Simple Guide: First 72 Hours After a Cyber Incident

A practical, experience-driven guide for leaders when it matters most

By: Shawn Awan, SkySec Founder & Lead Assessor

Cyber incidents don't announce themselves politely. They arrive quietly, spread quickly, and punish rushed decisions.

*What you do in the **first 72 hours** often determines:*

- *How much downtime you suffer*
- *Whether data loss is contained or escalates*
- *If insurance claims are honored or reduced*
- *How defensible your organization looks to regulators, parents, patients, or boards*

*This guide is written for **leaders**, not technicians. It reflects what actually works in the real world — not theory.*

Hour 0–1: Stop the Bleeding (Without Making It Worse)

***Your goal:** Contain damage while preserving options.*

Do this immediately

- *Isolate affected systems from the network (disconnect, don't destroy)*
- *Document what was observed: timestamps, error messages, ransom notes, odd behavior*
- *Identify what still works (email, phones, backups, core apps)*

Do NOT do this

- *Do not power off everything "just in case"*
- *Do not delete files, logs, or suspicious emails*
- *Do not let staff "try fixes" on their own*
- *Do not contact attackers yet*

Most orgs accidentally destroy evidence in the first hour. That mistake alone can cost six figures later.

Hours 1–24: Preserve Evidence and Regain Control

***Your goal:** Maintain leverage — legally, operationally, and financially.*

Preserve before you fix

- *System logs (firewalls, servers, cloud platforms)*
- *Authentication logs (especially admin and remote access)*
- *Backup status and timestamps*
- *Screenshots of impacted systems*

Control internal communications

- *Issue a short staff message: acknowledge an IT issue, instruct no troubleshooting*
- *Designate one point of contact for decisions*
- *Keep leadership updates factual and time-stamped*

Avoid common traps

- *Over-communicating too early*
- *Blaming individuals*
- *Letting vendors take unilateral action without oversight*

Days 1–3: Communicate Safely and Strategically
Your goal: *Stay accurate, compliant, and credible.*
External communication principles

- *Say only what you can verify*
- *Avoid technical speculation*
- *Align messaging across leadership, legal, and IT*

Insurance and legal reality

- *Insurers will ask:*
  - *When did the incident begin?*
  - *What evidence exists?*
  - *What controls were in place before the incident?*
- *Claims are weakened by missing logs, undocumented actions, or rushed remediation*

Cyber insurance is not automatic. It's conditional — and evidence matters.

The 5 Mistakes That Make Incidents Worse

1. *Turning systems off too early*
2. *Letting well-meaning staff "clean things up"*
3. *Calling too many vendors at once*
4. *Communicating before facts are confirmed*
5. *Treating the incident as purely technical instead of operational*

These mistakes don't come from incompetence — they come from ***panic****. Preparation removes panic.*

Why Preparation Changes Everything
Organizations that rehearse incident response:

- *Recover faster*
- *Reduce downtime costs*
- *Protect insurance coverage*
- *Maintain trust with stakeholders*

The difference is not tools. It's clarity under pressure.

A Final Thought From the Field
Every major incident I've worked on had the same pattern:

- *Leaders wanted to "just fix it"*
- *The real risk was invisible until it was too late*
- *The organizations that fared best had a plan before the incident*

You don't need perfection. You need readiness.

About SkySec
We help organizations prepare for incidents before they happen — and guide them calmly when they do. Our work focuses on clarity, defensibility, and real-world response, not fear or hype. If this guide raised questions, that's a good sign. Those questions are exactly what preparation is meant to answer