Reimagining cybersecurity – the cyber risk operations center in the age of artificial intelligence

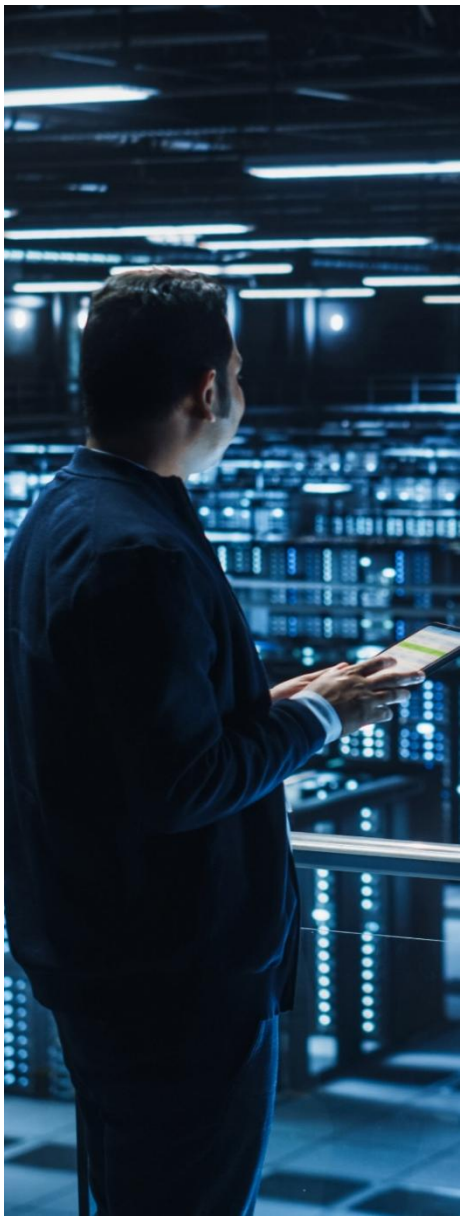
The better the question. The better the answer. The better the world works.

Shape the future with confidence

Reimagining cybersecurity — the cyber risk operations center in the age of artificial intelligence

From reactive defense to proactive, risk-driven enterprise enablement

Executive summary



Cybersecurity is entering a period of structural disruption.

For more than two decades, organizations have strengthened cybersecurity by adding tools, expanding teams and improving operational processes. These investments have improved visibility and response capabilities, yet many organizations continue to struggle with the same fundamental challenges: escalating threats, increasing costs and persistent difficulty aligning cybersecurity investment with business value.

At the same time, artificial intelligence (AI) is accelerating both attackers and defenders. Attack surfaces expand continuously, threat actors move faster than traditional response cycles and organizations are expected to make risk decisions at a pace that legacy cybersecurity models were never designed to support. Organizations are now operating in a **NAVI world — Nonlinear, Accelerated, Volatile and Interconnected (NAVI) —** where small changes can produce disproportionate impact, decision windows continue to compress, risk conditions shift rapidly and exposures propagate across ecosystems rather than remaining contained.

In this environment, leading organizations must move beyond understanding today's risk to anticipating tomorrow's exposure. Cybersecurity must increasingly provide forward-looking, predictive insight — highlighting emerging risk patterns, signaling where exposures are likely to materialize next and enabling action before impact occurs.

The issue is no longer a lack of technology or expertise. The issue is that the cybersecurity operating model itself has not evolved at the same pace as the environment it is meant to protect.

Cybersecurity must be reimagined, not incrementally improved.

This paper introduces the Cyber Risk Operations Center (C-ROC) as a next-generation cybersecurity operating model that places risk intelligence at the center of decision-making, aligns cybersecurity with business outcomes and leverages AI to orchestrate and increasingly execute responses — moving beyond accelerating activity to enabling decisive, risk-informed action.

Drawing on real-world implementation experience across regulated and less regulated industries, this paper explores:

- Why traditional cybersecurity operating models are breaking down
- How security operations are evolving into enterprise risk enablement
- The role of the C-ROC as a new foundation
- How AI reshapes the cyber workforce, threat landscape and attack surface
- What organizations must do now to prepare for autonomous, risk-driven cybersecurity

Section 1. The evolution of security operations

From fragmented defense to enterprise risk enablement

Cybersecurity did not evolve through deliberate design. It evolved through necessity.

