TRNSFRM

Cybersecurity. Compliance. Managed IT.

WHITE PAPER

The ROI of a vCISO

Why fractional security leadership outperforms full-time hires and basic managed services for the modern SMB.

Audience	SMB & mid-market executives, IT directors, CFOs
Purpose	Quantify the cost, coverage, and risk-adjusted ROI of a vCISO
Format	Comparison-driven white paper

WHITE PAPER · 2026 EDITION

trnsfrm.tech · Cleveland · Columbus, OH

Executive summary

Small and mid-sized businesses are inheriting enterprise-grade threats — ransomware, supply-chain attacks, regulator scrutiny under FTC Safeguards, HIPAA, CMMC, and cyber-insurance underwriting questionnaires that read like a CISO interview. Yet the median SMB cannot justify the $250K–$400K all-in cost of a full-time CISO, and a managed service alone cannot sign off on risk acceptance, board reporting, or regulator attestations.

The fractional, or virtual, CISO (vCISO) model closes that gap. This paper quantifies the comparison across three lenses: **cost**, **coverage**, and **risk-adjusted ROI**.

> **Three numbers to remember**
>
> **70–85%** lower annual cost vs. a full-time CISO hire
>
> **3–5x** faster path to insurance- and audit-ready posture
>
> **$1.6M+** average SMB breach cost avoided per material incident (IBM, 2024)

Why this question matters now

Three simultaneous pressures have made security leadership a board-level requirement for SMBs:

- **Regulatory:** FTC Safeguards, CMMC 2.0, HIPAA Security Rule updates, state privacy laws, and SEC disclosure rules now expect a named, qualified individual accountable for the program.
- **Insurance:** Cyber-insurance renewal questionnaires demand documented governance, MFA enforcement, IR plans, and tabletop exercises — typically owned by a CISO-level role.
- **Customer & supply chain:** Enterprise customers are flowing down vendor-risk questionnaires (SIG, CAIQ, CIS RAM) that assume a security program owner exists.

The three options on the table

When the board asks *“who owns security?”*, an SMB realistically has three answers. Each makes a different tradeoff between cost, coverage, and accountability.

Option A — Hire a full-time CISO

A senior security executive on payroll. Maximum focus and availability, but the cost (salary, equity, benefits, recruiting, ramp) is structurally misaligned with most SMB P&Ls.; Many SMBs also struggle to attract — and retain — a CISO who has run an enterprise program.

Option B — Lean on the MSP / MSSP alone

Outsource monitoring, patching, and response to a managed service. Strong on operational hygiene; weak on governance, risk acceptance, regulator dialogue, board reporting, and policy authorship. The MSP is a *doer*, not an *owner*.

Option C — Engage a fractional vCISO

A senior security leader retained on a fractional basis (typically 4–20 hours/week), accountable for strategy, governance, compliance, vendor risk, board reporting, and incident leadership — paired with the MSP/MSSP that executes the day-to-day.

Side-by-side comparison

Annualized figures based on US-market benchmarks (BLS, Robert Half, IANS Research) and TRNSFRM client engagements. Treat as planning-grade ranges, not quotes.

Dimension	Full-time CISO	MSP / MSSP only	Fractional vCISO
Typical annual cost	$250K – $400K+	$36K – $120K	$45K – $120K
Time to value	3–6 months ramp	Immediate (ops only)	30–60 days
Strategic ownership	Yes	No	Yes
Compliance attestation	Yes	Limited	Yes
Board / executive reporting	Yes	No	Yes
24/7 monitoring & response	Builds team	Yes	Via partner MSP
Vendor & supply-chain risk	Yes	Rare	Yes
Cyber-insurance support	Yes	Partial	Yes
Bench depth (specialists)	1 person	Tier-based	Team behind the seat

Dimension	Full-time CISO	MSP / MSSP only	Fractional vCISO
Hiring & retention risk	High	Low	Low
Best fit	$500M+ revenue, regulated	Stable ops, no audit pressure	$5M–$500M, audit / insurance / growth

The cost math, in detail

Buyers consistently underestimate the true loaded cost of a full-time CISO. Below is a planning-grade build for a mid-market hire in a US metro.

Cost component	Low	High	Notes
Base salary	$215,000	$310,000	BLS / Robert Half 2025 ranges, mid-market
Annual bonus (15–25%)	$32,250	$77,500	Performance-based
Equity / LTI (amortized)	$15,000	$50,000	If applicable
Benefits & payroll tax (~28%)	$73,150	$108,500	Health, 401k match, FICA, etc.
Recruiting (20% of base)	$43,000	$62,000	Amortized year 1
Tools, training, conferences	$10,000	$25,000	Per-seat tooling, certs
Total year 1, all-in	**$388,400**	**$633,000**	

Compare to a fractional vCISO engagement

TRNSFRM vCISO engagements typically run **$3,750–$10,000 / month** ($45K–$120K annually) for 4–20 hours/week of senior leadership time, policy and program artifacts, board reporting, vendor risk reviews, and incident leadership. That is **70–85% lower** than a full-time hire, with no recruiting risk, no bench gap, and no ramp.

