VYFORITY

Cyber security and business architecture advisory

The 72-hour clock starts *whether you are ready or not.*

Mandatory ransomware payment disclosure under the Cyber Security Act 2024, as a ten-step checklist across the four phases of the reporting window. Tick honestly: every unticked box is a step you would be improvising during a live incident.

72:00:00
The clock starts when the payment is made, or when you become aware a payment was made on your behalf.

Up to $99,000
Civil penalty for a body corporate. Applies to $3M+ turnover and critical-infrastructure entities. Seek legal advice.

HOURS 00:00-12:00

Phase 1 · The foundation

Establish command structure before any technical work begins.

- ☐ **01 Trigger definition confirmed**
  A named team member has reviewed the Act's definition of "ransomware payment". **Legal ambiguity here is the single most common compliance failure point.**
- ☐ **02 Disclosure lead appointed**
  One named individual (and one backup) owns the ASD submission. This role must be independent of the incident recovery team.
- ☐ **03 Cyber counsel on standby**
  Specialist cyber legal counsel is on retainer and reachable 24/7. They must review the disclosure draft before lodgement.

HOURS 12:00-36:00

Phase 2 · The evidence log

Build the mandatory evidentiary record while the incident is live.

- ☐ **04 Attack vector mapped**
  The specific technical vulnerability is identified and documented to the extent known by reasonable enquiry. **A blank entry is a red flag:** record what you know and the steps taken.
- ☐ **05 Threat actor comms preserved**
  All negotiation records are stored in an immutable, time-stamped log. Chain of custody must be unbroken.
- ☐ **06 Payment provenance documented**
  Cryptocurrency wallet address and transaction hash are recorded verbatim and verified against blockchain confirmation before submission.

HOURS 36:00-60:00

Phase 3 · The boardroom

Governance must run in parallel with the technical response, not after it.

- ☐ **07 Board decision tree activated**
  A pre-approved pay/no-pay framework with defined thresholds, escalation criteria and sign-off authority governs the payment decision.
- ☐ **08 Board attestation obtained**
  The board formally signs off on the disclosure as a true and accurate record. This attestation is a legal requirement, not a formality.

HOURS 60:00-72:00

Phase 4 · The submission

Final review and lodgement. One opportunity to get this right.

- ☐ **09 ASD reporting template lodged**
  The Australian Signals Directorate ransomware payment form is completed, reviewed by counsel, and submitted before hour 72.
- ☐ **10 Post-disclosure protocol ready**
  The submission is not the end. ASD will issue a Request for Further Information within days. **Without a documented response process, you will fail the post-disclosure audit.**

10/10
Top 1%. Audit-ready. Go to sleep.

7–9
Under real stress you'll miss the window. Drill it now.

Under 7
Active civil regulatory risk. Act this week.

The Disclosure Protocol Sprint

One focused two-hour session. We build your board decision tree, populate your ASD templates, and align your executive team. **Finished documents delivered from the session. Fixed fee: $5,500.** vyfority.com.au/ransomware

Dean Kastelic · former enterprise CISO · ex-KPMG Director
dean.kastelic@vyfority.com.au
vyfority.com.au