RTB Technologies | CyberCOP Program

Compliance, Oversight & Prevention

How much would you benefit by having a Cyber COP?

Cybersecurity Built to Stand Up to Scrutiny

CyberCOP helps firms establish defensible cybersecurity programs that hold up under legal, insurance, and client review.

Law, accounting, financial, and advisory firms are trusted with sensitive data. When a cyber incident occurs, the impact extends far beyond technical recovery.

Breaches are increasingly followed by lawsuits, insurance disputes, and detailed examination of leadership decisions.

CyberCOP exists to help firms move beyond basic compliance and build cybersecurity programs that are defensible, provable, and ready to withstand scrutiny.

Cyber Risk Is a Legal Exposure

Data breach litigation continues to increase. Class action lawsuits are filed more frequently, **pursued more aggressively**, and focused less on whether a breach occurred and more on whether **leadership exercised reasonable care** beforehand.

After an incident, the critical question is not what tools were used. It is whether the firm can demonstrate reasonable, **ongoing cybersecurity governance** with clear **evidence**.

Plaintiff attorneys routinely examine:

- Gaps between written policies and execution
- Lack of documented oversight & accountability
- Absence of independent risk evaluation
- Reactive decisions made after an incident

Cybersecurity is now judged in courtrooms, not just server rooms

CyberCOP is an integrated framework designed to reduce legal exposure and support defensibility before and after a cyber incident.

- **Compliance:** Aligns controls and documentation with insurance policy review, regulatory, contractual requirements, producing evidence that can be reviewed and relied upon.
- **Oversight:** Establishes continuous governance that demonstrates leadership accountability and reasonable care, which is critical during litigation and discovery.
- **Prevention:** Continuously identifies and reduces risk through recurring assessments and control validation, lowering both breach likelihood and downstream legal exposure.

CyberCOP is delivered through RTB's Fractional Chief Security Officer program. Each layer builds on the previous one and is a required part of maintaining a defensible cybersecurity posture.

CyberWatch (Level 1): Independent recurring risk assessments that establish & validate the firm's security baseline

Cyber Liability Guard (Level 2): Hands-on support to implement controls and maintain inspection-ready evidence

Fractional CSO (Level 3): Executive-level leadership that aligns cybersecurity with business risk and enforces accountability.

Together, these layers for a single governance program designed to withstand scrutiny.

Leonard Atlas, Strategic Sales Partner - Mission Profitable, Inc.

atlas@missionprofitable.com

310.684.3839

Learn more: www.rtbtechnologies.com/mpi

CyberCOP Investment Overview

Executive Cybersecurity as a Governance Program

The appearance of U.S. Department of Defense visual information does not imply or constitute DOD endorsement.

CyberCOP is delivered through RTB's Fractional Chief Security Officer program. It is not a menu of services. It is a single, integrated program designed to establish defensible cybersecurity governance over time.

Investment varies based on organizational size, complexity, and exposure. All engagements include CyberWatch, Cyber Liability Guard, and Fractional CSO leadership as progressive layers of the CyberCOP shield.

How CyberCOP Is Scoped

Every engagement begins with a Cyber Hygiene X-Ray, an initial assessment that evaluates:

- Data sensitivity & client risk
- Regulatory & insurance requirements
- Operational & technical complexity
- Current security maturity & evidence gaps

This allows CyberCOP to be tailored to real risk, not assumptions, while preserving full program integrity.

Our Credibility Is Battle-Tested

Military Precision.
Global Cyber Intelligence.
Private Sector Impact.

Led Buckley AFB to top 2 of 46 global sites in DoD Cyber Readiness

Former NSA and Intelligence Community cybersecurity experts

Extensive experience with private companies navigating complex cyber threats

CyberCOP Investment Ranges

The ranges below reflect typical annual investments based on organizational size and complexity

Small Organizations

$1,600 - $4,300 monthly

Typically fewer users, limited regulatory pressure, and simpler environments. Focus is on establishing baseline governance, documented controls, and defensible oversight.

Medium Organizations

$4,600 - $7,250 monthly

Growing complexity, increased third-party access, and rising insurance and client scrutiny. Emphasis shifts to recurring validation, stronger evidence management, and executive accountability.

Large Organizations

$7,150 - $12K monthly

Multiple sites, advanced infrastructure, regulatory obligations, and higher litigation exposure. Requires deeper oversight, formal reporting, and ongoing leadership involvement.

Enterprise Organizations

$11K - $18K+ monthly

High complexity, board involvement, and significant legal and reputational exposure. CyberCOP operates as an extension of executive leadership with continuous governance and defensibility focus.

Book your free, confidential consultation: www.rtbtechnologies.com/mpi