WHEN MINUTES MATTER: WHAT TO DO BEFORE, DURING, AND AFTER A CYBER CRISIS

You might not be in cybersecurity, but you are on the front line.

Every employee plays a critical role when a cyber incident strikes. Whether it's a phishing email, a lost device, or a ransomware attack, what you do (or don't do) in the first moments can shape how bad things get and how fast the organization recovers.

Why Cyber Crisis Response Matters

Cyberattacks are no longer rare, they're expected.

- On average, a cyberattack occurs every 39 seconds (University of Maryland).
- The time between initial breach and detection can be weeks or months.
- But public damage happens in minutes.

The Moment Something Feels Off...

You get a strange pop-up.
Your files won't open.
Your password doesn't work.
What now?

Don't panic. But don't delay.

- Stop what you're doing. Don't try to "fix it" yourself.
- Don't restart your machine. This could destroy digital evidence.
- Report it immediately to your IT or security team, the sooner they know, the faster they can contain the damage.

What Not to Do

- Don't share suspicious emails with coworkers, report them.
- Don't post on social media about the issue.
- Don't assume someone else is handling it.

Security is a team sport. In a crisis, every second and every click counts.

Training for Real World

CyberEd.io offers scenario-based simulations that walk you through real-world cyber crisis situations. You'll learn what to expect, who to contact, and how to help minimize impact when chaos hits.

If you've never practiced a breach response, you won't be ready when it's real.

Request your custom simulation to learn how to act fast, stay calm, and support your team when a cyber crisis hits. Because being prepared isn't just IT's job, it's everyone's.

ZERO HOUR: IS YOUR INCIDENT RESPONSE STRATEGY BUILT FOR REAL-WORLD PRESSURE?

In a real cyber crisis, you don't have hours. You have moments.

The effectiveness of your incident response isn't measured by the plan you wrote last quarter. It's measured by how your team performs when everything breaks, visibility is limited, and leadership is watching.

The Clock Starts at First Suspicion

- Mean time to detect still averages over 200 days in some sectors.
- Containment windows can close in less than 1 hour during active ransomware deployment.
- Internal confusion, unclear comms, or role ambiguity can double recovery time, or worse, force public disclosure before you're ready.

What We See in the Field

Too often, IR strategies look great on paper but fall apart under pressure:

- No clearly defined incident commander
- Delayed privilege revocation or account isolation
- Security tools generating alerts, but no workflow to triage them in real time
- Misalignment between technical containment and executive communication

War Game the Failure Points

This week's training at CyberEd.io focuses on hands-on, immersive incident response simulations, built for security leaders, SOC teams, and IR roles.
You'll practice:

- Leading an executive-ready IR briefing
- Making real-time decisions with incomplete data

- Containing lateral movement under active attack
- Syncing legal, comms, and technical response tracks
- These aren't tabletop theory sessions — they're pressure-tested simulations based on real-world breaches.

Build Muscle Memory, Not Just Playbooks

When the breach hits, you won't have time to read the plan. You'll need to execute it from muscle memory.

Train how you fight. Respond like it's real because one day, it will be.

Sign up for CyberEd.io's advanced Crisis Response Simulations to pressure-test your tools, workflows, and people. Don't wait until it's a headline. Be the team that's ready when the breach comes.