CYBER INCIDENT RESPONSE & NOTIFICATION PLAYBOOK

FOR SMALL & MEDIUM ENTERPRISES

USE DURING ACTIVE INCIDENTS

Insurance-Aligned • Regulator-Safe • Legally Defensible

PRE-POPULATE NOW — BEFORE AN INCIDENT

Insurance Policy #: ____

Insurance Breach Hotline: __________________________________

Incident Commander: _______________________________________

Backup Commander: ____

CONTENTS

Part	Title	Page
1	Incident Classification	3
2	First 60 Minutes Checklist	5
3	Notification Decision Matrix	8
4	Communication Templates	11
5	Incident Documentation	22
6	Common Mistakes	27
—	Quick Reference Card	30

HOW TO USE THIS PLAYBOOK

- Go to PART 1 — Classify your incident
- Follow the instruction for your classification
- Execute checklists in order
- Use templates exactly as written — do not improvise
- Document everything with exact times

CRITICAL DISCLAIMERS

- This playbook does not constitute legal advice
- Engage breach counsel for legal guidance
- Insurance policy terms control — review your specific policy
- All templates require counsel review before external use
- Notification requirements vary by jurisdiction

PART 1: INCIDENT CLASSIFICATION

Answer these questions in order. Stop when directed.

What Are You Seeing?

You See This	Classification	Go To
Ransom note, encrypted files, payment demand	RANSOMWARE	Section A below
Employee clicked link + entered password	CREDENTIAL COMPROMISE	Section B below
Unusual logins, unfamiliar access alerts	UNAUTHORIZED ACCESS	Section C below
Vendor informed you of breach at their end	VENDOR BREACH	Section D below
Customer reports identity theft linked to you	DATA EXPOSURE	Section E below
Suspicious email received but NOT clicked	FALSE POSITIVE	Section F below
Antivirus quarantined file automatically	FALSE POSITIVE	Section F below
Single failed login attempt	FALSE POSITIVE	Section F below

Section A: RANSOMWARE

CONFIRMED INCIDENT — IMMEDIATE ACTION REQUIRED

- Do NOT pay anything
- Do NOT contact attacker
- Disconnect systems from network (do NOT power off)
- **Call cyber insurance hotline NOW**

→ **GO TO PART 2**

Section B: CREDENTIAL COMPROMISE

SUSPECTED INCIDENT — TREAT AS CONFIRMED

- Do NOT reset password yet (may alert attacker)
- Disconnect affected device from network
- Call cyber insurance hotline within 60 minutes

→ **GO TO PART 2**

Section C: UNAUTHORIZED ACCESS

SUSPECTED INCIDENT

- Do NOT disable accounts yet
- Document exactly what you observed
- Call cyber insurance hotline within 60 minutes

→ **GO TO PART 2**

Section D: VENDOR BREACH

EXTERNAL INCIDENT — ASSESS YOUR EXPOSURE

- Request written details from vendor immediately
- Identify what data vendor had access to
- Contact cyber insurance for guidance

→ **GO TO PART 3 (Notification Matrix)**

Section E: DATA EXPOSURE

CONFIRMED INCIDENT

- Document how you learned of exposure
- Preserve all related communications
- **Call cyber insurance hotline NOW**

→ **GO TO PART 2**

Section F: FALSE POSITIVE

NO INCIDENT — DOCUMENT AND STOP

- Document what you observed
- Document why you classified as false positive
- No further action required

→ **STOP HERE**

PART 2: FIRST 60 MINUTES CHECKLIST

Complete in order. Check each box. Record exact times.

