EXTRAHOP

A CISO's Guide to Aligning with the CIO

Actionable Strategies and Steps for Building a High-Performing, Unified Command

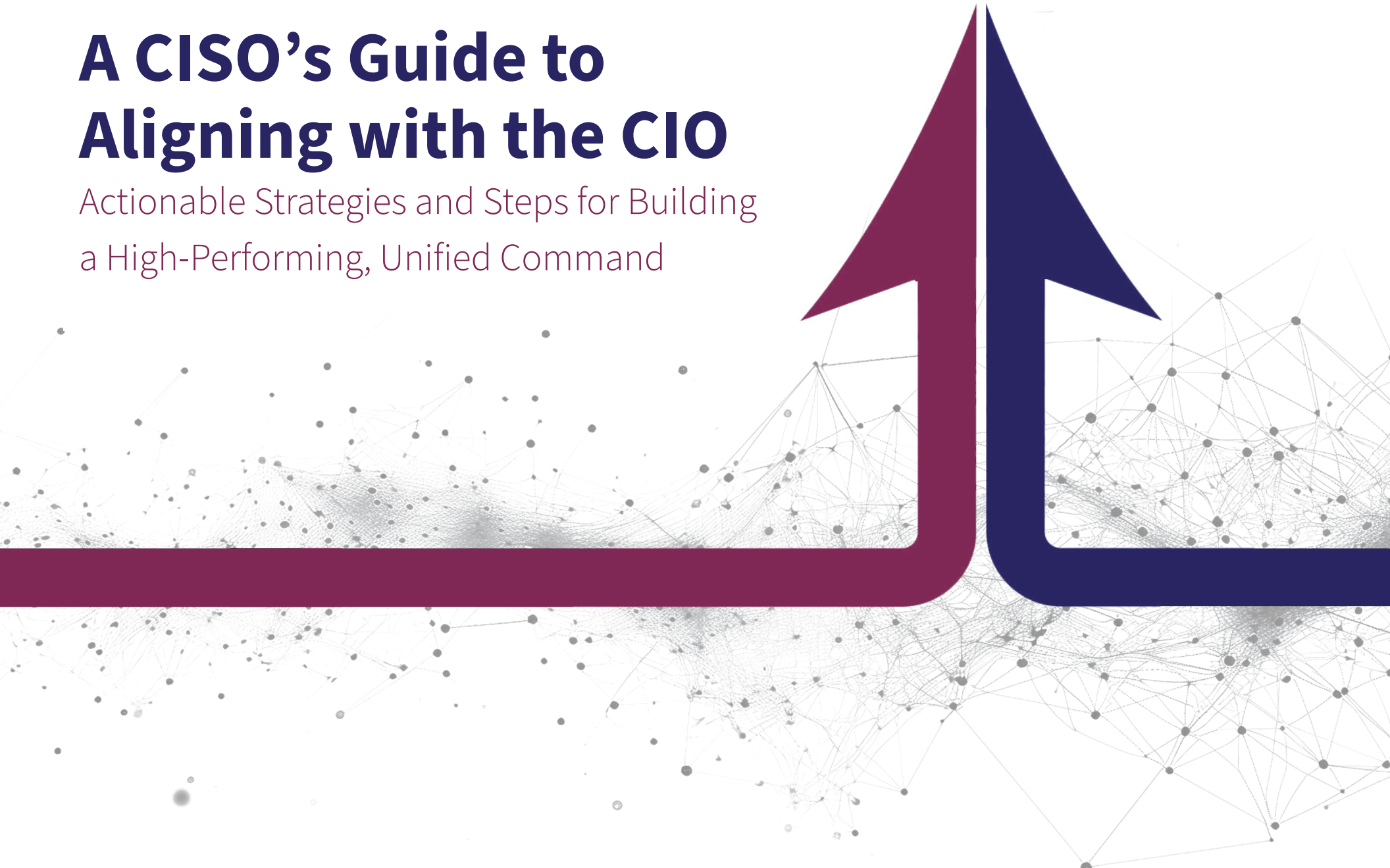


Table of Contents

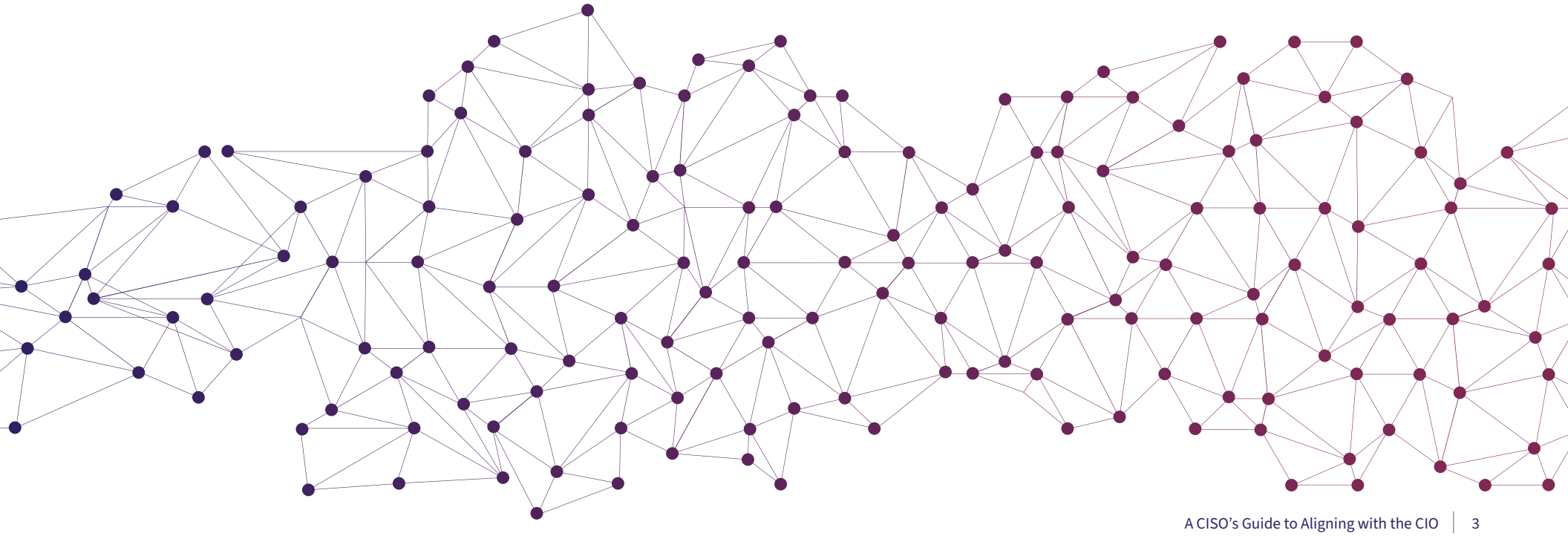
The Imperative for CISO-CIO Collaboration

To successfully execute any digital transformation initiative – whether it's a cloud migration or agentic artificial intelligence (AI) deployment – both the CISO and the CIO must share joint ownership and accountability, working collaboratively to embed resilience and trust into every phase of the project.

A strong CISO-CIO partnership enables faster, more secure digital transformations, elevates risk management, and directly fuels business success. To realize this strategic advantage, these roles should not be viewed as two distinctly different functions, but as unified partners.

Consider the adoption of agentic AI. While AI promises accelerated business operations and innovation, it also introduces unique risks that neither IT nor security can manage alone. The recent incident in which **Chinese state-sponsored actors leveraged Anthropic's AI coding tool to attack 30+ global organizations** provides a current, high-stakes case for unified CISO-CIO defense.

The reality is that during every new system deployment, infrastructure change, and innovation initiative, both the CISO and CIO must engage, integrating security and infrastructure to ensure that technology projects deliver mission-centered and secure business outcomes.



The Blurring of Security and Technology Functions

