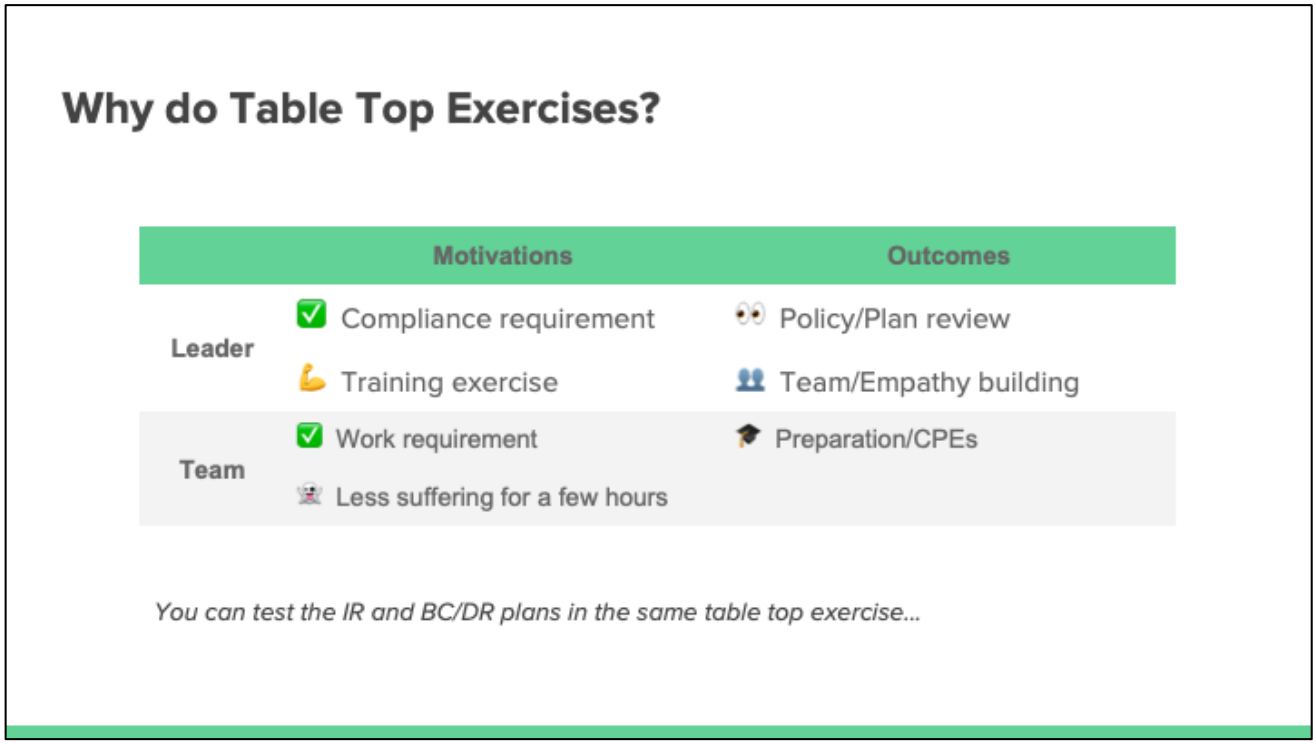
Incident Response, Gamification & Honey Badgers

Running RPG-style
IR Table Tops

Ursula Vernon’s images used with the express permission of the artist

Carlota Sage

vCISO Principal
Fractional CISO



Incident Response Table Tops (aka IR TTX) aren't just a good idea, they're industry best practice. And for compliance frameworks, they're a requirement!

Questions you should ask yourself:
What do you get out of it?
What does the gaming experience bring to your team?
How does this challenge people's assumptions? How are people different after they play the game?

What your team should get out of a TTX
Problem solving, prioritization, collaboration

Role Playing for IR/BC/DR

Role playing games are just that - players assume a role or identity whose skill/knowledge is leveraged to play the game.

The player may know more or less than the role they play.

You, as the game master, must guide the players to an outcome that fulfills the needs of the team.

Traditional role playing games, like Dungeons & Dragons, have very detailed worlds with a wealth of player character information and a variety of non-player characters to move the game along over hours or even years of game play. We don't need to be quite so complicated, but we do need to anchor the game in a few fundamentals.

Gamifi-what now? And why honey badgers??

Gamification = designing systems or interactions with game elements to leverage human motivations for specific psychological and behavioral outcomes.