Early security functions were fragmented and reactive, focused on protecting individual systems and responding to incidents after they occurred. As threats increased, organizations centralized monitoring and response through Security Operations Centers (SOCs), enabling scale and consistency.

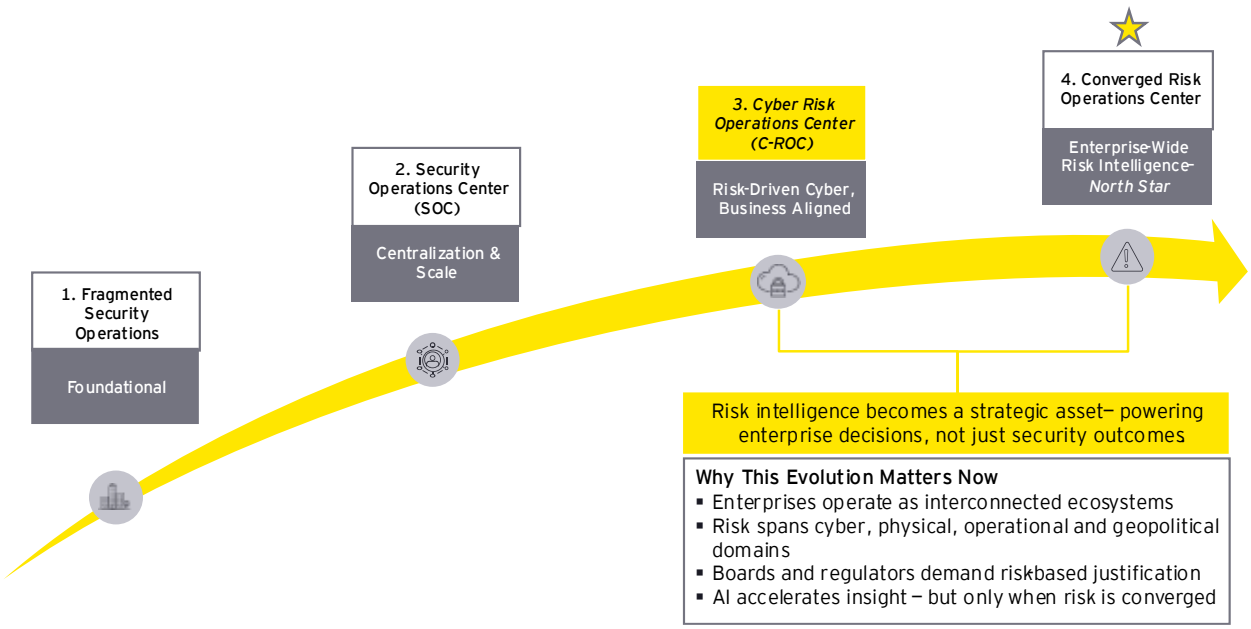
Over time, additional capabilities emerged:

- Threat intelligence integration
- Centralized tooling and analytics
- Governance, risk and compliance (GRC) programs
- Executive reporting and oversight

Each step improved operational maturity. Yet the underlying objective remained largely unchanged: improving security execution rather than driving action toward sustained, business-contextual risk reduction.

The Evolution of Security Operations to Enterprise Risk Enablement

From reactive defense to converged, business-driven risk intelligence



Today, cybersecurity is transitioning once again from operational defense toward enterprise risk enablement. Security operations must evolve beyond detecting and responding to threats and instead enable organizations to understand and manage risk continuously.

Section 2. Why cybersecurity must change now

Four converging forces are accelerating the need for change.

- *Speed asymmetry*

Recent advances (e.g., Mythos-class models) compress attack timelines from days/months to hours or minutes, pushing beyond traditional defensive, governance, and operating models. The mismatch between attacker speed and enterprise response has fundamentally altered the risk equation.

- *Economic pressure*

  Cybersecurity spending continues to grow, yet many organizations struggle to demonstrate measurable improvement in outcomes. CFOs increasingly demand clarity on whether investments are sufficient, appropriately allocated and aligned to business priorities.

