EXTRAHOP®

A CISO's Guide to Aligning with the General Counsel

Actionable strategies and steps to build a unified front against risk

Table of Contents

A Modern Take on an Effective Security Posture

CISOs: How closely aligned are you with your General Counsel?

The partnership between the Chief Information Security Officer (CISO) and the General Counsel is critical. While this truth has been discussed for years, today's dynamic and complex risk landscape has brought a new level of urgency to the concept.

Consider the massive SolarWinds supply chain attack that impacted tens of thousands of companies around the globe in 2020. In late 2023, the U.S. Securities and Exchange Commission (SEC) sent an unmistakable message by charging both SolarWinds and its CISO with securities fraud, citing misleading public statements and weak disclosure controls that put customers, operational integrity, and the company's reputation at risk, delayed proper remediation, and misrepresented the true severity of the security vulnerability.

SolarWinds raised the stakes for CISOs in more ways than one, but perhaps what stands out most is the ever-growing need for an emphasis on the CISO and General Counsel partnership. Had a stronger relationship been in place, one that aligned on a disciplined process for risk assessment and public disclosure, both sides could have established a legal and technical defense that might have preempted or significantly mitigated the SEC's charges.

When your relationship with the General Counsel is strong, your organization is better positioned to clearly define risk, respond to incidents with operational and legal alignment, and communicate effectively with regulators in a way that stands up to scrutiny. In the SolarWinds case, the absence of those collaborative frameworks not only played a role in the breach, but also in the severity of the fallout.

From Separation to Synergy

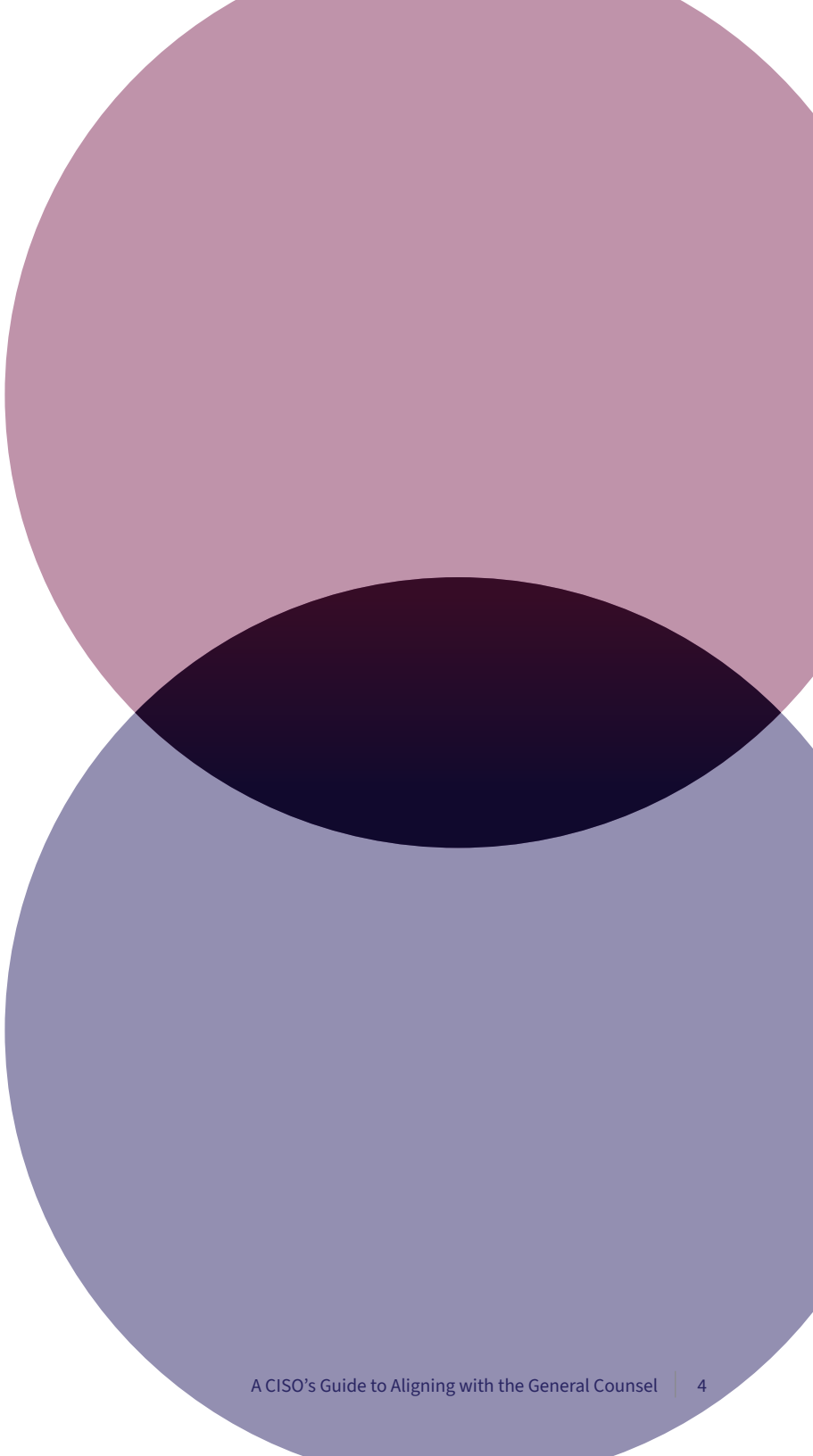
Historically, the roles of the CISO and the General Counsel were seen as separate and distinct, often operating in isolation from one another. Cybersecurity was viewed as a purely technical issue and legal teams were focused on business law. However, recent security incidents prove that this approach only exacerbates risk.

