

Ransomware tabletop exercise

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

- 0:00 Ground rules and roles — 10 minutes
- 0:10 Injects 1 to 8, about eight minutes each
- 1:15 Hot debrief, while it is still fresh

Print on card stock if you have it. Cut along the dashed lines — two straight cuts a sheet. Keep the inject cards face down until their time comes.

FREE · CYBER-SAFE.CA/TABLETOP

Ground rules

- No laptops open except the note-taker's. No searching for the answer.
- Never say “we would probably”. Say who does it, and by when.
- “I don't know” is the most useful sentence in the room. The note-taker writes down every one of them. Those are the findings.
- Nobody is being tested. The plan is being tested.
- The facilitator owns the clock. A good discussion does not earn extra time — a real incident would not give you any.
- Nothing said here commits you to anything with a regulator, an insurer or a customer.

CANADA CYBER-SAFE · RANSOMWARE TABLETOP

ROLE CARD 1 OF 6

Owner or managing director

You are the only person who can authorise spending money or stop the business trading. Everything that costs or halts something comes to you.

WRITE THIS DOWN BEFORE INJECT 1

The largest sum you could authorise today without asking anyone — and who signs if you cannot be reached.

If you are not in the room, the exercise has already found something.

CANADA CYBER-SAFE · RANSOMWARE TABLETOP

ROLE CARD 2 OF 6

Operations lead

You know what work is in progress, which customers notice first, and what cannot slip. You translate “the server is down” into what it costs by the hour.

WRITE THIS DOWN BEFORE INJECT 1

How long the business can run with no files, no email and no phone system before a customer is genuinely harmed.

You will be asked what you can run on paper. Have a real answer.

CANADA CYBER-SAFE · RANSOMWARE TABLETOP

Finance or bookkeeper

You hold banking, payroll and the insurance policy. In most organisations this size, you hold them alone.

WRITE THIS DOWN BEFORE INJECT 1

Where the cyber policy number and the 24-hour notification line actually are, and who could find them without you.

Notice how often the room turns to you — and what happens on the card where you are unreachable.

CANADA CYBER-SAFE · RANSOMWARE TABLETOP

Customer and public contact

You own what customers, suppliers and anyone else outside the building are told, and when.

WRITE THIS DOWN BEFORE INJECT 1

The three customers who must hear from a person rather than an email — and who holds their mobile numbers.

You will have to speak before you know the facts. That is the job.

CANADA CYBER-SAFE · RANSOMWARE TABLETOP

IT liaison

You are the single point of contact with the IT provider. You are probably not an engineer, and that is fine — your job is to ask for things in writing and chase them.

WRITE THIS DOWN BEFORE INJECT 1

Your provider's out-of-hours number, who answers it, and what the contract promises about response times.

Your value today is knowing what you are entitled to ask for.

CANADA CYBER-SAFE · RANSOMWARE TABLETOP

Note-taker

You solve nothing. You record decisions, the time they were made, who made them, who was told — and every question the room could not answer.

WRITE THIS DOWN BEFORE INJECT 1

Open the decision log now. You will not have time to set it up once the room starts talking.

Use the decision log. Your notes are the only thing that outlives today.

CANADA CYBER-SAFE · RANSOMWARE TABLETOP

Monday 07:14

Files are opening slowly

Priya in accounts messages the office group: “Is the shared drive slow for anyone else? Some of my files won't open and the names look wrong.”

Nobody else has arrived yet. There is no ticket, no alert and no email from anyone.

DECIDE NOW

What happens in the next ten minutes, and who does it? Name the person, not the role. Now say what happens if that person does not pick up.

07:41

The note

A file called READ-ME-NOW.txt has appeared in every folder on the shared drive. It says your files are encrypted, that 240 GB has been copied out, and that the price rises in 72 hours. Two more staff have arrived. One has already opened the file on her own laptop.

DECIDE NOW

Do you disconnect anything? Who has the authority to take the business offline — and can you reach them right now, on a number you know by heart?

08:15

Your IT provider

You reach your IT provider. They will raise a ticket; the first available engineer is 14:00. Pressed, they mention their remote support tool logged an unusual session on Saturday evening.

