



COMPUTER TIES IT RESOURCE CENTER • PLANNING WORKSHEET

Cybersecurity Incident Response Planning Worksheet

The information you will want in front of you on the worst day, written down on a day when nothing is wrong.

FILLABLE PDF

Type into any field, then save or print a copy.

EDITION

Version 1.1 • September 2026

QUESTIONS?

(517) 788-6393 • computer-ties.com

During a real incident, the delay is almost never technical. It is somebody trying to remember a phone number, working out who is allowed to authorize taking systems offline, or looking for an insurance policy nobody has read.

This worksheet collects that information in one place. It takes about half an hour and it is the cheapest preparation you will ever do.

Print it, and keep the printed copy somewhere else

If this document only exists on the network, and the network is the problem, you do not have it. Print a copy. Keep one at the office and one somewhere off site. Give a copy to whoever would be making decisions.

How to use this document

Fill this in with whoever runs the organization. Several of these are decisions somebody has to make in advance, not facts to look up.

Review it once a year and whenever people change roles or leave. An out-of-date contact list is worse than none, because people trust it.

The words you will hear, and what they actually mean**Incident response**

The plan for what happens between something going wrong and things being normal again. A fire drill, not a fire extinguisher.

Containment, eradication, recovery

The three stages, in order. Stop it spreading, get it out, get back to work. Skipping straight to recovery is how organizations get hit twice by the same intruder.

Out-of-band communication

Talking to each other using something other than the systems that may be compromised. If an intruder is reading the email, do not coordinate the response in email.

Preserving evidence

Leaving the affected machine intact so somebody can work out what happened. Not sweeping up the broken glass before the police arrive.

IC3

The FBI's Internet Crime Complaint Center at ic3.gov, where cybercrime and wire fraud are reported. Reporting quickly matters, particularly where money has moved.



1 The First Fifteen Minutes

This is what you want somebody to be able to do without asking permission.

- ☐ Disconnect the affected computer from the network. Unplug the cable or turn off the Wi-Fi. Leave it switched on.
Switching it off can destroy information that helps work out what happened and how far it went.
- ☐ Do not delete anything, do not wipe anything, and do not start reinstalling.
- ☐ Tell whoever is named in section 2, immediately.
- ☐ Write down the time, what was noticed, and by whom.
- ☐ Stop using any account you think may be affected, and change its password from a different device.
- ☐ If money may have moved, call the bank right away, then report it to the FBI at ic3.gov.
A fraudulent transfer can sometimes be stopped or recalled, but the chance falls away quickly with every hour that passes. This is one of the few situations where minutes genuinely count.
- ☐ Do not discuss it outside the organization until somebody has decided what is being said.

2 Who Gets Called

First person to call, internally

Their mobile number

Second person, if the first is unreachable

Our IT provider

Their number, and the after-hours number

Whoever leads the organization

Who	Organization	Phone	When we would call them



■ Prompts

- ☐ Your insurance broker, and the claims number on your cyber policy.
- ☐ Legal counsel.
Involving them early can matter for how the response is handled and recorded.
- ☐ Your bank, and your payment processor.
- ☐ Your accountant or payroll provider, if pay or payments could be affected.
- ☐ Local law enforcement, and the FBI Internet Crime Complaint Center at [ic3.gov](https://www.ic3.gov).
- ☐ Any regulator or agency you are required to notify.
- ☐ Key customers or partners, if their information or their systems could be involved.

3 Who Decides

Decide these now. In the moment, the person who notices the problem is rarely the person allowed to act on it.

Who can authorize taking systems offline

Who can authorize emergency spending, and up to what

Who speaks to the press, if it comes to that

Who does all this if that person is unreachable

Who can authorize sending everyone home

Who decides whether to notify customers

Who decides we are back to normal

4 What Matters Most

In a serious incident you will not restore everything at once. Decide the order now, while nobody is panicking.

System or information	Why it is critical	Restore in what order	Who knows how



System or information	Why it is critical	Restore in what order	Who knows how

5 Where Things Are Kept

Where our backups are

Who can access them

Where our equipment list is kept

Where our network documentation is kept

Where administrator passwords are kept, and who can get them

Where our insurance policy is kept

Where the printed copy of this worksheet is kept

The point of this section

Every line here should have an answer that does not depend on the systems being available. If the answer to any of them is 'on the server' or 'in an email', that is the thing to fix this week.

6 What You Would Need to Tell People

You do not need to write the message now. You do need to know in advance who you might be required to tell, because that answer takes days to research and hours to act on.

- ☐ Do we hold health information, and would HIPAA breach notification apply to us?
It applies to more organizations than people expect, including those working on behalf of a healthcare provider.
- ☐ Do we hold criminal justice information, and what would our agency and the state require?
- ☐ Do we hold federal tax information, and would IRS reporting requirements apply?
- ☐ Do we take card payments, and what would our processor and PCI DSS require?
- ☐ What does Michigan law require us to do if personal information is exposed?
- ☐ What does our cyber insurance policy require, and how quickly?
- ☐ Do any of our contracts require us to notify a customer, and within what time?

- ☐ Would we need to tell staff that their own information was involved?

Notification is a legal question, not a technical one

Whether you are required to notify anyone, who, and by when, depends on what information was involved and which rules apply to you. Work this out with legal counsel and, where relevant, your insurer. Getting it wrong in either direction causes problems.

7 Keeping a Record

Start writing things down from the first minute. Memory is unreliable under stress, and this record matters afterwards for your insurer, your lawyer, and any investigation.

Date and time	What happened or what we did	Who

8 Afterwards

- ☐ Work out how it happened, not just what broke.
- ☐ Fix the underlying cause, not only the symptom.
- ☐ Check whether the same weakness exists anywhere else.
- ☐ Change anything about how you responded that did not work.
- ☐ Update this worksheet with what you learned.
- ☐ Tell staff what happened and what changed. People take it more seriously after a real one.
- ☐ Keep the record. You may need it for a long time.



■ Review record

Organization

Completed by

Date

Next review

Copies kept where

About this worksheet

This is a preparedness tool. It is not a formal incident response plan, and it is not legal, insurance, or regulatory advice. Organizations with obligations under HIPAA, CJIS, IRS requirements, PCI DSS, the FTC Safeguards Rule, defense contracting requirements, state law, or an insurance policy should build a plan that meets those requirements and review it with appropriate legal and compliance help. A completed copy identifies people, systems, and where sensitive things are kept, and should be protected accordingly.

If something is happening right now

Existing Computer Ties customers should call the Help Desk rather than working from a printed sheet. If you are not a customer and you think you have a live incident, call the office and say so. For everyone else, the useful time to talk about this is well before you need to.

NEW PROJECTS AND PLANNING

(517) 788-6393

EXISTING CUSTOMER SUPPORT

(517) 905-3168

2903 West Michigan Avenue, Jackson, MI 49202 • computer-ties.com • Serving Jackson since 1990

