Transforming cyber complexity into cost optimization and strengthen maturity

Thought Leadership

April 2026

The better the question. The better the answer.
The better the world works.

EY
Shape the future with confidence

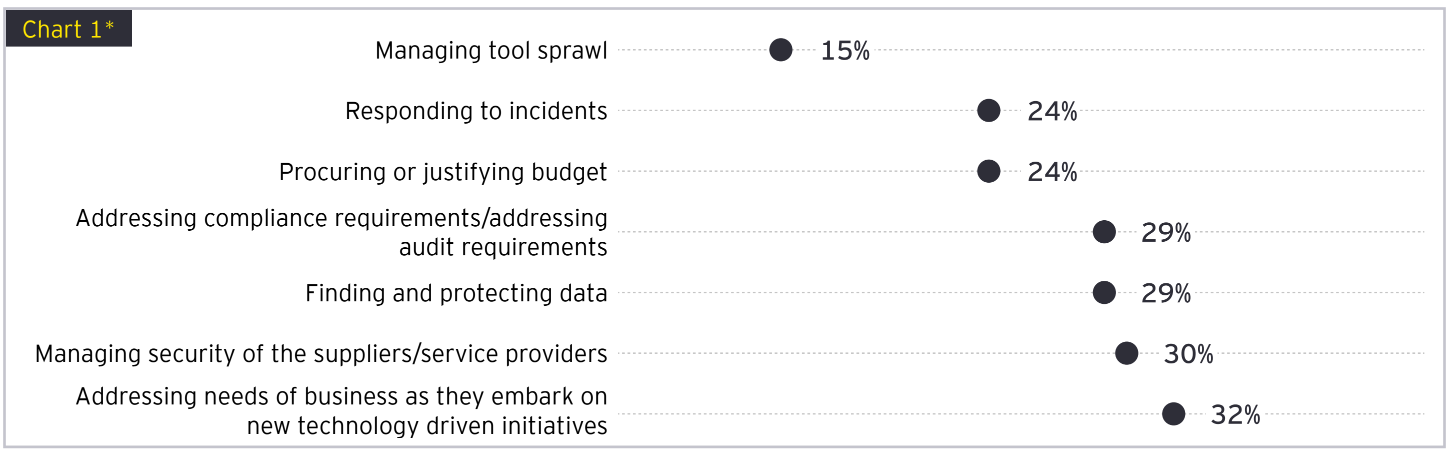
Security Complexity Through the Executive Lens

Cybersecurity spend is rising, yet unmanaged complexity is diluting ROI, fragmenting risk visibility, and driving up operational and compliance costs.

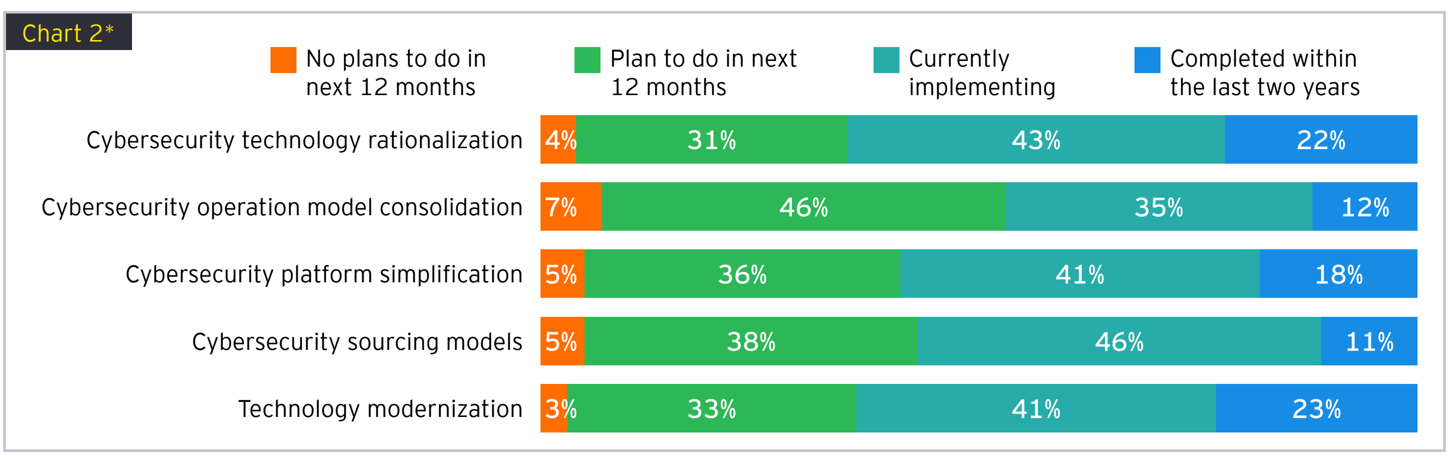
In brief:

- Cyber leaders face **escalating spend with diminishing value**, driven by overlapping platforms, tool sprawl, and fragmented service-provider ecosystems that weaken end-to-end security outcomes.
- Organizations continue to struggle with **incomplete, stitched-together risk visibility**, as insights remain scattered across disparate tools, dashboards, and multiple service providers—making it harder for executives to make confident decisions.
- **Operational strain and compliance pressure are intensifying**, with overwhelmed security teams, growing skill shortages, and expanding regulatory obligations stretching already complex control environments.

Top challenges of cybersecurity operations



Cost optimization strategies of Cybersecurity function

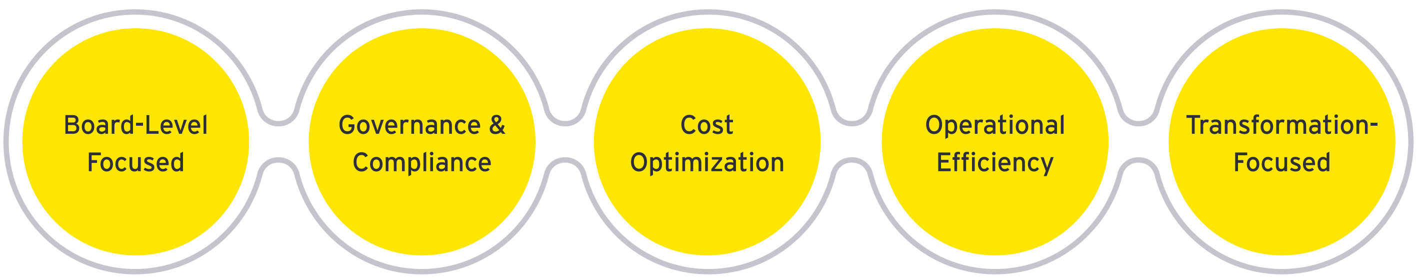


[*Source: EY Survey Intelligence Platform; Global Cybersecurity Leadership Insights Study 2025]