DO THESE NOW

☐ Write down current time: ___:___AM/PM on __/__/____TZ: ____
☐ Your name and role: ______________________________
☐ Take photos/screenshots of everything unusual on screens
☐ Disconnect affected systems from network (unplug cable or disable WiFi)
☐ DO NOT power off computers
☐ Locate cyber insurance policy number: ________________
☐ Locate cyber insurance breach hotline: ________________
☐ **CALL cyber insurance breach hotline**
☐ Record who you spoke to: ______________________________
☐ Record claim number if given: ________________
☐ Tell all staff: STOP using affected systems
☐ Tell all staff: DO NOT discuss externally
☐ Start Incident Timeline Log (Part 5)

DO NOT DO THESE

PROHIBITED ACTIONS — MAY DESTROY EVIDENCE OR VOID INSURANCE

- Do NOT turn off computers — destroys volatile evidence
- Do NOT delete any files or emails — destroys evidence
- Do NOT wipe or reinstall systems — voids insurance
- Do NOT restore from backup — may reinfect, destroys evidence
- Do NOT pay ransom — voids insurance without approval
- Do NOT contact attacker — may worsen situation
- Do NOT post on social media — creates liability
- Do NOT talk to media — creates liability
- Do NOT admit fault to anyone — creates liability
- Do NOT hire forensics without insurer approval — may not be covered
- Do NOT hire lawyer without insurer approval — may not be covered
- Do NOT send notifications without lawyer review — creates liability

Actions That Void Insurance

Action	Consequence
Late notice to insurer (>24-72 hrs)	Claim denial or reduction
Using non-approved forensics vendor	Costs not covered

Using non-approved legal counsel	Costs not covered
Paying ransom without written approval	Payment not covered
Destroying evidence	Claim denial
Public admission of fault	Coverage defense compromised

Evidence to Preserve

☐ Screenshots of error messages/ransom notes: Location: _____________
☐ Phishing emails (do not delete): Location: _____________
☐ Security software alerts: Location: _____________
☐ Attacker communications: Location: _____________
☐ Affected hardware (secure physically): Location: _____________
☐ Access logs if visible: Location: _____________
☐ Paper documents related to incident: Location: _____________

PART 3: NOTIFICATION DECISION MATRIX

Determine who to notify based on data involved. Counsel confirms all decisions.

Step 1: Identify Data Category

Category	Contains	Examples
A	High-sensitivity identifiers	SSN, driver's license #, passport #, financial account + access code, biometric
B	Health information	Medical records, diagnoses, prescriptions, health insurance info
C	Financial data	Credit/debit card numbers, bank account numbers
D	Standard personal info	Name + email, name + phone, name + address
E	Business data only	Internal documents, operational data, no personal info

Step 2: Determine Notification Requirements

Find your data category. Read across for each recipient.

Data Category	Insurer	Customers	Regulators	Vendors
A (SSN, DL#, financial)	**YES — 24 hrs**	**YES**	**YES**	Check contracts
B (Health/PHI)	**YES — 24 hrs**	**YES**	**YES**	Check contracts
C (Payment cards)	**YES — 24 hrs**	**YES**	**LIKELY YES**	Check contracts
D (Name + contact)	**YES — 48 hrs**	**COUNSEL**	**COUNSEL**	Check contracts
E (Business only)	**YES — 48 hrs**	**NO**	**NO**	Check contracts
Unknown	**YES — 24 hrs**	**COUNSEL**	**COUNSEL**	Check contracts

Notification Details

Cyber Insurer

- WHEN: Within 24 hours. Sooner is better.
- HOW: Call breach hotline first. Written notice same day.
- TEMPLATE: Part 4, Section 4.1

Customers

- WHEN: After investigation confirms scope. Counsel sets timing.
- HOW: Written notice. Method depends on jurisdiction.

