

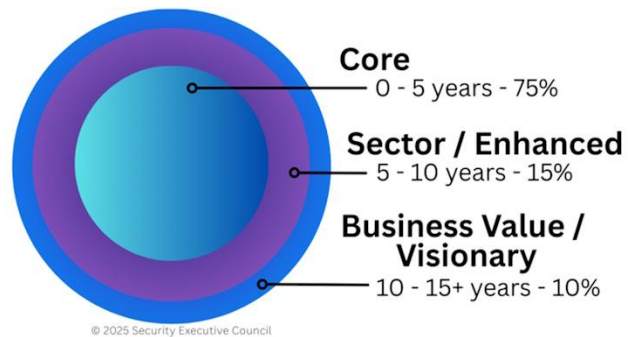
Demonstrating Value > Building Influence >

When Security Becomes a Valued Part of the Business

Security Industry Profile

On a SEC Security State of the Industry SEC staff and [Tier 1 Security Leaders](#) discussed the CSO Path to Adding Business Value. The SEC has conducted extensive research with more than four hundred companies. In some of its earliest from 2007, which is still relevant today, it found that about 75% of CSOs had been in their roles five years or less, typically focusing on core programs: investigations, workplace violence, security technology, and executive protection.

Those who remained in their roles for five to ten years tended to become deeply engaged in sector-specific programs such as financial services, energy, or oil and gas, where regulatory demands shape the work. This group represented roughly 15% of leaders studied.



Only a small number, about 10%, reached the ten- to fifteen-year mark and focused on initiatives that added measurable business value. Achieving that level requires two things:

1. A CSO who understands how to create and demonstrate value, and
2. A company that is organizationally and financially ready to support that work.

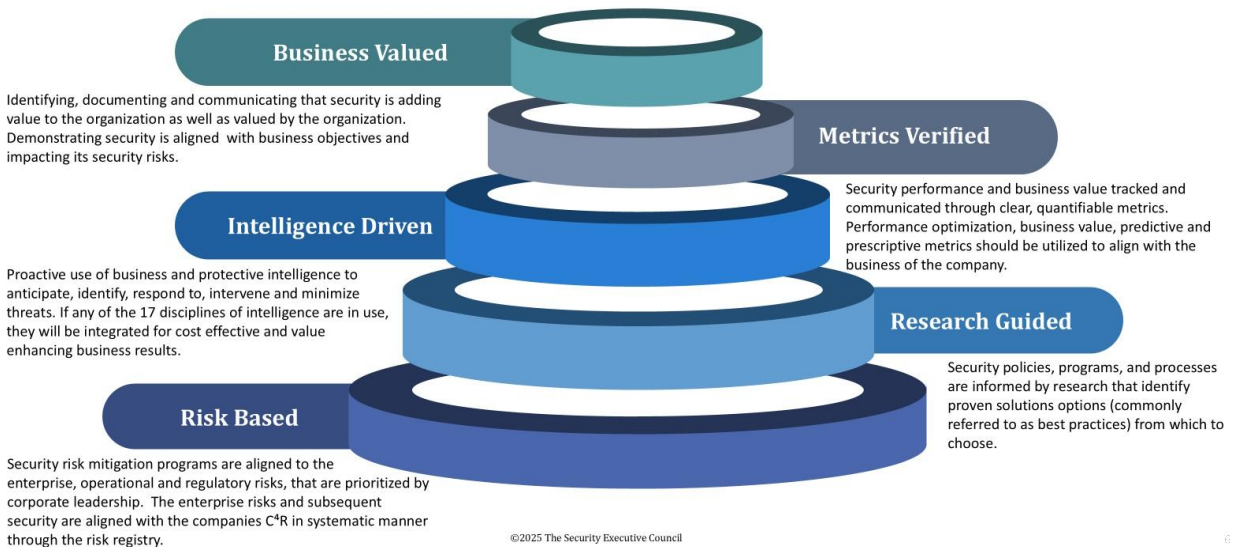
Without both, security leaders remain limited to operational responsibilities rather than contributing to the business's broader success.

From 3G to 5D

The SEC finds that some security programs are evolving from the traditional “3G” model, Gates, Guns, and Guards, to what the SEC calls Five-Dimensional Security. This doesn’t replace physical protection, investigations, or access control; it builds on them.

The challenge with 3G is that’s where most of the money and management attention goes. Because security risk management isn’t taught in business schools, executives often define security solely as physical protection and technology systems.

The Five-Dimensional Model



The 5D model reframes that perception. It is based on the security organization being:

- Risk-based
- Research-guided
- Intelligence-driven
- Metrics-verified
- Business-valued

These characteristics replace opinion with evidence. At senior levels in an organization, decisions are made on data and value, not personal belief. Achieving “5D security” requires more than technical improvements, it also demands organizational readiness to support risk-based, data-informed, and business value-focused security leadership.

Security Executive Brand Image

Security Leadership Research Institute Research on Security Program Domains

CSO Security Domain Responsibilities



© 2025 Security Executive Council

SEC research across 400 companies has shown that:

- Over 70% of CSOs have responsibility for the green domains, the traditional core of security.
- About 50% cover the blue domains.
- Less than 25% handle purple domains.
- About 15% handle gold domains.
- Only 10% manage the red domains.

