

Ransomware: facilitator's guide

Ninety minutes. Eight injects. One Monday morning that goes wrong in the order these things actually go wrong.

The scenario in one paragraph

A slow file share at 07:14 becomes a ransom note at 07:41. The first free engineer is at 14:00, the backups stopped nineteen days ago without telling anyone, and by mid-afternoon it is a privacy matter with clocks attached.

What this is, and what it is not

This is a discussion exercise. Nobody touches a system, nothing is switched off, and no technical knowledge is required by anyone in the room including you. Eight events are read aloud in sequence and the group decides what it would do.

It is not an assessment, an audit, or a certification of anything. It produces a record of what your organisation would do and a list of what it does not yet know. That list is the deliverable. An exercise that produces no findings was facilitated too gently.

THE HONEST LIMIT

An exercise tells you how people would decide. It cannot tell you whether a control works. If today makes you want to test one, it has done its job.

What you need

- Ninety minutes and a room with a door. Not a video call if you can avoid it.
- Between four and eight people. Fewer and there is no disagreement; more and somebody hides.
- The printed deck, cut up, inject cards face down and in order.
- One note-taker with the decision log open, who does nothing else.
- A visible clock. Your phone on the table, face up, is enough.

Running order

CLOCK

WHAT

NOTES FOR YOU

0:00	Ground rules and roles	Read the ground rules card aloud. Hand out role cards. Give everyone two minutes to write the line on their own card.
0:10	Inject 1	Read it aloud, then stop talking. Let the silence do the work.
0:18	Inject 2	The first real decision. Watch for who claims authority.
0:26	Inject 3	Play a complication card here if the room is comfortable.
0:34	Inject 4	Expect this one to run long. Let it.
0:44	Inject 5	Uncomfortable by design. Do not rescue them.
0:52	Inject 6	Make somebody say the difficult sentence out loud, to another person in the room.
1:00	Inject 7	Named owners and dates. Slow down here.
1:08	Inject 8	Do not let the room resolve it neatly. Seven minutes, then stop.
1:15	Hot debrief	Fifteen minutes. The note-taker reads back every “I don’t know”.

The three ways a tabletop fails

The expert takes over

One person who knows the subject answers everything and the room goes quiet. This produces a comfortable exercise and no findings. Thank them, then ask somebody else the same question — and ask what happens when that person is on holiday.

The room solves the wrong problem

Groups drift into how it happened, because that is more interesting than what to do next. Bring them back: this exercise is about the decisions, not the forensics.

Everyone agrees too quickly

Fast agreement usually means the question was not understood. Play a complication card. That is what they are for.

Inject by inject: what you are actually looking for

Each card is built around a finding that small organisations reliably have. You are not steering the room toward an answer — you are making sure the question does not get skipped.

INJECT 01 · MONDAY 07:14 · FILES ARE OPENING SLOWLY

Nobody owns the first ten minutes

Almost every room debates what is happening instead of naming who acts. If you hear “someone should probably call IT”, that is your first finding.

Also listen for: Whether anyone says the word “disconnect” before the ransom note appears.

INJECT 02 · 07:41 · THE NOTE

Authority to stop trading is undefined

Taking the business offline costs money, so most people wait for permission that nobody has been given. Push until the room names the person and the phone number.

Also listen for: Whether the owner can be reached on a number someone knows without looking it up.

INJECT 03 · 08:15 · YOUR IT PROVIDER

The contract nobody has read

Small organisations rarely know what their provider owes them in an incident. The Saturday session detail is deliberate — watch whether anyone asks whether the provider was the route in.

Also listen for: Whether anyone asks who owns the backups and the Microsoft tenant.

INJECT 04 · 09:00 · THE BACKUPS

Backups are believed, not verified

The single most common real finding. The useful discussion is not the technology — it is who could tell you what was lost, and how long that would take.

Also listen for: Whether anyone can say what a working day of lost data actually contains.

INJECT 05 · 10:30 · THE POLICY

Helping fast can void the cover

Rooms find this uncomfortable, which is the point. Nothing here is wrong-doing — it is the instinct to fix things colliding with terms nobody read at renewal.

Also listen for: Whether anyone has ever read the policy's incident conditions.

INJECT 06 · 12:00 · EVERYONE WANTS TO KNOW

Silence is a decision

Most groups want to wait until they know more. Ask what the customer does in the meantime, and what the reporter writes if nobody calls back. Make someone say the two sentences out loud.

Also listen for: Whether staff were given anything to say before they were asked.

INJECT 07 · 14:20 · TAKEN, NOT JUST LOCKED

The incident becomes a privacy matter

This is where a technical problem becomes a legal one with clocks attached. Do not let the room settle on “we’d ask the lawyer”. Ask who calls the lawyer, and whether anyone has that number.

Also listen for: Whether anyone separates the federal position from Quebec’s.

INJECT 08 · 16:45 · THE OFFER

The decision nobody wants

Do not resolve this. The value is in discovering whether the organisation has ever decided its position in advance. A decision made under a 24-hour discount is not a decision.

Also listen for: Whether anyone mentions sanctions screening, or asks whether the insurer would even permit it.

The hot debrief

Fifteen minutes, in the same room, before anyone opens a laptop.

- What is the first thing we would change on Monday, and who owns it?
- Which decision took longest, and why?
- How many times did somebody say “I don’t know”? Read them out.
- Who did we assume would be available who might not be?
- What would we have needed on paper, and where would it be?
- What did we learn today that we did not know at the start of the hour?

Afterwards

1. Write the after-action report within two days, while it is fresh. Four or five findings, each with a named owner and a date.
2. Complete the evidence-of-exercise record and file it. One page.
3. Book the next exercise before you leave the room.
4. Change the runbook. An exercise that changes nothing was entertainment.

WHERE THE LINE FALLS

Canada Cyber-Safe does not remediate what it assesses. Running this exercise yourself keeps you entirely independent of us — and buying it does not stop us assessing your organisation later. We say which side of that line a purchase falls on before you buy, not after.

Crib sheet

Keep this in front of you while you run it. Everything you need for the ninety minutes, without looking anything up.

#	CLOCK	HEADLINE	THE ONE QUESTION YOU MUST NOT LET THEM SKIP
01	Monday 07:14	Files are opening slowly	What happens in the next ten minutes, and who does it?
02	07:41	The note	Do you disconnect anything?
03	08:15	Your IT provider	What do you ask them for, in writing, within the hour?
04	09:00	The backups	What happened in the last nineteen days that you cannot afford to lose?
05	10:30	The policy	What have you already done that could affect the claim?
06	12:00	Everyone wants to know	Who speaks, to whom, and in what order?
07	14:20	Taken, not just locked	Is there a real risk of significant harm?
08	16:45	The offer	Who decides?

Debrief, fifteen minutes

- What is the first thing we would change on Monday, and who owns it?
- Which decision took longest, and why?
- How many times did somebody say “I don’t know”? Read them out.
- Who did we assume would be available who might not be?
- What would we have needed on paper, and where would it be?
- What did we learn today that we did not know at the start of the hour?

If the room stalls

- Ask the quietest person in the room the same question.
- Ask “who does that, by name?” and wait.
- Play a complication card.
- Ask what happens if the person they just named is unavailable.