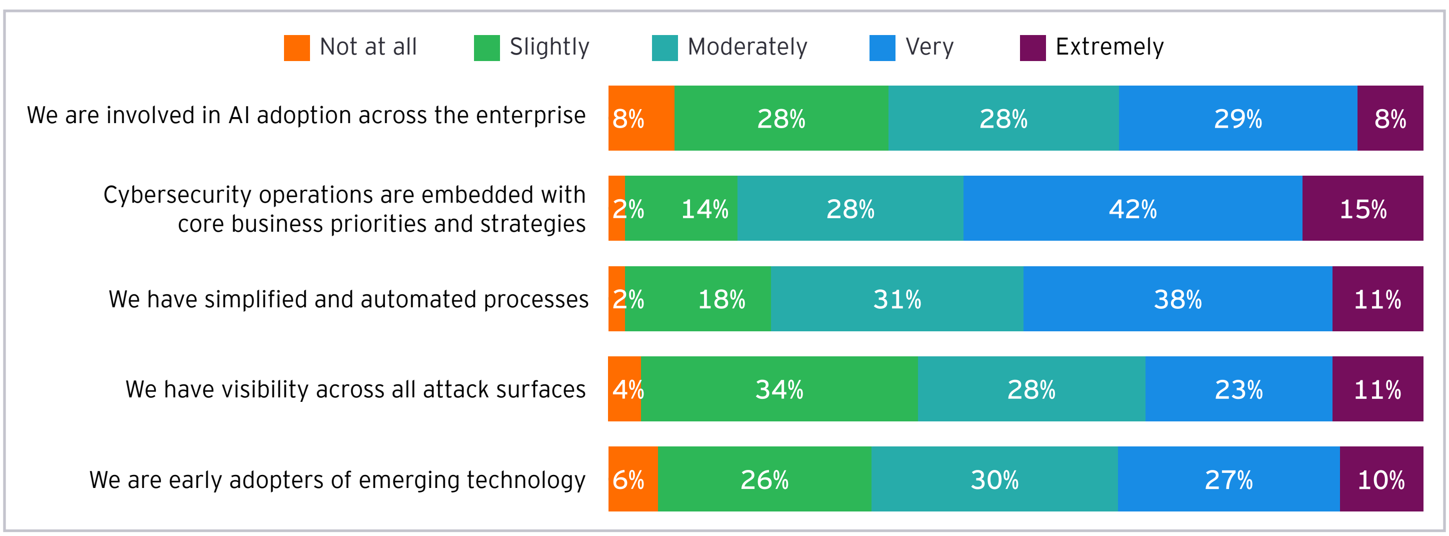
The issue is not under-investment in security, but unmanaged complexity that dilutes value and visibility.

Elevating security: From complexity to a unified, risk-led cyber architecture

To break free from today's fragmented and tool-heavy security environment, cybersecurity functions must evolve from managing growing stacks of point solutions to operating a simplified, integrated, **AI-supported**, and business-aligned security architecture. Leaders are redefining security simplification with the following attributes:



Current cybersecurity approach by various organizations



Organizations adopting security simplification and AI-enabled architectures are achieving clearer visibility, stronger governance, and measurable reductions in cost and risk.

Provide boards with unified, business-relevant insights that clearly connect cyber investment, residual exposure, and operational performance — enabling informed, risk-aligned capital decisions

Modernize the security stack with a platform-led, risk-aligned architecture that scales with digital transformation, accelerates innovation, and strengthens enterprise resilience

Strengthen control ownership and accountability through simplified architectures, automated evidence flows, and integrated Cyber GRC — reducing audit fatigue and improving regulatory defensibility

Reduce noise, unify telemetry, and streamline workflows to materially improve detection and response — freeing teams to focus on strategic priorities instead of managing fragmented tools

Expose redundant tools, unused licenses, and inefficiencies across sourcing models — unlocking 15%–30% cost-to-run savings and enabling reinvestment into automation, AI, and higher-value capabilities

1. Board-Level Focused

Boards are increasing cybersecurity investment, yet confidence in outcomes remains uneven. Nearly **30% of large enterprises now spend more than $100M annually on cybersecurity**, while cybersecurity budgets continue to rise as a percentage of overall IT spend year over year. Despite this, **close to 56% of C-level executives strongly believe cybersecurity is embedded in core business priorities**, and fewer than half believe CISOs are viewed as true strategic partners at the C-suite level. This gap underscores why boards must move beyond spend and tool proliferation toward a **unified, risk-led view of residual exposure, cost-to-run, and value delivered**. Organizations that elevate cybersecurity to a board-level risk and capital allocation discussion are better positioned to demand accountability, make informed trade-offs, and ensure cyber investments materially reduce enterprise risk rather than expanding complexity.*