Most programs include only 5–10 of these 24 domains. The focus for this briefing was on the gold domains. The domains that deliver the greatest business value. These domains share a security nexus; they require security expertise yet are often managed elsewhere in the organization. For example:

- In pharmaceuticals, product security often sits outside security.
- In retail, loss prevention and asset protection may be separate.
- Few organizations include employment screening, supplier vetting, or supply chain integrity under security.
- In utilities, theft of service is often excluded.

Yet these are the very programs that add measurable value to the business. Areas such as special investigations, counterfeit protection, and supply chain security generate significant financial impact, often directly contributing to the bottom line.

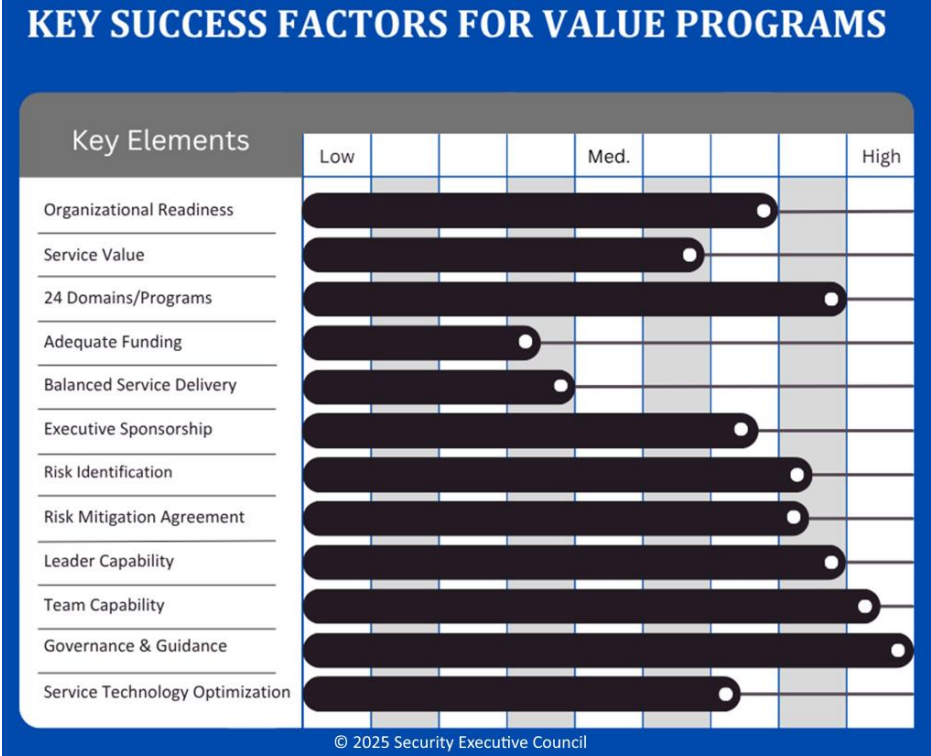
High-Value Program Characteristics

High-value security programs share common traits:

- They are fact-finding and investigative in nature.
- They often have a criminal justice, regulatory, or enforcement connection.
- They address malicious behavior, an area where security professionals excel.
- They rely on healthy skepticism and evidence-based judgment.

These are, by definition, security-centric disciplines, yet too often they are managed elsewhere in the business.

Key Success Factors for Business-Valued Programs



SEC research has identified 12 core elements that enable security programs to deliver measurable business value. No organization excels in all areas, but programs that rate mid-to-high across a majority are on the path to value success.

Examples include:

- Defined risk ownership: Has the program’s risk been clearly identified and accepted by senior management?
- Leadership agreement: Do executives and business unit owners support the program?
- Capability readiness: Does the team have the expertise and structure to execute effectively?

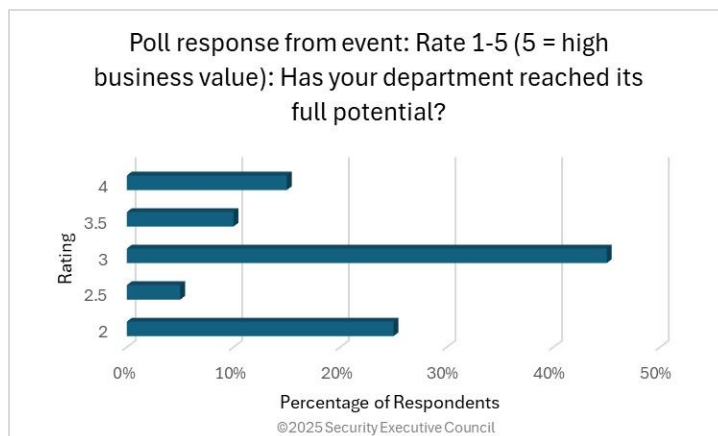
Achieving business value requires alignment, support, and competence, both from the organization and from security leadership.