*Honey Badger don't give a sh*t - they shake off venomous snake bites that would kill a grown human. Use IR Table Tops to help your teams shake off cybersecurity attacks!*

You can introduce gaming elements to manage the table top without forcing your team to literally play a game.

The important thing is to allow for creative thinking - stop being prisoners of our own expertise. Break down the silos and tunnel vision! Use your players' imagination to really drive a good discussion.

Young animals (ex: kittens, puppies, fox kits) play to practice hunting. Using gaming elements in an IR TTX is similar to this

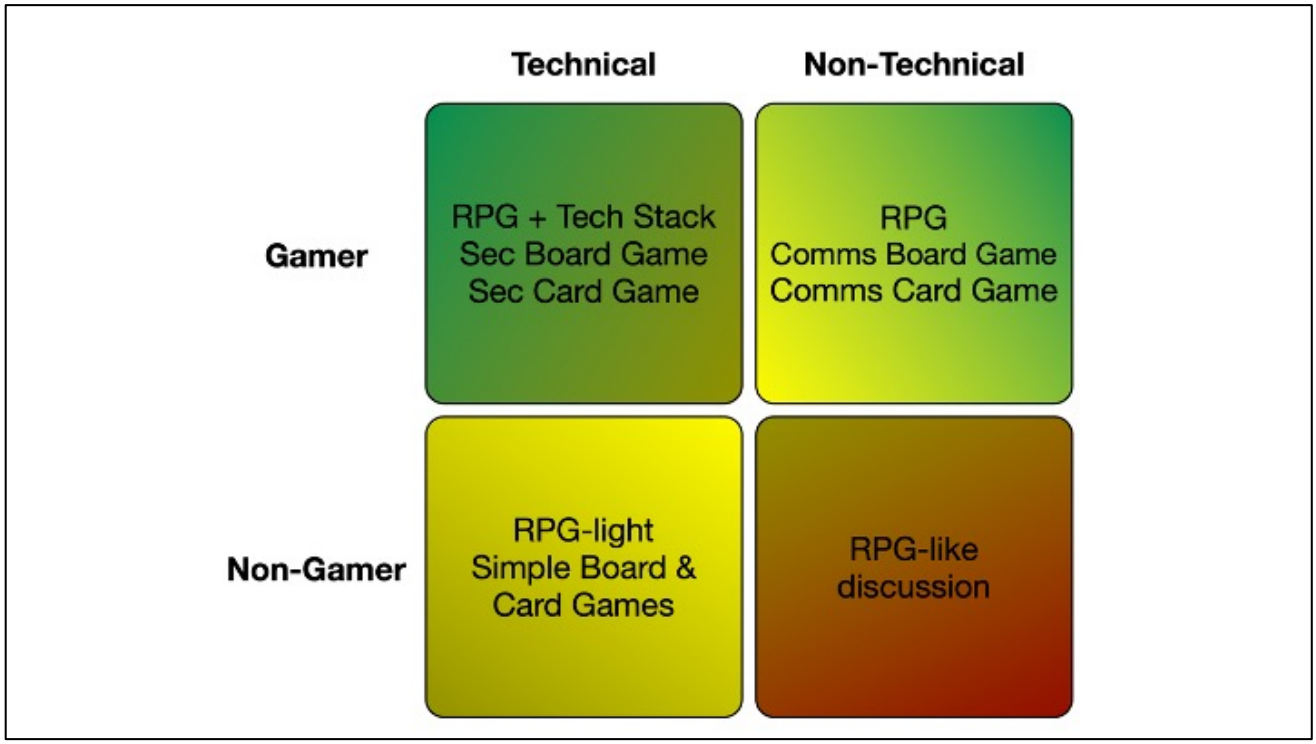
Note: Chris Sanders has a great thread on the nuances of gamification wrt Capture-the-Flag events… https://twitter.com/chrissanders88/status/1463509769185120265

Lots of Gaming Options

Great list at https://adam.shostack.org/games.html

Lots of options for gamers
Board/Card games vs. Role Playing Games

RPG Game theory = the study of role playing games as a social or artistic phenomenon

