

# Cyber Incident Evidence Log

A fillable timeline and evidence checklist for account compromise, ransomware, vendor breach, BEC, or system outage.

## Incident basics

Discovery date / time

First known event date / time

Systems / accounts affected

Data potentially affected

Operations affected

## Evidence preserved

Original emails / headers

☐ Check when verified / completed

Identity / login logs

☐ Check when verified / completed

System / cloud logs

☐ Check when verified / completed

Vendor incident notices

☐ Check when verified / completed

Payment / bank records

☐ Check when verified / completed

Backup status recorded

☐ Check when verified / completed

Evidence location

# Cyber Incident Evidence Log

A fillable timeline and evidence checklist for account compromise, ransomware, vendor breach, BEC, or system outage.

## Response actions

### Accounts isolated / secured

☐ Check when verified / completed

### Incident responder contacted

☐ Check when verified / completed

### Bank contacted if funds moved

☐ Check when verified / completed

### MFA / credentials reset

☐ Check when verified / completed

### Insurer notified

☐ Check when verified / completed

### Law enforcement / IC3 reference

## Timeline & costs

### Key timeline notes

### Downtime start / end

### Forensic / restoration costs

### Lost operations / transactions

### Next action and owner