PCC LEARNING CENTER

Cyber Incident: First 60 Minutes Checklist

A practical response aid for business leaders

The first hour is about disciplined escalation, evidence preservation, proportionate containment, and controlled decisions. Use this worksheet with your incident-response plan and qualified technical, legal, insurance, and communications advisers.

If an incident may be happening now

Call your established IT or cybersecurity response provider using a trusted number. If people are in immediate danger, contact emergency services. Do not delay urgent financial-fraud reporting to your bank.

DATE

TIME DETECTED

REPORTED BY

INCIDENT COORDINATOR

RECORD KEEPER

INITIAL OBSERVATION

Response aid only: this does not replace a tested plan, professional investigation, legal advice, or insurer direction.

First 10 Minutes: Recognize and Escalate

Stabilize the situation, create a reliable record, and reach the people authorized to direct containment.

- [ ] 1 If there is immediate danger to people, call emergency services and follow life-safety procedures first.
- [ ] 2 Note the current time, who reported the issue, what they observed, and how they can be reached.
- [ ] 3 Contact your designated IT or cybersecurity response provider using a known, trusted number - not contact details supplied in a suspicious message.
- [ ] 4 Tell the employee to stop interacting with suspicious messages, websites, prompts, or payment requests.
- [ ] 5 Keep the affected device powered on unless the response lead directs otherwise. Do not reboot, wipe, or run cleanup tools.
- [ ] 6 If instructed or clearly necessary to stop active spread, isolate the affected device from networks without erasing it; document exactly what was disconnected.
- [ ] 7 Use a separate, known-clean device and communication channel if email, Teams, or the company network may be compromised.
- [ ] 8 Start the incident log. Record every action, time, decision, person contacted, and instruction received.

PHASE COMPLETED / REVIEWED BY	TIME	NEXT UPDATE

10-30 Minutes: Scope and Contain

Follow the response lead's direction. Containment should reduce harm while preserving evidence and business options.

- [ ] 1 Identify affected people, accounts, devices, applications, locations, data, vendors, and business processes based on current evidence.
- [ ] 2 Record indicators such as sender address, phone number, domain, file name, alert text, transaction details, and screenshots without forwarding malicious content.
- [ ] 3 Preserve relevant messages, logs, files, alerts, and device state. Do not delete suspicious email or alter original evidence.
- [ ] 4 For a suspected account compromise, have an authorized administrator revoke active sessions and secure the account from a known-clean device.
- [ ] 5 Reset credentials only through an approved process and in the sequence directed by the response lead; address recovery methods, MFA, tokens, and connected applications.
- [ ] 6 For suspected payment or banking fraud, call the financial institution immediately using a verified number and request its fraud procedure.
- [ ] 7 Do not broadly block, disable, or shut down systems without considering evidence preservation, safety, operational impact, and attacker visibility.
- [ ] 8 Establish the next decision point and update time, even when scope remains uncertain.

PHASE COMPLETED / REVIEWED BY	TIME	NEXT UPDATE

30-60 Minutes: Activate the Business Response

Bring the right decision-makers together, protect confidentiality, and create a controlled plan for the next several hours.

- [ ] 1 Notify the designated executive incident owner and assign one incident coordinator and one written record keeper.
- [ ] 2 Locate the incident-response plan, cyber-insurance policy, critical vendor contacts, system inventory, and business-continuity procedures.
- [ ] 3 Contact the cyber insurer or broker promptly when the event may be covered; follow notice and approved-provider requirements before incurring major costs.
- [ ] 4 Engage legal counsel when personal information, regulated data, contracts, law enforcement, employee monitoring, or notification duties may be involved.
- [ ] 5 Decide who may communicate with employees, customers, vendors, insurers, banks, law enforcement, and the public. Share verified facts only.
- [ ] 6 Set an internal information boundary: who needs to know, what channel is trusted, and where incident records will be maintained.
- [ ] 7 Document current scope, business impact, containment status, unresolved questions, owners, deadlines, and the next leadership update.
- [ ] 8 Do not restore systems, declare the incident over, pay an attacker, or make external assurances without authorized professional direction.

PHASE COMPLETED / REVIEWED BY	TIME	NEXT UPDATE

Incident Record and Immediate Priorities

Capture verified facts separately from assumptions. Keep this record in the location and communication channel approved by the incident coordinator.

AFFECTED PEOPLE / ACCOUNTS

AFFECTED DEVICES / SYSTEMS / LOCATIONS

KNOWN OR SUSPECTED BUSINESS IMPACT

CONTAINMENT ACTIONS ALREADY TAKEN

EVIDENCE PRESERVED / LOCATION

PEOPLE AND ORGANIZATIONS CONTACTED

Avoid These First-Hour Mistakes

A hurried action can destroy evidence, alert an attacker, interrupt operations unnecessarily, or create legal and insurance complications.

- X Do not delete suspicious messages, logs, files, or alerts.
- X Do not reboot, reimage, wipe, or run cleanup tools without direction.
- X Do not use potentially compromised email or messaging for the response.
- X Do not negotiate with, pay, or publicly engage an attacker yourself.
- X Do not promise customers or employees that data is safe before facts are established.
- X Do not contact every employee, customer, regulator, or law-enforcement agency reflexively; coordinate legal and communications decisions.
- X Do not assume a password reset alone ends an account compromise.
- X Do not let urgency erase the record: time-stamped documentation is part of the response.

Next leadership update

TIME	UPDATE OWNER	DECISIONS NEEDED

TOP THREE PRIORITIES FOR THE NEXT TWO HOURS