- TEMPLATE: Part 4, Section 4.2

Regulators

- WHEN: Varies by state (typically 30-60 days). HIPAA = 60 days.
- HOW: Counsel files. Each state has different requirements.
- TEMPLATE: Part 4, Section 4.5 (counsel prepares)

Vendors

- WHEN: Check contracts. Often 24-72 hours.
- HOW: Written notice per contract terms.
- TEMPLATE: Part 4, Section 4.4

PART 4: COMMUNICATION TEMPLATES

TEMPLATE RULES

- Use exactly as written
- Fill in brackets only
- Do not add language
- Counsel reviews all external communications

4.1 INSURER NOTICE

Template — Neutral Tone

INSURANCE NOTICE TEMPLATE

```
To: [INSURER NAME]
Policy Number: [NUMBER]
Date: [DATE]

RE: Notice of Potential Claim – Security Incident

This notice is provided pursuant to the above-referenced policy.

DISCOVERY: [DATE] at [TIME] [TIMEZONE]

DESCRIPTION: On [DATE], we identified [BRIEF FACTUAL DESCRIPTION
– e.g., "indicators of unauthorized access to our network" or
"a ransomware message on employee workstations"]. We are
investigating the scope and nature of the incident.

CONTAINMENT STATUS: [Active / Partially Contained / Contained]

DATA TYPES POTENTIALLY INVOLVED: [List categories – e.g.,
"customer names and email addresses" or "unknown, under
investigation"]

ESTIMATED SCOPE: [Number of individuals, or "under investigation"]

REQUESTS:
1. Confirmation of coverage
2. Approved forensics vendor list
3. Approved breach counsel list
4. Claim number
5. Adjuster contact information

INCIDENT CONTACT: [Name, Title, Phone, Email]

We will provide updates as investigation progresses.
```

```
[SIGNATURE]
```

Language to Avoid — Insurer

DO NOT SAY	SAY INSTEAD
"We failed to..."	"We are investigating..."
"Our security was inadequate"	"We are assessing the security environment"
"We caused..."	"An incident occurred..."
"All data was stolen"	"Scope is under investigation"
"We are liable"	[Never state — legal conclusion]
"This was preventable"	[Never state — admits negligence]

WHY IT MATTERS: Insurer notices become evidence. Admissions may be used to deny coverage.

4.2 CUSTOMER NOTICE

Template — Neutral Tone

CUSTOMER NOTICE — NEUTRAL

```
Dear [CUSTOMER NAME],

We are writing to inform you of a security incident that may have
involved some of your personal information.

WHAT HAPPENED:
[1-2 sentences. Example: "On [DATE], we discovered that an
unauthorized party may have accessed certain systems containing
customer information."]

WHAT INFORMATION WAS INVOLVED:
[List specific data types confirmed by investigation]

WHAT WE ARE DOING:
Upon discovering this incident, we [describe actions – e.g.,
"immediately engaged outside security experts and notified law
enforcement"]. We are implementing additional safeguards.

WHAT YOU CAN DO:
[List protective steps appropriate to data type – e.g., "monitor
your financial statements" or "consider placing a fraud alert"]

FOR MORE INFORMATION:
Contact [PHONE/EMAIL] or visit [URL].

[If offering credit monitoring: "We are providing [SERVICE] at no
cost. Enroll at [URL] using code [CODE]."]

Sincerely,
[NAME, TITLE]
```

Template — Reassuring Tone

CUSTOMER NOTICE — REASSURING

```
Dear [CUSTOMER NAME],

Protecting your information is important to us. We are writing to
tell you about a security incident and the steps we are taking.

WHAT HAPPENED:
[1-2 sentences – same facts, softer framing]
```

```
WHAT INFORMATION WAS INVOLVED:
[List specific data types]

WHAT WE ARE DOING:
As soon as we learned of this incident, we took action. We brought
in outside security experts and are strengthening our systems.

WHAT YOU CAN DO:
While we have no indication your information has been misused, we
recommend [protective steps].

FOR MORE INFORMATION:
Our dedicated team is available at [PHONE/EMAIL].

[If offering credit monitoring: "As a precaution, we are providing
[SERVICE] at no cost."]

Thank you for your patience.

Sincerely,
[NAME, TITLE]
```

Language to Avoid — Customer

DO NOT SAY	SAY INSTEAD
"Your data was breached"	"may have been involved"
"We apologize for our failure"	"We regret any inconvenience"
"This will never happen again"	[Do not make this claim]
"Your data is now safe"	"We have taken steps to address the incident"
"Hackers stole..."	"An unauthorized party may have accessed..."