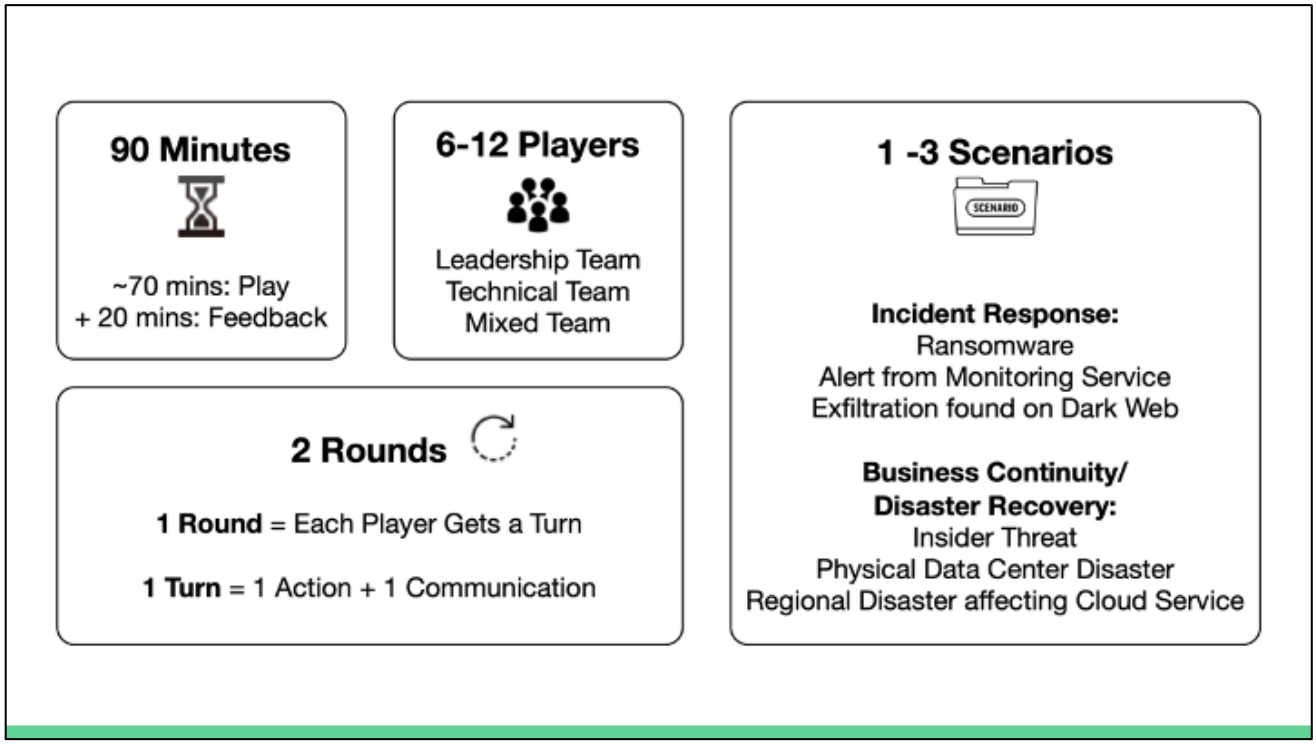


Note that some people *just aren't gamers*, and games as a method of learning *will fall flat*. Focus on the story telling!

With a less technical and less-gamer inclined group, you will need to drop the obvious game elements to keep them engaged. You can still use game elements to help you determine outcomes.