Insights from Four Corporate Security Leaders

Across industries and organizational models, the most effective security leaders share a common success factor: their programs are valued by the business.

That value is not declared, instead it’s earned, through alignment, intelligence, collaboration, and measurable contribution to enterprise goals.

In the Security State of the Industry leadership discussion, four senior security executives described how their teams moved from traditional protection models to integrated, intelligence-led programs that business leaders view as essential.



Their collective message: when security demonstrates relevance, partnership, and performance, it becomes part of the company’s competitive strength.

Growing with the Business: From Loss Prevention to Enterprise Value

One leader described how a retail-based loss prevention function transformed into an enterprise security organization aligned with every part of the business.

Originally focused on audits, investigations, and safety, the team expanded its scope to include brand enforcement, investigations, and enterprise risk management as the company grew through acquisition.

Operating now under their core pillars, leadership, operations, risk, and change management,

the team's evolution has been fueled by partnerships and credibility. Security earned its seat at the table by helping business leaders meet their objectives, not by demanding compliance.

By embedding in operations, identifying advocates, and translating traditional retail capabilities into enterprise value, the department became a trusted business partner further proof that maturity and trust drive perception of value.

Demonstrating Tangible Business Impact: Global Brand Protection

Another security leader focused on how value was proven through data and financial results.

After a major acquisition doubled the company's size, the Global Security team built a brand protection program that began as a \$100,000 pilot and now represents half of the department's global budget.

Using market intelligence and visual analytics, the team showed executives the real cost of counterfeit products and the economic value of prevention and recovery, quantified in millions of dollars saved.

The program's credibility came from:

- Staying aligned with business priorities,
- Demonstrating measurable outcomes, and
- Maintaining constant visibility with executive leadership.

In short, brand protection moved from a defensive posture to a revenue-preserving business function, an unmistakable demonstration of value.

Proving Economic Worth through Insider Risk Management

A third speaker described how the company's insider risk program evolved from a compliance requirement into one of the organization's most valuable assets.

Originally driven by Department of Defense regulations, the initiative expanded to protect the company's intellectual property, trade secrets, and competitive intelligence across global operations.

The team built a program integrating proactive monitoring, secure offboarding, and intensive investigations. Losses prevented and data recovered have been measured and validated by finance in billions of dollars, which the business recognized as proof of worth.

Key to success was the company's fully converged security model, blending physical and cyber

expertise to produce a single, integrated risk picture.

This leader made clear that convergence is not about structure, it's about coordinated performance and shared outcomes. When security helps preserve economic value, it becomes a strategic necessity.

Creating Value through Fit-for-Purpose Resilience

The fourth leader faced a different challenge: proving value during a corporate spin-off.

Consultants initially recommended a minimalist “guards and gates” model. Instead, the security director argued for a business-integrated, intelligence-led resilience program that included business continuity, crisis management, and anti-counterfeiting.

Operating with a small global team of fewer than 20 professionals in 140 countries, the department's credibility was built on precision and partnership.

In particular, its supply chain security program demonstrated how value is created by right-sizing protection to fit the business. Rather than replicating the high-cost model of its former parent company, the new program used risk-based targeting, simplified processes, and measurable KPIs.

Through collaboration with the Security Executive Council (SEC) and other experts, the team aligned performance with business needs, showing that simplicity, intelligence, and adaptability generate measurable return.

What Makes Security Valued by the Business

Across all four programs, the leaders described similar pathways to earning trust and recognition inside their organizations. Their experiences form a model for how security becomes a valued function:

Driver of Value	How It's Demonstrated
Business Alignment	Security priorities mirror enterprise priorities. Every initiative ties to business outcomes.
Intelligence and Insight	Data, market monitoring, and analysis inform decisions and demonstrate relevance.
Measurable Impact	Value is quantified in revenue preserved, losses prevented, and risk reduced.
Partnership and Advocacy	Relationships with executives, HR, Legal, IT, and operations create influence and trust.

Fit-for-Purpose Design	Programs are scaled and adapted to the business, not copied from larger models.
Integration and Convergence	Physical, cyber, and product security collaborate to present one risk picture.
Credible Leadership and Team Culture	Small, capable, mission-driven teams deliver consistent, visible results.

The Value-Focused Security Leader

These four leaders represent a new model of the security executive. One who speaks the language of risk, resilience, and business performance. They measure success by business outcomes: continuity maintained, brand integrity preserved, insider losses prevented, and global operations secured.

Their programs are lean, data-driven, and collaborative, but above all, they are valued.

Because when security contributes to the organization's goals, protecting revenue, reputation, and resilience, it stops being a cost center and becomes a core business enabler.



Conclusion

Across the industries represented in this briefing, these four stories reveal a single reality: Security is most valued when it helps the business succeed.

Programs that integrate intelligence, measure impact, and build lasting partnerships don't have to justify their existence, their worth is self-evident. The lesson for all security leaders is clear: to be valued, security must not only protect the enterprise it must perform for it.

Visit the Security Executive Council web site to view more resources in the [Demonstrating Value : Building Influence](#) 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/>