WHY IT MATTERS: "May have been involved" preserves accuracy. Guarantees create liability. Admissions become evidence.

4.3 INTERNAL STAFF NOTICE

Template — Neutral Tone

STAFF NOTICE — NEUTRAL

```
To: All Staff
From: [NAME, TITLE]
Date: [DATE]
Subject: IT Systems – Action Required

We are addressing an IT matter that requires your immediate attention.

REQUIRED ACTIONS:
1. Stop using [AFFECTED SYSTEMS] until further notice
2. Do not attempt to troubleshoot systems showing unusual behavior
3. Report any unusual activity to [CONTACT] at [PHONE/EMAIL]
4. Do not discuss this matter outside the company

We will provide updates when available.

[NAME, TITLE]
```

Template — Reassuring Tone

STAFF NOTICE — REASSURING

```
To: All Staff
From: [NAME, TITLE]
Date: [DATE]
Subject: IT Systems Update

Our security monitoring identified some activity we are reviewing.
We are addressing it promptly.

HOW YOU CAN HELP:
1. Avoid using [AFFECTED SYSTEMS] for now
2. Report anything unusual to [CONTACT]
3. Keep this matter internal while we complete our review

We will share updates as our review progresses.

Thank you,
[NAME, TITLE]
```

Language to Avoid — Staff

DO NOT SAY	SAY INSTEAD

"We have been hacked"	"We identified an IT matter"
"Your personal data was stolen"	"We are investigating"
"This is an emergency"	"This requires attention"
"Management failed"	[Never state]
"Do not tell anyone"	"Keep this internal"

WHY IT MATTERS: Staff emails are discoverable. Panic language undermines response.

4.4 VENDOR NOTICE

Template — Neutral Tone

VENDOR NOTICE

```
To: [VENDOR CONTACT]
From: [YOUR NAME, TITLE]
Date: [DATE]
Subject: Security Incident Notification – [AGREEMENT NAME]

Pursuant to Section [X] of our agreement dated [DATE], we are
notifying you of a security incident.

SUMMARY:
[1-2 factual sentences]

DATA POTENTIALLY INVOLVED:
[Categories relevant to this vendor relationship]

STATUS:
We are investigating with outside experts.

REQUESTED ACTION:
Review your logs for unusual activity related to our integration.
Advise of any concerns.

CONTACT:
[Name, Phone, Email]

[SIGNATURE]
```

Language to Avoid — Vendor

DO NOT SAY	SAY INSTEAD
"Your systems caused this"	"We are investigating all aspects"
"We are liable for..."	[Never state — legal conclusion]
"All shared data was compromised"	"Scope is under investigation"

4.5 REGULATOR NOTICE

COUNSEL MUST PREPARE ALL REGULATORY FILINGS

- Regulatory notices have specific legal requirements
- Requirements vary by jurisdiction
- Wrong content or format may result in penalties
- This template is for reference only — do not send without counsel review

Reference Template — For Counsel Use

REGULATOR NOTICE — REFERENCE ONLY

```
[COUNSEL MUST PREPARE AND REVIEW]

To: [REGULATORY BODY]
From: [COMPANY NAME]
Date: [DATE]
Subject: Data Security Incident Notification

REPORTING ENTITY:
Name: [LEGAL COMPANY NAME]
Address: [ADDRESS]
Contact: [NAME, TITLE, PHONE, EMAIL]

INCIDENT:
Date of Incident: [DATE or RANGE]
Date of Discovery: [DATE]
Description: [COUNSEL-APPROVED TEXT]

AFFECTED INDIVIDUALS:
[NUMBER] residents of [JURISDICTION]
Information types: [LIST PER JURISDICTION REQUIREMENTS]

INDIVIDUAL NOTIFICATION:
Sent: [DATE]
Method: [MAIL/EMAIL]

REMEDIATION:
[COUNSEL-APPROVED DESCRIPTION]

[SIGNATURE]
```

PART 5: INCIDENT DOCUMENTATION

Use these templates to create defensible records for insurers and regulators.

