Resource · Exercise playbook

Ransomware Tabletop Exercise

90 minutes · For SMB leadership teams · Industry-agnostic

Setup (15 minutes before the meeting)

- **Room:** one conference room or video call. Phones off the table.
- **Attendees:** owner/CEO, senior IT, finance, legal, communications, operations. 5–8 people.
- **Roles:** facilitator (reads injects, keeps time), notetaker, timekeeper.
- **Ground rules:** no blame. The goal is to surface gaps, not to find who to fire.

The scenario

It is 6:47 AM on a Tuesday. The on-call IT engineer wakes up to a call from the warehouse manager: "None of the computers will boot. Every screen has a red message about Bitcoin." Initial check: 80% of endpoints encrypted. Shared file server encrypted. Backup server encrypted. Phone system up. Email (cloud) up. Accounting system (third-party) — status unknown.

Start the clock. 90 compressed minutes to work through the first six hours.

Inject 1 — 6:50 AM (5 min in)

The ransom note demands 8 BTC (~$640,000). 72 hours before the price doubles. The note claims 240 GB of exfiltrated data will be published if you don't pay.

Decision points:

- Who calls whom right now? Who is the incident commander?
- Do you contact law enforcement? Cyber insurance? Legal counsel? In what order?
- What do you tell employees arriving for the morning shift?

Inject 2 — 7:30 AM (40 min in)

Your cyber insurance carrier returns your call. They only honor the policy if you use their pre-approved IR firm. The IR firm is available in 90 minutes; $50,000 retainer plus $400/hour.

Decision points:

- Does the policy actually cover ransomware payment? Business interruption? Forensics?
- What's the answer if IR tells you to pay? What if they tell you not to?
- Who has signing authority for the retainer — *right now*, with systems down?

Inject 3 — 8:45 AM (75 min in)

Backup vendor reports: yes, on-site backups encrypted, but a 48-hour-old offsite snapshot exists. Estimated recovery time: 36 hours. A 3-week-old monthly snapshot is available immediately.

Decision points:

- What systems do you restore first? Where is the recovery priority list?
- Do you have hardware to run on while production is restored?
- What do you do with 48 hours of lost transaction data?

Debrief (last 15 minutes)

Three rounds:

1. **What worked?** Each attendee names one decision the team made well.
2. **What's missing?** Each attendee names one gap.
3. **30/60/90?** The team picks the top three gaps and assigns owners + dates.

Notetaker delivers a one-page memo (*Gap · Owner · Due date*) within 48 hours.

Want us to facilitate?

CCRAMM runs facilitated tabletops for SMBs and professional offices throughout Central PA and the Mid-Atlantic. An outside facilitator surfaces the gaps your team has learned to walk around. ccrammts.com/cybersecurity.