anchor@anchor-cyber:~$ man incident-response

ANCHOR CYBER SECURITY LLC

Incident Response — PICERL

SANS's operational IR model. Six phases, each with a different job and a different way to fail — the split between Containment and Eradication is the one people collapse most often, and it's the one that costs the most when they do.

CSF's RESPOND/RECOVER Functions tell you *what* outcomes matter. PICERL is the *order of operations* during an actual incident — use this card mid-incident, use the CSF Field Reference for the audit/gap-analysis side of the same work.

1 Preparation — before anything happens

DO — IR plan with named owner and authority (RS.MA-01), tested contact list, backups verified restorable, logging actually retained somewhere an attacker can't delete it.

PITFALL — A written plan nobody has ever run through once. An untested plan is a document, not a capability.

2 Identification — is this actually an incident

DO — Confirm scope and severity before declaring — what systems, what data, how did you find out.

PITFALL — Treating every alert as an incident, or the opposite — normalizing real signal as noise until it's too late.

3 Containment — stop it from getting worse, right now

DO — Short-term: isolate the affected system. Long-term: patch the immediate hole without destroying evidence.

PITFALL — Jumping straight to Eradication before containment is actually stable — the attacker still has a foothold while you're busy cleaning up.

4 Eradication — remove the actual cause, not just the symptom

DO — Remove malware/access, close the root-cause vulnerability, confirm nothing persistent survived (scheduled tasks, new accounts, backdoors).

PITFALL — Rushing to Recovery because containment "felt" successful — comprehensive eradication checks get skipped under time pressure.

5 Recovery — back to normal, deliberately

DO — Restore from a verified-clean backup, monitor closely post-restore, confirm the fix holds under real load.

PITFALL — Restoring from a backup that was never integrity-checked, or that predates when the attacker got in.

6 Lessons Learned — feeds back into Preparation

DO — After-action report: what happened, what worked, what didn't, what changes as a result. This is the step that makes PICERL a loop, not a checklist.

PITFALL — Skipping this once the fire's out — it's the only phase with no urgency attached, which is exactly why it's the one that gets dropped.

```
$ ir --who-to-call
```

Fill in before an incident, not during one.

ROLE	NAME / CONTACT
Incident commander	
Technical lead	
Legal counsel	
Cyber insurance carrier / broker	
Outside forensics (on retainer if possible)	
Law enforcement (local + FBI IC3)	
Client / regulator notification owner	

src: SANS 504 Incident Response Cycle · PICERL model exit 0