5.1 Incident Summary Template

INCIDENT SUMMARY — PRIVILEGED AND CONFIDENTIAL

```
Document ID: [IR-YEAR-NUMBER]
Prepared by: [NAME, TITLE]
Date: [DATE/TIME/TIMEZONE]

═══════════════════════════════════════════════════════════════
DISCOVERY
═══════════════════════════════════════════════════════════════
Date: [DATE]
Time: [TIME]
Timezone: [TZ]
Discovered by: [NAME, TITLE]
Method: [How the incident was identified]

═══════════════════════════════════════════════════════════════
CLASSIFICATION
═══════════════════════════════════════════════════════════════
[ ] Suspected — under investigation
[ ] Confirmed — response in progress
[ ] Contained

═══════════════════════════════════════════════════════════════
DESCRIPTION
═══════════════════════════════════════════════════════════════
[State facts only. What was observed. No speculation about cause.]

═══════════════════════════════════════════════════════════════
SYSTEMS INVOLVED
═══════════════════════════════════════════════════════════════
[List systems where involvement is identified or suspected]

═══════════════════════════════════════════════════════════════
DATA CATEGORIES
═══════════════════════════════════════════════════════════════
[ ] A — High-sensitivity (SSN, DL#, financial account)
[ ] B — Health information
[ ] C — Financial (payment cards, bank accounts)
[ ] D — Standard PII (name + contact)
[ ] E — Business data only
[ ] Unknown — under investigation
```

```
═══════════════════════════════════════════════════════════════
SCOPE
═══════════════════════════════════════════════════════════════
Individuals: [NUMBER or "under investigation"]
Records: [NUMBER or "under investigation"]
Jurisdictions: [LIST or "under investigation"]

═══════════════════════════════════════════════════════════════
CONTAINMENT
═══════════════════════════════════════════════════════════════
Status: [Active / Partial / Contained]
Date/time contained: [IF APPLICABLE]

═══════════════════════════════════════════════════════════════
INSURER STATUS
═══════════════════════════════════════════════════════════════
Verbal notice: [DATE/TIME/CONTACT]
Written notice: [DATE/TIME]
Claim number: [NUMBER]
```

5.2 Timeline Log Template

INCIDENT TIMELINE LOG — PRIVILEGED AND CONFIDENTIAL

```
Incident ID: [ID]
Log started: [DATE/TIME/TZ]
Maintained by: [NAME]

INSTRUCTIONS:
• Record every action chronologically
• Use exact times with timezone
• State facts only — no speculation
• Initial each entry

═══════════════════════════════════════════════════════════════
Entry: 001
Date: [DATE]  Time: [TIME]  TZ: [TZ]
Recorded by: [NAME] [INITIALS]
Type: [ ] Observation  [ ] Action  [ ] Communication  [ ] Decision

What happened:
[FACTS ONLY]

Who was involved:
[NAMES/ROLES]

Documentation created:
[SCREENSHOTS, NOTES, ETC.]
═══════════════════════════════════════════════════════════════
Entry: 002
[SAME FORMAT]
═══════════════════════════════════════════════════════════════
Entry: 003
[SAME FORMAT]
═══════════════════════════════════════════════════════════════
[CONTINUE SEQUENTIALLY]
```

5.3 Evidence Log Template

EVIDENCE LOG — PRIVILEGED AND CONFIDENTIAL

```
Incident ID: [ID]
Log maintained by: [NAME]
Started: [DATE]

═══════════════════════════════════════════════════════════════
Item: E-001
Description: [WHAT IS IT]
```

```
Type: [ ] Digital  [ ] Physical  [ ] Documentary
Source: [WHERE OBTAINED]
Collected: [DATE/TIME/TZ]
Collected by: [NAME]
Stored at: [LOCATION]
Access limited to: [NAMES]
Hash (if digital): [SHA-256]
═══════════════════════════════════════════════════════════════
Item: E-002
[SAME FORMAT]
═══════════════════════════════════════════════════════════════

CHAIN OF CUSTODY

Item: [E-XXX]
Date/Time: [DATE/TIME]
From: [NAME]
To: [NAME]
Purpose: [WHY TRANSFERRED]
Released by: _____________ (signature)
Received by: _____________ (signature)
```

PART 6: COMMON MISTAKES

These errors create liability, void insurance, or damage legal position.