- *AI acceleration*

  AI reduces the cost and complexity of attack development while increasing defensive complexity. Organizations must manage both external threats and internal risks introduced by rapid AI adoption. The current cybersecurity model was optimized for stability. The environment is now defined by acceleration.

- *Trust and confidence*

  Beyond speed, cost and AI acceleration, trust has emerged as a primary differentiator for customers, partners, regulators and investors. Cybersecurity failures erode confidence far beyond immediate financial impact, affecting brand equity, market valuation and long-term stakeholder trust. Conversely, organizations that demonstrate disciplined, risk-driven cybersecurity build confidence that they can operate reliably in a volatile, interconnected environment.

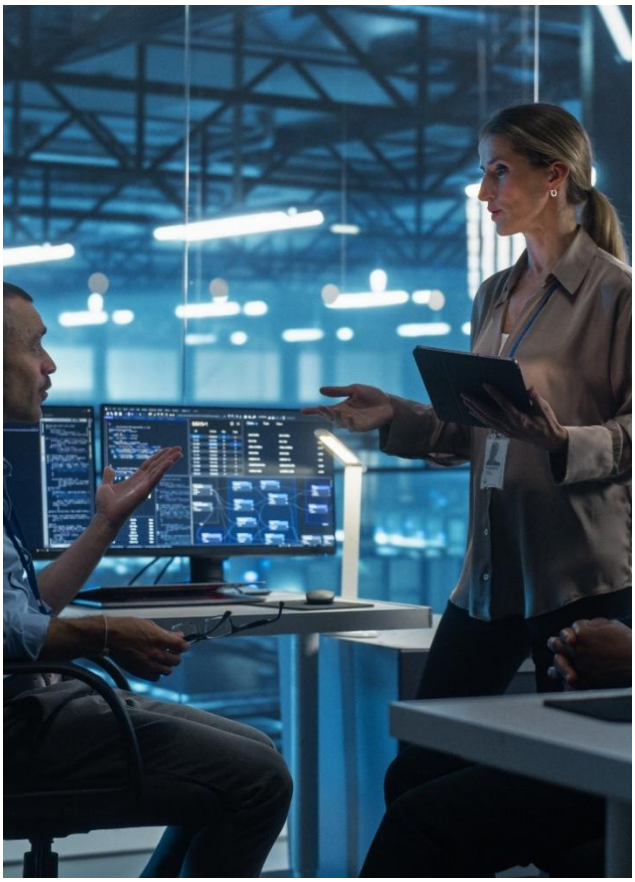
Getting cybersecurity "right" is no longer just about protection — it is about sustaining trust at enterprise scale.

Section 3. The structural limits of today's cybersecurity model

Despite advances in tooling, many cybersecurity organizations still operate using assumptions established decades ago.

Investment decisions are frequently justified through:	Operationally, security functions rely on:	This creates predictable results:
▪ Industry benchmarks ▪ Maturity models ▪ Percentage of IT or revenue spending ▪ Historical precedent	▪ Periodic risk assessments ▪ Static control evaluations ▪ Reactive prioritization of alerts and vulnerabilities	▪ Chief information security officers (CISOs) spend a disproportionate time defending budgets. ▪ Risk ownership remains concentrated within security. ▪ Cybersecurity is perceived primarily as a cost center. ▪ Business leaders lack decision-grade insight into cyber risk trade-offs.

The challenge is not execution — it is alignment. Cybersecurity produces technical insight but insufficient business intelligence for decision-making. Security teams can often explain vulnerabilities, threat actors and control gaps in detail, yet struggle to translate this information into clear implications for revenue, operations, regulatory exposure or strategic objectives. As a result, executives are asked to make risk decisions without a shared language, consistent framing or explicit trade-off analysis. Without alignment between technical risk signals and business outcomes, cybersecurity remains operationally effective but strategically constrained — limiting its ability to enable proper risk oversight and influence enterprise decisions at speed.



Section 4. The Cyber Risk Operations Center (C-ROC)

The C-ROC represents a shift from cybersecurity as an operational function to cybersecurity as a NAVI-native risk intelligence capability.

Designed for a NAVI world, the C-ROC enables organizations to sense, interpret and act on risk continuously — rather than relying on static plans or delayed reactions.