Table Top Setup

Img Src = Ursula Vernon

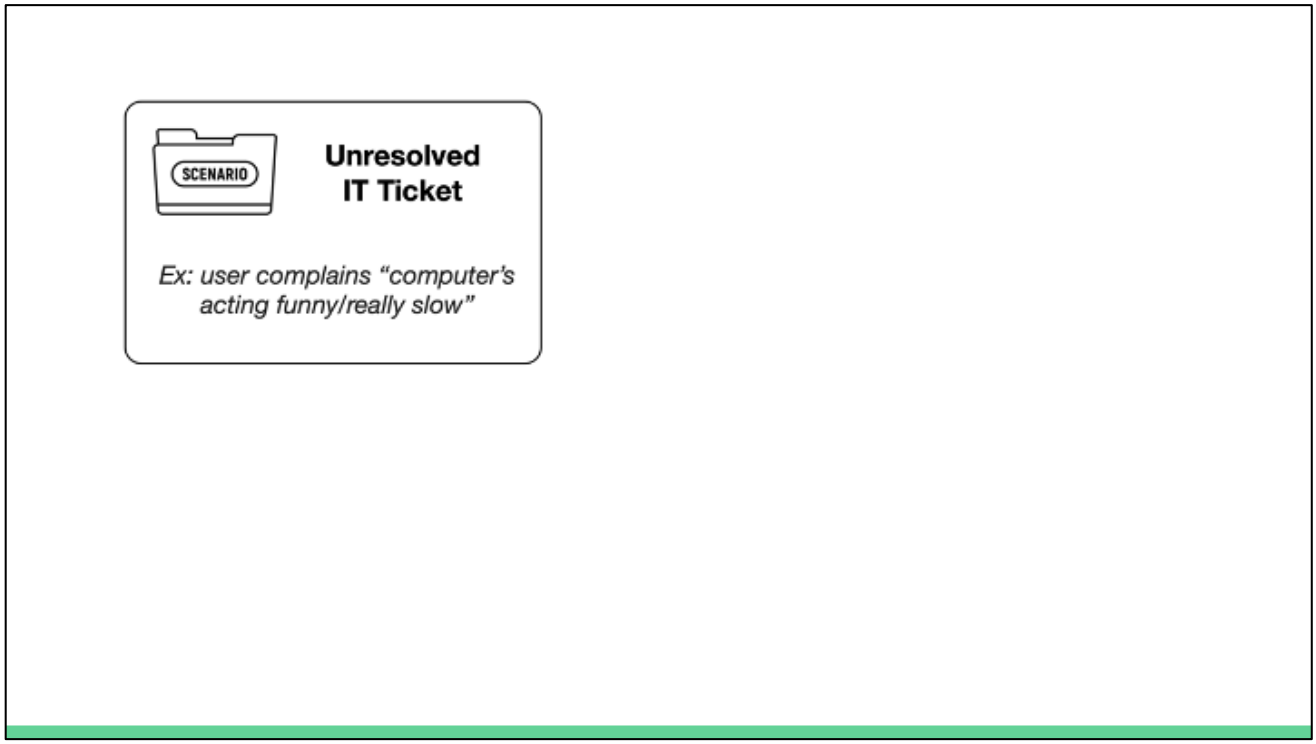


Don’t worry about your security tech stack unless your TTX is directly for the security team itself.

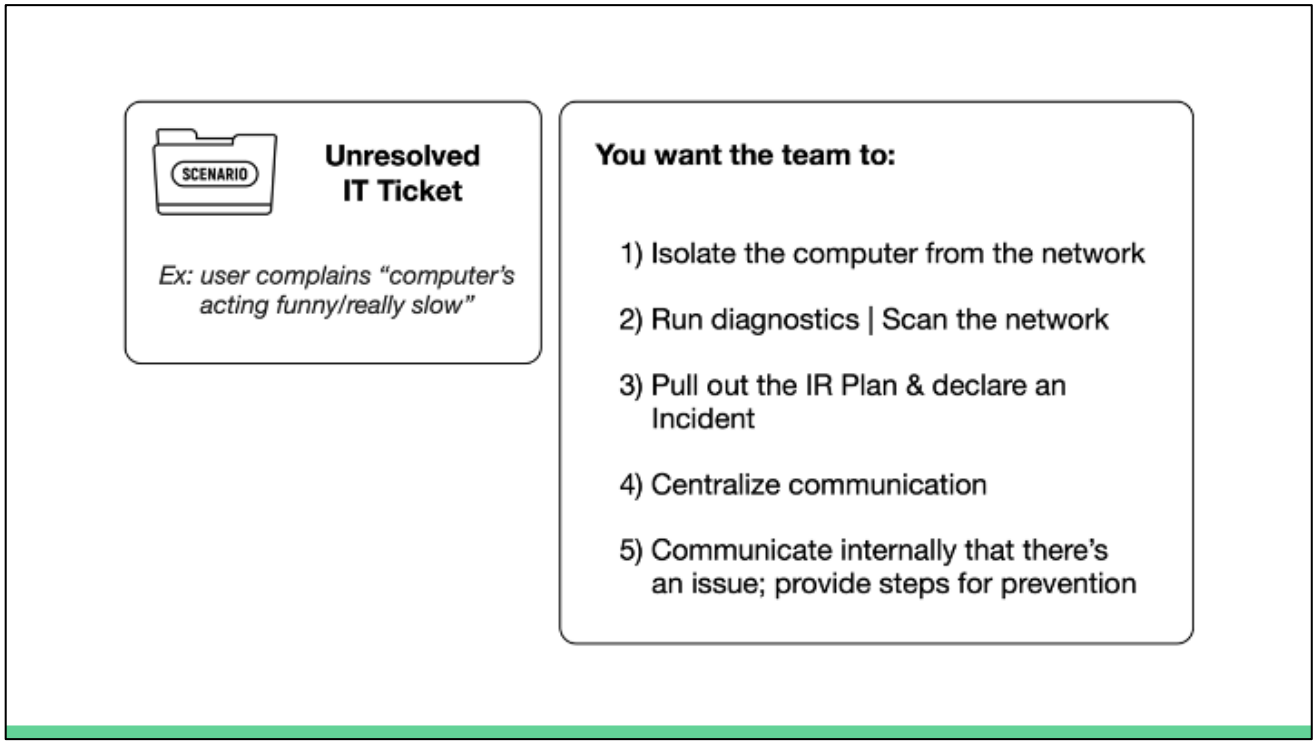
These are gaming elements that you as the IR TTX leader can use to manage your TTX.

