ONTIC | SEC SECURITY EXECUTIVE COUNCIL

CHECKLIST

Proving the Value of Corporate Security

Despite being responsible for protecting businesses, funding challenges can be a roadblock for corporate security teams. It often comes down to fighting the stigma that security is a cost center and ensuring that key stakeholders understand appropriate funding is vital to securing the business's assets, employees, and bottom line.

To help you get the budget, respect, and support you need to effectively protect your organization's workforce and property, we've partnered with the Security Executive Council (SEC) to prepare a comprehensive checklist.

Evaluate Real and Perceived Program Effectiveness

Examine how effective your program is today

Senior management believes your corporate security program adds value to the organization	□
You and your team wield the influence necessary to eliminate and/or mitigate risky business practices	□
Management owns the risk and accepts responsibility for people and asset protection	□
Personnel (employees, contractors, etc.) support your efforts and consistently comply with security regulations	□
You are able to fix, eliminate and/or mitigate vulnerabilities with little-to-no downtime	□
You are able to demonstrate your role in ensuring profitability within the organization	□

Understand Your Internal Audience

Grow a deeper understanding of your "internal customers" and earn their buy-in

Develop personas for all internal stakeholders • Observe stakeholders in day-to-day interactions • Sit in on or lead stakeholder meetings • Participate in ad-hoc conversations	□

Continued on next page

Send out a survey to gauge how people feel about the existing security program • Select simple but specific questions *Example: "Please rate your confidence in the visitor badging system on a scale of 1 to 10."* • Ensure questions are relevant to each audience *Example: "As an HR leader, how satisfied are you with the check-in process for candidates visiting the building?"* • Include open-ended questions that allow comments *Example: "If you could change anything about the organization's on-site security, what would it be?"*	□
Conduct interviews that ask about stakeholder's goals and objectives • Select someone outside the security team to conduct the interview • Partner with a professional security research and advisory group • Create a base set of questions and tailor them to each audience • Leave time for questions and comments	□

Make the Case

Educate and inform your organization on the benefits of a robust corporate security program.

Outline lesser-known benefits • Explain how corporate security supports the enterprise's risk management strategy • Clarify how the business owns the risk, but security mitigates it • Validate the importance of working as a team with other functions • Provide context on security's role in gathering information from crises to prepare for future situations • Provide examples as to how security can meet the needs of the organization using emerging issues intelligence • Explain how security develops critical incident management plans using its creative planning, rigorous testing, and swift decision-making capabilities • Frame processes on how security monitors and mitigates incidents from many domains *Example: pandemic, climate change, supply chain, social unrest, workplace violence, and more* • Share calculated benefits of a multi-disciplinary security team that includes data analysts and technologists • Explain the benefits of frictionless access controls and integrated security systems • Explain how your team gathers facts and communicates in a crisis • Inform how fusion, risk and security operations centers are becoming 24×7×365 and generating an ROI • Explain how security is evolving to distribute responsibilities and benefits across the internal network	□
Demonstrate security's value to the business • Identify the root cause of business loss, risk and vulnerability • Highlight how security can collaboratively help, learn, alleviate, or mitigate this loss through frank and open conversations about risk • Identify potential partners in mitigating risk *Example: CFOs, HR leaders, IT leaders, facilities leaders, and legal and compliance leaders*	□

Continued on next page

Measure and report performance • Run security as a business • Approach every problem with the interest of the business • Seek solutions that empower the business • Track and measure your efforts • Centralize your security data • Break down your data silos, e.g., integrate with Finance, HR, Procurement, Real Estate, Risk Claims, etc. • Pilot, test and Invest in a platform that allows you to unify data governance and end-to-end audit tracking • Communicate and foster cross-team collaboration • Communicate through all relevant channels with the workforce on a regular cadence • Share data insights with all employees including near misses • Ensure you're sending immediate notifications about potential threats	□
Communicate brand reputation and business continuity • Illustrate how you've reduced the frequency or severity of key risks over time • Communicate security "wins" through growth, revenue, and other business metrics	□

Get our guide to proving the value of your program

Download our guide to learn how to evaluate, qualify, quantify, and prove the value of your corporate security program. You can also reach out to the SEC and Ontic for support from our experts.

Download Now