Security Program Strategy & Operations > Strategic Planning/Management >

Leading During Turbulent Times

Turbulent times often bring uncertainty, chaos, and challenges, marked by rapid change, instability, or conflict. During such periods, leaders must adapt their approaches to navigate effectively. Consider the following to amplify leadership impact and augment decision-making during unsettled times.

Consistent Communication

During challenging times, it's crucial to stay heard amidst the chaos. Begin with an impactful brand story for Security that highlights its value to the business. Successful security leaders often rely on a well-crafted story catalog or "master" to tailor briefing materials that align with the audience's needs and the organization's culture. Some of the major components include:

- A detailed history (e.g., timeline of program development)
- Strategic initiatives and strategic plan with current year areas of focus, the next several years' areas of focus, and how it's tied to funding.
- How your program is organized and at what capacity.
- Value analysis status (e.g., customer use, customer satisfaction, cost by customer).
- Snapshots of the current program state such as a heat map or SWOT analysis to quickly frame up challenges (e.g., gaps, security risks) and highlight direction.
- Developed business value metrics.
- Due diligence on emerging trends that may impact the company and security.

Stay in touch with your internal customers. For example, you can develop simple questionnaires about the effectiveness or value of your services. Use them to:

- Gain insight into how internal customers perceive security.
- Understand what is working and what is not.

- Engage end-users to be a part of the solution.
- Generate data for presentations or charts on security’s perceived value throughout the organization.
- Show satisfaction over time to senior management.

Another option is to try to set up brief internal stakeholder interviews to gain insight into their issues. Use them to:

- Explore “buy-in” or understanding of new security plans.
- Determine stakeholders’ security-related concerns.
- Encourage stakeholder ownership of security success.
- Roll-up results for senior management briefings.
- Adjust security decisions or plans.

Enable Your Team

The security team may require enhanced leadership support to navigate effectively through challenging times. Providing clear guidance and adaptable strategies can help them maintain focus, resilience, and alignment with organizational goals.

- Model collaborative and positive culture. Many corporate security departments have seen their development in this area stymied when leaders fail to exemplify the appropriate behaviors from the top.
- Set clear goals. The security team can’t work as a cohesive unit unless its leadership defines and reiterates its mission and goals.
- Encourage risk taking. If the security team expects every new idea to be shot down, they will stop looking for them.
- Get out of the way. Providing some level of autonomy with one’s staff is imperative if they are to gain confidence and trust in their own decision making.
- Encourage communication. Setting rules and boundaries for the tone of meetings and communications can help ensure that all team members feel safe sharing information, thoughts, and critiques.

Build or Foster Cross-Functional Partnerships

SEC subject matter experts have reported that in the C-Suite, there is an expectation that all business functions engage actively with their stakeholders across the organization to build understanding, share information, and optimize processes. Corporate security is not exempt from that expectation.

Thriving in today's complex, global business environment demands not only agility in managing security threats but also the ability to take calculated risks—expanding into new markets, investing in innovation, and forging new partnerships. The corporate security function plays a pivotal role in facilitating smart risk-taking by delivering robust risk intelligence and ensuring the safety and security of the organization's physical assets, personnel, and operations across all ventures—not merely within the confines of a few programs under its direct oversight.

When building and executing a strong cross-functional program—such as those addressing workplace violence or global security operations centers—the process itself brings valuable additional benefits. Activities like stakeholder interviews, socialization, and consensus building foster stronger collaboration and shared understanding among teams. A critical element in ensuring successful partnerships is the formal documentation of agreements, roles, policies, and processes. This step not only solidifies commitments but also provides a clear roadmap for future operations.

Strategic Thinking

Unsettling times often force leaders to spend much of their energy “putting out fires.” However, our subject matter experts offer several recommendations to help clients reclaim and expand their strategic thinking time, enabling a more forward-looking and effective approach.

- Put it on the schedule. Block out a time to think strategically about the function and treat it like an important meeting – no cancelling.
- Meet with stakeholders. Ask them about their top objectives and risks, and about their perception of security. Ask about key changes, plans, coming investments, and forecasts.
- Meet with leaders in other functions and invite them to your meetings. Ask them about their objectives and risks, and how security can help meet them.
- Tour your company's sites.
- Find a mentor either within or outside your company.
- Read the business' 10K or similar financial reports.
- Develop your team with next generation leaders you can rely on, so you can free up more time to think about the big picture.
- Make sure your team has annual performance objectives and personal development plans and follow up to see how well they're being met.

Go Above and Beyond

Exceed the expectations of your internal customers by thinking beyond the basics of security mitigation. While your customers may request A, B, and C, your unique perspective as a corporate security and risk expert allows you to identify and communicate potential risks like X, Y, and Z. Don’t limit your approach to conventional methods or past incidents; instead, incorporate all relevant information to ensure comprehensive risk management. Share these insights with business leaders to empower them to make informed, strategic decisions.

Maximize the potential of your discovery skills. When conducting risk and threat assessments, you likely examine factors such as the geographical area, political and social climates, and historical incidents. But do you limit your focus to lagging indicators—data reflecting past events—or do you extend your discovery efforts to identify leading indicators that signal emerging risks? By broadening your perspective, you can uncover valuable insights that proactively shape risk management strategies.

Leverage data and analytical methods to guide decision-making. While intuition can occasionally yield the right answer, an analytical approach provides a consistently reliable framework for tackling complex problems. As risks continue to grow in complexity, the role of data analysis in security will expand—encompassing tasks such as synthesizing information, identifying patterns within disordered data, and deriving actionable conclusions.

Relying on questionable data, limited information, opinions, or ingrained corporate history can lead to unfavorable outcomes. Instead, deconstruct complex problems into smaller, manageable components to uncover solutions. These incremental wins can accumulate, eventually leading to transformative "ah-ha" moments that drive impactful decisions.

Recognize how risk evolves due to current events, organizational changes, geopolitical dynamics, and economic shifts. Conduct a thorough reassessment of your organization's security risks, ensuring that your programs, services, and mitigation strategies reflect these developments. Prioritize revised plans and initiatives, aligning them seamlessly with the organization's updated directions and overarching goals.

Although difficult, turbulence also brings opportunities for growth. Just as storms can clear the air, these times can lead to breakthroughs, fresh perspectives, and resilience. Throughout history, turbulent eras have often sparked innovation and redefined the world, proving that even chaos has the potential to inspire transformation.

Visit the Security Executive Council web site to view more resources in the Security Program Strategy & Operations : Strategic Planning/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/