Example Scenarios

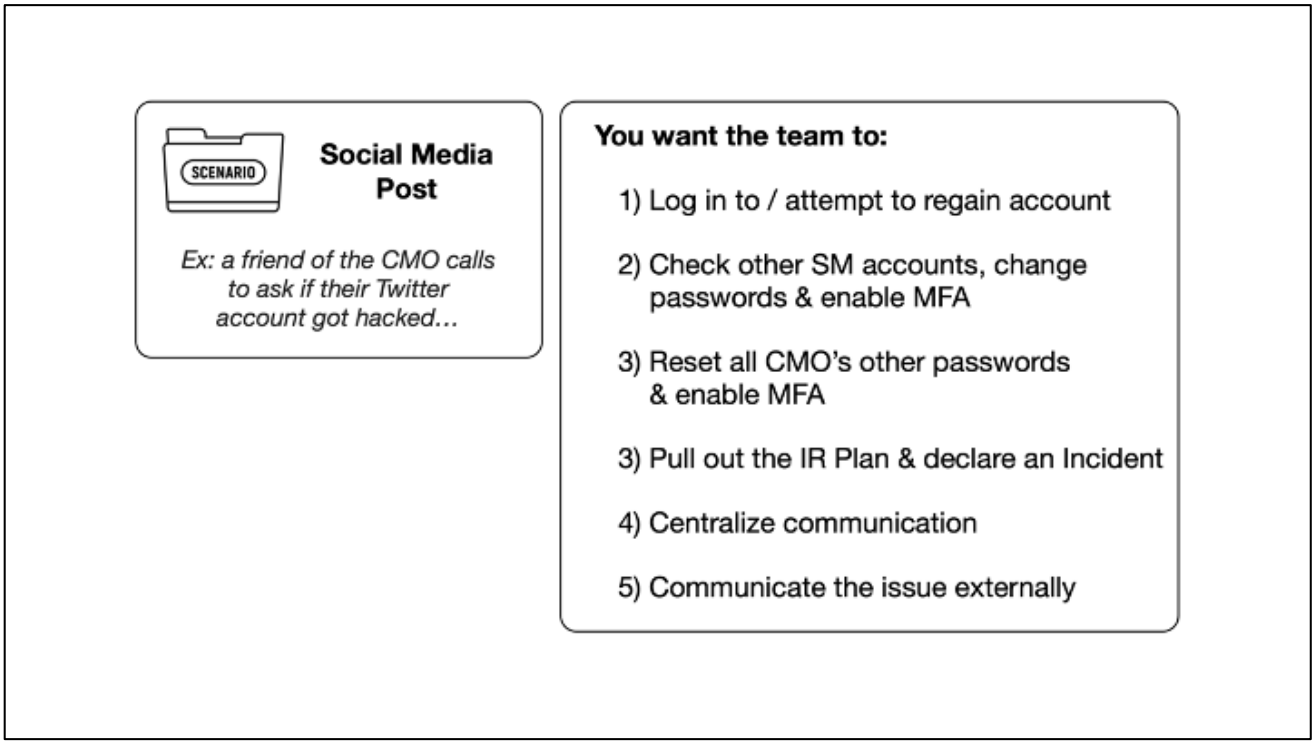
Role play can be as simple as encouraging conversations between teammates. As the TTX Leader, you are looking for specific behaviors that you can praise/reward



To get a role play started, pick someone and tell them that they're a user in Accounting whose computer has begun running really, really slow. Maybe their cursor keeps jumping around. If the team member is deeply technical, remind them that in this scenario, they have to turn off their technical brain. Then ask them, "What do you do?" Let them talk through how they would handle it - maybe they turn the computer off and back on again. You could roll a die in the background to decide if things stay the same or get worse - or you could just say things get worse! Once they decide to call the Help Desk, pick someone else in the group to pretend to answer the phone….

