VYFORITY

Cyber security and business architecture advisory

Most breaches aren't detected. *They're announced.*

By a ransom note, a journalist's call, or the AFP. Vyfority's compromise assessment answers the question before someone else does: passive scanning and digital forensics to determine whether a compromise is underway, contain it early if it is, and establish root cause. Discreet, fixed fee, defined window.

Assume breach, then check

Intruders routinely sit in networks for weeks or months before anyone notices. Mature organisations treat compromise as possible and verify, rather than trusting the silence.

Passive and discreet

Passive scanning and forensic artefact analysis: no agent rollout, no operational disruption, no rumour mill. Most of your organisation never knows the question was asked.

An answer either way

"Yes, and contained early" beats discovery by ransom note. "No, with evidence" is currency with boards, insurers and acquirers. Both are worth having.

WHEN TO ASK THE QUESTION

Silence is not evidence

Nothing on the dashboard says "breach in progress". Capable intruders are quiet by design: they read mail, map suppliers, stage access and wait for the moment that pays. The organisations that find them early are the ones that went looking. The rest find out when someone else tells them, and by then the timing, the narrative and the cost all belong to the attacker.

THE THREE SCENARIOS THAT WARRANT A LOOK

Something feels wrong. Odd sign-ins, a mail rule nobody created, a supplier's incident, a staff credential in a breach dump, a quiet tip from a customer or agency. A suspected breach deserves a discreet, evidence-based answer in days, not a hopeful wait.

A deal or a transition. Acquiring a company means acquiring whoever is inside its network. New CEOs, CFOs and boards inherit the same uncertainty. A compromise assessment turns "we believe it's clean" into a verified baseline.

Assurance on your terms. Validating that a past incident's remediation actually held, or a periodic assume-breach check between assessments, so the first honest look isn't forced on you by events.

What we will and won't tell you. A compromise assessment provides evidence-based confidence within the scope examined, never a blanket guarantee; be wary of anyone who offers one. If compromise is found, we contain it, establish root cause, and work alongside your insurer, your lawyers and any panel responders rather than around them, with evidence preserved and privilege respected.

THE METHOD · FIXED FEE, DEFINED WINDOW

01

Scope

Agree the question, the systems that matter most and the logistics of discretion: who knows, who doesn't, and how findings will be handled. Where counsel wants privilege over the work, we structure for it from the start.

02

Hunt

Passive scanning and digital forensics across the traces intruders actually leave: sign-in patterns, mail rules and forwarding, persistence mechanisms, lateral movement, data staging. Evidence, not intuition.

03

Contain

If something is live: immediate containment of the access, coordinated with your insurer and legal advisers, with evidence preserved to the standard those processes require. Early discovery keeps the options yours.

04

Resolve

Root cause established and a hardening path to close it for good. If the environment is clean: a **documented statement of findings** your board, insurer or acquirer can rely on.

Find out on your terms

Every other way of learning about a compromise is worse: the ransom note, the journalist, the regulator, the customer who heard first. A compromise assessment is quiet, fixed fee, run in a defined window, and led personally by a former enterprise CISO. Whatever the answer, it becomes yours to act on rather than react to.

Dean Kastelic · Founder, former enterprise CISO
dean.kastelic@vyfority.com.au
linkedin.com/in/deankastelic · vyfority.com.au