Without alignment around objectives and responsibilities, organizations struggle to achieve effective responses. When a breach occurs, teams that aren't aligned may pursue conflicting priorities: Cybersecurity may focus on rapid containment, while legal prioritizes evidence preservation.

Without a shared understanding of goals, clearly defined roles, and agreed-upon processes for both immediate response and future remediation, this misalignment can lead to inefficiencies and increase the risk of costly mistakes.

GDPR violations represent a prime, highly visible example of what happens when security and legal teams fail to find alignment. As of the publication of this report, GDPR fines can be levied in amounts up to €20 million or 4% of global turnover (whichever is greater).

This regulatory evolution merges technical and legal responsibilities into a single compliance imperative. Incident response plans must now account for legal disclosure timelines, and security metrics need legal review for accuracy in regulatory reports. Without a strong partnership with the General Counsel, your organization risks turning what should be manageable security events into potentially costly violations and penalties that make headlines.



The Benefits of an Effective CISO–General Counsel Partnership

Your partnership with the General Counsel is not just about resolving threats; it's about building a proactive defense that protects the entire organization. This alliance safeguards everything from the company's reputation to its financial health, transforming risk management from a reactive scramble to a focused, process-driven, and outcome-oriented exercise.

UNIFIED RISK MANAGEMENT

Unified, strategic alignment creates defensible security postures that demonstrate due diligence to regulators and stakeholders. Should a security breach occur, the organization will be able to prove that it took every reasonable measure to prevent, detect, and quickly respond, making it clear that the business operates with security principles in mind.

STRONG INCIDENT RESPONSE

In the heat of a security incident, every second counts. A strong partnership with your General Counsel prevents day-of anxiety, infighting, and fumbles that can derail the response before it even gets off the ground. In one incident, a company's IT team, rushing to get systems back online after a breach, unknowingly destroyed critical evidence by reformatting the affected hard drives. This hasty decision, made without legal guidance, created a serious legal problem when regulators later arrived to collect the evidence.

As a CISO, you know that recovery isn't only about technically recovering your computer systems; it's about recovering as a business entity, which means fulfilling legal duties and protecting operational integrity. A close, working CISO-General Counsel partnership is the best means of ensuring that your company emerges from a breach with its reputation and legal standing undiminished.

SHARED ACCOUNTABILITY

Building this partnership also helps ensure that new initiatives commence in a responsible, legally defensible way. When your team brings a pending project to the General Counsel for review, the General Counsel can provide legal guidance around potential liability. This way, both teams fully understand the technical and business risks before the project goes live. Shared accountability allows for early-stage risk management and mitigation, protecting the company while moving business forward securely and responsibly.