Mistake 1: Over-Disclosure

What It Looks Like	Why It Hurts	Correct Approach
Telling customers "all data stolen" before confirmed	Creates liability for unconfirmed claims	Wait for investigation
Announcing breach publicly before required	Triggers lawsuits before facts known	Counsel controls timing
Providing technical details to media	May not be required; aids attackers	Disclose minimum required

Mistake 2: Emotional Language

What It Looks Like	Why It Hurts	Correct Approach
"We are devastated"	Becomes litigation evidence	Neutral language only
"This is a catastrophe"	Undermines professional response	"We identified an incident"
"We got hit hard"	Creates panic	"We are investigating"

Mistake 3: Delayed Insurer Notice

What It Looks Like	Why It Hurts	Correct Approach
Waiting to "know more"	Most common claim denial reason	Call within 60 minutes
Waiting until Monday	Breaches 24-72 hour requirement	Call immediately
Calling after 72 hours	May void coverage entirely	Update as you learn more

Mistake 4: Admitting Fault

What It Looks Like	Why It Hurts	Correct Approach
"We should have updated"	Used against you in lawsuits	"Under investigation"
"Our security failed"	May void insurance	"Reviewing circumstances"
"We are responsible"	Becomes permanent record	Let investigation determine

Mistake 5: Poor Timelines

What It Looks Like	Why It Hurts	Correct Approach
"Around noon"	Undermines credibility	"12:15 PM EST"
Reconstructing from memory	Creates gaps regulators question	Document in real-time

Missing entries	Weakens legal defense	Entry for every action

Mistake 6: Improvising Language

What It Looks Like	Why It Hurts	Correct Approach
Writing notice without template	Inconsistent statements	Use templates exactly
"Personalizing" communications	May make problematic promises	Counsel reviews all
Adding reassurances	May admit things you shouldn't	No improvisation

QUICK REFERENCE CARD

Print this page. Post near workstation.

FIRST 30 MINUTES

☐ 1. RECORD time: ___:___ on __/__/__

☐ 2. SCREENSHOT everything unusual

☐ 3. DISCONNECT from network (do NOT power off)

☐ 4. FIND insurance policy #: _______________

☐ **5. CALL insurance hotline: _______________**

☐ 6. TELL staff: stop systems, no external talk

☐ 7. START timeline log

DO NOT

✗ Power off computers
✗ Delete anything
✗ Wipe or reinstall
✗ Pay ransom
✗ Contact attacker
✗ Post on social media
✗ Talk to media
✗ Admit fault

KEY CONTACTS

Insurance Hotline: ______________________________

Policy Number: ________________________________

Incident Commander: ____________________________

Backup: ______________________________________

LEGAL DISCLAIMER

IMPORTANT — READ CAREFULLY

This playbook provides general operational guidance for responding to cybersecurity incidents. It does not constitute legal advice and does not create an attorney-client relationship.

Laws, regulations, and insurance requirements vary significantly by jurisdiction and change over time. The information in this playbook may not be current or applicable to your specific situation.

You must consult qualified legal counsel for advice specific to your incident, jurisdiction, and circumstances. You must review your specific insurance policy for coverage terms, conditions, and requirements.

No representation or warranty is made that following this playbook will result in any particular legal, regulatory, or insurance outcome.

All communication templates in this playbook must be reviewed and approved by qualified legal counsel before use in actual incidents.

By using this playbook, you acknowledge that you have read and understood this disclaimer.

— END OF PLAYBOOK —