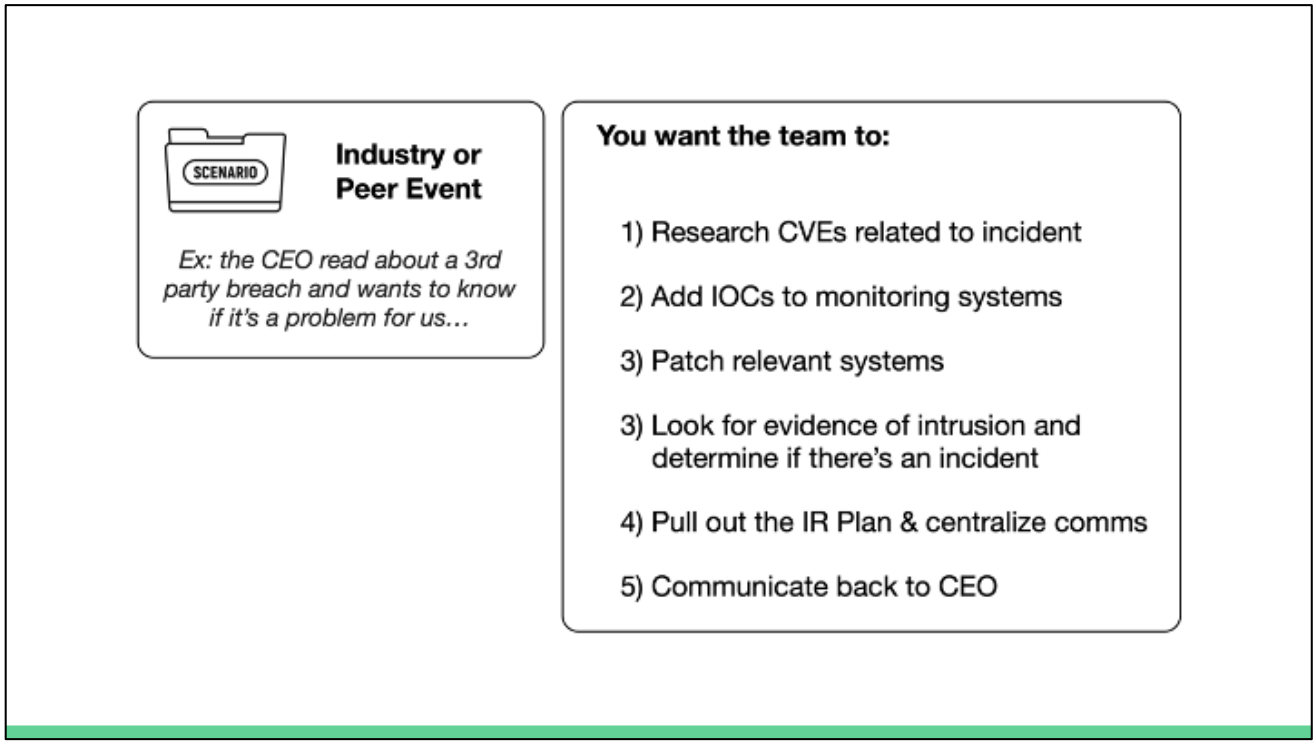


As your Help Desk either helps the user or pulls in other roles to help solve the problem, there are certain things you want to see your team do. Decide on those ahead of time - but don't forget, your players may come up with great solutions that you didn't think of, and that's okay!



If your players are all from the technical team, leveraging scenarios that target the least tech savvy groups in your organization can help build empathy.