Security and technology roles have become inseparable, creating overlapping responsibilities that demand tighter alignment. Unmanaged differences in executive focus – like the CIO optimizing for speed versus the CISO optimizing for security – can create significant organizational misalignment and friction.

This tension is becoming even more pronounced as emerging technologies reshape the enterprise operating model. As more organizations begin to implement agentic AI throughout the business, the CIO's deployment and automation strategy must be jointly executed with the CISO to address security risks (e.g., sensitive data access) and compliance gaps in tandem.

A collaborative approach ensures organizations capture the benefits of agentic AI, embedding security and compliance from the get-go, and supporting innovation without reducing the speed of progress. Historically, security has often been perceived as an impediment to progress, but aligning CISO and CIO priorities transforms security into an accelerator.

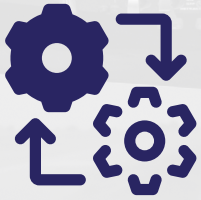
Divided ownership, however, can complicate this alignment. When critical functions are shared, new operational silos emerge. With business continuity and disaster recovery, for example, shifting to the CISO while the CIO retains control of relevant infrastructure and budget, many organizations have experienced severe friction. In the event of a **ransomware attack**, a multi-day budget approval delay could drastically increase recovery costs.

Driving the Business Forward: When Security and Infrastructure Leadership Align

Proactive CISO-CIO alignment unlocks advantages that compound over time, directly elevating business performance and giving your organization a powerful, competitive edge.

