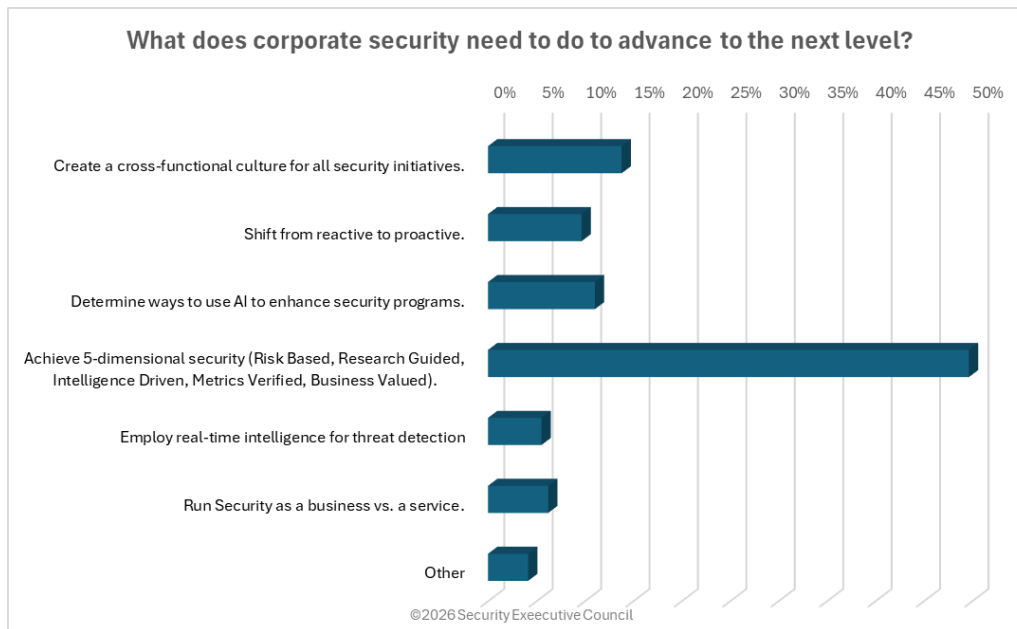


Security Program Strategy & Operations > Emerging Issues >

Security Barometer Results: The Future of Corporate Security

Corporate security is often reduced to the old "gates, guns, and guards" (3G) stereotype. In reality, the field has evolved into a strategic discipline focused on identifying and managing risks so the business can operate and grow with confidence.

This security barometer quick poll is investigating what corporate security needs to accomplish to truly advance to the next level.



The "Other" answer largely consisted of "All of the above" and "Choosing a comprehensive,

cross-functional, joint engagement approach to security”.

The survey participants were offered the opportunity to provide explanations or comments about their answers.

Below is a selection of some of the responses, edited to preserve anonymity.

- The key change is convergence and understanding that corporate security covers multiple domains, including physical security, cyber, and personnel security. In cases where decentralized or federated models are used, cross-functional collaboration is key and should be led by corporate security.
- Strategically, Governance should be up there too to ensure that your security program will be defensible and stress-tested.
- We need to stop assessing "Security," especially physical security as a standalone effort. Physical security can and should be the catalyst to drive an effort to Bridge the Protective Silos (Physical, Cyber, BCM, EM/CM, Supply, EH&S, HR, Compliance, Legal, Financial, Audit, ...) into a joint mission to develop, maintain and improve Operational Resilience. This mission can be anchored in a FUTURE Operations Center model that supports shared consciousness and joint operational capabilities.
- Corporate Security was reduced when Information/Cyber Security advanced and nested under the CIO/CTO. Compliance and regulatory regiments labeled non-cyber/non-technical security as "physical security" which is only one component of security practices. With "physical security" reporting channels and functions scattered and limited regulatory guidelines outside of small sectors of critical infrastructure, the challenges will remain.
- These five dimensions create a security program that is proactive, measurable, intelligence-informed, and tightly aligned to business value transforming security from a cost center into a strategic enabler.
- A successful security program is truly cross-functional in ways that go after theft, fraud, embezzlement, workplace harassment and any kind of threat or violence towards individuals, facilities, or the business at large.
- Security professionals often face challenges in securing adequate funding and resources because they communicate in terms of threats, vulnerabilities, and controls—while the C-suite focuses on revenue, risk, and competitive advantage. Through the convergence of physical and cybersecurity, physical security leaders must bridge the gap between security and business priorities. Practical approaches include:
 - Articulating security value in business terms that resonate with the C-suite
 - Eliminating silos and redundancies through integrated risk management (GRC & ERM)
 - Aligning security investments with organizational priorities
 - Build measurable ROI into security program design
- The next major shift in security will be driven by AI. Hands down!
- Open dialog must be achieved by explaining security procedures to employees instead of the old "just do it". When security procedures are explained in a relevant way,

employees will help be a force multiplier by participation.

- Recently corporate security has faced resistance from management because of the “business as usual” attitude. Most of those in corporate security fail to justify their actions as well as their needs because they don't have enough time to pay attention to the 5-dimensional security as a result management is not convinced to offer its full support.
- The need for corporate security to function in the business environment is more critical now than ever. For security professionals to understand the foundational building blocks and nuances of their corporate culture is required in order to provide the level of protection needed in the complex business environment. This means speaking the language of business (metrics and value added, not consumed) and being a persuasive advocate for safety and security throughout all organizational elements.

Visit the Security Executive Council web site to view more resources in the [Security Program Strategy & Operations : Emerging Issues](#) 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/>