Coverage: what each option actually *delivers*

Capability	Full-time CISO	MSP only	vCISO + MSP
Written security program & policies	✓	Templates	✓
Risk register & risk acceptance	✓	—	✓
Compliance roadmap (HIPAA / FTC / CMMC)	✓	Partial	✓
Vendor & third-party risk reviews	✓	—	✓
Tabletop exercises & IR leadership	✓	Runbooks only	✓
Cyber-insurance application support	✓	Partial	✓
Quarterly board / executive reporting	✓	—	✓
24/7 SOC, EDR, patching, backups	Builds team	✓	✓ (via partner)
Identity & access engineering	Builds team	✓	✓

The risk-adjusted ROI model

ROI for security leadership is best modeled as *risk avoided* × *probability reduction*, less the program cost. Using IBM's 2024 *Cost of a Data Breach* benchmark for SMBs (~$3.31M average; ~$1.6M for organizations under 500 employees) and conservative probability reductions, the payback is typically inside year one.

Worked example — 200-employee professional-services firm

Variable	Value
Estimated breach cost (IBM SMB benchmark)	$1,600,000
Annualized probability of material incident (baseline)	18%
Annualized loss expectancy (baseline)	$288,000
Probability reduction from mature program (Ponemon)	–40%
Annualized loss expectancy (with vCISO program)	$172,800
Annualized risk avoided	$115,200
vCISO program cost	$78,000
Net annualized benefit	**$37,200**
Insurance premium reduction (typical)	10–25%
Audit / questionnaire labor savings	120–240 hrs/yr

Interpretation: the program pays for itself on pure risk avoidance, before counting insurance savings, won deals from completed security questionnaires, or the avoided cost of a failed audit. Most engagements break even inside 9 months.

When to choose which model

Choose…	If you…
Full-time CISO	Are >$500M revenue, in a heavily regulated sector (financial, healthcare, defense prime), and can
MSP / MSSP only	Have stable operations, no near-term audit, no enterprise customers issuing security questionnaire
Fractional vCISO	Are $5M–$500M revenue, face cyber-insurance renewal, an audit (HIPAA / FTC / CMMC / SOC 2)

How TRNSFRM delivers vCISO

Our vCISO engagements are built on the **IT Resilience Framework™** — a three-phase operating model that gets a program from *unknown* to *audit-ready* in 90 days and keeps it there.

01 **Assess.** Inventory assets and data, score current controls against the relevant framework (HIPAA, FTC Safeguards, CMMC, NIST CSF), baseline risk, and produce an executive risk register.

02 **Build.** Author policies, harden identity and access, deploy logging and EDR through the partner MSP, run a tabletop exercise, and stand up the cyber-insurance and vendor-risk artifacts.

03 **Transform.** Move from project to program: continuous monitoring, quarterly board reporting, annual control testing, third-party risk reviews, and regulator-ready evidence on demand.

What's included every month

- Named senior vCISO + access to specialist bench (engineering, GRC, IR)
- Quarterly executive / board report with KPIs and risk trend
- Annual risk assessment and policy refresh
- Vendor & third-party risk reviews on request
- Cyber-insurance application & renewal support
- Incident leadership and tabletop exercises
- Direct line to the MSP/MSSP partner running 24/7 operations

Decision checklist

If you can answer **yes** to two or more, a vCISO is the highest-ROI move on the table:

■ Have you been asked for a SOC 2, HIPAA, FTC Safeguards, or CMMC attestation in the last 12 months?

■ Has a customer sent you a security questionnaire (SIG, CAIQ, vendor risk) in the last 6 months?

■ Did your last cyber-insurance renewal include MFA, EDR, IR plan, or training questions you weren't sure how to answer?

■ Has your board or owner asked who owns cyber risk — and the answer was unclear?

■ Have you suffered a security incident, near-miss, or business-email-compromise event in the last 24 months?

■ Is your MSP doing a great job operationally but unable to sign off on risk acceptance or speak to a regulator?

Ready to model the ROI for your business?

Book a 30-minute discovery call. We'll size the right vCISO engagement for your headcount, regulatory exposure, and growth plan — and show you the breakeven point in your numbers.

trnsfrm.tech/vciso · info@trnsfrm.tech · Cleveland · Columbus, OH

Sources: IBM Security *Cost of a Data Breach Report* (2024); Ponemon Institute *State of Cybersecurity in SMBs*; US Bureau of Labor Statistics; Robert Half *2025 Salary Guide*; IANS Research *CISO Compensation*; TRNSFRM client engagements. Figures are planning-grade ranges.