CISO PROTECTION

A close partnership with your General Counsel can directly protect your career and personal liability. In the blink of an eye, you can go from being an attack victim to the subject of a lawsuit, fending off accusations of negligence or a breach of fiduciary duty from regulators and shareholders.

This partnership can help you build a legally defensible security posture that proves due diligence and safeguards your reputation and career, while also helping you review and claim coverage through Directors and Officers (D&O) insurance or other liability policies, mitigating personal financial ruin.

7 Ways to Build a Strong CISO–General Counsel Partnership

Regardless of where you are in your career, whether you're a brand-new CISO or a seasoned pro, there are simple steps that you can take today to bridge the divide between legal and security, transforming what could be a liability into a source of business resilience.

1 **Outline goals and key milestones from the get-go.**

Schedule a 90-minute working session with your General Counsel to determine "what are our most valuable assets or crown jewels, the ones for which we would legally be in dire straits, in the event of a breach?" and "what is a defensible posture?" Create a shared document that ranks assets by both business value and legal risk, and then align your security controls and budget allocation accordingly. This ensures that your security program protects what matters most.

2 **Schedule quarterly security-legal check-ins.**

Schedule quarterly meetings between CISO and General Counsel teams to review emerging threats, regulatory changes, and business initiatives that could impact security risk. Document decisions, action items, and risk assessments from each session to build a record that helps teams stay aligned.

Pro Tip: Start Early

Establish a trust-based relationship and effective communication protocols with your counterpart early on. This proactive approach can make incidents far less stressful, increase response efficiency, and help manage high-stakes situations more effectively, ensuring a seamless, coordinated effort when it counts.

3 **Implement cross-functional training programs.**

Establish regular education sessions where security teams learn about the legal implications of technical decisions and where legal teams gain understanding of cybersecurity constraints and capabilities.

Leverage real case studies from your industry to walk through incidents step-by-step, analyzing how technical decisions impacted legal outcomes and how legal constraints shaped security responses, creating practical knowledge that teams can apply to their work immediately.

4 **Conduct tabletop exercises with the whole team.**

Run simulations that include both security and legal teams to build working relationships, establish clear roles, and streamline communication protocols before incidents occur.

Track how long it takes your teams to make decisions during exercises, using the data to identify bottlenecks and to improve response efficiency. After each exercise, capture the decision-making criteria that each team used in a shared document, and codify this into repeatable processes that preserve institutional knowledge across personnel changes.

5 Work together to identify and mitigate potential third-party risks.

Collaborate on security requirements for vendors and develop security contract language/clauses that address both technical security requirements and liability allocation, ensuring contract consistency and reducing risk.

Beyond initial contract signing, establish ongoing monitoring protocols. Create processes for regular security reviews, especially for critical suppliers, with legal team review of any material changes to vendor security posture or contract terms.

6 Create joint incident response protocols.

Develop comprehensive procedures defining when, in the event of a breach, the legal counsel should engage, evidence preservation requirements, and coordination between containment and investigation.

In this process, you may want to pre-agree upon and pre-position specialized legal counsel or any other outside specialty service groups that may be needed in the event of a breach, so that they can be activated within hours of an incident—rather than rushing to find qualified help after the fact.

7 Build a unified means of managing regulator relationships.

Find a way to coordinate interactions with regulators and auditors to present a cohesive organizational voice that demonstrates comprehensive risk management maturity, strengthening regulator confidence.

Establish feedback loops that capture regulator recommendations, concerns, and observations—from both security and compliance perspectives—then transform this input into improvements across both domains, while documenting how the changes led to organizational enhancements that demonstrate continuous risk management maturity.