Rather than introducing another tool or reporting layer, the C-ROC integrates:

People	Clear decision rights and accountability	Technology	Integrated security and risk data
Process	Continuous risk-driven workflows	Data	Quantitative and qualitative risk intelligence

The outcome is not simply improved visibility but improved enterprise decision-making.

Core outputs of a mature C-ROC

A fully operational C-ROC enables:

1	**Business-aligned risk appetite and tolerance**	2	**Continuous first-party risk assessment**
	Shared understanding of acceptable risk across business and technology leadership		Automated assessment of exposure translated into business and financial terms
3	**Continuous third-party risk intelligence**	4	**Risk-aligned strategy and investment planning**
	Visibility into ecosystem risk across suppliers and partners		Investment decisions grounded in risk reduction, economic impact and business priorities
5	**Operational monitoring and prioritization**	6	**Persona-based risk reporting**
	Continuous identification and prioritization of exposures that materially affect business outcomes		Decision-ready insights tailored for executives, boards and operational leaders
7	**Continuous risk-driven action**		
	Increasingly AI-orchestrated and human-governed actions that reduce prioritized business risk		

C-ROC as an ecosystem orchestrator

Modern cybersecurity environments are not defined by a lack of tools but by fragmentation. Most organizations operate dozens of platforms across security operations, risk management, technology operations and the business — each producing signals, insights and actions within their own domain.

The C-ROC does not replace this ecosystem. Instead, it orchestrates it. The C-ROC integrates signals from across the cybersecurity, technology and business landscape and translates them into a unified, risk-oriented view that supports enterprise decision-making.

By connecting operational telemetry, threat intelligence, asset and exposure data, and business context, the C-ROC enables cyber and business leaders to see not just what is happening, but what matters, why it matters and what trade-offs are available.

This orchestration layer is what allows cybersecurity to move from fragmented execution to coordinated, risk-driven action, without requiring wholesale replacement of existing capabilities.

How the C-ROC operates in practice

The defining characteristic of a C-ROC is not reporting — it is workflow.

Traditional models separate functions:

- GRC assesses risk periodically.
- Vulnerability management prioritizes by severity.
- Security operations responds to alerts.
- Finance reviews investments annually.

In a C-ROC model, these activities are connected through a continuous loop:

Operational data feeds risk intelligence continuously. Risk thresholds guide prioritization. Security provides recommendations, and the business makes informed trade-offs. Actions are executed and measured against risk outcomes. Cybersecurity shifts from reactive execution to continuous decision enablement.

Section 5. From cost center to decision enablement

One of the most persistent challenges in cybersecurity is demonstrating value.

Executives consistently ask:

- Are we spending enough?
- Are we spending in the right places?
- What should we fund next?

Traditional answers rely on comparison rather than insight.

A C-ROC-enabled model reframes the conversation. Security no longer defends spending; it enables structured decisions:

- Is an investment regulatory or mandatory?
- Does it materially reduce risk?
- Over what time frame is value realized?
- What risk is accepted if investment is deferred?

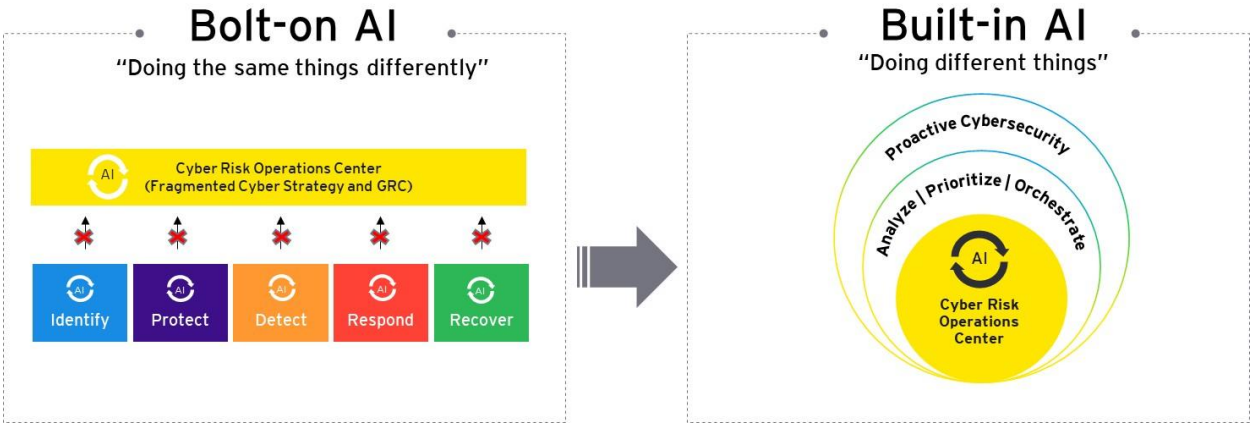
Security provides recommendations. The business makes informed decisions. Risk acceptance becomes explicit rather than implicit. This shift fundamentally changes how cybersecurity is perceived within the enterprise.

