

# HOW AND WHY TO RUN INCIDENT DRILLS



Often, it seems like it's only a matter of time before something goes wrong. When you are in the middle of production and the software goes wonky, it affects every level of your company. Customer service declines, employees panic, and everyone is in a state of disarray. It doesn't have to be this way.

The whole team needs to be prepared for any scenario. This requires foresight and planning.

All of us have participated in a fire drill at some point in our lives. The fire alarm goes off and we all file out the office doors to a designated meeting spot away from the building. We've done it so often that it becomes an immediate response to stand up from our desk and proceed along the route. We chat along the way, our stress doesn't elevate, and we don't even think about what to do next. Our feet simply know where to take us.

Emergency personnel run drills as well. They practice multiple scenarios from small individual trauma to major disaster relief.

Before deploying into enemy territory soldiers are subjected to various situations until their bodies simply react automatically. In the heat of battle, their lives depend on the automatic response they have been trained to perform. This reduces the feeling of shock in a dangerous situation, allowing the soldier to rely on reflex responses.

How does this apply to your company? In the midst of designing new products and experiences for your customer, you have to be ready to react to any scenario while still providing continuity and

excellence in service. At BMC, we know you rely on us and that's why we run incident drills. Since anything can happen, it's important to be prepared.

## Running Incident Drills

To be effective and create a low-stress, reflex response, it's important to remember that practice makes perfect. To help make drills run smoother, for example, the entire team should join in once a month to run new emergency scenarios. Set it up like a game and provide each person with clear roles and objectives.

The goal is to come together to consider different risk scenarios and prepare for potential problems. Each scenario you create should identify a new or modified threat, a specific process in response to the threat, and any assets impacted.

## How to get started

- Designate a game master, a single individual to facilitate the exercise.
- Break the drill into meaningful learning points.
- At the onset, explain the exercise to the entire team and make sure they understand.
- Encourage open dialogue about how your company would handle the scenario while focusing on key learning points.
- Include members of other business units that would be affected in the scenario.
- Follow up on gaps identified during the drill.

[Managing changes](#), especially emergency changes, is a difficult task which requires a deep understanding of the organization, its systems, and the people working within them. Carefully balancing the resources required to successfully accomplish a task is essential for ensuring that emergency situations are addressed effectively.

So, let's say you have the systems in place to minimize risk and prevent problems. However, to be prepared fully to provide optimal service, you need to be ready for anything. The incident drill may be inspired by:

- a situation that has already occurred and was poorly handled,
- a situation where you watched a competitor struggle and wondered how you would handle the same, or
- a potential problem in the making.

Wherever you draw your inspiration, running a drill will help answer those questions and alleviate worry.

## Game master

Designate a game master. This is the individual who will organize the drill from conception to completion. This person knows every detail and will have prepared various stages of the incident set up before it begins.

Here are some of the key parts the game master will need to put into place.

- Identify a process to be tested.

- Create a scenario. This is the incident that triggers the drill.
- Determine the impact it will have on the organization.
- Identify any additional problems that the drill may create based on the responses.
- Have a clear deadline for the incident to be handled.
- Create follow-up questions that address the process and its results.
  - What was the actual threat
  - What assets were impacted
  - How did the team handle the situation
  - Where is there room for improvement
  - Did the drill uncover additional problems
- Before beginning the drill have a written play by play of all of the above to refer to throughout the drill.
- Record the event and the team's responses and insights

## Keep the paperwork

Create two folders.

The first is an Incident Drill Playbook. In this, you will keep the play by play source sheet created by the game master. This will allow you to return to various drills to refine responses. It will also give you a starting point as you create the next incident drill. Over time, you will create a large file of scenarios from which to pull.

The second folder is an Incident Drill Evaluations. In this folder you will write up reports of which drill was run, how different players responded, the record keeper's notes, and the discussion questions and answers that followed the drill.

## Other players

The game master is the organizer but there are other key players you will need to identify.

- Initial responder
- Investigators
- Record keeper
- Client liaison

The game master begins by laying out the scenario to a team member. That team member is the initial responder and will have to decide if the problem dictates a major incident response.

Depending on the scenario and the needs that arise, the initial responder will then identify team members who have the expertise to respond. These individuals become the investigators, doing detailed research into the problem.

The next individual that the initial responder will identify is the record keeper. This person's job is to chronicle each step taken throughout the drill.

As the investigators are diving into the problem and the record keeper is keeping a written log, the next important role to identify is the client liaison. This person is responsible for communicating with the internal and external people affected by the scenario. This is a vital role to make sure clients are aware of what is taking place and how it will affect their own productivity.

The initial responder continues to manage each of the team players. This person is responsible for oversight, keeping a level head, and leading everyone to a resolution.

## When incidents happen

We work hard to build services and infrastructure you can rely on that minimizes the occurrence of incidents. This can make it tricky to troubleshoot possible problems, because we continue to get ahead of them. However, when they do arrive, the combination of our services with the prepared, level-headed team around you will get things running smoothly again in no time. How do we know this? Because it works for us.

[Application performance management \(APM\)](#) is one of the ways we minimize your risk. It prevents and takes on the role of every player, from game master to liaison.

APM leverages artificial intelligence to help IT organizations and application owners, support and developers manage the performance of business critical applications. It's how we help you detect and resolve application performance issues fast!

Think of the APM as the initial responder. It is first alerted to the problem because it is constantly monitoring performance. When a problem is identified, it troubleshoots the issue and leverages machine learning and advanced analytics to catch the problem before it impacts the end user.

Through the use of probable cause analysis, the APM is able to find the root of the cause fast and then prioritize and assign events, much as the investigators would do during an incident drill. Throughout the process, it discovers and defines applications to identify impacted tiers.

We continue to problem shoot and run incident drills. You can trust a team made up of AI and humans ready to act by troubleshooting incident possibilities long before they happen.