

Security Leadership > Next Generation Security Leader >

Eleven Ways to Encourage Strategic Thinking

Created by Bob Hayes, Managing Director and Kathleen Kotwica, Ph.D., EVP and Chief Knowledge Strategist, Security Executive Council

Security Leaders we have worked with 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. We offer 11 key strategic areas that direct reports should take on.

1. 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.

2. 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.

3. 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.

4. 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 security leader needs to know how to roadmap protection architecture and how to manage information crises at the speed of the Internet.

5. Adding business value with mission assurance and profit and loss performance.

The successful security leader of tomorrow must understand both how to add value and how to show it. Risk mitigation is no longer just consequence protection. Security leaders need to demonstrate security's revenue influence and cost avoidance in return-on-investment calculations and operating statement results.

6. 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.

7. Governing compliance and social responsibility for brand equity.

The connection between ethical performance—including compliance and community care—and market performance is increasingly relevant. Research by the Ethisphere Institute shows that the most ethical performers are rewarded in the marketplace. How can security leaders play a role in stronger ethical performance?

8. 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.

9. 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 at all levels for sustainable results. Ongoing risk assessments must be included in project and program management along with continuous education and training.

10. 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.

11. 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.

Visit the Security Executive Council website for other resources in the [Security Leadership: Next Generation Security Leader](#) 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 here: <https://www.securityexecutivecouncil.com/>