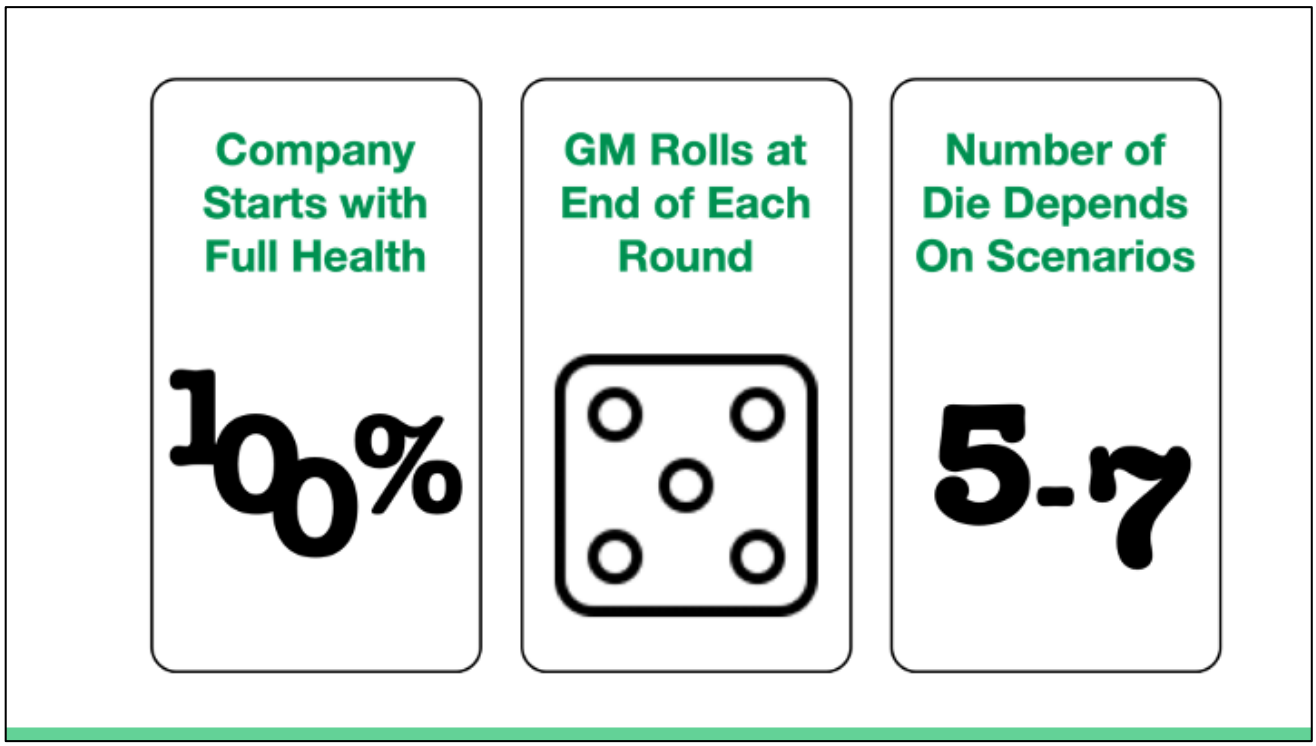
If you have a mix of technical and non-technical players, less technical scenarios can also help keep them engaged.



This scenario is a great example of how a request from a non-technical role can lead to some more technical actions.

Adding Scoring

Img Src = Owen Slater Photography



Another bit of gamification is to add a simple scoring structure to your game. You can define this simply, or even assign points completely arbitrarily like the game show “Who’s Line is it Anyway?”

Mapping to Real Life Consequences

Company Health	Interpretation
81-100%	Your company's credibility and product are intact!
61-80%	The incident and/or your company's handling of it are trending on Twitter, but should recover. IT/Sec teams roll to see if anyone gets fired.
41-60%	The company suffers a hit to their stock. C-Suite rolls to see if anyone gets fired.
21-40%	Your company becomes target for a hostile takeover. Everyone rolls to see if they make it through the acquisition.
<= 20%	Your company closes its doors permanently.
0%	Your company not only closes, C-Suite rolls to see who gets indicted.

If you do decide to add some scoring, you can map it to consequences. This should be done very tongue-in-cheek - if you feel your players will take this too seriously, you don't need to add it.

Recap

In case you need it...

And that's it. With a small investment in preparation and a bit of gamification, you can create a great role-play style table top to help your team practice their incident response, business continuity and disaster recovery skills!

Questions?


WHAT'S THE POINT OF IT ALL, COMEDIC BADGER? WHY DO WE BOTHER?
BECAUSE IF WE DIDN'T, MANY THINGS THAT NEED SECURING WOULD GO UNSECURED.
...I... DON'T WANT TO LIVE IN THAT WORLD.
EXACTLY.
MCMONGARTH.COM