FASTER, MORE SECURE INNOVATION

CISO-CIO alignment moves organizations past costly, reactive security patching and remediation, reducing the surface area for risk and improving time-to-market for new business capabilities.



OPTIMIZED RESOURCE ALLOCATION

CISO and CIO alignment drives greater budgetary accountability. In turn, this facilitates the implementation of high-impact tooling and the elimination of redundant solutions, maximizing the return on investment (ROI) across the entire technology and security infrastructure.

UNIFIED RISK MANAGEMENT AND RESILIENCE

A shared strategy eliminates internal friction, enabling the organization to execute a swift, optimized response that minimizes downtime and the financial impact of incidents.

From Separate Functions to Unified Command: 3 Ways to Transform the CISO-CIO Partnership

Fast, secure growth demands a fundamental shift in how your organization manages technology risk. This shift requires abandoning outdated organizational boundaries. The CISO and CIO can no longer operate as separate functions that only occasionally intersect.

Instead, security and infrastructure leaders must present a united front, moving from reactive defense to proactive enablement. Achieving this requires three fundamental changes to how CISOs and CIOs operate.

1 Implement Shared Oversight for Infrastructure Decisions

Ensure that the CISO and the CIO each have a seat at the table when technology decisions are made. Mandating mutual input establishes accountability early in the lifecycle. It also prevents misalignment, costly reworking, and audit issues that result in friction and stagnation.

The necessity of this approach is amplified as organizations deploy agentic AI. In these instances, the CIO must decide which processes to automate, ensure that infrastructure can scale reliably, and define performance metrics while simultaneously addressing integration with existing systems, workflow efficiency, and potential operational bottlenecks.

At the same time, the CISO must evaluate data access, privacy, and compliance requirements, identify security gaps, and define guardrails and monitoring protocols. When the CISO and CIO make decisions together, they can successfully navigate technical and security trade-offs, establish unified controls, and agree on operational protocols, ensuring that agents deliver business value both safely and effectively.

When both leaders access the same insights, troubleshooting shifts from “what happened” to “what do we do next.” ExtraHop acts as the connective tissue between functions, offering a unified view of the environment so both leaders can move in lockstep.

This shared visibility becomes critical as organizations deploy agents that operate autonomously across systems, enabling leaders to quickly identify unexpected agent behavior, detect employees deploying unapproved or “shadow” agents, verify adherence to company policies, and coordinate responses before minor issues escalate into operational disruptions.

2 Establish Structured Collaboration Routines

Shared oversight is only effective if it’s reinforced. Beyond aligning on individual decisions, CIOs and CISOs need predictable forums to maintain trust and through which to surface issues before they become blockers.

Regular touchpoints, such as weekly check-ins to track emerging priorities, monthly strategic planning sessions, and quarterly strategy reviews create a cadence that keeps both functions synchronized.

These structured routines help ensure that collaboration extends beyond isolated projects, building accountability and transparency, and leading to cascading net-positive effects across the organization’s broader operating model.

3 Create a Single Source of Truth

Unified dashboards and common metrics eliminate the finger-pointing dynamic that can emerge when leaders operate from disparate data sources. A shared, fact-based foundation must offer complete visibility into network transactions and dependencies. A unified view is particularly critical during incidents, when speed, alignment, and coordination determine outcomes.

Executive Alignment Will Power the Next Wave of High-Performance

The future of secure, high-speed innovation isn't determined by technology alone. Rather, it's defined by the internal synergy created when the CISO and CIO operate together — speaking with one voice. Collaborative alignment between these two roles generates immediate, measurable value that extends far beyond the security function.

Integrated leadership is not only a reliable predictor of sustained risk maturity, but of organizational agility. How organizations structure the CISO-CIO relationship today will determine the business's ability to compete tomorrow.

Real-world results: See how **Ulta Beauty** achieves unified visibility across its digital transformation projects with ExtraHop.

About ExtraHop

ExtraHop empowers enterprises to stay ahead of evolving threats with the most comprehensive approach to network detection and response (NDR).

Since 2007, the company has helped organizations across the globe extract real-time insights from their hybrid networks with the most in-depth network telemetry. ExtraHop uniquely combines NDR, network performance monitoring (NPM), intrusion detection (IDS), and packet forensics in a single, integrated console for complete network visibility and unparalleled context that supports data-driven security decisions. With a powerful all-in-one sensor and cloud-scale machine learning, the ExtraHop RevealX™ platform enhances SOC productivity, reduces overhead, and elevates security postures.

Unlock the full power of network detection and response with ExtraHop.
To learn more, visit **extrahop.com** or follow us on LinkedIn.

EXTRAHOP