YOUR CYBER RISK SCORE

36 / 74

Material gaps

Most Canadian oil & gas mid-market operators land in this range. That does not make it safe — it means the baseline cyber posture across the sector is genuinely insufficient for the 2026-2027 threat environment. The questions below are where your specific exposure lives.

19	11	30+	24/7
YEARS IN	YRS · ZERO BREACHES	M&A DEALS	OWNED NOC/SOC

WHERE YOUR EXPOSURE LIVES

Your highest-priority gaps

The questions below scored lowest — and each one represents a real, concrete exposure. Critical Controls (weighted 2×) appear first because their failure most directly enables a material event.

CRITICAL CONTROL

If you discovered a breach at 2am, do you know who to call and what to do?

You answered: No

When a breach happens, the first 24 hours decide whether you recover quickly or spend weeks rebuilding. Without a written incident response runbook and named contacts, you lose critical hours figuring out who to call, what to preserve, and what to disclose — exactly when speed matters most.

Most operators can draft a usable runbook in an afternoon. Almost none do until after the first incident. By then the window is closed.

CRITICAL CONTROL

Would a monitoring service catch a Saturday-night attack within minutes?

You answered: Not sure

"Not sure" is functionally "no" in front of a 2026 cyber insurance underwriter. Most regional Calgary MSPs that advertise 24/7 SOC are reselling a third-party SOC with a 15-minute call-tree latency baked in. When the attack lands at 2:47am Saturday, the difference between owned-NOC infrastructure and resold alert-forwarding is measured in damage, not minutes.

The diligence question worth asking your provider: "Is the SOC analyst on shift right now an employee of the firm we are paying, or two layers removed?"

HIGH IMPACT

Are your backups isolated from your production network?

You answered: Partially

Modern ransomware targets backups first. Attackers spend their first days inside the environment specifically locating, encrypting, or deleting backup repositories. "Partially isolated" means the attacker who lands inside your environment can probably reach them — and the carrier underwriting your 2026 renewal knows it.

The 2026 standard: immutability (cryptographic write-once, even by admins), test-restore cadence (quarterly minimum with logs), and offline-copy architecture (at least one copy not network-reachable).

HIGH IMPACT

Do you have evidence (not just attestation) of MFA on every admin account?

You answered: Attested, not evidenced

Five years ago, "we have MFA" was enough to tick the box. In 2026, carriers ask which type (SMS-based MFA is now treated roughly the same as no MFA) and they require evidence, not attestation. Screenshots are being replaced with logs in the questionnaire flow.

The standard is FIDO2-based phishing-resistant authentication for all admin access. The math runs against operators who treat MFA as a checkbox.

What we'd recommend, in priority order

Within 30 days: Draft and tabletop the incident response runbook. Two hours of work removes the worst gap on this report.

Within 90 days: Validate that your NOC/SOC provider is owned, not resold. Walk through one CVE response with the analyst who would handle a 2am incident.

Within 180 days: Move from SMS-based MFA to FIDO2 across all admin access. Document the immutable backup architecture with a successful test-restore log. Run the score again — most operators move from "Material gaps" to "Defensible" inside two quarters.

Want a 30-minute review of this report with a sitting CIO?

James D. Boyd, Vencer's founder and current CIO at Valeura Energy, runs a free 30-minute review of any cyber score report. No pitch deck. No proposal. Just the honest conversation about what's most exposed and what's worth doing first.

Book the 30-min review →

WHAT THIS IS. WHAT THIS ISN'T.

Calibrated self-assessment based on 19 years of operator data. Not a full audit. The audit version is a 30-min CIO review with a defensible report you can take to your board, your CFO, and your broker. Free, genuinely.

→ Book the 30-min review

About the score: The Vencer Cyber Risk Self-Score is calibrated against eleven consecutive years of zero-breach client outcomes and 30+ M&A IT diligence engagements. Critical Controls (×2 weight) are the gaps that most directly enable a material event; High Impact controls compound the consequences when something goes wrong.

What we do: Vencer Group is Calgary's managed IT and cybersecurity partner for Canadian energy mid-market since 2007. 24/7 NOC/SOC across ESIEM (Canada) and Echo Protocol (Singapore) — owned sister entities, not third-party resold. Same stack a Fortune 500 SOC runs.