

Crisis Simulation Checklist: How to Run a 30-Minute Crisis Drill With Your Team

A Practical Field Guide from Crisis IQ Partners



CRISIS IQ
PARTNERS

Could Your Team Handle a Crisis in the Next 30 Minutes?

This 30-minute crisis simulation exercise is designed to help your team practice real-world decision-making, communication, and leadership under pressure — before a real crisis hits.

Whether you're facing a cyberattack, a reputational threat, or an operational breakdown, this structured simulation helps you find and fix vulnerabilities in your organization's response system.

Why This Drill Matters

Crises don't wait for ideal conditions.

They strike fast — disrupting operations, confusing communication channels, and testing leadership alignment.

Your **first 30 minutes** determine whether you maintain control or spiral into chaos.

This simulation guide is designed for **small and mid-sized organizations** that want to:

- Evaluate their real-time communication and leadership effectiveness.
- Identify blind spots in their crisis response plan.
- Build a repeatable, scalable readiness exercise they can run quarterly.

You'll walk away with actionable insights, measurable readiness scores, and a stronger, more confident team.

The 30-Minute Crisis Simulation Framework

A simple, flexible structure that defines the **Who, What, Where, When, and How** of a short but powerful readiness exercise.





WHO: Participants

Role	Description
Incident Leader (Facilitator)	Runs the drill, introduces the scenario, controls timing, and manages debrief.
Crisis Team (3–6 people)	Represent leadership, communications, operations, HR, and IT.
Observers/Note-takers	Track decisions, timing, message clarity, and overall communication flow.

💡 *Facilitator note:* Assign roles clearly — ambiguity creates valuable tension and surfaces real communication gaps.

WHAT: Scenario Setup

Choose one of these crisis categories (or create your own):

-  **Cyber Incident:** Data breach, ransomware, or customer data exposure
-  **Operational Disruption:** Equipment failure or supply chain breakdown
-  **Reputational Event:** Negative media coverage or viral customer complaint
-  **Safety Threat:** Weather emergency, onsite accident, or security concern

Write a short, vivid prompt:


“It’s 9:17 a.m. Your servers go down. Customer complaints are flooding in, and a local reporter just tweeted about the outage. You have 30 minutes before the story spreads.”

Make it as realistic as possible to your company — the more authentic the setup, the more revealing the outcomes.

WHERE: Environment

Conduct the simulation in your **actual working environment** — not a hypothetical one. Use the same communication systems you rely on every day:

- Microsoft Teams, Slack, or email threads
- Your real phone tree or escalation protocol
- Existing response templates or communication chains

 *Facilitator note:* Real tools reveal real gaps. Don’t invent processes you wouldn’t use in an actual crisis.

WHEN: The 30-Minute Timeline

Time	Phase	Focus	Facilitator Prompts
0–5 min	Briefing	Introduce the scenario and confirm roles.	“Who’s in charge? What’s our priority?”
6–10 min	Information Gathering	Team identifies known facts and missing data.	“What do we know right now? Who can verify?”
11–15 min	Decision Point #1	Determine the initial response or message.	“What should we say publicly first?”
16–20 min	Communication	Draft and approve messages internally and externally.	“Who signs off? How fast can we get it out?”
21–25 min	Escalation	Introduce a twist or new challenge.	“Breaking: 20 customers have posted complaints online.”
26–30 min	Debrief	Review team performance.	“What worked, what failed, and what will we fix?”

HOW: Debrief and Scoring

After the simulation, rate your team in the **five pillars of crisis readiness** below.
Use a 1–5 scale (1 = Poor, 5 = Excellent).

Pillar	Description	Score (1–5)
Leadership & Accountability	Were decision rights clear and acted upon quickly?	
Communication	Were messages accurate, timely, and aligned?	
Planning & Prevention	Did your existing crisis plans actually help?	
Response Agility	How well did the team adapt to new information?	
Recovery Readiness	Did the team stabilize operations or next steps?	
Total Score		

Total Score Interpretation:

20–25:  Crisis-Ready — Strong, decisive, and coordinated.

15–19:  Moderate Risk — Functional but needs refinement.

Below 15:  Vulnerable — High exposure to operational or reputational damage.

Your Next Step: Turn Practice Into Readiness

Running a single drill is powerful — but *building a culture of readiness* transforms your organization's resilience.

Crisis IQ Partners helps small and mid-sized organizations prepare for the unexpected through expert-led simulations, crisis readiness assessments, and tailored response plans.

◆ **Schedule your Crisis Readiness Audit** today to benchmark your organization against industry leaders and close the gaps before the next disruption.

Call us at 404-403-4630 or email us at info@crisisiqpartners.com