host of spreadsheets, graphs and trend lines. Effective, actionable risk management requires disciplined analysis. Security leaders who want to show their business-based contribution to the organization must know how to a) understand the data they're collecting to identify risks, and b) use that data to tell a compelling story of performance and value to the organization.

• **Influencing Community Preparedness and Resilience for Emerging Global Risks.** Catastrophic manmade and natural risks will continue to threaten organizations and communities, making crisis and continuity management ever important. Security leaders need to be versed on the latest global requirements for preparedness compliance, and they must take steps to create community alliances to help build resilience and protect brand.

• **Managing Information Protection, Breaches and Situational Intelligence.** Brand stakeholders require confidence. Information ranging from intellectual property assets to personal identifiers must be protected from persistent physical and cyber threats. The next generation of security leaders needs to know how to roadmap protection architecture and how to manage information crises at the speed of the Internet.

• **Adding Business Value with Mission Assurance and Profit & Loss Performance.** The successful security leader of tomorrow must understand both how to add value and how to show it. Security leaders need to demonstrate security's revenue influence and cost avoidance in return-on-investment calculations and operating statement results.

• **Researching Next Generation Organizations, Programs and Leadership Style.** Security leaders who understand their organization, its employees and their own leadership development are in a strong position to accurately benchmark and gauge program success. They must learn the steps to evaluate themselves and their organizations against industry research to inform their role and corporate readiness.

• **Governing Compliance and Social Responsibility for Brand Equity.** The connection between ethical performance – including compliance and community care – and market performance is increasingly relevant. How can security leaders play a role in stronger ethical performance?

• **Conducting Assignment, Contract, Hire, Incident and Transaction Diligence.** With estimated global fraud exceeding $2.6 trillion (ACFE) and identity theft at epidemic levels, organizations need multi-factor authentication of persons, cargo, conveyances and information. Errors, omissions and fraud are increasingly discoverable with well integrated and layered security solutions that will likely be required by evolving compliance.

• **Transferring Risk Mitigation Competence.** Risk mitigation has become increasingly cross-functional; it's important for security leaders to know how to identify, develop and retain talent all levels for sustainable results. Ongoing risk assessments must be included in project and program management along with continuous education and training.

• **Building Strategic Brand Alliances and Community.** Public and private community partnerships with clients, governmental agencies, peer organizations and trade associations can augment the in-house resources. Security leaders need to know how to build these partnerships and to sustain them for the greatest benefit to all.

• **Applying Proven Practices and Solution Innovations.** Innovative solutions can lend confidence to common risk situation management? Solution evaluation should include pilots that allow for the measurement of cost savings, loss avoidance and opportunity improvements. Proven solutions should optimize core organizational processes and outcomes.

Do you agree that these 11 topics are the areas the next generation needs a firm grasp on? Do you think other issues are more important than these? Contact us at contact@secleader.com to tell us about it. SECURITY

About the Columnists

Bob Hayes is Managing Director of the Security Executive Council (www.securityexecutivecouncil.com). Kathleen Kotwica, PhD, is EVP and Chief Knowledge Strategist for the Security Executive Council.