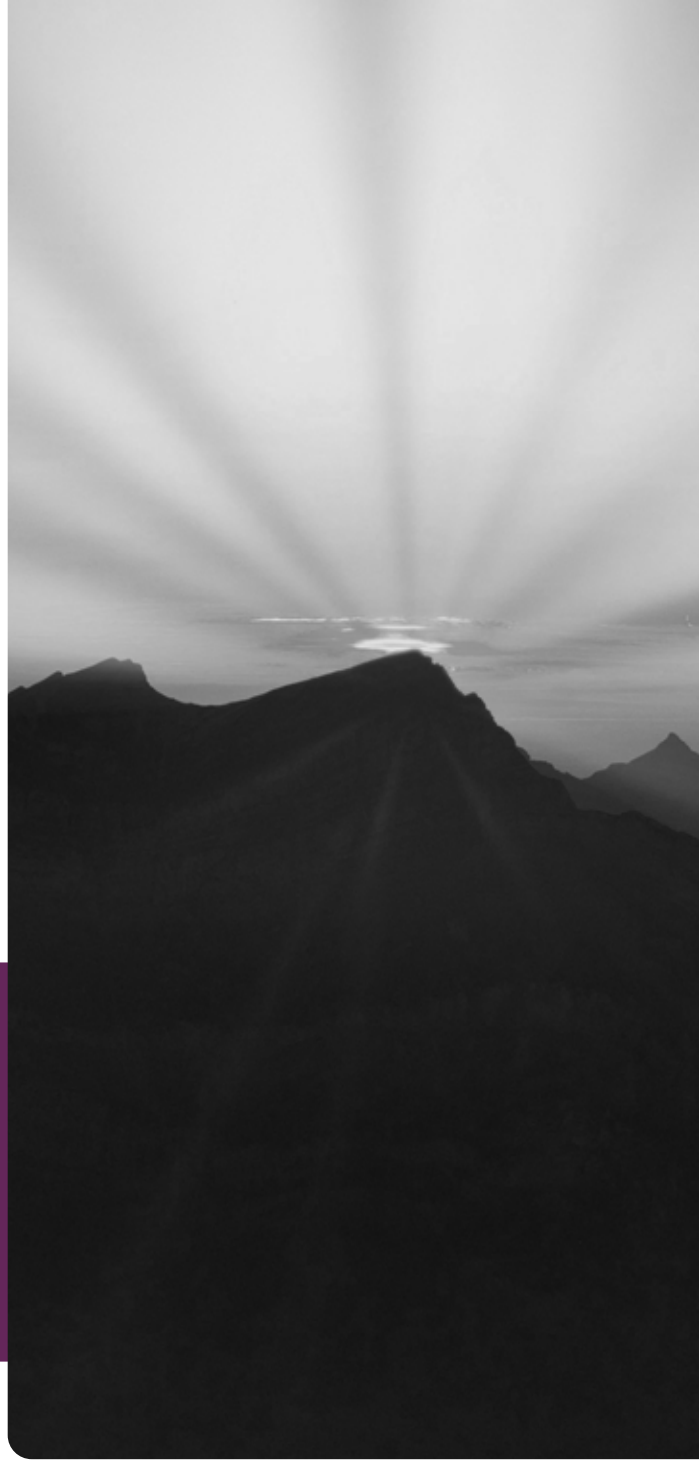
Creating Common Ground Through Shared Visibility

The seven strategies outlined in the previous section—from quarterly check-ins to managing regulator relationships—all focus on the goal of building trust and aligning processes before a breach occurs.

However, even carefully laid out plans and the strongest of personal rapport can crumble during an active security incident.

The most resilient CISO–General Counsel partnerships are often supported by unified visibility, with shared access to the same information. When you both can see the same insights in real-time—the timeline of events, affected systems, and the scope of exposure—you avoid conflicting interpretations of what happened.

The future of enterprise security is not defined by technology. It's defined by the internal synergy created when the CISO and General Counsel speak with one voice. Your strategic alignment with the General Counsel demonstrates risk maturity that stakeholders recognize as a competitive advantage.



Access to consistent, high-quality information is a non-negotiable in creating legally defensible security decisions, ensuring aligned, compliant disclosure, protection of your own career, and business resilience.

ExtraHop delivers comprehensive network visibility and contextual insights that drive more effective outcomes with the ExtraHop RevealX™ network detection and response (NDR) platform. **Learn more today**.

About ExtraHop

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

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 management, intrusion detection, and 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®