DECIDE NOW

What do you ask them for, in writing, within the hour? Who holds your contract with them — and does anyone in this room know what it says about an incident?

09:00

The backups

Backups exist. The most recent one that completed successfully finished nineteen days ago. The job has failed silently every night since, and the alerts went to an inbox nobody reads.

DECIDE NOW

What happened in the last nineteen days that you cannot afford to lose? Who can answer that — and how long would it take them to answer it properly?

10:30**The policy**

Your broker confirms you hold cyber cover. The policy requires you to use the insurer's appointed responder, to notify within 72 hours, and to make no external statements without approval. You have already engaged your own IT provider and emailed all staff.

DECIDE NOW

What have you already done that could affect the claim? Who makes the call to the insurer, and what do they say you have done so far?

12:00**Everyone wants to know**

Staff are speculating in a WhatsApp group you are not in. A customer emails asking why their order confirmation never arrived. A local business reporter leaves a voicemail asking you to confirm "a cyber incident".

DECIDE NOW

Who speaks, to whom, and in what order? Write out the first two sentences you would say to a customer while you still do not know what was taken.

14:20**Taken, not just locked**

The responder confirms data left the network before anything was encrypted: an HR folder with social insurance numbers and banking details for 34 staff, and a client list with contact details for around 900 people. Six of your staff work in Quebec.

DECIDE NOW

Is there a real risk of significant harm? Who makes that assessment, who records it, and what are your clocks — to the Privacy Commissioner, to the individuals, and separately under Quebec's Law 25?

16:45**The offer**

An email arrives at the owner's personal address. The price drops by 40 per cent if paid within 24 hours. Attached is a readable extract of the HR file as proof. The sender is courteous and offers a discount for a fast decision.

DECIDE NOW

Who decides? What would you need to establish before that decision could even lawfully be made? Say out loud what paying would actually buy — and what it would not.

The only one who can pay

Your bookkeeper is on a flight to Vancouver and is the only person with banking access. She lands in four hours.

PUT IT TO THE ROOM

Does this change the decision they just made? If it does not, ask them to say why not — out loud, in one sentence.

Hand this to the facilitator, not the room. Play it when a decision has been made too easily.

CANADA CYBER-SAFE · RANSOMWARE TABLETOP

The password file

Your domain registrar and DNS logins were kept in a spreadsheet on the drive that is now encrypted.

PUT IT TO THE ROOM

Does this change the decision they just made? If it does not, ask them to say why not — out loud, in one sentence.

Hand this to the facilitator, not the room. Play it when a decision has been made too easily.

CANADA CYBER-SAFE · RANSOMWARE TABLETOP

Helpful on LinkedIn

A member of staff posted “well, this is a fun Monday” at 09:20, with a photograph of the ransom note on their screen.

PUT IT TO THE ROOM

Does this change the decision they just made? If it does not, ask them to say why not — out loud, in one sentence.

Hand this to the facilitator, not the room. Play it when a decision has been made too easily.

CANADA CYBER-SAFE · RANSOMWARE TABLETOP

The clause nobody read

Your largest customer's contract requires notification of any security incident within 24 hours. Nobody has opened that contract since it was signed.

PUT IT TO THE ROOM

Does this change the decision they just made? If it does not, ask them to say why not — out loud, in one sentence.

Hand this to the facilitator, not the room. Play it when a decision has been made too easily.

CANADA CYBER-SAFE · RANSOMWARE TABLETOP

An awkward invoice

Your IT provider's contract lapsed two months ago and has been running month-to-month. They raise two unpaid invoices before agreeing to continue.

PUT IT TO THE ROOM

Does this change the decision they just made? If it does not, ask them to say why not — out loud, in one sentence.

Hand this to the facilitator, not the room. Play it when a decision has been made too easily.

The only copy

Two of the encrypted files are the sole signed copies of client contracts. There is no other version anywhere.

PUT IT TO THE ROOM

Does this change the decision they just made? If it does not, ask them to say why not — out loud, in one sentence.

Hand this to the facilitator, not the room. Play it when a decision has been made too easily.