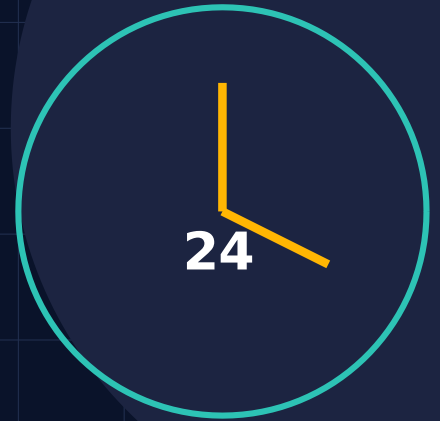


BLUE HARBOR EDITIONS

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

Copyright © 2026 Blue Harbor Editions. All rights reserved. The buyer can fill out and adapt the templates for personal or internal use in their business. You may not resell, distribute, or publish substantial portions of the guide without written permission.

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

Cyber Incident: The First 24 Hours	2
Important Warning.....	2
Copyright and License	2
Emergency card: the first 15 minutes	3
How to use the manual	4
Operational index	5
TAKING CONTROL	10
1. Event, suspicion or accident?	11
2. The five non-negotiable priorities	12
3. S1-S4 Gravity Matrix	13
4. Roles for teams of one to ten people	14
5. The clean channel and minimal operations room	15
6. Contain without destroying evidence	16
THE 24-HOUR TIMELINE	17
7. Minute 0-15: Declare and stabilize	18
Don't.....	18
8. Minute 15-60: Define the initial perimeter	19
9. Hour 1-2: Contain identities, devices, and payments	20
Identity	20
Devices and network	20
Payments	20
10. Hour 2-4: Support, continuity and obligations	21
11. Hour 4-8: Check containment	22
12. Time 8-12: Decide communications and reset	23
13. Time 12-24: controlled recovery and open floor	24
14. Who to contact and in what order	25
TWELVE PLAYBOOKS	26

15. Compromised email inbox	27
Signs and confirmations to look for	27
Sequence of operations	27
16. Ransomware or data extortion	28
Signs and confirmations to look for	28
Sequence of operations	28
17. Fake payment and business email compromise	29
Signs and confirmations to look for	29
Sequence of operations	29
18. Lost or stolen laptop or phone	30
Signs and confirmations to look for	30
Sequence of operations	30
19. Malware or suspicious application	31
Signs and confirmations to look for	31
Sequence of operations	31
20. Compromised cloud or administrator account	32
Signs and confirmations to look for	32
Sequence of operations	32
21. Compromised website or e-commerce	33
Signs and confirmations to look for	33
Sequence of operations	33
22. Stolen social or ad account	34
Signs and confirmations to look for	34
Sequence of operations	34
23. Public sharing or incorrect sending of data	35
Signs and confirmations to look for	35
Sequence of operations	35
24. DDoS, unreachable site or severe degradation	36
Signs and confirmations to look for	36
Sequence of operations	36
25. Vendor or SaaS incident	37
Signs and confirmations to look for	37
Sequence of operations	37
26. Unauthorized internal access	38
Signs and confirmations to look for	38
Sequence of operations	38

RECOVERY, DATA AND COMMUNICATIONS	39
27. Reclamation or reconstruction?	40
28. Credential rotation order	41
29. Restore backups without reinfection	42
30. Communicate with staff, customers and partners	43
31. Data breach and 72-hour deadline	44
32. NIS, CSIRT, Police & Insurance	45
33. The next 72 hours, 7 days, and 30 days	46
SEDICI TEMPLATE	47
Cyber emergency card	48
Matrix of verified contacts	49
Initial Assessment S1-S4	50
Incident History Log	51
Map of the assets involved	52
Inventory of evidence	53
Decision Register	54
Account and credential containment	55
Communications Register	56
Preliminary assessment of data breach	57
Notification preparation by stages	58
Draft communication to customers or partners	59
Urgent Supplier Questionnaire	60
Recovery Validation Card	61
Post-incident review	62
30-day strengthening plan	63
30-day plan - continued	64

CHECKLIST AND REFERENCES	65
20 Operational Checklists - Group 1	66
01 - Accident Declaration	66
02 - Clean channel.....	66
03 - Device isolation	66
04 - Account email.....	66
05 - Ransomware.....	66
20 Operational Checklists - Group 2	67
06 - Fraudulent payment	67
07 - Lost device	67
08 - Cloud/admin	67
09 - Website/e-commerce	67
10 - Social/advertising	67
20 Operational Checklists - Group 3	68
11 - Data leak	68
12 - Supplier	68
13 - Evidence	68
14 - Data breach.....	68
15 - Communications.....	68
20 Operational Checklists - Group 4	69
16 - Secrets rotation	69
17 - Backup restore	69
18 - Return to production	69
19 - Monitoring	69
20 - Incident closure	69
Frequently Asked Questions	70
Should I turn off my computer?	70
Can I change all passwords right away?	70
If I don't see encrypted files, isn't it ransomware?	70
Do I have to pay the ransom?	70
Does every incident have to be notified to the Guarantor?.....	70
Do the 72 hours start from the attack?	70
Does CSIRT Italia replace the complaint?	70
Can I notify customers right away?.....	70
When can I close the incident?	70
How do I know if the supplier has solved?	70
Essential glossary	71
Official sources and updates	72