2. Governance & Compliance

Governance and compliance remain one of the most operationally strained areas of cybersecurity. **Over 90% of organizations are investing in governance automation, around 43% maintain that they have high satisfaction with C-suite integration of cybersecurity into key business decisions**. Fragmented tooling and manual evidence collection continue to drive audit fatigue, unclear control ownership, and inconsistent regulatory reporting. A unified, risk-led cyber architecture integrates Cyber GRC directly into operational platforms, enabling **continuous, evidence-based compliance** rather than periodic audit exercises. This shift allows organizations to harmonize overlapping regulatory requirements, establish enforceable accountability, and provide boards and regulators with defensible proof that controls are effective in practice—not merely documented.*

3. Cost Optimization

Cybersecurity cost optimization is already delivering measurable value—but only where simplification is deliberate. Around **64% of organizations are currently implementing cybersecurity technology rationalization, and nearly 59% have simplified platforms**, with a subset reporting annual savings exceeding $2.5–$5M from platform simplification alone. Importantly, **nearly 74% of C-suite executives reinvested these savings to remediate control weaknesses**, while **68% redirected funds toward automation and AI initiatives**, reinforcing that cost optimization and maturity are not mutually exclusive.

A unified cyber architecture exposes redundant tools, underutilized licenses, and inefficient sourcing models—allowing organizations to structurally reduce total cost of ownership while reinvesting in capabilities that materially strengthen resilience.*

4. Operational Efficiency

Operational inefficiency remains a persistent consequence of cyber complexity. **Ninety seven percent of organizations are automating detection and response processes**, more than **35% still face a mean time to respond (MTTR) measured in days**, not hours. However, where automation is embedded within simplified, integrated architectures, results improve materially: **over 65% of organizations have experienced reduced MTTD and MTTR, and for around 76% of cyber teams, automation has freed capacity to deliver additional cyber priorities and collaborate more closely with the business.** A unified, risk-led architecture reduces alert noise, consolidates telemetry, and clarifies ownership—allowing security teams to operate with speed, focus, and confidence rather than being overwhelmed by fragmented tools and manual workflows.*

5. Transformation-Focused

Cyber transformation is increasingly tied to enterprise value creation, not just risk avoidance. **Cybersecurity functions are now significantly involved in technology adoption, innovation, and business transformation initiatives in more than 50% of organizations**, contributing a **median of 11%–30% of overall project outcomes** where engaged early. Organizations that simplify and modernize their cyber architectures report stronger impacts on **innovation velocity, market responsiveness, brand trust, and workforce productivity**. This evidence reinforces a critical message for C-suite leaders: cyber maturity is not achieved through incremental tooling, but through **platform-led, risk-centric transformation** that scales automation, embeds governance, and positions cybersecurity as a strategic enabler of growth, resilience, and long-term enterprise value.*

*Source, Cybersecurity: From value protection to value creation | EY - Global

From Cyber Complexity to Measurable Enterprise Value

Security Simplification creates the foundation for measurable improvements in visibility, cost-to-serve, governance, operational speed, and enterprise scalability.

Unified Cyber Insights for the Board

A single, unified dashboard presenting risk, cost-to-run, and performance metrics in a decision-ready view—enabling informed, timely, and accountable board-level decisions.

Compliance Acceleration

Streamline reporting and control mapping through integrated Cyber GRC alignment, enabling faster audits and stronger regulatory defensibility.