Section 6. Reimagining cybersecurity in the age of AI

AI does not just accelerate cybersecurity — it also amplifies the NAVI characteristics of the environment. AI increases nonlinearity in attack impact, accelerates both offense and defense, introduces volatility through rapid experimentation, and deepens interconnected risk across platforms, data and ecosystems.

What if we reimagined cybersecurity with AI at the core?

From value protection to value creation in cybersecurity



The limits of bolt-on AI: Many organizations apply AI to existing tools and workflows, improving efficiency and accelerating response. While valuable, this approach preserves legacy operating models and fragmented decision-making. AI increases speed but not necessarily effectiveness.

- *Built-in AI: redesigning cybersecurity itself*

A built-in AI approach recognizes that AI changes three fundamental dimensions of cybersecurity.

- *The cyber workforce*

Cybersecurity has historically scaled through people. The volume and velocity of modern threats make this approach unsustainable.

AI agents increasingly perform data aggregation, analysis, correlation and execution tasks. Human roles evolve toward oversight, interpretation and orchestration.

The future cyber workforce combines human judgment with autonomous execution, shifting from manual operation to risk-driven supervision.

- *The continuously evolving threat landscape*

AI accelerates attacker capability and reduces the cost of exploitation. Simultaneously, organizations introduce new internal risks through AI adoption, data exposure and rapid experimentation. Threat environments are continuous rather than episodic, requiring continuous sensing and prioritization.

- *The expanding attack surface*

Modern enterprises operate within interconnected digital ecosystems. Cloud services, APIs, third-party integrations and AI-enabled platforms continuously expand exposure beyond traditional organizational boundaries. Security must shift from protecting assets to managing exposure dynamically based on business impact.

- *AI as execution, risk intelligence as direction*

In a C-ROC model, AI operates within defined risk thresholds and governance boundaries. Risk intelligence provides direction; AI executes action. Automation increases consistency and speed while preserving human accountability and decision authority.

This alignment enables cybersecurity to move toward proactive, autonomous operation without sacrificing oversight or control.

Section 7. The north star: autonomous, risk-driven cybersecurity risk management

The objective of modern cybersecurity is not eliminating risk but managing it continuously and transparently at enterprise speed.

A mature C-ROC enables:

- Continuous risk sensing and prioritization
- Risk-aligned orchestration of remediation and response
- Faster escalation and disclosure decisions
- Resilience through informed trade-offs

This future is emerging today, but it requires intentional redesign rather than incremental improvement.

Conclusion: reimagining cybersecurity

If cybersecurity were designed today — in a world defined by AI, interconnected systems and continuous risk — it would not resemble the operating models most organizations are currently using.

Cybersecurity must evolve from reactive defense to enterprise risk enablement.

The C-ROC represents an opportunity to align cybersecurity with business decision-making, enable intelligent automation and prepare organizations for a future where speed, intelligence and adaptability define resilience.

In a world that is NAVI, incremental adaptation is no longer sufficient. Organizations must intentionally design cybersecurity operating models that are resilient to uncertainty, capable of rapid recalibration and aligned business decision-making at speed.

Organizations that act early will not only reduce risk more effectively but also gain the clarity and speed required to compete in an increasingly uncertain environment.

The views expressed by the authors are not necessarily those of Ernst & Young LLP or other members of the global EY organization.

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, multi-disciplinary 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.

US SCORE no. 30291-261US
2603-11492-CS
ED None

ey.com