

A cyber incident isn't a matter of if – but when.

Our Incident Response & Digital Forensics services help you prepare for, respond to, and recover from security breaches with speed and clarity. Whether you're planning ahead or in the middle of a crisis, we're here to guide you.

What We Do

We help organisations:

- Build and test their incident response plans
- Respond quickly to active threats or data breaches
- Analyse the root cause of security incidents
- Communicate clearly with stakeholders, regulators, or boards
- Recover securely and reduce risk of recurrence

We operate both **proactively** (planning & tabletop exercises) and **reactively** (real-time response & forensic analysis).

Services Offered

Incident Response Planning

- **Strengthen Preparedness** - Develop a tailored, practical incident response plan
- **Clarify Responsibilities** - Define roles, triggers, contact trees, and communication protocols
- **Ensure Compliance** - Align with compliance standards: ISO 27001, ISM, NIST CSF, Essential Eight
- **Build Resilience** - Integrate with existing business continuity/disaster recovery plans



Tabletop Exercises

- **Drive Readiness** - Facilitate simulation scenarios for execs, IT, and business units
- **Practice with Confidence** - Test IR plans in safe, low-stress environments
- **Sharpen Performance** - Evaluate decision-making, response timing, and escalation paths
- **Enhance Continuously** - Optional reporting and improvement plan



Active Incident Response

- **Respond Rapidly** - On-call assistance during live incidents (ransomware, phishing, malware, etc.)
- **Coordinate Effectively** - Coordination of containment, eradication, and recovery steps
- **Navigate Critical Decisions** - Advice on disclosure, insurance engagement, and comms



Digital Forensics & Root Cause Analysis

- **Uncover the Cause** - Identify how the breach occurred and what was impacted
- **Trace the Threat** - Recover logs, trace attacker movement, and verify data access
- **Deliver Clear Evidence** - Provide evidence for internal use or external reporting
- **Support Accountability** - Support for law enforcement or insurance claims if required





Who This Is For

- **Councils and NFPs** with limited in-house security resources
- **SMBs** concerned about ransomware, phishing, or supply chain compromise
- **Organisations** that have experienced a breach and need clarity
- **Teams** preparing for ISO 27001, Essential Eight, or insurance requirements
- **Executives and boards** wanting to improve cyber resilience

What Our Clients Say

"We had no formal IR plan, and when we got hit with a phishing attack, vCISO.One helped us contain it, reassure our board, and walk through every step. Their calm, practical approach made all the difference."

— Operations Director, Community Services Organisation

Deliverables You'll Receive

- | | |
|---|---|
| ✓ IR Plan or Playbook (customised) | ✓ Post-incident report + lessons learned |
| ✓ Tabletop Summary & Recommendations | ✓ Communication templates (internal/external use) |
| ✓ Forensic investigation report (if applicable) | ✓ Optional integration with GRC or vCISO programs |

Why It Matters

Cyber insurance providers, regulators, and clients increasingly expect you to:

- | | |
|------------------------------------|--|
| • Have a documented IR plan | • Contain and report incidents quickly |
| • Run exercises and test responses | • Preserve evidence and recover securely |

We help you meet those expectations — and protect your people, data, and reputation.

Optional Add-Ons

- Integration with managed detection & response (MDR)
- Staff phishing simulations and awareness training
- Policy development (IR, breach notification, escalation matrix)
- Executive cyber briefings or board simulations
- Secure cloud backup and recovery guidance

Prepare Now – or Get Help Fast

We're available for both **proactive planning** and **urgent incident response**.

Schedule an IR Readiness Call