Cost Reduction

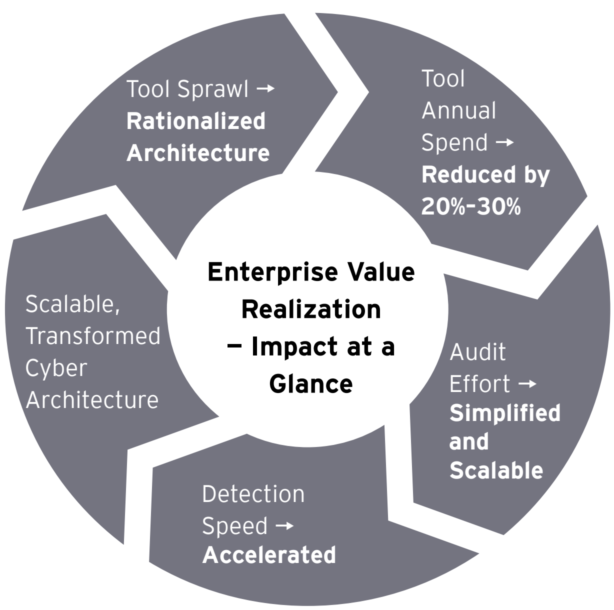
Realize 15%–30% cost reduction by simplifying the cybersecurity landscape through technology rationalization, platform consolidation, operating-model optimization, and streamlined sourcing—while strengthening risk coverage and security outcomes.*

Improved detection & Response

Improve signal clarity and reduce noise to accelerate detection and response, lowering Mean Time to Detect (MTTD) and operational exposure.

Operational Agility

Enable faster adoption of high-value technologies while reducing operational friction, training overhead, and integration complexity.



Security Simplification transforms cyber complexity into cost efficiency, defensible governance, accelerated response, and enterprise-wide value realization.

*Source, Cybersecurity: From value protection to value creation | EY - Global

What Good Looks Like: Maturity Markers

In a mature security operating model, simplification enables a cyber function that delivers unified business insights, defensible compliance, optimized cost-to-serve, faster operational execution, and a scalable modern architecture — turning fragmented complexity into measurable, enterprise-level value.

Enterprise-Aligned Cyber Insights

Cyber performance, risk exposure, and cost-to-run are presented in a unified, business-relevant way, enabling informed board-level decisions.

Continuous, Defensible Compliance

Controls operate with clear accountability and automated evidence flows, reducing audit fatigue and strengthening regulatory confidence.

Optimized Cost-to-Serve

Redundant tools are eliminated, licenses are fully utilized, and the rationalized portfolio delivers 15%-30% measurable savings while improving capability coverage.

High-Velocity Cyber Operations

Integrated workflows, reduced alert noise, and targeted automation accelerate detection and response, increasing cyber team productivity and operational precision.

Scalable, Transformed Cyber Architecture

A platform-led, risk-aligned design that supports innovation, automates core processes, and scales with enterprise growth and digital transformation priorities.

Conclusion: Turning Security Simplification into a Strategic Advantage

Security Simplification evolves cybersecurity into a unified, outcome-driven capability that delivers enterprise-aligned insights, continuous and defensible compliance, optimized cost-to-serve, high-velocity operations, and a scalable modern architecture. By rationalizing portfolios, embedding automation, and strengthening governance, organizations reduce noise, improve resilience, and unlock measurable business value—positioning cybersecurity as a strategic contributor to growth, performance, and long-term enterprise advantage.

“

These maturity markers make Security Simplification more than a cost exercise — they turn it into the operating backbone of modern cybersecurity, enabling unified visibility, efficient execution, and faster, more strategic risk decisions.

Special thanks to Sai Lakshmi Sathyanarayana, Eknathraaj Thirumurthy Kannan, Deb Sekhar Bose & Swagat Sourav.

EY | Building a better working world

EY is building a better working world by creating new value for clients, people, society and the planet, while building trust in capital markets.

Enabled by data, AI and advanced technology, EY teams help clients shape the future with confidence and develop answers for the most pressing issues of today and tomorrow.

EY teams work across a full spectrum of services in assurance, consulting, tax, strategy and transactions. Fueled by sector insights, a globally connected, multidisciplinary network and diverse ecosystem partners, EY teams can provide services in more than 150 countries and territories.

All in to shape the future with confidence.

ED None

ey.com