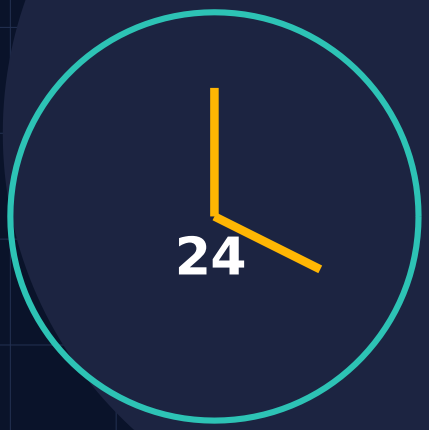
BLUE HARBOR EDITIONS



CYBER INCIDENT

THE FIRST 24 HOURS

Contingency plan for freelancers

and small businesses

16 TEMPLATE | 20 CHECKLIST | 12 PLAYBOOK

0-15 MIN

1 HOUR

4 HOURS

24 HOURS

CONTAIN. DOCUMENT. RESTORE.

Clear decisions when every minute counts.

BLUE HARBOR STUDIO

2026 EDITION | CODE BH-008 | UPDATED ON JULY 20, 2026

Cyber Incident: The First 24 Hours

Contingency Plan for Freelancers and Small

Businesses Blue Harbor Editions - BH-008 - English

Edition 2026

VERSION AND CONTROL

Version 1.0. Sources checked on July 20, 2026. Channels, obligations and interfaces of suppliers change: always check the official sources and conditions applicable to your case.

Important Warning

This guide is an educational and organizational tool. It is not a substitute for a professional incident response service, a lawyer, a DPO, an employment consultant, an insurer, a bank, a provider or the authorities. It does not certify compliance and does not guarantee the recovery of data or money.

If there is an immediate physical risk, call 112. If money is involved, contact the bank immediately through an official number. If the attack is active, use a device and channel that you think are clean to coordinate the response.

Copyright and License

Emergency card: the first 15 minutes

FIRST RULE

Don't improvise a cleanup. Contain the damage, preserve the evidence, and record every decision.

[ ] Write down the exact time you discovered the issue and who reported it.

[ ] Shifts coordination to a device and channel that is not involved in the incident.

[ ] If a device is actively compromised, disconnect it from the network without deleting any files or logs. [ ] If a payment is involved, call the bank immediately and ask for a hold or recall.

[ ] Appoints a person in charge and a person to keep the chronological record.

[ ] Capture screenshots, messages, times, URLs, senders, and alerts without interacting with suspicious files. [ ] Contact the provider or an incident response professional from the clean channel.

[ ] Do not send public communications until facts and permissions are verified.

NUMBERS TO PREPARE BEFORE

IT provider or MSP - bank - cyber insurance - legal advisor/DPO - hosting/cloud - Postal Police - internal contact person.

How to use the manual

During an accident you don't read a book from start to finish. You use the timeline, then the specific playbook and finally the templates. The priority is to make repeatable decisions with the available information, without confusing speed with haste.

- Before the incident: Fill out contacts, roles, essential inventory, and severity thresholds.
- In the first 15 minutes: Use the Emergency Card and open the Incident Log.
- Within an hour: Identify what is known, what is hypothesized, and what needs to be verified.
- Within four hours: Contains prioritized identities, devices, services, and payments.
- Within 24 hours: Initiate controlled recovery, legal assessments, and authorized communications.
- After the incident: Turn each lesson into a change with a manager and deadline.

Profile	Minimal Liability	Support to be activated
Freelance	Owner	Provider, bank, legal/DPO if necessary
Team 2-5	Incident lead + log keeper	MSP/Supplier & Account Manager
Small company	Lead + Technician + Communications	Management, DPO/legal, insurance
Regulated activity	Roles under the plan	Authorities and advisors as required

Operational index