

The First 24 Hours After a Cyber Incident

What Leaders Do Next Matters Most

0-4 Hrs

Stabilize

- *Activate Response*
- *Preserve Evidence*
- *Assess Scope*

4-12 Hrs

Contain

- *Isolate Systems*
- *Disable Accounts*
- *Rotate Credentials*

12-24 Hrs

Communicate

- *Employee Updates*
- *Customer Messaging*
- *Legal & Regulatory*

Critical Leadership Actions

- ✓ Activate incident response team
- ✓ Understand scope before acting
- ✓ Preserve evidence
- ✓ Contain further damage
- ✓ Establish executive communications
- ✓ Document every decision

Common Mistakes

- ✗ Wiping systems too quickly
- ✗ Communicating before facts are known
- ✗ Treating it as only an IT issue
- ✗ Failing to preserve evidence
- ✗ Using compromised email systems
- ✗ Assuming only one system is affected

Communication Priorities

Employees:

- Share facts, not assumptions
- Explain operational impacts
- Create a single source of truth
- Avoid internal speculation

Customers:

- Acknowledge the incident
- Explain investigation status
- Commit to future updates
- Don't overpromise

First 24-Hour Checklist

- | | |
|--|---|
| ☐ Activate response team | ☐ Notify stakeholders |
| ☐ Establish secure communications | ☐ Engage legal and cyber insurance |
| ☐ Preserve evidence | ☐ Prepare employee messaging |
| ☐ Isolate affected systems | ☐ Prepare customer messaging |
| ☐ Secure compromised accounts | ☐ Continue investigation |

This resource was developed using guidance from the Cybersecurity and Infrastructure Security Agency (CISA) Cybersecurity Incident & Vulnerability Response Playbooks and industry incident response best practices.

[Access the full CISA Cybersecurity Incident & Vulnerability Response Playbook](#)